1 Lezione 1

Partiamo da un esempio: il teorema di Rolle. Scriviamone il ben noto enunciato:

Teorema 1.1. *Sia* $f : [a, b] \longrightarrow \mathbb{R}$ *una funzione continua in* $[a, b]$ *e derivabile in* $]a, b[$. *Sia inoltre:* $f(a) = f(b)$. *Allora esiste un punto* $x_0 \in]a, b[$ *tale che* $f'(x_0) = 0$.

Il teorema può essere considerato da due punti di vista molto diversi: possiamo innanzitutto cercare di capire il suo significato. Guardiamo cioè l'aspetto intuitivo. Per visualizzarlo pensiamo ad una semplificazione: immaginiamo un'automobilina che percorre delle montagne russe, partendo da un punto A e arrivando ad un punto B alla stessa altezza di A. È evidente che nel suo tragitto ci saranno dei momenti in cui si troverà in una posizione orizzontale (ed è intuitivo che ciò avviene—perlomeno—nei punti o di massimo o di minimo). Formulato in questo modo, il teorema dovrebbe essere del tutto chiaro anche a chi non ha conoscenze matematiche. Quello che però si vuole mettere in risalto ora è il secondo punto di vista: l'aspetto formale. Si parla di una *funzione*. Vediamo allora qual è la definizione di funzione. Una funzione $f : X \longrightarrow Y$ è un sottoinsieme del prodotto cartesiano $X \times Y$ tale che $\forall x \in X \; \exists! y \in Y : y = f(x)$. Si parla di *intervallo* $[a, b]$ definito come $\{x \in \mathbb{R} \mid a \leq x \leq b\}$, quindi si usano i numeri reali $\mathbb{R}$ che a loro volta dovrebbero essere definiti in qualche modo (usando la teoria degli insiemi) e si usa una relazione d'ordine sui numeri reali che, come ogni relazione, è un sottoinsieme di $\mathbb{R} \times \mathbb{R}$ con determinate proprietà. Si parla poi di una funzione *continua*. Ricordiamo che una funzione è continua in un intervallo se è continua in y_0, $\forall y_0 \in [a, b]$ e continua in un punto y_0 significa che $\lim_{x \to y_0} f(x) = f(x_0)$, cioè:

$$\forall \epsilon > 0 \; \exists \delta > 0 : |x - x_0| < \delta \text{ e non}(x = y_0) \rightarrow |f(x) - f(y_0)| < \epsilon$$

L'enunciato è poi composto a sua volta da una implicazione "$\rightarrow$", perché ha la forma *Se vale ... allora ...*, la tesi, infine, può essere espressa con $\exists x_0 \in]a, b[$: $f'(x_0) = 0$. Se "smontiamo" quindi pezzo a pezzo l'enunciato del teorema di Rolle, alla fine ci ritroviamo a manipolare insiemi e simboli quali: $\wedge$, $\vee$, $\neg$, $\rightarrow$, $\leftrightarrow$, $\forall$, $\exists$.

I primi cinque simboli sono detti *connettivi logici*, gli ultimi due si dicono *quantificatori* (rispettivamente *universale* ed *esistenziale*), e il linguaggio formale che andremo ad usare sarà composto da combinazioni opportune di questi simboli (opportune significa: seguendo certe precise regole), assieme ai due ulteriori simboli $=$ e $\in$. Inoltre useremo lettere come $a, b, \ldots, x, y, \ldots$ o $X, Y, \ldots$ per indicare le *variabili* (che per noi saranno gli insiemi). Le combinazioni dei connettivi, quantificatori e variabili che si ottengono si chiamano *formule* del linguaggio. Più precisamente, le formule sono costruite in questo modo:

- sono formule espressioni della forma: $x = y$ o $x \in y$ (dove x e y sono qualsivoglia variabili)
- se ϕ e ψ sono formule, allora lo sono anche:

$$\phi \wedge \psi, \; \phi \vee \psi, \; \neg\phi, \; \phi \rightarrow \psi, \; \phi \leftrightarrow \psi, \; \forall x\phi, \exists x\phi$$

Useremo anche le parentesi "(" e ")" per specificare la precedenza con cui vanno intese le espressioni scritte.

Vediamo alcuni esempi di formule.

$$\neg\exists x\forall y\ y \in x, \quad \forall x\forall y(x \in y \vee (x = y \vee y \in x)), \quad \exists x\neg(x = x).$$

Prima di chiederci il significato di queste formule, constatiamo che dal punto di vista formale sono corrette, perché costruite ricorsivamente, usando le due regole scritte sopra. Se vogliamo dare un significato alla prima formula, assumendo che stia parlando di insiemi, essa afferma che "non c'è un insieme che contiene tutti gli insiemi". La seconda, interpretata sempre nell'ambito di insiemi, afferma che presi comunque due insiemi o sono uguali o uno dei due appartiene all'altro. La terza dice che esiste un insieme che è diverso da sè stesso. Le formule scritte si riferiscono agli insiemi ma noi non assumiamo di sapere cosa sono gli insiemi, quindi... ancora un po' di pazienza.

Comunque, per esercizio, cosa potrebbe mai affermare la formula:

$$\forall y\neg(y \in x)?$$

Cerchiamo ora, come esempio, una formula che possa esprimere il fatto che esiste l'intersezione di due insiemi a e b. La soluzione potrebbe essere:

$$\exists x\forall y(y \in x \leftrightarrow (y \in a \wedge y \in b))$$

(Ancora una volta: per ora non sappiamo cosa sono gli insiemi, ma se lo sapessimo, questa potrebbe essere la formula che afferma l'esistenza di un insieme x che è l'insieme intersezione $a \cap b$).

Analogamente si potrebbe fare per l'unione.

Esempio 1.2. Per cominciare a prendere un po' di familiarità con gli insiemi, si supponga di avere un universo che possiede *solamente* i seguenti insiemi:

$$a = \{b, c\}, \quad b = \{\}, \quad c = \{e\}, \quad d = \{c, e\}, \quad e = \{b\}$$

La notazione anticipa la notazione che in seguito useremo per gli insiemi e significa che nel nostro universo ci sono solo 5 insiemi e tra essi valgono alcune relazioni di appartenenza, come: $b \in a$ o $e \in c$, ecc. Quali delle seguenti affermazioni è vera?

- $(b \in c \to a \in a)$;
- $(e \in c \wedge a \in c)$;
- $\exists k\ k \in d$;
- $\forall s\exists t\ s \in t$;
- $\forall s\exists t\ t \in s$.

Un'ultima osservazione: può destare sorpresa il fatto che si scrivano espressioni come $x \in y$ dove x e y sono insiemi. Verrebbe da pensare che x, essendo un elemento di y, non è necessariamente un insieme. Questo dubbio dovrebbe svanire non appena costruiamo gli insiemi con gli assiomi di Zermelo Fraenkel.

2 Gli assiomi di Zermelo Fraenkel

La necessità di introdurre rigorosamente la teoria degli insiemi nasce dal fatto che una teoria "vaga", "imprecisa" come quella che era stata sviluppata a fine del XIX secolo si era dimostrata contradditoria. Il problema più evidente era stato messo in luce all'inizio del 1900 da Bertrand Russell, si tratta del ben noto *pardosso di Russell*, che è il seguente:
Consideriamo l'insieme U definito nel seguente modo: $U = \{x \mid x \notin x\}$ (Per esempio $\emptyset$ è un elemento di U). Quindi U è definito dalla condizione di essere fatto da quegli elementi che soddisfano una certa proprietà $P(x)$ dove $P(x)$ significa "x non appartiene a sè stesso". Se fosse $U \in U$, allora vorrebbe dire che vale $P(U)$, ma $P(U)$ afferma che $U \notin U$, se invece succedesse che $U \notin U$ allora U soddisfacerebbe $P(x)$ (con $x = U$), e quindi $U \in U$. Otteniamo così una contraddizione: la teoria degli insiemi, nel modo poco preciso in cui di solito si introduce, non può stare in piedi.

Il tentativo di risolvere il problema che nasce dal paradosso di Russell, ha portato allo sviluppo di varie formulazioni rigorose della teoria degli insiemi. Quella che forse si è rivelata di maggior successo è la teoria di Zermelo Fraenkel (ZF), che andremo ora ad introdurre. Certamente dovrà essere tale da evitare, perlomeno, il paradosso di Russell (e possibilmente altri paradossi).

Prima di entrare nei dettagli, un'osservazione. Quando definiamo un insieme ci viene del tutto naturale usare una formulazione del tipo: "consideriamo l'insieme A fatto con quegli elementi z che soddisfano alla condizione $C(z)$", cioè, scritto in sintesi: $A = \{z \mid C(z) \text{ è vera}\}$. L'insieme U introdotto sopra è di questa forma, ma esempi ce ne sono infiniti: l'immagine di una funzione $f : X \longrightarrow Y$ è definito come $\{y \mid \exists x \in X \ y = f(x)\}$, o, meglio, $\{y \in Y \mid \exists x \in X \ y = f(x)\}$, le funzioni continue in un intervallo $]a, b[$ sono definite come $\mathcal{C}^0(]a, b[) = \{f \mid \forall x_0 \in]a, b[\ (\exists \lim_{x \to x_0} f(x) = l \ \wedge f(x_0) = l)\}$. Vedremo tra un po' come questo modo di definire un insieme deve essere reso più preciso. Un problema del paradosso di Russell nasce proprio dal fatto che quando definiamo U come l'insieme di certi elementi x non andiamo a specificare in quale ambito vada preso x. L'idea più spontanea è considerare x scelto nell'insieme che contiene tutti gli insiemi. Ma il paradosso suggerisce che questo insieme non può esistere.

Si può dire che il filo conduttore della teoria di ZF sia quello che gli insiemi vengono via via costruiti a partire dall'insieme vuoto, un po' come si è visto per le formule dove, partendo da alcune formule di base, con opportune regole, si construiscono tutte le altre formule.

La teoria di ZF non dice esplicitamente cosa sono gli insiemi e gli elementi di un insieme, ma li identifica (potremmo dire che li circoscrive o delimita) attraverso gli assiomi e le formule dedotte dagli assiomi.

2.1 ZF1, ZF2, ZF3

Vediamo i primi tre assiomi della teoria di Zermelo Fraenkel (useremo la notazione $y \notin x$, che è un'abbreviazione di $\neg(y \in x)$):

ZF1 Assioma di estensionalità:

$$\forall x \forall y (x = y \leftrightarrow \forall z (z \in x \leftrightarrow z \in y))$$

ZF2 Assioma dell'insieme vuoto:

$$\exists x \forall y (y \notin x)$$

ZF3 Assioma delle coppie:

$$\forall x \forall y \exists z \forall w (w \in z \leftrightarrow (w = x \vee w = y))$$

Le formule ora scritte possono essere intese come semplici espressioni formali ottenute dalle regole dette per costruire formule ma naturalmente è opportuno associare ad esse un significato, e così si potrà fare anche per tutte le altre formule che da esse possono essere dedotte.

Pertanto vediamo quale significato si possa associare ai tre assiomi ora scritti.
ZF1: specifica l'uguaglianza tra due insiemi. Due insiemi sono uguali se e solo se hanno gli stessi elementi.
ZF2: Afferma che esiste un insieme: l'insieme vuoto.
ZF3: Afferma che dati due qualunque insiemi esiste un insieme i cui elementi sono precisamente i due insiemi dati.

L'importanza dei tre assiomi sarà (almeno in parte) spiegata dalle prossime applicazioni.

Teorema 2.1. *L'insieme vuoto esite ed è unico.*

Dimostrazione. Siano x e y due insiemi vuoti, cioè tali che $\forall z\ \neg(z \in x)$ e $\forall z\ \neg(z \in y)$. Preso dunque z, l'affermazione $z \in x \to z \in y$ è vera (ricordare che $p \to q$ significa $\neg p \vee q$, dunque nel nostro caso significa $\neg(z \in x) \vee z \in y$ che è quindi vera). Analogamente vale $z \in y \to z \in x$ e quindi $\forall z\ (z \in x \leftrightarrow z \in y)$ e allora, per ZF1, $x = y$. Pertanto, se c'è un insieme vuoto, questo è unico, ma per ZF2, un insieme vuoto c'è. □

L'insieme vuoto si indica con $\emptyset$.

La dimostrazione ora scritta non è puramente formale e fa uso del significato che abbiamo dato agli assiomi. È però importante notare che, note che siano tutte le regole di inferenza della logica, si potrebbe mutare in una dimostrazione puramente formale che fa cioè solo manipolazione di simboli. Tanto per essere più convincenti, vediamo come si potrebbe scrivere la dimostrazione facendo esclusivo uso della logica formale. Scriviamo riga per riga i vari passaggi, sottintendendo che il passaggio da una riga alla successiva è giustificato dalle regole della logica. Ecco qui alcune di tali regole:
(R_1) se si può scrivere p allora si può anche scrivere $p \vee q$,
(R_2) $(\neg p) \vee q$ può essere sostituito da $p \to q$,
(R_3) $\forall z\ p(z)$ assieme a $\forall z\ q(z)$ può essere sostituito da $\forall z\ p(z) \wedge q(z)$,
(R_4) $p \to q$ e $q \to p$ si può sostituire con $p \leftrightarrow q$.
Ecco quindi alcune righe che mostrano come, partendo da queste regole, si può scrivere una dimostrazione formale del fatto che due insiemi vuoti sono uguali:

$\forall z\ \neg(z \in x) \quad \forall z\ \neg(z \in y) \quad$ (ipotesi)
$\forall z\ (\neg(z \in x) \vee (z \in y)) \quad \forall z\ (\neg(z \in y) \vee (z \in x)) \quad (R_1)$
$\forall z\ (z \in x \to z \in y) \quad \forall z\ (z \in y \to z \in x) \quad (R_2)$
$\forall z\ (z \in x \to z \in y) \wedge (z \in y \to z \in x) \quad (R_3)$
$\forall z\ (z \in x \leftrightarrow z \in y) \quad (R_4)$
$x = y$ (per l'assioma ZF1).

D'ora in avanti non faremo più questo genere di dimostrazioni puramente formali, ma useremo una via di mezzo, cioè passeremo senza problemi dall'aspetto formale delle formule al significato che ad esse attribuiamo. In linea di principio, la dimostrazione formale è comunque sempre possibile.

L'assioma ZF3 dice che dati due insiemi x e y esiste un insieme i cui elementi sono x e y. Non ne afferma l'unicità che può però essere ottenuta applicando opportunamente l'assioma ZF1.

Se x e y sono due insiemi, l'(unico) insieme che ha per elementi x e y si può indicare con $\{x, y\}$. Si chiama insieme coppia (non ordinata).

Cos'è l'insieme $\{x, x\}$? Come conseguenza di ZF1, esso è l'insieme il cui unico elemento è x. Lo indicheremo con $\{x\}$ (e si chiama *singoletto* o *singleton*). In particolare abbiamo che se x è un insieme, allora esiste anche l'insieme $\{x\}$. In particolare, oltre a $\emptyset$ esistono $\{\emptyset\}$, $\{\{\emptyset\}\}\ldots$ Questo fatto però non implica ancora che esiste un insieme con infiniti elementi: per ora sappiamo solo che dai tre assiomi segue che gli insiemi con cui abbiamo a che fare non sono finiti, ma nessuno ci garantisce che la loro totalità formi un insieme.

L'insieme $\{x, y\}$ non rappresenta la coppia *ordinata* costituita da x e y. Dall'assioma ZF1 si ottiene infatti subito che $\{x, y\} = \{y, x\}$. Vogliamo quindi ora introdurre la definizione di coppia ordinata. Dati cioè due insiemi x e y, vogliamo un insieme che denotiamo con (x, y) tale che se $(x, y) = (a, b)$, allora $x = a$ e $y = b$. La seguente è una possibile definizione di coppia ordinata:

Dati due insiemi x e y, poniamo $\langle x, y\rangle$ per l'insieme $\{\{x\}, \{x, y\}\}$, che viene detto *coppia ordinata* (con prima coordinata x e seconda coordinata y).

L'esistenza dell'insieme $\{\{x\}, \{x, y\}\}$ è garantita da ZF3.

Teorema 2.2. *Siano x, y, z, t insiemi tali che $\langle x, y\rangle = \langle z, t\rangle$. Allora $x = z$ e $y = t$.*

Dimostrazione. Usiamo una proprietà dell'uguaglianza che non abbiamo ancora esplicitato e cioè che se $x = y$, allora $\{x\} = \{y\}$. Se $\langle x, y\rangle = \langle z, t\rangle$, allora, per definizione:

$$\{\{x\}, \{x, y\}\} = \{\{z\}, \{z, t\}\}.$$

Per ZF1, l'elemento $\{x\}$ dell'insieme di sinistra deve stare anche nell'insieme di destra. Quindi $\{x\} = \{z\}$ o $\{x\} = \{z, t\}$. Se $\{x\} = \{z\}$, per ZF1, $x = z$. Inoltre deve essere $\{x, y\} = \{z\}$ o $\{x, y\} = \{z, t\}$. Ancora una biforcazione: $x = y$ o $x \neq y$. Se $x = y$, allora, per ZF1, $\{x, y\} = \{x\}$, quindi, per ZF1, $\{\{x\}, \{x, y\}\} = \{\{x\}, \{x, x\}\} = \{\{x\}\}$. Per ZF1 allora $\{z, t\}$ deve essere uguale a $\{x\}$. Sempre per ZF1, $x = y = z = t$, quindi $x = z$ e $y = t$. Se $x \neq y$, allora, se fosse $\{x, y\} = \{z\}$, per ZF1 si avrebbe $y = z$ e quindi, siccome assumiamo

$x = z$, abbiamo $x = y$, contraddizione. Allora $\{x, y\} = \{z, t\}$, ma $x = z$, quindi $y = t$. I casi rimanenti si provano in modo analogo. □

Esercizio 1. Completare la dimostrazione.

Possiamo ora definire le terne ordinate, le quaterne ordinate, ecc. In generale, possiamo dire che se $x_1, x_2, \ldots, x_n$ sono insiemi con $n \geq 3$, allora si può definire, ricorsivamente:

$$\langle x_1, x_2, \ldots, x_n \rangle = \langle x_1, \langle x_2, \ldots, x_n \rangle \rangle$$

Esercizio 2. Spiegare che $\{x, \{y\}\}$ non è un buon modo di definire una coppia ordinata (cioè non soddisfa alla condizione data subito prima della definizione 2.1).

Naturalmente vi sono altri modi per associare a due insiemi x e y un insieme che abbia la proprietà della coppia ordinata. Ad esempio un'altra definizione di coppia ordinata potrebbe essere: $\{\{x\}, \{\{x\}, \{x, y\}\}$. In generale, una coppia ordinata (quando non è necessario esplicitare il modo in cui è stata definita) si indica con (x, y).

3 Lezione 2

3.1 Gli assiomi ZF4, ZF5, ZF6

Prima di introdurre i prossimi tre assiomi, ricordiamo un'abbreviazione: la formula $\forall z(z \in x \to z \in y)$ si abbrevia con $x \subseteq y$.

Precedentemente abbiamo richiamato il fatto che una funzione tra due insiemi A e B è un particolare sottoinsieme del prodotto cartesiano degli insiemi A e B. Il prodotto cartesiano è un insieme di coppie ordinate (che sappiamo, dalla teoria ingenua degli insiemi) che dovrebbe essere definito come $\{(a, b) \mid a \in A \wedge b \in B\}$, dove (a, b) è la coppia ordinata come definita nella precedente sezione. I tre assiomi finora introdotti non sono sufficienti per definire il prodotto cartesiano. Vediamo allora altri 3 assiomi che, tra le varie applicazioni, avranno proprio quella di permettere di definire $A \times B$.

ZF4 Assioma di separazione

$$\forall x \exists y \forall z(z \in y \leftrightarrow (z \in x \wedge \phi(z)))$$

dove $\phi(z)$ è una formula del linguaggio (contenente la variabile z).

ZF5 Assioma dell'insieme delle parti:

$$\forall x \exists y \forall z(z \in y \leftrightarrow z \subseteq x)$$

ZF6 Assioma dell'unione:

$$\forall x \exists y \forall z(z \in y \leftrightarrow \exists w(z \in w \wedge w \in x))$$

Innanzitutto vediamo il significato degli assiomi (già in parte chiarito dal loro nome).
L'assioma ZF4 afferma che dato un insieme x, si può ottenere un sottoinsieme di x fatto da tutti quegli elementi di x che soddisfano ad una certa proprietà. D'ora in poi, per indicare l'insieme y, usiamo la ben conosciuta notazione $\{z \in x \mid \phi(x)\}$.
L'assioma ZF5 afferma che se x è un insieme, esiste l'insieme di tutti i sottoinsiemi di x, cioè quello che si chiama l'insieme delle parti di x. Esso si indica con $\mathscr{P}(x)$.
L'assioma ZF6 dice che dato un insieme x esiste un insieme che è costituito da tutti gli elementi che sono elementi di qualche elemento di x. In altre parole, questo significa che, se x è un insieme i cui elementi sono insiemi, esiste l'unione di tutti gli elementi di x. La notazione che usiamo per questo insieme è: $\cup x$.

Ognuno dei tre assiomi inizia con $\forall x \exists y \ldots$ In tutti e tre i casi si può dimostrare (usando ZF1) che l'insieme y è unico, quindi le tre definizioni $\{z \in x \mid \phi(x)\}$, $\mathscr{P}(x)$ e $\cup x$ date sopra determinano i corrispondenti insiemi in modo univoco.

Abbiamo già anticipato l'assioma ZF4 quando abbiamo osservato che molto spesso si vanno a considerare insiemi della forma $\{z \mid C(z) \text{ è vera}\}$, l'insieme U

del paradosso di Russell era definito in questo modo, ma in ZF4 c'è una grossa limitazione: gli z vanno scelti in un insieme x dato a priori, quindi l'assioma di separazione permette di costruire solamente sottoinsiemi *di un insieme dato*. L'insieme $U = \{x \mid x \notin x\}$ certamente non è di questo tipo, perché non si specifica dove x va scelto.

L'assioma ZF5 assicura l'esistenza dell'insieme di tutti i sottoinsiemi di un dato insieme x.

Per quanto riguarda l'assioma ZF6, notiamo che se x e y sono due insiemi, allora, per ZF3, esiste l'insieme $\{x, y\}$. Applichiamo ad esso l'assioma ZF6: si ottiene che esiste un insieme c tale che $z \in c$ se e solo se $z \in x$ oppure $z \in y$, cioè c è l'unione degli insiemi x e y. In questo caso $\cup\{x, y\}$ si indica con $x \cup y$. Se x, y, z sono tre insiemi, possiamo considerare $\{x, y\}$ e $\{z\}$ usando ZF3 come già visto, possiamo allora fare l'unione $\{x, y\} \cup \{z\}$ che indichiamo con $\{x, y, z\}$ e con ZF6 possiamo allora ottenere $\cup\{x, y, z\}$ che indichiamo con $x \cup y \cup z$. Analogamente, se partiamo da degli insiemi $x_1, \ldots, x_n$, possiamo ottenere l'insieme $\{x_1, \ldots, x_n\}$ e quindi, da ZF6, l'insieme $x_1 \cup \cdots \cup x_n$. L'assioma ZF6 è però più potente, perché permette di considerare anche l'unione di infiniti insiemi.

Vediamo ora come ottenere l'intersezione di due insiemi x e y. Si potrebbe esser tentati di porre la definizione: $x \cap y = \{z \mid z \in x \wedge z \in y\}$, usando l'assioma ZF4, ma questa formulazione non è corretta, perché per applicare l'assioma ZF4 bisogna avere un insieme in cui gli elementi z possono appartenere. Una soluzione allora è la seguente:

Definizione 3.1. Se x e y sono due insiemi, allora si pone:

$$x \cap y = \{z \in x \cup y \mid z \in x \wedge z \in y\}$$

Analogamente, se x è un insieme non vuoto, si pone:

$$\cap x = \{z \in \cup x \mid \forall y(y \in x \to z \in y)\}$$

Vediamo ancora come si può definire il complementare di un insieme: se x è un insieme e $y \subseteq x$ è un suo sottoinsieme, allora si definisce il complementare di y in x (usando ZF4) come: $x \setminus y = \{z \in x \mid z \notin y\}$. Se definissimo il complementare di un insieme x semplicemente come $\{z \mid z \notin x\}$ da x unito al complementare di x si otterrebbe che tutto l'universo è un insieme e questo porterebbe al paradosso di Russell.

Vediamo infine come sia possibile definire il prodotto cartesiano di due insiemi X e Y. La definizione, versione "ingenua", potrebbe essere questa:
$X \times Y = \{\langle x, y\rangle \mid x \in X, y \in Y\}$
ma questa formulazione, ancora una volta, non è contemplata da ZF4. Il problema nasce dal fatto che bisonga avere un insieme che contenga tutte le coppie $\langle x, y\rangle$, cioè che abbia per elementi gli insiemi $\{\{x\}, \{x, y\}\}$. Si noti che $\{x\}$ e $\{x, y\}$ sono sottoinsiemi di $X \cup Y$, quindi elementi di $\mathscr{P}(X \cup Y)$, quindi $\{\{x\}, \{x, y\}\}$ è un sottoinsieme di $\mathscr{P}(X \cup Y)$ e pertanto un elemento di $\mathscr{P}(\mathscr{P}(X \cup Y))$. Allora adesso possiamo definire il prodotto cartesiano di due insiemi X e Y:

Definizione 3.2. Dati due insiemi X e Y, il *prodotto cartesiano* $X \times Y$ è definito da:

$$\{z \in \mathscr{P}(\mathscr{P}(X \cup Y)) \mid \exists x \exists y((x \in X \wedge y \in Y) \wedge z = \langle x, y \rangle\}$$

La definizione ora è coerente con ZF4.

Una volta nota la costruzione del prodotto cartesiano di due insiemi, si può, ricorsivamente, definire il prodotto cartesiano di un qualunque numero finito di insiemi, semplicemente basta osservare che:

$$X_1 \times \cdots \times X_n = X_1 \times (X_2 \times \cdots \times X_n)$$

Se A e B sono due insiemi, possiamo definire un'applicazione tra A e B in questo modo:

Definizione 3.3. Si dice che f è un'applicazione tra gli insiemi A e B se $f \subseteq A \times B$ e se, inoltre:

$$\forall a(a \in A \to \exists b(b \in B \wedge \langle a, b \rangle \in f \wedge \forall b'(\langle a, b' \rangle \in f \to b' = b)))$$

Quanto scritto non è altro che la nota condizione che f associa ad ogni elemento di A un ben determinato elemento di B, tradotto in linguaggio formale.

Infine, un'ultima definizione:

Definizione 3.4. Siano X e Y insiemi. Allora si pone:

$$X^Y = \{f \in \mathscr{P}(Y \times X) \mid f \text{ è una funzione}\}$$

L'insieme X^Y esiste per conseguenza dei precedenti assiomi ed è l'insieme di tutte le funzioni da Y in X.

4 Lezione 3

4.1 Gli assiomi ZF7, ZF8, ZF9

Concludiamo l'elenco degli assiomi della teoria di Zermelo Fraenkel con gli ultimi tre:

ZF7 Assioma dell'infinito

$$\exists x \left(\emptyset \in x \wedge \forall y (y \in x \rightarrow y \cup \{y\} \in x)\right)$$

ZF8 Assioma di rimpiazzamento

$$\forall x \exists y \forall y' \left(y' \in y \leftrightarrow \exists x' \left(x' \in x \wedge \phi(x', y')\right)\right)$$

dove $\phi(s,t)$ è una formula tale che:

$$\forall s \exists t \left(\phi(s,t) \wedge \forall t' \left(\phi(s,t') \rightarrow t' = t\right)\right)$$

ZF9 Assioma di fondazione

$$\forall x \exists y \left(y \in x \wedge x \cap y = \emptyset\right)$$

Vediamo ora di capire il significato dei tre assiomi e di capire alcune delle loro conseguenze. L'assioma ZF7 afferma l'esistenza di un insieme x con le seguenti proprietà: 1) l'insieme vuoto sta in x, 2) se y è un insieme, elemento di x, anche $y \cup \{y\}$ sta in x. Formalmente, queste due condizioni assomigliano molto alla formulazione che si dà al principio di induzione e su questo punto ritorneremo in seguito. Per intanto osserviamo che conseguenza dell'assioma ZF7 è che esiste un insieme che contiene (almeno) i seguenti elementi:

$$\emptyset, \quad \{\emptyset\}, \quad \{\emptyset, \{\emptyset\}\}, \quad \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \quad \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\}, \ldots$$

Forzando un po' i tempi, si potrebbe dire che questo insieme contiene i numeri $0, 1, 2, 3, \ldots$ e in effetti ZF7 vedremo che è essenziale per la definizione dell'insieme dei numeri naturali $\mathbb{N}$.

L'assioma ZF8 richiede un po' di attenzione per essere compreso. Intanto vediamo che la formula $\phi(s,t)$ con la condizione scritta sopra si può interpretare dicendo che, tramite ϕ si può associare ad ogni insieme s un unico insieme t, potremmo cioè dire che da ϕ si ottiene una funzione $\tilde{\phi}$ che associa ad ogni insieme s un insieme $t = \tilde{\phi}(s)$. Naturalmente $\tilde{\phi}$ non si può intendere come una funzione di quelle definite nella lezione precedente, perchè non è esplicitato il dominio, ma pensarla come funzione è utile per comprendere l'assioma ZF8. Allora l'assioma dice: comunque preso un insieme x esiste un insieme y i cui elementi sono esattamente gli elementi della forma $\tilde{\phi}(x')$ con $x' \in x$; cioè, detto in modo più sintetico, dato x e una formula con le condizioni indicate in ZF8, esiste l'insieme $y = \tilde{\phi}(x)$.

L'assioma ZF8 ha varie, importanti applicazioni. Una di queste consiste nel riuscire a provare che esistono insiemi i cui elementi sono:

$$\{\mathbb{N}, \mathscr{P}(\mathbb{N}), \mathscr{P}(\mathscr{P}(\mathbb{N})), \ldots\}$$

e la possibilità di sapere che esiste un siffatto insieme risulta utile per dimostrare alcune proprietà dei numeri cardinali. Per ora, non approfondiremo ulteriormente la discussione su ZF8.

Per quanto riguarda l'assioma ZF9, vediamo con un primo esempio, cosa permette di ottenere. Supponiamo ci sia un insieme x tale che $x \in x$. Allora, per ZF9, l'insieme $\{x\}$ è tale che contiene un y tale che $y \cap \{x\} = \emptyset$, ma se $y \in \{x\}$, necessariamente $y = x$ e quindi $x \cap \{x\} = \emptyset$. Se dunque $x \in x$, poiché anche $x \in \{x\}$, abbiamo un assurdo. In particolare, la totalità $\mathcal{V}$ degli insiemi non può essere un insieme (se lo fosse, avremmo $\mathcal{V} \in \mathcal{V}$). Osserviamo poi quanto segue: la teoria degli insiemi sviluppata dagli assiomi di Zermelo Fraenkel permette di ottenere tutti gli insiemi di cui necessitiamo in matematica partendo dall'esistenza dell'insieme vuoto e di un insieme infinito, costruito con ZF7, a partire dall'insieme vuoto. Ogni insieme che viene poi ottenuto applicando gli assiomi ha per elementi ancora insiemi. Quindi accade che un insieme x_0 ha elementi che sono insiemi. Consideriamo uno di essi, diciamo x_1. Essendo x_1 un insieme, esso avrà per elementi insiemi. Prendiamo uno di essi, diciamo x_2. Così facendo, si ottiene una sequenza come la seguente:

$$\cdots x_{n+1} \in x_n \cdots \in x_3 \in x_2 \in x_1 \in x_0. \tag{1}$$

La costruzione ora presentata degli elementi $x_0, x_1, \ldots$ richiede di fare delle scelte di elementi appartenenti ad insiemi. Questo fatto verrà discusso in seguito (quando parleremo dell'assioma della scelta), ma il punto che si vuole focalizzare ora è un altro: si vuole semplicemente far vedere che è del tutto ragionevole chiedersi se sia possibile avere una sequenza infinita di insiemi come quelli scritti in (1). Supponiamo dunque di avere una sequanza di elementi come in (1), e supponiamo che formino un insieme X i cui elementi, quindi, sono $x_0, x_1, x_2, \ldots$ L'assioma ZF9 serve a dire che questa sequenza non può essere infinita. Infatti, per ZF9 esiste un $y \in X$ tale che $y \cap X = \emptyset$. Ma y sarà un x_m per qualche m. Se esistesse x_{m+1}, allora avremmo $x_{m+1} \in X$ e $x_{m+1} \in y$, quindi $x_{m+1} \in y \cap X$ e questo è assurdo.

Qui si conclude la breve discussione sulla teoria assiomatica degli insiemi di Zermelo Fraenkel. Nella prossima lezione parleremo ancora di un assioma, che è l'assioma della scelta e che completa la lista di assiomi generalmente accettati per sviluppare i concetti matematici. Prima di chiudere questa lezione, però, ancora un'osservazione. La teoria di Zermelo Fraenkel nasce per superare una palese contraddizione messa in evidenza da Russell, ma chi ci garantisce che non ci possano essere altre contraddizioni nascoste nella teoria? La prima tentazione sarebbe quindi quella di dire: adesso che abbiamo sistemato la matematica in maniera rigorosa definendo degli assiomi da cui si deriva tutto, dimostriamo che questa teoria non ha contraddizioni. Purtroppo questo non è possibile: nel 1930 Kurt Gödel ha dimostrato che se una teoria è sufficientemente potente da

permette di definire i numeri naturali, allora la teoria non può dimostrare la sua consistenza. Una prima infarinatura sui teoremi di Gödel può essere il sito di wikipedia. Vedi:
`https://it.wikipedia.org/wiki/Teorema_di_completezza_di_G%C3%B6del`

5 Lezione 4

5.1 L'assioma della scelta

Una volta introdotto un linguaggio e degli assiomi che permettono di sviluppare in maniera rigorosa la teoria degli insiemi, possiamo ora continuare le nostre considerazioni ritornando ad usare le notazioni usuali, consapevoli comunque che, essendo concise, mancano spesso di precisione, ma consapevoli anche che, con gli strumenti che abbiamo introdotto, la precisione può essere facilmente ricostruita. Vediamo alcuni esempi: se A e B sono due insiemi, la proiezione canonica $p : A \times B \longrightarrow A$ è definita da $p(a, b) = a$. La definizione $p(a, b) = a$ non rientra nel tipo di definizioni consentite dal linguaggio introdotto, ma vediamo come si può rimediare. Ricordando come abbiamo definito le funzioni, p deve essere un sottoinsieme di $(A \times B) \times A$ e più precisamente $p = \{<< x, y >, z >\in (A \times B) \times A \mid z = x\}$. L'insieme p così definito soddisfa la definizione di funzione e p corrisponde alla proiezione canonica di $A \times B$ su A. In modo analogo si può definire la proiezione canonica $q : A \times B \longrightarrow B$.

Consideriamo un altro esempio: se parliamo di immagine $f(A)$ di una funzione $f : A \longrightarrow B$, intendiamo dire che consideriamo l'insieme $\{y \in B \mid \exists x \in A\, y = f(x)\}$ e questo insieme esiste per conseguenza dell'assioma ZF4 di separazione, anche se la formula $y = f(x)$ non è ancora una formula corretta nel linguaggio introdotto. Si tratta quindi di specificare meglio cosa si intende per $y = f(x)$. Allora una definizione di $f(A)$ che rientra nella formulazione direttamente riconducibile al nostro linguaggio potrebbe essere:

$$f(A) = \{y \in B \mid \exists x \in A\, (< x, y >\in f)\}.$$

Ancora un'indicazione: abbiamo accennato al fatto che dagli assiomi ZF1, ..., ZF9 è possibile costruire l'insieme dei numeri naturali. La sua effettiva costruzione verrà fatta in seguito, però già da adesso utilizzeremo l'insieme $\mathbb{N}$ con le sue proprietà (e così pure useremo gli insiemi $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e le loro proprietà, riservandoci di approfondire la loro costruzione nelle lezioni successive).

Per introdurre l'assioma della scelta, partiamo da qualche esempio:

Sia $f : A \longrightarrow B$ un'applicazione suriettiva. Esiste un'applicazione g da B in A tale che $f(g(b)) = b$ per ogni $b \in B$? (Si noti che se g esiste, necessariamente è iniettiva).

Pensiamo ad un caso particolarmente semplice: sia $A = \{1, 2, 3, 4\}$ e $B = \{5, 6, 7\}$ e sia $f(1) = 5,\ f(2) = 6,\ f(3) = 7,\ f(4) = 6$. L'applicazione f è suriettiva. In questo caso possiamo trovare una funzione g tale che $g \circ f = 1_B$, basta prendere per ogni $b \in B$ un elemento in A tale che $f(a) = b$, quindi $g(5) = 1, g(6) = 2, g(7) = 3$. Il fatto che gli insiemi A e B hanno un numero finito di elementi (in realtà basta sapere che B ha un numero finito di elementi), permette di dare alla funzione g una descrizione in un numero finito di passi. E questa costruzione può essere facilmente codificata nel linguaggio formale che abbiamo introdotto (in effetti basta dire che $g = \{\langle 5, 1\rangle, \langle 6, 2\rangle, \langle 7, 3\rangle, \langle 6, 4\rangle\}$).

Passiamo ora ad un caso un po' più complesso: sia ora il dominio di f dato da $\mathbb{N}$, quindi supponiamo di avere un'applicazione $f : \mathbb{N} \longrightarrow B$ suriettiva. Se

cerchiamo di procedere come nell'esempio precedente e cioè prendere per ogni $b \in B$ un elemento a in $\mathbb{N}$ tale che $f(a) = b$ può succedere che l'elemento a sia da scegliere in un insieme infinito (perché $f^{-1}(b)$ può essere infinito) e quindi può diventare problematico indicare la sua scelta con una formula che necessariamente deve essere espressa con una formula finita. In questo caso, però, la struttura dei numeri naturali (e in particolare il fatto che ogni insieme non vuoto di numeri naturali ha elemento minimo) ci può essere d'aiuto. Possiamo dunque definire, per ogni $b \in B$, $g(b)$ come il minimo dell'insieme $\{n \in \mathbb{N} \mid f(n) = b\}$. In questo modo g è definita in un numero finito di passi. Altri casi possono essere più problematici. Nel caso generale, dovremmo poter scegliere, per ogni $b \in B$ un elemento $a_b \in f^{-1}(\{b\})$, cioè dovremmo avere un'applicazione $h : \cup\{f^{-1}(\{b\}) \mid b \in B\} \longrightarrow A$. Per superare l'ostacolo c'è in realtà bisogno di un nuovo assioma:

Assioma della scelta: Sia $\mathscr{F}$ un insieme di insiemi non vuoti. Allora esiste una funzione $h : \mathscr{F} \longrightarrow \cup\mathscr{F}$ tale che, per ogni $A \in \mathscr{F}$ vale: $h(A) \in A$.
h è detta una *funzione di scelta*.

L'assioma dice che per ogni elemento A di $\mathscr{F}$ si può scegliere un elemento in A. L'assioma si limita a dire che esiste la possibilità di fare la scelta, non dice come effettivamente vada fatta.

Osservazione 5.1. Si noti che se X è un insieme non vuoto, allora l'affermazione "sia $x \in X$", cioè la scelta di un elemento nell'insieme X, può certamente essere garantita dall'assioma della scelta, ma in realtà l'utilizzo di tale assioma non è necessario, in quanto affermare che X non è vuoto significa affermare che $\neg(\forall x(x \notin X))$, che si convete in $\exists x \in X$. La stessa considerazione si applica ad un insieme finito $X_1, \ldots, X_n$ di insiemi: scegliere degli elementi $x_1 \in X_1, \ldots, x_n \in X_n$ può essere fatto *senza* far ricorso all'assioma della scelta. Quindi l'assioma si applica soprattutto quando abbiamo a che fare con "infinite scelte", cioè con un insieme $\mathscr{F}$ che sia infinito.

Come prima applicazione dell'assioma della scelta, vediamo che da esso segue la possibilità di trovare, per un'applicazione suriettiva $f : A \longrightarrow B$, una sua inversa destra g. In questo caso basta prendere $\mathscr{F} = \{f^{-1}(\{b\}) \mid b \in B\}$, allora $\cup\{f^{-1}(\{b\}) \mid b \in B\} = A$ e la funzione di scelta h permette di definire g: $g(b) = h(\{f^{-1}(b)\})$.

Vi sono molte formulazioni equivalenti dell'assioma della scelta:

Teorema 5.2. *Le seguenti affermazioni sono equivalenti tra loro ed equivalenti all'assioma della scelta:*

1. *per ogni insieme $\mathscr{F}$ costituito da insiemi non vuoti e a due a due disgiunti, esiste una funzione $h : \mathscr{F} \longrightarrow \cup\mathscr{F}$ tale che $h(A) \in A$ per ogni $A \in \mathscr{F}$.*

2. *Per ogni insieme M non vuoto esiste una funzione $h : \mathscr{P}(M) \setminus \{\emptyset\} \longrightarrow M$ tale che $h(A) \in A$ per ogni $A \subseteq M$, $A \neq \emptyset$.*

Dimostrazione. L'assioma della scelta banalmente comporta la condizione (1). Vediamo che (1) implica (2). Sia M non vuoto. Consideriamo

$$\mathscr{F} = \{A \times \{A\} \mid A \in \mathscr{P}(M),\ A \neq \emptyset\}.$$

Questa definizione di $\mathscr{F}$ permette di trasformare $\mathscr{P}(M)$ in un insieme di insiemi a due a due disgiunti, per poter applicare la condizione (1).
Vediamo ora che (2) implica l'assioma della scelta. Sia $\mathscr{F}$ un insieme di insiemi non vuoti. È sufficiente considerare $M = \cup\mathscr{F}$. □

Esercizio 3. Mettere a posto i dettagli della dimostrazione.

Esercizio 4. Provare che l'assioma della scelta è equivalente ad avere che ogni $f : A \longrightarrow B$ suriettiva ammette inversa destra.
(Suggerimento: per provare che ogni applicazione suriettiva ammette inversa destra implica l'assioma della scelta, usare la condizione (1) e la funzione $\phi : \cup\mathscr{F} \longrightarrow \mathscr{F}$ data da $\phi(x) = A_x$, dove A_x è quell'elemento di $\mathscr{F}$ tale che $x \in A_x$.)

Nelle lezioni precedenti abbiamo definito il prodotto $A \times B$ di due insiemi A e B e quindi anche il prodotto di un numero finito di insiemi. Si può però definire anche il prodotto infinito di un qualunque insieme di insiemi $\{A_i \mid i \in I\}$ (indicato con $\prod_{i\in I} A_i$):
Si pone:

$$\prod_{i\in I} A_i = \{f : I \longrightarrow \cup_{i\in I} A_i \mid f(i) \in A_i\}$$

Si può facilmente provare che:

Teorema 5.3. *L'assioma della scelta è equivalente ad affermare che il prodotto di una famiglia $\{A_i \mid i \in I\}$ di insiemi non vuoti è non vuoto.*

L'assioma della scelta è stato introdotto da Zermelo ma la sua accettazione da parte dei matematici è stata molto controversa. Comunque nel 1940 Gödel dimostrò che l'assioma della scelta era consistente con gli assiomi di Zermelo Fraenkel e successivamente, nel 1963, Cohen provò che l'assioma della scelta era indipendente dagli assiomi ZF, cioè non poteva essere provato internamente alla teoria. Pertanto accettare o non accettare l'assioma della scelta è, per così dire, una questione di gusti personali. Il fatto è che dall'assioma della scelta seguono molti risultati importanti che altrimenti non potrebbero essere provati. Ne elenchiamo brevemente alcuni:

- Ogni insieme non vuoto ammette un buon ordinamento (cioè ammette un ordinamento totale tale che ogni sottoinsieme non vuoto ha minimo elemento);
- Un'unione numerabile di insiemi vuoti è un insieme vuoto;
- Lemma di Zorn;

- Se G è un gruppo, ammette un sottogruppo abeliano massimale;
- Ogni anello commutativo unitario ammette ideale massimale;
- Se V è uno spazio vettoriale, allora V ammette una base:
- ...

5.2 Soluzione esercizi

Soluzione esercizio 3: Vediamo i dettagli del fatto che la condizione (1) implica la condizione (2). La famiglia $\mathscr{F}$ è fatta da insiemi a due a due disgiunti, quindi esiste, per la condizione (1), un'applicazione $h : \mathscr{F} \longrightarrow \cup\mathscr{F}$ tale che $h(A \times \{A\}) \in A \times \{A\}$. Sia $p : A \times \{A\} \longrightarrow A$ la proiezione sulla prima componente. Allora $p(h(A \times \{A\})) \in A$ e quindi $h \circ p : \mathscr{P}(M) \setminus \{\emptyset\} \longrightarrow M$ è l'applicazione cercata.
Per completare la dimostrazione che la condizione (2) implica l'assioma della scelta, dato $\mathscr{F}$ e preso, come suggerito, $M = \cup\mathscr{F}$, sia $h : \mathscr{P}(M) \setminus \{\emptyset\} \longrightarrow M$ l'applicazione la cui esistenza è assicurata dall'ipotesi (e quindi $h(A) \in A$). Allora l'applicazione $\mathscr{F} \longrightarrow \cup\mathscr{F}$ è la restrizione di h a $\mathscr{F}$.
Soluzione esercizio 4: Si è già visto che l'assioma della scelta permette di provare che ogni applicazione suriettiva $f : A \longrightarrow B$ ammette inversa destra (cioè esiste un'applicazione $g : B \longrightarrow A$ tale che $g \circ f = 1_B$). Vediamo ora il viceversa, supponiamo quindi di sapere che ogni applicazione suriettiva ammette inversa destra e proviamo che allora vale l'assioma della scelta. Basta allora provare che vale la condizione (1) del teorema 5.2. Sia allora $\mathscr{F}$ un insieme di insiemi disgiunti e consideriamo l'applicazione $f : \cup\mathscr{F} \longrightarrow \mathscr{F}$ data da $f(a) = A$ dove A è quell'unico insieme di $\mathscr{F}$ a cui a appartiene (è qui che si usa il fatto che gli elementi di $\mathscr{F}$ sono a due a due disgiunti). L'applicazione f è suriettiva e quindi ammette un'inversa destra $h : \mathscr{F} \longrightarrow \cup\mathscr{F}$. Sia $A \in \mathscr{F}$ e sia $a = h(A)$. Poiché $f(h(A)) = A$, abbiamo che $f(a) = A$ ma, per defnizione di f, $a \in A$.

5.3 approfondimento sul Lemma di Zorn

In questa sezione approfondiamo il lemma di Zorn e il modo in cui usualmente viene utilizzato. Si ricordi che un insieme A si dice parzialmente ordinato se su A è definita una relazione d'ordine parziale (che indichiamo con $<$), cioè una relazione $<$ sugli elementi di A (quindi un sottoinsieme di $A \times A$) tale che non vale $a < a$ per ogni $a \in A$ e se $a < b$ e $b < c$, allora $a < c$. Se poi, per ogni $a, b \in A$, o $a < b$ o $a = b$ o $b < a$, allora la relazione d'ordine si dice totale (altrimenti si dice parziale). Quindi in una relazione d'ordine parziale, non tutti gli elementi dell'insieme sono confrontabili tra loro. Il simbolo $\leq$ viene anche spesso usato per indicare una relazione d'ordine (parziale o totale). Si pone semplicemente: $a \leq b$ se $a < b$ o se $a = b$.

Un tipico (e importante) esempio di insieme con relazione d'ordine parziale è il seguente: Sia X un insieme (non vuoto). Sia A l'insieme delle parti di X, cioè $A = \{B \mid B \subseteq A\}$. Se definiamo su A la relazione $B_1 < B_2$ se $B_1 \subset B2$

(o $B_1 \leq B_2$ se $B_1 \subseteq B_2$), abbiamo una relazione d'ordine parziale (è totale solo nel caso che A abbia un solo elemento).

Se A è un insieme ordinato, si dice una *catena* di A un sottoinsieme di A che, rispetto alla relazione d'ordine di A, è totalmente ordinato. Se A è totalmente ordinato, ovviamente, ogni sottoinsieme di A è una catena. Se ad esempio A è l'insieme delle parti dell'insieme $X = \{1, 2, 3\}$, allora $\{\{1, 2\}, \{2, 3\}\}$ non è una catena (i suoi due elementi non sono confrontabili: né $\{1, 2\}$ è contenuto in $\{2, 3\}$, né viceversa), mentre l'insieme $\{\{1, 2\}, \{1, 2, 3\}, \{1\}\}$ è una catena.

Se A è un insieme parzialmente ordinato e se B è un sottoinsieme di A, si dice che $a \in A$ è un *maggiorante* per B se $b \leq a$ per ogni $b \in B$, cioè se a è maggiore di ogni elemento di B. Se A è un insieme non vuoto, ordinato e se ogni catena di A ammette maggiorante, allora A si dice un insieme *induttivo*.

Si dice infine che m è un estremo superiore di un insieme parzialmente ordinato A se in A non ci sono elementi maggiori di m (cioé se, per ogni $a \in A$ o $a \leq m$ o a e m non sono confrontabili).

Vediamo ora alcuni esempi di insiemi induttivi:

Esempio 5.4. Sia V uno spazio vettoriale e sia Σ l'insieme costituito con tutti i sottoinsiemi di V che sono fatti da elementi linearmente indipendenti. Allora Σ è induttivo (rispetto alla relazione d'ordine data dall'inclusione: $B \leq C$ se $B \subseteq C$).

Dimostrazione. Innanzitutto, osserviamo che Σ non è vuoto (se $v \in V$ è un vettore non nullo allora è linearmente indipendente e quindi $\{v\}$ è un elemento di Σ). Per definizione, dobbiamo provare che ogni catena di Σ ammette almeno un elemento maggiorante. Sia quindi $C \subseteq \Sigma$ una catena di Σ, quindi un sottoinsieme totalmente ordinato. Ogni elemento di C è costituito da un insieme W di vettori linearmente indipendenti. Consideriamo allora l'insieme $M = \cup_{W \in C} W$, cioè M è l'insieme fatto da tutti i vettori che stanno in qualche elemento della catena C. Certamente avremo che $W \leq M$ per ogni $W \in C$. Per provare quindi che M è un maggiorante, bisogna provare che M sta in Σ, cioè che l'insieme M è fatto da elementi linearmente indipendenti e quest'ultima affermazione significa provare che presi comunque un numero finito di vettori $v_1, \ldots, v_n \in M$, questi sono linearmente indipendenti. Però, poiché M è fatto dall'unione degli insiemi di C, abbiamo che, per ogni $i = 1, \ldots, n$ esiste $W_i \in C$ tale che $W_i \in C$. Gli elementi $W_1, \ldots, W_n$ sono a due a due confrontabili (perché C è totalmente ordinato) e quindi c'è tra essi il più grande di tutti, sia W_m. Allora, per ogni i, $v_i \in W_i \subseteq W_m$, quindi $v_1, \ldots, v_n$ sono tutti contenuti in $W_m \in Sigma$ e allora sono linearmente indipendenti. Questo prova che C ammette maggiorante. □

Esempio 5.5. Sia G un gruppo. Allora l'insieme Σ di tutti i sottogruppi abeliani di G è un insieme induttivo (rispetto alla relazione d'ordine data dall'inclusione).

Dimostrazione. L'insieme Σ non è vuoto (se $g \in G$ è un elemento di G, il gruppo ciclico generato da g è un sottogruppo abeliano di G e quindi sta in Σ. Anche ora, sia C una catena di Σ e, come prima, consideriamo l'insieme $M = \cup_{W \in C} W$.

Quindi M è un'unione di gruppi abeliani. Inoltre $W \leq M$ per ogni $W \in C$, se quindi riusciamo a vedere che M sta in Σ, allora è un maggiorante di C. Per far vedere che M sta in Σ bisogna far vedere che M è un gruppo abeliano. In generale non è vero che unione di gruppi (o gruppi abeliani) è ancora un gruppo (o un gruppo abeliano), però il fatto che C è una catena permette di arrivare alla conclusione. Infatti, siano $g, h \in M$ due elementi di M, allora esistono $W_1, W_2 \in C$ tali che $g \in W_1$ e $h \in W_2$. Ma W_1 e W_2 sono tra loro confrontabili, quindi per esempio sarà $W_1 \subseteq W_2$ e quindi $g, h \in W_2$, allora $gh^{-1} \in W_2$ e pertanto $gh^{-1} \in M$ (e questo prova che M è un gruppo) inoltre, essendo W_2 abeliano, $gh = hg$ e quindi M è abeliano. □

Esempio 5.6. Sia A un anello commutativo unitario. Allora l'insieme Σ degli ideali propri di A (cioè degli ideali di A propriamente contenuti in A) è un insieme induttivo (rispetto alla relazione d'ordine data dall'inclusione). Si noti che un maggiorante di una catena deve essere un ideale proprio (se non fosse proprio, conterrebbe l'elemento 1, ma allora un elemento della catena di ideali conterrebbe anche l'elemento 1 e non sarebbe proprio).

Dimostrazione. L'insieme Σ non è vuoto, perché $(0) \in \Sigma$. Sia C una catena di Σ, proviamo che C ha elemento maggiorante per l'ordinamento. Consideriamo $M = \cup_{W \in C} W$. M è un ideale (si vede nello stesso modo in cui si è provato, nell'esempio precedente, che l'unione di una catena di gruppi è un gruppo), e quindi Σ è induttivo. □

Dopo questi veloci richiami sugli insiemi ordinati, veniamo al lemma di Zorn:

Teorema 5.7. *Le seguenti condizioni sono equivalenti:*

1. *Assioma della scelta;*
2. (Lemma di Zorn.) *Ogni insieme parzialmente ordinato induttivo, ammette elemento massimale.*

(Si omette la dimostrazione).
Partendo quindi dall'assioma della scelta, e usando il lemma di Zorn, è possibile ottenere molte proprietà matematiche importanti. Ad esempio:

Teorema 5.8. *Ogni spazio vettoriale ammette una base.*

Dimostrazione. Come si è visto nell'esempio 5.4, l'insieme degli elementi linearmente indipendenti di uno spazio vettoriale è induttivo, quindi, per Zorn, esiste un elemento massimale $\mathcal{M}$. Tale elemento genera V (se non generasse V, ci sarebbe un elemento v che non sta nello spazio vettoriale generato da $\mathcal{M}$, ma allora $\mathcal{M} \cup \{v\}$ sarebbe fatto da elementi linearmente indipendenti e sarebbe più grande di $\mathcal{M}$). Quindi $\mathcal{M}$ è una base di V in quanto è un sistema di generatori fatto da elementi linearmente indipendenti. □

Teorema 5.9. *Ogni gruppo contiene un sottogruppo abeliano massimale.*

Dimostrazione. Dall'esempio 5.5, l'insieme dei sottogruppi abeliani di un gruppo è induttivo, quindi, per Zorn, ammette elemento massimale. □

Teorema 5.10. *Ogni anello commutativo unitario, ammette un ideale massimale.*

Dimostrazione. Dall'esempio 5.6 abbiamo che l'insieme degli ideali propri è induttivo, quindi, per Zorn, esiste un elemento massimale $\mathcal{M}$. □

6 Lezione 5

6.1 I numeri naturali

Vediamo ora come sia possibile, a partire dagli assiomi ZF1, ..., ZF9, costruire l'insieme $\mathbb{N}$ dei numeri naturali.

Definizione 6.1. Dato un insieme x, il *successore* di x, indicato con x^+ è l'insieme $x^+ = x \cup \{x\}$.

In particolare:

$$\begin{aligned} \emptyset^+ &= \emptyset \cup \{\emptyset\} = \{\emptyset\} \\ \emptyset^{++} &= (\emptyset^+)^+ = \{\emptyset, \{\emptyset\}\} \\ \emptyset^{+++} &= (\emptyset^{++})^+ = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \end{aligned}$$

Si vede, semplicemente dalla definizione, che $x \subseteq x^+$, inoltre, osservando gli elementi scritti, pare che x^+ abbia un elemento in più di x, questo in effetti può essere dimostrato:

Proposizione 6.2. *L'insieme x^+ ha un elemento in più dell'insieme x.*

Dimostrazione. L'insieme x^+ ha come sottoinsieme l'insieme x, quindi certamente contiene tutti gli elementi di x. Ma contiene anche l'elemento x. Questo è un elemento in più, infatti se così non fosse, allora avremmo $x \in x$ e questo è in contraddizione con l'assioma ZF9. □

Definizione 6.3. Un insieme y si dice *induttivo* se $\emptyset \in y$ e se $x^+ \in y$ per ogni $x \in y$.

Si vede subito che se y_1 e y_2 sono due insiemi induttivi, allora $y_1 \cap y_2$ è induttivo.

L'assioma ZF7 afferma l'esistenza di un insieme induttivo. Allora si definisce $\mathbb{N}$ come il più piccolo insieme induttivo, quindi come l'intersezione di tutti gli insiemi induttivi. Più precisamente: Sia y un insieme induttivo (la cui esistenza, come detto, è garantita dall'assioma ZF7). Consideriamo l'insieme X di tutti i sottoinsiemi z di y che sono induttivi, cioè, in accordo con ZF4: $X = \{z \in \mathscr{P}(y) \mid z \text{ è induttivo}\}$. Allora si pone:

Definizione 6.4. L'insieme dei numeri naturali $\mathbb{N}$ è definito da:

$$\mathbb{N} = \bigcap X.$$

Osservazione 6.5. Si noti che per definire l'insieme $\mathbb{N}$ si è usata la definizione di intersezione (v. def. 3.1) che nasce direttamente da ZF6.

Osservazione 6.6. Si noti che se t è un altro insieme induttivo (non necessariamente sottoinsieme di y), allora, come detto, $t \cap y$ è un insieme induttivo ed è un sottoinsieme di y, quindi $\mathbb{N}$ risulta essere l'intersezione di *tutti* i sottoinsiemi induttivi, non solo dei sottoinsiemi induttivi di y.

Un numero naturale è un elemento di $\mathbb{N}$. Se $x, y \in \mathbb{N}$ sono due numeri uguali, x e y sono uguali come insiemi, cioè hanno gli stessi elementi (ZF1).

È facile vedere che vale:

Teorema 6.7. *L'insieme $\mathbb{N}$ è induttivo.*

Definizione 6.8. La funzione $S : \mathbb{N} \longrightarrow \mathbb{N}$ data da: $S(x) = x^+$ si dice *funzione successore*. Si conviene di scrivere 0 al posto di $\emptyset \in \mathbb{N}$, mentre 0^+ si indica con 1, 1^+ si indica con 2, ecc.

Vale:

Teorema 6.9. *Sia $A \subseteq \mathbb{N}$ un qualunque sottoinsieme. Se vale:*

- *A contiene 0;*
- *se $n \in A$, allora $n^+ \in A$;*

allora $A = \mathbb{N}$.

Dimostrazione. A è un insieme induttivo, ma $\mathbb{N}$ è l'intersezione di tutti gli insiemi induttivi, quindi $\mathbb{N} \subseteq A$ e allora $A = \mathbb{N}$. □

È chiaro che il teorema precedente altro non è che il principio di induzione.
Guardando alla definizione dei numeri naturali 0, 1, 2 data, si vede che vale:

$$1 = \{0\}, \quad 2 = \{0, 1\}, \quad 3 = \{0, 1, 2\}, \ldots$$

quindi, con questa notazione, ogni numero contiene tutti i numeri "precedenti", anzi, in questo modo si possono proprio definire i numeri precedenti:

Definizione 6.10. Se $m, n \in \mathbb{N}$, si definisce $m < n$ se $m \in n$ (si scrive $m \leq n$ se $m < n$ o $m = n$).

Vediamo le proprietà della relazione $<$ definita su $\mathbb{N}$.

Teorema 6.11. *La relazione $\in$ ($o <$) di $\mathbb{N}$ è una relazione d'ordine totale, cioè vale*

1. *per ogni $n \in \mathbb{N}$, $n \notin n$ (cioè non vale $n < n$);*
2. *se $m < n$ e $n < p$, allora $m < p$;*
3. *per ogni $m, n \in \mathbb{N}$ o $m < n$, o $m = n$ o $n < m$.*

Dimostrazione. Per provare la transitività della relazione d'ordine (la proprietà (2)), fissiamo m ed n e usiamo induzione su p. Sia

$$A = \{p \in \mathbb{N} \mid \text{se } m < n < p \text{ allora } m < p\}$$

(La notazione $m < n < p$ sta ad indicare $m < n \wedge n < p$). Proviamo che A è induttivo. Ricordiamo che $m < n$ significa che $m \in n$. Innanzitutto $0 \in A$

(perché $m \in n \in 0$ è falso).
Sia ora $p \in A$, vediamo che $p^+ \in A$. Quindi, sapendo che $m \in n \in p \to m \in p$ dobbiamo vedere che se $m \in n \in p^+$, allora $m \in p^+$. Ma $n \in p^+$ significa $n \in p$ o $n \in \{p\}$, cioè, in quest'ultimo caso, $n = p$. Se $n \in p$, abbiamo $m \in n \in p$ e quindi $m \in p$ per ipotesi induttiva, pertanto $m \in p^+$. Se $n = p$, da $m \in n$ otteniamo $m \in p$ e di nuovo $m \in p^+$.
Per quanto riguarda la proprietà (1), si consideri l'insieme $A = \{n \in \mathbb{N} \mid n \notin n\}$. Per induzione si vede facilmente che A è induttivo, cioè $A = \mathbb{N}$.
Infine, anche il punto (3) si può provare per induzione, usando le proprietà di $\in$ stabilite in precedenza. □

Vale:

Teorema 6.12. *Per ogni $m, n \in \mathbb{N}$ si ha:*

1. $0 \neq n^+$;
2. *se $m \in n$ allora $m^+ \in n^+$;*
3. *Se $m^+ = n^+$, allora $m = n$.*

Dimostrazione. Il punto (1) è immediato: se $n^+ = n \cup \{n\} = \emptyset$, allora $n \in \emptyset$, che è assurdo.
Il punto (2) si può provare con l'induzione (v. teorema 6.9), cioè: fissiamo m e consideriamo l'insieme:

$$A = \{n \in \mathbb{N} \mid P(n)\}$$

dove $P(n)$ è la formula seguente: "$m \in n \to m^+ \in n^+$". Vediamo che A è induttivo. Innanzitutto $0 \in A$ (perché $m \in 0$ è falsa, quindi l'implicazione $P(0)$ è vera). Supponiamo ora che valga $P(n)$ e vediamo se vale $P(n^+)$. Assumiamo quindi $m \in n^+$ (e dobbiamo quindi vedere se $m^+ \in n^{++}$). Allora $m \in n \cup \{n\}$, quindi o $m \in n$ (e in questo caso allora, da $P(n)$, si ottieme $m^+ \in n^+$ e quindi $m^+ \in n^{++}$, usando la transitività di $\in$ e il fatto che $n^+ \in n^{++}$) oppure $m = n$ (e in questo caso otteniamo $m^+ = n^+$ e quindi anche ora $m^+ \in n^{++}$).
Il punto (3) dice: $m \cup \{m\} = n \cup \{n\}$. Quindi o $m \in \{n\}$ e allora $m = n$, oppure $m \in n$. Se $m \in n$, allora $m^+ \in n^+$ (per il punto (2)), allora $m^+ \in m^+$ che è contro l'assioma ZF9 (vedi anche esercizio 5). □

Nel 1889 Peano, per identificare i numeri naturali, evidenziò varie proprietà alle quali essi avrebbero dovuto soddisfare. Queste proprietà, che vanno sotto il nome di *assimi di Peano*, sono le seguenti:

Definizione 6.13. Si dice che un insieme X soddisfa gli assiomi di Peano se X contiene un elemento speciale 0_X e su X è definita un'applicazione $S : X \longrightarrow X$ che verifica le seguenti condizioni:

1. S è iniettiva;
2. Per ogni $x \in X$, $0_X \neq S(x)$;

3. per ogni sottoinsieme A di X che contiene 0_X e tale che, se contiene x, contiene anche $S(x)$, vale: $A = X$.

Se prendiamo per 0_X l'elemento 0 di $\mathbb{N}$ (cioè $\emptyset$) e se definiamo $S(n) = n^+$, i risultati precedenti provano che $(\mathbb{N}, 0, S)$ soddisfa agli assiomi di Peano.

Si può dimostrare che se $(X, 0_X, S_X)$ e $(Y, 0_Y, S_Y)$ sono due insiemi che soddisfano gli assiomi di Peano, allora esiste un'applicazione biiettiva $f : X \longrightarrow Y$ tale che $f(0_X) = 0_Y$ e $f(S_X(x)) = S_Y(f(x))$ per ogni $x \in X$. La dimostrazione, che si fa per induzione, non è immediata e viene qui omessa.

Definizione 6.14. Sia $(X, <)$ un insieme totalmente ordinato. Allora l'ordinamento $<$ si dice un *buon ordinamento* se ogni sottoinsieme non vuoto di X ammette minimo (cioè se per ogni $B \subseteq X$, $B \neq \emptyset$, esiste un $m \in B$ tale che $m \leq n$ per ogni $n \in B$).

Teorema 6.15. *L'insieme $\mathbb{N}$ con la relazione d'ordine data da $\in$ è un insieme bene ordinato.*

Dimostrazione. Sia $B \subseteq \mathbb{N}$, $B \neq \emptyset$. Supponiamo che B non abbia minimo. Definiamo il seguente sottoinsieme di $\mathbb{N}$:

$$A = \{n \in \mathbb{N} \mid m \notin B \text{ per ogni } m \leq n\}$$

Partendo dall'ipotesi che B non ha minimo, proviamo per induzione che A è induttivo e quindi coincide con $\mathbb{N}$. Innanzitutto si vede facilmente che $0 \in A$, infatti se 0 stesse in B sarebbe ovviamente il minimo di B. Sia ora $n \in A$ e vediamo che $n^+ \in A$. Se $n \in A$, allora, se $m \leq n$, $m \notin B$. Per provare che $n^+ \in A$ basta vedere che $n^+ \notin B$ (infatti, se $m \leq n^+$ allora o $m \leq n$, e allora, per induzione, $m \notin B$ oppure $m = n^+$, se riusciamo a vedere che $n^+ \notin B$, abbiamo che se, $m \leq n^+$ allora $m \notin B$ e quindi $n^+ \in A$). Supponiamo quindi che $n^+ \in B$. Poiché se $m < n^+$, $m \notin B$, avremmo che n^+ sarebbe il minimo di B, contro l'ipotesi da cui siamo partiti. Quindi $n^+ \in A$. Allora $A = \mathbb{N}$ e questo comporta che $B = \emptyset$, contro l'ipotesi. □

Come ben noto, due numeri naturali si possono sommare e moltiplicare tra loro. Vediamo come si può introdurre l'operazione di somma. Il modo in cui si definisce è del tutto intuitivo, ma la dimostrazione rigorosa richiede del lavoro.

Teorema 6.16. *Esiste un'applicazione $A : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ che soddisfa alle seguenti condizioni:*

1. *$A(\langle n, 0\rangle) = n$ per ogni $n \in \mathbb{N}$;*
2. *$A(\langle n, k^+\rangle) = (A(\langle n, k\rangle))^+$ per ogni $n, k \in \mathbb{N}$.*

L'applicazione A ci servirà per definire la somma (ponendo $n+k = A(\langle n, k\rangle)$) e quindi il significato dell'applicazione A dovrebbe essere chiaro: afferma che $n + 0 = n$ e $n + (k + 1) = (n + k) + 1$.

Dimostrazione. (Cenno). Fissiamo $m \in \mathbb{N}$. Definiamo la funzione:

$$A_m : \mathbb{N} \times \{m\} \longrightarrow \mathbb{N}$$

nel seguente modo: se $m = 0$, $A_0(\langle n, 0\rangle) = n$ e, $A_{m^+} = (\langle n, m\rangle)^+$, quindi possiamo dire che A_0 è il sottoinsieme di $\mathbb{N} \times \{0\} \times \mathbb{N}$ dato da $A_0 = \{\langle\langle n, 0\rangle, n\rangle \mid n \in \mathbb{N}\}$ e A_{m^+} è un analogo sottoinsieme di $\mathbb{N} \times \{m^+\} \times \mathbb{N}$, dato da: $A_{m^+} = \{\langle\langle n, m^+\rangle, (A_m(n, m))^+\rangle \mid n \in \mathbb{N}\}$. Pertanto, per ogni $m \in \mathbb{N}$ è definita A_m. Consideriamo allora l'insieme $U = \{A_m \mid m \in \mathbb{N}\}$ e quindi l'insieme $A = \cup U$. Si vede che A è un'applicazione $\mathbb{N}\times\mathbb{N} \longrightarrow \mathbb{N}$ che soddisfa le condizioni richieste. □

Si definisce quindi la somma in $\mathbb{N}$ data da $m + n = A(m, n)$.

Esempio 6.17. Vediamo di calcolare $2 + 3$ usando la definizione e pertanto la funzione A definita nel precedente teorema. Vale:

$$\begin{aligned} 2+3 &= A_3(2,3) \\ &= (A_2(2,2))^+ \\ &= ((A_1(2,1))^+)^+ \\ &= (((A_0(2,0)^+)^+)^+ \\ &= ((2^+)^+)^+ \\ &= (3^+)^+ \\ &= 4^+ \\ &= 5 \end{aligned}$$

Vediamo ora di calcolare $3 + 2$, sempre seguendo la definizione:

$$\begin{aligned} 3+2 &= A_2(3,2) \\ &= (A_1(3,1))^+ \\ &= ((A_0(3,0))^+)^+ \\ &= (3^+)^+ \\ &= 4^+ \\ &= 5 \end{aligned}$$

Per quanto riguarda il prodotto, si può procedere in modo analogo. Si definisce un'applicazione $M : \mathbb{N}\times\mathbb{N} \longrightarrow \mathbb{N}$ usando le seguenti condizioni: $M(n, 0) = 0$, $M(n, m^+) = M(n, m) + m$. Si può dimostrare che la somma e il prodotto sono associativi e commutativi e che vale la legge di distributività della somma con il prodotto. Lo strumento principale per ottenere questi risultati anche in questo caso è, come è lecito aspettarsi, l'induzione. Analogamente si possono verificare le note relazioni che legano la relazione d'ordine con la somma e il prodotto (cioè, per ogni $a, m, n \in \mathbb{N}$ vale: se $m < n$ allora $a + m < a + n$; se $a > 0$ e se $m < n$, allora $am < an$).

Esercizio 5. Provare che vale:

1. Per ogni $n \in \mathbb{N}$, risulta $n \notin n$;

2. Sia $n \in \mathbb{N}$, con $n \neq 0$. Allora esiste un $m \in \mathbb{N}$ tale che $n = m^+$;

3. Sia $n \in \mathbb{N}$, $n \neq 0$. Allora $0 \in n$.

4. Per ogni $n \in \mathbb{N}$ tra n e n^+ non ci sono altri elementi.

Soluzioni. Il punto (1) si può fare per induzione su n. Se $n = 0$ è chiaro. Sia vero per n, vediamo che vale per n^+. Supponiamo che $n^+ \in n^+$. Essendo $n^+ = n \cup \{n\}$, si ha $n^+ \in n$ o $n = n^+$. Per come è definito n^+, vale sempre $n \in n^+$, allora, per transitività, $n \in n$, contro l'ipotesi induttiva. Se invece $n^+ = n$, poichè, nuovamente, $n \in n^+$, abbiamo che $n \in n$ di nuovo contro l'ipotesi induttiva.
Il punto (2) si prova anche per induzione. Sia $A = \{n \in \mathbb{N} \mid n = 0 \vee \exists m \in \mathbb{N}(n = m^+\}$. Chiaramente $0 \in A$ e, se $n \in A$, allora consideriamo n^+, esso sta in A perché basta prendere $m = n$.
Il punto (3) si vede ancora per induzione, provando che l'insieme $A = \{n \in \mathbb{N} \mid n = 0 \vee 0 \in n\}$ coincide con $\mathbb{N}$.
Il punto (4) si pulò vedere in questo modo: Sia $u \in \mathbb{N}$ tale che $n < u < n^+$. Allora $u \in n \cup \{n\}$. Quindi $u \in n$ o $u \in \{n\}$. Se $u \in n$, allora $u < n$, assurdo, se $u \in \{n\}$, allora $u = n$, anche assurdo.

6.2 Insiemi finiti

Ricordiamo che l'insieme $\mathbb{N}$ dei numeri naturali ha per elementi gli insiemi:

$$0 = \emptyset, \quad 1 = \{0\}, \quad 2 = \{0, 1\}, \quad 3 = \{0, 1, 2\}, \ldots$$

e si noti che 0 ha zero elementi, 1 ha un elemento, 2 ha due elementi, ecc., allora questa constatazione si può estendere con la seguente:

Definizione 6.18. Diremo che un insieme X ha n elementi se esiste una biiezione tra l'insieme n e l'insieme X. In questo caso si dice che X è un insieme *finito*. Se un insieme non è finito, si dice *infinito*.

Se invece la biiezione che si trova per un insieme X è con tutto $\mathbb{N}$, allora:

Definizione 6.19. Se X è un insieme per cui c'è una biiezione $f : \mathbb{N} \longrightarrow X$, allora X si dice che è *infinito numerabile*.

Naturalmente un insieme infinito numerabile (e in particolare $\mathbb{N}$) dovrebbe risultare infinito. Vedremo a breve che infatti le cose stanno proprio così. Necessitiamo del seguente risultato:

Teorema 6.20. *Per ogni $n \in \mathbb{N}$, se $f : n \longrightarrow n$ è iniettiva, allora f è suriettiva.*

Dimostrazione. La dimostrazione si fa per induzione su n. Per $n = 0$ (o $n = 1 = \{0\}$) il risultato è immediato. Assumiamo il risultato vero per n e proviamo che è vero per n^+. Sia $f : n^+ \longrightarrow n^+$ iniettiva. Ricordiamo che $n^+ = n \cup \{n\}$ e quindi uno degli elementi nel dominio di f è n. Consideriamo quindi $f(n)$ e distinguiamo due casi: $f(n) = n$ o $f(n) \in n$. Nel primo caso, per ogni $x \in n^+$, $x \neq n$ l'immagine $f(x)$ non può essere n perché f è iniettiva e già $f(n)$ vale n, quindi la restrizione di f al sottoinsieme n di n^+ dà una funzione $g : n \longrightarrow n$ che è iniettiva e quindi anche suriettiva, per ipotesi induttiva. Quindi anche f è suriettiva. Nel secondo caso (se $f(n) \neq n$) sia allora $f(n) = i$ con $i \in n$. Consideriamo l'elemento $n \in n^+$ nel codominio di f. Se tale n non fosse nell'immagine di f, allora essa sarebbe tutta contenuta in n e quindi la restrizione di f al dominio n sarebbe un'applicazione iniettiva (al pari di f) da n in sè. Allora, per induzione, sarebbe anche suriettiva e quindi ci sarebbe un $j \in n$ tale che $f(j) = i$. Ma questo contraddice l'iniettività di f perché avremmo $j \neq n$ e $f(j) = f(n)$. Pertanto esiste un $k \in n$ tale che $f(k) = n$. Definiamo un'applicazione $g : n \longrightarrow n$ data da: $g(k) = i$ e $g(h) = f(h)$ se $h \neq k$. L'immagine di g è contenuta in n e g è iniettiva. Quindi, per induzione, è suriettiva. Dalla suriettività di g segue subito anche la suriettività di f. □

Corollario 6.21. *Se X è un insieme finito e se $f : X \longrightarrow X$ è iniettiva, allora f è anche suriettiva.*

Dimostrazione. Se X è finito, sia $h : n \longrightarrow X$ biiettiva. Allora abbiamo che l'applicazione $n \longrightarrow n$ data da $h^{-1} \circ f \circ h$ è un'applicazione iniettiva da n in sè, quindi anche suriettiva, pertanto f è suriettiva. □

Corollario 6.22. *Se X è un insieme finito e se $f : X \longrightarrow X$ è suriettiva, allora f è anche iniettiva.*

Dimostrazione. Poiché f è suriettiva, per ogni y del codominio X di f esiste un x nel dominio tale che $f(x) = y$. Allora possiamo definire un'applicazione $g : X \longrightarrow X$ tale che $g(y) = x$ con x tale che $f(x) = y$. Pertanto $f(g(y)) = y$ e quindi g è un inversa destra di f, allora f è un'inversa sinistra di g e quindi g è iniettiva e allora anche suriettiva e quindi biiettiva. Allora anche f è biiettiva. □

Corollario 6.23. *Siano $m, n \in \mathbb{N}$, con $m \neq n$. Allora non ci può essere una biiezione tra m e n.*

Dimostrazione. Supponiamo che sia $m < n$ e consideriamo una biiezione $f : n \longrightarrow m$. Sia g la restrizione di f a $m \subseteq n$. Quindi $g : m \longrightarrow m$ è iniettiva e quindi, per il teorema precedente, anche suriettiva. Sia $k \in n \setminus m$. Allora $f(k)$ è un elemento di m e quindi esiste $h \in m$ tale che $g(h) = f(k)$, ma $g(h) = f(h)$ e questo contraddice l'iniettività di f. □

Possiamo ora provare un risultato che spesso viene detto il *principio della piccionaia* (riferendosi al fatto che se abbiamo una piccionaia con n fori e se ci sono più di n piccioni che vanno ad occuparla, ci sarà almeno un foro in cui ci sono almeno due piccioni).

Corollario 6.24. *Sia A un insieme finito, sia B un sottoinsieme proprio di A e $f : A \longrightarrow B$ un'applicazione. Allora esistono almeno due elementi di A che sono mandati da f nello stesso elemento di B.*

Dimostrazione. Se non ci fossero due elementi di A mandati nello stesso elemento di B da f, allora f sarebbe iniettiva e quindi la restrizione di f a B sarebbe inietiva e quindi suriettiva. Preso $a \in A \setminus B$, consideriamo $f(a) \in B$, pertanto esiste un $b \in B$ tale che $f(b) = f(a)$ e in questo modo otteniamo una contraddizione. □

Corollario 6.25. *Sia n un numero naturale. Allora non ci può essere una biiezione tra n e $\mathbb{N}$.*

Dimostrazione. Sia $f : \mathbb{N} \longrightarrow n$ una biiezione. Consideriamo la restrizione di f ad n. È un'applicazione iniettiva da n in sè, quindi anche suriettiva. Ma se prendiamo $k \in \mathbb{N}$, $k \notin n$, anche $f(k) \in n$ e quindi f non può essere iniettiva. □

L'immediata conseguenza del precedente corollario è che $\mathbb{N}$ non può essere un insieme finito, quindi l'insieme dei numeri naturali, come c'era da aspettarsi, è un insieme infinito.

Si osservi ancora che si può vedere che $\mathbb{N}$ non è un insieme finito perché è facile trovare applicazioni iniettive da $\mathbb{N}$ in sè che non sono suriettive. Un facile esempio è dato dall'applicazione $f : \mathbb{N} \longrightarrow \mathbb{N}$ tale che $f(n) = 2n$.

7 Lezione 6

Nelle precedenti lezioni abbiamo visto gli assiomi di Zermelo Fraenkel che permettono di definire in modo rigoroso la teoria degli insiemi, da essi abbiamo poi visto come si può definire l'insieme $\mathbb{N}$ dei numeri naturali e le sue proprietà (l'ordinamento, l'operazione di somma e di prodotto). Una volta introdotti i numeri naturali, si possono costruire gli altri insiemi di numeri. La costruzione di $\mathbb{Z}$ è ben nota: l'idea da cui si parte è che un numero intero può sempre esser visto come la differenza di due numeri naturali, in molti modi differenti (ad esempio $-2 = 3 - 5 = 4 - 6 = 10 - 12 = \ldots$ oppure $4 = 5 - 1 = 7 - 3 = \ldots$) Due coppie (m, n) e (m', n') di numeri naturali individuano lo stesso intero se $m - n = m' - n'$, ma per dare un senso a questa differenza bisogna già disporre dei numeri interi, però essa è equivalente alla relazione $m + n' = m' + n$ che invece si può sempre considerare in $\mathbb{N}$. Allora la costruzione degli interi viene fatta considerando le coppie ordinate (m, n) con $m, n \in \mathbb{N}$ e definendo una relazione di equivalenza su queste coppie: $(m, n) \sim (m', n')$ se $m + n' = m' + n$. L'insieme $\mathbb{Z}$ dei numeri interi altro non è che l'insieme delle classi $[(m, n)]$. Le operazioni su $\mathbb{Z}$ possono essere facilmente definite a partire dalle operazioni di $\mathbb{N}$, $([(m, n)] + [(p, q)] = [(m + p, n + q)]$ e $[(m, n)] \cdot [(p, q)] = [(mp + nq, mq + np)])$ così come l'ordinamento. Per quest'ultimo si pone $[(m, n)] < [(m', n')]$ se $m + n' < m' + n$ in $\mathbb{N}$. In questo modo $\mathbb{Z}$ diventa un anello commutativo, unitario e con un ordinamento totale. Inoltre l'ordinamento totale soddisfa ad alcune proprietà:

Teorema 7.1. *Sia $\mathbb{Z}$ l'anello degli interi con la relazione d'ordine sopra definita. Allora vale:*

- *Per ogni $a, b, c \in \mathbb{Z}$, se $a < b$ allora $a + c < b + c$;*
- *Per ogni $a, b \in \mathbb{Z}$ e per ogni $c \in \mathbb{Z}$, $c > 0$, se $a < b$ allora $ac < bc$.*

Vediamo quindi che $\mathbb{Z}$ diventa un anello con una relazione d'ordine totale soggetta a opportune relazioni di compatibilità con la sua struttura algebrica.

7.1 Il campo $\mathbb{Q}$ dei razionali

La costruzione di $\mathbb{Q}$ si può fare con un procedimento molto simile a quello utilizzato per costruire $\mathbb{Z}$ a partire da $\mathbb{N}$. La costruzione è più generale e permette di costruire, a partire da un dominio d'integrità A il *campo dei quozienti* $Q(A)$. Accenniamo velocemente al procedimento che si segue.
Si considera l'insieme prodotto $B = A \times (A \setminus \{0\})$, cioè l'insieme delle coppie (a, b) con $a, b \in A$ e $b \neq 0$. Si definisce una relazione di equivalenza su B data da: $(a, b) \sim (a', b')$ se $ab' = a'b$ e sull'insieme quoziente $B/\sim$ (i cui elementi si indicano con la notazione $[(a, b)]$ o, meglio, con a/b) si definisce una struttura di anello ponendo $a/b + c/d = (ad + bc)/bd$ e $a/b \cdot c/d = ac/bd$. Si vede che $B/\sim$ diventa un campo che contiene (una copia isomorfa di) A.

Anche i numeri razionali o i numeri reali (che dobbiamo ancora definire) hanno una relazione d'ordine totale compatibile con le operazioni di somma e prodotto, quindi conviene trattare l'argomento in modo più generale.

7.2 Anelli ordinati

Sia A un anello (che assumeremo commutativo e unitario).

Definizione 7.2. L'anello A si dice *ordinato* se esiste un sottoinsieme $P \subseteq A$ tale che

- $0 \notin P$;
- Per ogni $a \in A$, $a \neq 0$ vale una e una sola delle condizioni: $a \in P$ o $-ainP$;
- P è chiuso per prodotti e per somme.

È chiaro che $P \neq \emptyset$ in quanto, per la seconda condizione scritta sopra, o 1 o -1 deve stare in P. Si pone poi $N = \{a \in A \mid -a \in P\}$. Gli elementi di P si dicono *positivi*, gli elementi di N si dicono negativi. È chiaro che vale $A = P \cup \{0\} \cup N$ e $P, N, \{0\}$ fanno una partizione di A.

Se A è un anello ordinato, si definisce una relazione $<$ in A data da: $a < b$ se $b - a \in P$ (ovviamente $a > b$ significa che $b < a$). Si vede subito che $a \in P$ se e solo se $a > 0$ e $a \in N$ se e solo se $a < 0$ e inoltre $a > 0$ se e solo se $-a < 0$.
Vale:

Teorema 7.3. *Sia (A, P) un anello ordinato, allora la relazione $<$ è una relazione d'ordine totale, tale che*

- *per ogni $a, b, c \in A$, se $a < b$, allora $a + c < b + c$;*
- *per ogni $a, b, c \in A$ con $c > 0$, se $a < b$, allora $ac < bc$.*

Dimostrazione. Il fatto che $<$ sia una relazione d'ordine totale segue subito dalle proprietà di P. Se $a < b$ allora $b - a \in P$, quindi $(b + c) - (a + c) \in P$ e pertanto $a + c < b + c$, se $a < b$ e $c > 0$, $b - a, c \in P$, allora il loro prodotto è in P e quindi $ac < bc$. □

Si può facilmente verificare anche il viceversa, cioè:

Teorema 7.4. *Se in un anello A è definita una relazione d'ordine totale $<$ tale che soddisfi alle due condizioni del teorema 7.3, allora, posto $P = \{a \in A \mid a > 0\}$, (A, P) è un anello ordinato.*

La dimostrazione è lasciata per esercizio.

Esempio 7.5. Una conseguenza del teorema 7.1 è che l'anello $\mathbb{Z}$ è un anello ordinato secondo la definizione 7.2.
Analogamente, gli anelli (campi) $\mathbb{Q}$ o $\mathbb{R}$ ($\mathbb{R}$ verrà approfondito nel seguito) sono

altri esempi di anelli ordinati.
Se $A = \mathbb{Q}[x]$ è l'anello dei polinomi, può essere reso un anello ordinato, ponendo, per ogni $f \neq 0$, $f > 0$ se $\mathrm{LC}(f) > 0$ (con $\mathrm{LC}(f)$ si intende il coefficiente direttivo di f, cioè il coefficiente del monomio di grado massimo di f).
L'anello (campo) $\mathbb{C}$ dei numeri complessi non può essere dotato di struttura di anello ordinato (conseguenza del fatto che, come viene evidenziato nel prossimo elenco di proprietà degli anelli ordinati, ogni quadrato di un elemento non nullo è positivo).

Dato un anello ordinato, si verificano facilmente le seguenti proprietà:

1. Se $a > b$, allora $-b > -a$;
2. Se $a > b$ e $c > d$, allora $a + c > b + d$;
3. Se $a > b$ e $c > 0$, allora $ac > bc$;
4. Se $a > b$ e $c < 0$, allora $bc > ac$;
5. Se $a > 0$ e $b < 0$, allora $ab < 0$;
6. Se $a < 0$ e $b < 0$, allora $ab > 0$;
7. Se $a \neq 0$, allora $a^2 > 0$ (in particolare, $1 > 0$);
8. Se $a > 0$ e $0 < m < n$ con $m, n \in \mathbb{N}$, allora $ma < na$ (si ricordi che ma significa $a + a + \cdots + a$ m–volte).

Si verifica facilmente che:

Proposizione 7.6. *Un anello ordinato è un dominio d'integrità di caratteristica* 0.

Se A è un anello ordinato e $B \subseteq A$ è un sottoanello di A, allora si può definire su B una struttura di anello ordinato ponendo $b_1 < b_2$ in B se $b_1 < b_2$ in A (equivalentemente, se l'insieme degli elementi positivi di B è dato da $B \cap P$, dove P è l'insieme degli elementi postivi di A).

Esercizio 6. Provare che se A e B sono due anelli (anche non ordinati), allora non può esistere nessuna relazione d'ordine totale sull'anello prodotto $A \times B$ che lo renda anello ordinato.

Se (A, P) e (A', P') sono due anelli ordinati, allora un isomorfismo di anelli $f : A \longrightarrow A'$ si dice *isomorfismo di anelli ordinati* se $f(P) \subseteq P'$. Si verifica che se $f(P) \subseteq P'$, allora $f(P) = P'$ (infatti, se $p' \in P'$, sia $p \in P$ tale che $f(p) = p'$; se $p \notin P$, allora $-p \in P$ e quindi $f(-p) = -f(p) = -p' \in P'$ e si avrebbe così una contraddizione).

Dalla precedente proposizione, abbiamo che un anello ordinato contiene sempre (una copia isomorfa di) $\mathbb{Z}$ come anello ordinato.

La definizione di valore assoluto, data usualmente per i numeri reali, si può riproporre in un qualunque anello ordinato:

Definizione 7.7. Sia A un anello ordinato e sia $a \in A$. Allora si pone $|a|$ (*valore assoluto* di a) l'elemento di A dato da a se $a \geq 0$, o da $-a$ se $a < 0$.

Anche in un anello ordinato A valgono le note proprietà del valore assoluto, cioè:

Proposizione 7.8. *Se A è un anello ordinato allora, per ogni $a, b \in A$, si ha:*

1. *Se $b > 0$ allora $|a| < b$ equivale $a - b < a < b$;*
2. $|a \cdot b| = |a| \cdot |b|$;
3. $|a + b| \leq |a| + |b|$;
4. $| \, |a| - |b| \, | \leq |a \pm b| \leq |a| + |b|$.

Dimostrazione. Il primo caso si vede facilmente: se $|a| \leq b$ e $a \geq 0$, allora $a \leq b$. Inoltre, essendo $-b < 0$, avremo $-b < 0 \leq a < b$, analogamente se $a < 0$. Viceversa, se $-b < a < b$ e se $a \geq 0$, allora $|a| < b$, se $a < 0$, essendo $-b < a$ otteniamo $-a < b$ e quindi anche ora $|a| < b$. Il secondo e il terzo caso sono immediati, basta trattare separatamente tutte le possibilità (a positivo, nullo o negativo, b positivo, nullo o negativo).
Vediamo il quarto caso: se nel terzo caso si sostituisce b con $-b$ si ottine: $|a - b| \leq |a| + |b|$, quindi abbiamo $|a \pm b| \leq |a| + |b|$. Se, sempre nel terzo caso, scriviamo $a - b$ al posto di a, si ottiene $|a| \leq |a - b| + |b|$, cioè $|a| - |b| \leq |a - b|$; scambiano in quest'ultima espressione a con b si ha $|b| - |a| \leq |a - b|$, quindi, usando il primo punto, $| \, |a| - |b| \, | \leq |a - b|$. La tesi allora segue facilmente sostituendo, in quest'ultima espressione, $-b$ al posto di b. □

Definizione 7.9. Un anello ordinato A si dice *archimedeo* se vale la seguente condizione: per ogni $a, b \in A$ con $a > 0$, $b > 0$ esiste un $n \in \mathbb{N}$ tale che $na > b$.

Esempio 7.10. Gli anelli $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ sono anelli ordinati archimedei.
L'anello ordinato $\mathbb{Q}[x]$ introdotto nell'esempio 7.5, invece, non è archimedeo.

Se un anello ordinato è anche un campo, si chiama (ovviamente) campo ordinato. In un campo ordinato valgono naturalmente tutte le proprietà degli anelli ordinati a cui se ne aggiungono altre due:

Proposizione 7.11. *Se a è un elemento non nullo di un un campo ordinato, allora a e a^{-1} sono "dello stesso segno" (cioè entrambi positivi o entrambi negativi). Inoltre, se in un campo ordinato vale $a > b > 0$, allora $b^{-1} > a^{-1} > 0$.*

Dimostrazione. Se $a > 0$ e se fosse $a^{-1} < 0$, si avrebbe $-a^{-1} > 0$ e quindi $-1 > 0$, cioè $1 < 0$, che è assurdo. Da $a > b > 0$, moltiplicando per $(ab)^{-1}$, si ottiene $b^{-1} > a^{-1} > 0$. □

Osservazione 7.12. Si osservi che, se A è un campo ordinato, la condizione di essere archimedeo si vede facilmente che equivale alla condizione:

- Per ogni $\varepsilon \in A$, $\varepsilon > 0$ esiste un $n \in \mathbb{N}, n \neq 0$, tale che $1/n < \varepsilon$

(ovviamente, $1/n$ significa l'inverso in A di $1+1+\cdots+1$ (somma fatta n volte)).

Un anello ordinato si dice *denso in sè* se, per ogni $a, b \in A$ con $a < b$ esiste un $c \in A$ tale che $a < c < b$ (quindi tra a e b sono compresi infiniti elementi). Ad esempio, l'anello $\mathbb{Z}$ non è denso in sè (si veda l'esercizio 5, punto (4)).

Proposizione 7.13. *Sia K un campo ordinato. Allora K è denso in sè.*

Dimostrazione. Sia 1 l'unità di K. Si verifica subito che l'elemento $c = (2 \cdot 1)^{-1}(a + b)$ è compreso tra a e b. □

Per il prossimo risultato, si suppone che sia nota la costruzione del campo dei quozienti di un dominio d'integrità, accennata all'inizio della sezione.

Teorema 7.14. *Sia A un anello ordinato (e quindi un dominio d'integrità) e sia Q il campo dei quozienti di A. Allora l'ordinamento di A può essere prolungato, in unico modo, ad un ordinamento su Q.*

Dimostrazione. Sia a/b un elemento di Q (con $b \neq 0$). Consideriamo b^2 che è necessariamente positivo (in A e in Q). Supponiamo di avere un ordinamento in Q per cui a/b sia positivo. Allora $a/b \cdot b^2 > 0$ e quindi $ab > 0$ (analogamente, se $a/b < 0$, allora $ab < 0$). Quindi il segno di a/b è deciso dal segno dell'elemento ab (che sta in A). Quindi, se si può prolungare l'ordinamento di A su Q, si può fare in unico modo. Poniamo allora $a/b > 0$ se e solo se $ab > 0$. Questa definizione è indipendente dalla scelta che rappresenta a/b, perchè, se $a/b = c/d$, allora $ad = bc$, da cui, moltiplicando per ac, si ottiene $a^2cd = abc^2$ e, siccome a^2 e c^2 sono positivi, ab e cd devono avere lo stesso segno. Vediamo se dunque, definendo $a/b > 0$ se e solo se $ab > 0$, troviamo un ordinamento che estende l'ordinamento di A e rende Q un anello ordinato. Se $a \in A$ è positivo in A, allora $a = a^2/a$ è positivo anche in Q e quindi l'ordinamento di Q estende quello di A. Se $a/b > 0$ e $c/d > 0$, si vede facilmente che $a/b + c/d = (ad + bc)/bc$ è positivo (perchè $(ad + bc)(bc)$ è positivo), così come è pure positivo $a/b \cdot c/d$. □

In base alle proprietà degli anelli ordinati, possiamo vedere che l'ordinamento che abbiamo definito su $\mathbb{Z}$ (conseguenza dell'ordinamento definito su $\mathbb{N}$, v. teorema 6.11) è l'unico possibile volendo ottenere un anello ordinato (infatti si è stabilito che in un qualunque ordinamento, deve essere $1 > 0$ pertanto $1 + 1 = 2$ deve essere anche positivo e quindi, in qualunque ordinamento, tutti i numeri naturali non nulli devono essere positivi). L'ordinamento di $\mathbb{Z}$ si estende poi in unico modo nell'ordinamento su $\mathbb{Q}$ (che è il campo dei quozienti di $\mathbb{Z}$) e pertanto anche $\mathbb{Q}$ ha un'unica struttura di campo ordinato.

Dal fatto che ogni dominio d'integrità di caratteristica zero contiene (una copia isomorfa di) $\mathbb{Z}$, si ottiene facilmente che ogni anello ordinato contiene, come sottoanello ordinato, l'anello degli interi. Analogamente, ogni campo ordinato contiene (una copia isomorfa) del campo ordinato $\mathbb{Q}$. In particolare $\mathbb{Z}$ è il più piccolo anello ordinato, mentre $\mathbb{Q}$ è il più piccolo campo ordinato.

$q_<$	$q_>$	$q_<^2$	$q_>^2$
1	2	1	4
1.4	1.5	1.96	2.25
1.41	1.42	1.9881	2.0164
1.414	1.415	1.999396	2.002225
1.4142	1.4143	1.99996164	2.00024449
1.41421	1.41422	1.9999899241	2.0000182084
1.414213	1.414214	1.999998409369	2.000001237796
1.4142135	1.4142136	1.99999982358225	2.00000010642496
...	...	...	...

Tabella 1: Approssimazioni della soluzione positiva dell'equazione $x^2 - 2 = 0$.

8 Costruzione dei numeri reali

Iniziamo ora ad esporre vari approcci per la costruzione dei numeri reali. Il fatto che i numeri razionali non fossero sufficienti per rappresentare le misure dei segmenti che si ottengono con costruzioni geometriche, era noto già nell'antichità. I primi esempi sono la misura della diagonale di un quadrato di lato 1 (o, se si preferisce, il rapporto tra la diagonale di un quadrato e il suo lato) o il rapporto tra la diagonale e il lato di un pentagono.

In queste lezioni vogliamo vedere come, a partire dai numeri razionali, si possa costruire l'insieme (il campo) dei numeri reali. Vi sono molte costruzioni diverse tra loro, noi ne analizzeremo alcune. C'è da notare che, come vedremo, il campo dei numeri reali che si viene a costruire è unico (a meno di isomorfismi), quindi qualunque strada si scelga, alla fine il risultato sarà sempre lo stesso.

La prima osservazione che facciamo è che il campo $\mathbb{Q}$ è, come si è visto, un campo ordinato, quindi in $\mathbb{Q}$ ci sono due operazioni (somma e prodotto) che soddisfano agli assiomi di campo e c'è poi una relazione d'ordine totale per la quale valgono le condizioni del teorema 7.3. Nonostante la ricchezza della struttura di $\mathbb{Q}$, ci si accorge però che esso non è sufficiente a rappresentare tutti i numeri di cui necessitiamo quando ad esempio consideriamo le soluzioni di equazioni come $x^2-2=0$ o $x^3-5=0$. Se in particolare cerchiamo una soluzione positiva di $x^2 - 2 = 0$ (che, si vede, non può essere un numero razionale), procedendo per tentativi, ci accorgiamo che, se c'è una soluzione, dovrebbe essere compresa tra i numeri razionali 1.4 e 1.5 (perché $1.4^2 = 1.96$ e $1.5^2 = 2.25$) o tra i numeri razionali 1.41 e 1.42 (perché $1.41^2 = 1.9981$ e $1.42 = 2.0164$) e così via e possiamo quindi costruire una tabella come la tabella 1, dove $q_<$ indica un numero razionale il cui quadrato è minore di 2, mentre $q_>$ indica un numero razionale il cui quadrato è maggiore di 2. Come si vede, con una tabella come questa si riesce a "racchiudere" il numero irrazionale $\sqrt{2}$ (ammesso esista) tra numeri razionali ($q_<$ e $q_>$). Si noti che, se i numeri reali effettivamente esistono e sono un campo ordinato che estende $\mathbb{Q}$, allora necessariamente, se $q_<^2 < 2$, deve accadere che $q_<$ è minore di $\sqrt{2}$ e analogamente, se $q_>^2 > 2$, allora $q_>$ deve essere maggiore di $\sqrt{2}$, infatti abbiamo visto che in un campo ordinato, se a, b

sono positivi e $a < b$, allora $a^2 < b^2$.

Possiamo quindi concludere questa introduzione con una (banale) osservazione: i numeri razionali sembrano suggerire l'esistenza anche di altri numeri anche se non stanno in $\mathbb{Q}$.

La prima costruzione dei numeri reali che presentiamo fa riferimento ad un lavoro di Cantor.

8.1 Ampliamenti cantoriani

In questo paragrafo tratteremo il problema da un punto di vista piuttosto generale, lavorando quindi con un campo ordinato K invece che con il particolare campo $\mathbb{Q}$.

Avremo bisogno di alcune nozioni di base sulle successioni numeriche che sicuramente sono note. Le riprendiamo brevemente in un ambito generale.

Sia K un campo ordinato (si pensi, come esempio, al campo $\mathbb{Q}$ dei numeri razionali). Una successione di K è, per definizione, un'applicazione $a : \mathbb{N} \longrightarrow K$. Una successione si indica anche con $(a_0, a_1, a_2, \ldots)$ o con $(a_n)_{n\in\mathbb{N}}$ o, semplicemente, con $(a_n)_n$. Tutte le nozioni che sono state date per le successioni di numeri reali in un corso di analisi si possono ripetere per i campi ordinati. Passiamole velocemente in rassegna:
Una successione $(a_n)_n$ si dice che ha limite $l \in K$ (o che converge ad $l \in K$) se vale:
Per ogni $\varepsilon \in K,\ \varepsilon > 0$ esiste un $n_\varepsilon \in \mathbb{N}$ tale che $|a_n - l| < \varepsilon$ per ogni $n > n_\varepsilon$.

Abbiamo quindi ripetuto la ben nota definizione, ma adattata ad un campo ordinato qualunque.

Se una successione $(a_n)_n$ ha per limite 0, si dice *infinitesima*. Per le successioni su un campo ordinato K valgono risultati analoghi a quelli visti per le successioni di numeri reali, in particolare si può dimostrare esattamente come nel caso dei numeri reali (utilizzando le disuguaglianze introdotte nella proposizione 7.8), che vale:

- Unicità del limite;
- l'operazione di limite commuta con l'operazione di somma e prodotto di successioni;
- una successione $(a_n)_n$ convergente, è limitata (cioè esiste un $r \in K$ tale che $|a_n| < r$ per ogni $n \in \mathbb{N}$).

Una nozione fondamentale per la costruzione che intendiamo esporre è la nozione di successione di Cauchy, che per comodità ripetiamo:

Definizione 8.1. Sia $(a_n)_n$ una successione nel campo ordinato K. Essa si dice di Cauchy se per ogni $\varepsilon \in K,\ \varepsilon > 0$ esiste un $n_\varepsilon \in \mathbb{N}$ tale che $|a_m - a_n| < \varepsilon$ per ogni $m, n > n_\varepsilon$.

Si dimostra facilmente che una successione convergente è anche di Cauchy (la dimostrazione è un'applicazione della disuguaglianza triangolare, cfr. proposizione 7.8). Si può poi dimostrare che, *nel campo dei numeri reali*, una

successione di Cauchy è anche convergente. È proprio questo risultato che può essere usato per costruire i numeri reali. L'idea che si segue è la seguente: dato un numero reale (ad esempio $\sqrt{2}$) si può trovare una successione a coefficienti razionali che converge verso quel numero reale ed è quindi di Cauchy (nell'esempio scritto sopra, è ragionevole attendersi che sia la successione fatta dai numeri razionali contenuti nelle righe della colonna $q_<$ sia l'altra successione, ottenuta dalle righe della colonna $q_>$, convergono a $\sqrt{2}$). Viceversa, data una successione che è costituita da elementi razionali e che è di Cauchy, deve convergere in $\mathbb{R}$, quindi individua un numero reale. Allora abbiamo che ogni successione di Cauchy in $\mathbb{Q}$ individua un numero reale r e, viceversa, dato un numero reale r, se troviamo una successione a coefficienti in $\mathbb{Q}$ che converge verso r, allora abbiamo una successione di Cauchy in $\mathbb{Q}$ che individua r. A prima vista si potrebbe dire che vi è quindi una corrispondenza biunivoca tra numeri reali e successioni di Cauchy in $\mathbb{Q}$. Se così fosse, potremmo definire i numeri reali proprio come successioni di Cauchy a coefficienti in $\mathbb{Q}$. In realtà le cose sono un po' più complesse, perché la corrisponenza non è biunivoca: ci sono molte successioni di Cauchy che convergono allo stesso numero r. Però si può rimediare: se diciamo che due successioni di Cauchy in $\mathbb{Q}$ sono equivalenti se convergono allo stesso numero reale, potremmo quozientare l'insieme delle successioni di Cauchy rispetto a questa relazione di equivalenza e ottenere pertanto un insieme che può essere considerato l'insieme dei numeri reali. Questa è la traccia che ora vogliamo seguire, partendo da un campo ordinato K qualunque. Vediamo ora i dettagli della costruzione.

Proposizione 8.2. *Valgono le seguenti proprietà:*

- *Ogni successione $(a_n)_n$ di Cauchy è limitata;*
- *Se $(a_n)_n$ è una successione di Cauchy (in K) e se esiste un $q \in K$, $q > 0$ tale che $|a_n| > q$ per ogni $n \in \mathbb{N}$, anche la successione $\left(a_n^{-1}\right)_n$ è di Cauchy.*
- *Se $(a_n)_n$ è una successione di Cauchy e se $(b_n)_n$ è una successione tale che esiste un $m \in \mathbb{N}$ per cui vale $a_n = b_n$ per $n > m$, allora anche $(b_n)_n$ è di Cauchy.*
- *La successione costante $(a, a, a, \ldots)$ è di Cauchy, se $(a_n)_n$ è di Cauchy, anche la successione $(-a_n)_n$ è di Cauchy.*

Dimostrazione. Il primo punto si vede facilmente, osservando che $|a_n - a_m| < 1$ per m ed n abbastanza grandi (da un certo k in poi). Allora $|a_n| = |a_n - a_k + a_k| \leq |a_n - a_k| + |a_k| < 1 + |a_k|$. Quindi $\max\{|a_0|, |a_1|, \ldots, |a_{k-1}|, 1 + |a_k|\}$ è una limitazione per a_n.
Per quanto riguarda il secondo punto, fissato ε, vale: $|a_m - a_n| < \varepsilon$ per m ed n grandi abbastanza. Allora (usando i risultati della proposizione 7.8), abbiamo $|a_m^{-1} - a_n^{-1}| = |a_m - a_n| \cdot |a_m^{-1} \cdot a_n^{-1}| < \varepsilon q^{-2}$.
Il terzo punto è immediato, in quanto per m ed n abbastanza grandi, a_n conicide con b_n.
L'ultimo punto è immediato. □

Altre proprietà delle successioni di Cauchy che avremo modo di usare in seguito:

Proposizione 8.3. *Sia $(a_n)_n$ una successione di Cauchy in K, con K campo ordinato. Se la successione $(a_n)_n$ non converge a zero, allora esiste un $q \in K$, $q > 0$, tale che $|a_n| > q$ per n abbastanza grande. Inoltre, nelle stesse ipotesi, gli elementi a_n della successione o sono sempre positivi dopo un certo valore di n o sono sempre negativi.*

Dimostrazione. Se $(a_n)_n$ non converge a 0 allora NON vale:
$\forall \varepsilon \in K, \varepsilon > 0\ \exists n_\varepsilon : |a_n| < \varepsilon\ \forall n > n_\varepsilon$
cioè: $\exists \varepsilon > 0 : \forall n_\varepsilon\ \exists n > n_\varepsilon$ such that $|a_n| \geq \varepsilon$. Quest'ultima affermazione si può reinterpretare dicendo che esiste un $q_1 \in K$, $q_1 > 0$ tale che $|a_n| \geq q_1$ per infiniti n. Usiamo ora il fatto che $(a_n)_n$ è di Cauchy, quindi se in particolare prendiamo $\varepsilon = q_1/2$, otteniamo che $|a_n - a_m| < q_1/2$ per m ed n abbastanza grandi. Scegliamo m tale che valga $|a_m| \geq q_1$, pertanto:
$|a_m| = |a_m - a_n + a_n| \leq |a_m - a_n| + |a_n| < q_1/2 + |a_n|$, da cui $|a_n| > |a_m| - q_1/2 \geq q_1/2 > 0$ per n abbastanza grande. Scelto $q = q_1/2$, abbiamo la tesi. Per la seconda parte della proposizione, abbiamo che $|a_m - a_n| < q/2$ per m ed n abbastanza grandi. Sapendo inoltre che $|a_n| > q$ per $n > \overline{n}$, scegliamo m in modo che sia anche maggiore di $\overline{n}$. Allora, se $a_m > 0$, vale $a_m > q$. Inoltre $-q/2 < a_n - a_m < q/2$, quindi $a_n > a_m - q/2$ e quindi $a_n > q/2$ per n abbastanza grande. Analoga dimostrazione nel caso $a_m < 0$.

□

Vediamo ancora qualche risultato sulle successioni di Cauchy:

Proposizione 8.4. *Se $(a_n)_n$ e $(b_n)_n$ sono due successioni di Cauchy, allora le successioni $(a_n + b_n)_n$ e $(a_n b_n)_n$ sono di Cauchy.*

Dimostrazione. Per quanto riguarda la somma, la tesi si ricava subito dall'osservazione che $|a_m + b_m - (a_n + b_n)| \leq |a_n - a_m| + |b_m - b_n|$; per quanto riguarda il prodotto, invece, vale: $|a_m b_m - a_n b_n| = |a_m b_m - a_m b_n + a_m b_n - a_n b_n| \leq |a_m||b_m - b_n| + |b_n||a_m - a_n|$ e da queste disuguaglianze, ricordando che le successioni di Cauchy sono limitate, segue subito la tesi. □

Sia ora M l'insieme di tutte le successioni di Cauchy sul campo ordinato K. Dall'ultima proposizione, segue che se su M definiamo la somma $(a_n)_n + (b_n)_n$ di due successioni come la successione $(a_n + b_n)_n$ e il prodotto $(a_n)_n \cdot (b_n)_n$ come la successione $(a_n \cdot b_n)_n$ otteniamo che M è chiuso per somme e prodotti, inoltre è facile verificare che la somma ha un elemento neutro, dato dalla successione costante 0, il prodotto ha anche elemento neutro, dato dalla successione costante 1 e M risulta un anello commutativo unitario. Sia I l'insieme di tutte le successioni infinitesime (cioè le successioni che hanno per limite 0). L'insieme I è un sottoinsieme di M ma di più, risulta essere un ideale. Infatti I è un gruppo abeliano rispetto alla somma e se $(a_n)_n \in I$ e $(b_n)_n \in M$, allora la successione $(a_n b_n)_n$ converge a 0 e quindi sta in I. Pertanto possiamo considerare l'anello quoziente M/I che, al pari di M, è un anello commutativo unitario. Vale:

Teorema 8.5. *L'anello M/I è un campo che contiene una copia isomorfa del campo K.*

Dimostrazione. Proviamo che un elemento $[(a_n)_n]$ di M/I non nullo è invertibile. Se $[(a_n)]$ è non nullo, allora $(a_n)_n$ non converge a 0, quindi esiste $q \in K$ tale che $|a_n| > q$ per $n > k$, con k opportuno. Costruiamo ora una nuova successione $(b_n)_n$ tale che $b_n = q + 1$ se $n \leq k$ e $b_n = a_n$ se $n > k$ abbiamo che $(b_n)_n$ differisce da $(a_n)_n$ solo per un numero finito di valori quindi è di Cauchy, non può convergere a 0 e $a_n - b_n$ è una successione che da un certo punto in poi vale 0, quindi converge a 0 e allora sta nell'ideale I. Pertanto $[(a_n)_n] = [(b_n)_n]$. Per la proposizione 8.2 la successione $\left(b_n^{-1}\right)_n$ è di Cauchy e si vede subito che $[(b_n)_n]$ è l'inverso di $[(a_n)_n]$, pertanto M/I è un campo.
Per provare che M/I contiene una copia isomorfa di K, basta considerare l'applicazione $f :\longrightarrow M/I$ data da $f(u) = [(u)_n]$ dove $(u)_n$ è la successione costante $(u, u, u, \ldots)$. □

In base a quest'ultimo risultato, possiamo allora dire che il campo M/I, che indichiamo con $\overline{K}$, è un sopracampo di K. Poiché il campo K è ordinato, possiamo vedere se riusciamo a definire un ordinamento su $\overline{K}$. Prendiamo un elemento $[(a_n)_n]$ non nullo di $\overline{K}$. Dalla proposizione 8.3 abbiamo che $(a_n)_n$ o è da un certo punto in poi sempre fatta da elementi positivi (maggiori di un $q \in K$ positivo) o negativi (minori di un $-q$ con $q \in K$ positivo). Possiamo allora definire un ordinamento su $\overline{K}$ dicendo che $[(a_n)_n] > 0$ se la successione $(a_n)_n$, da un certo n in poi, è fatta da elementi tutti maggiori di un $q \in K$ positivo. La definizione è indipendente dal rappresentante della classe perché, se $[(a_n)_n] = [(b_n)_n]$, allora $a_n - b_n$ ha per limite 0, quindi se $(a_n)_n$ da un certo n in poi è sempre maggiore di un numero positivo, analoga proprietà vale anche per $(b_n)_n$. In questo modo abbiamo definito gli elementi positivi (e quindi anche quelli negativi) di $\overline{K}$ e si vede subito che in questo modo $\overline{K}$ diventa un campo ordinato che estende il campo ordinato K.

Definizione 8.6. Il campo $\overline{K}$ costruito nel modo detto si dice *ampliamento cantoriano* del campo K.

Un'ultima proprietà di un ampliamento cantoriano è la seguente:

Proposizione 8.7. *Se K è archimedeo, allora anche $\overline{K}$ è archimedeo.*

Dimostrazione. Siano $[(a_n)_n]$ e $[(b_n)_n]$ due elementi positivi di $\overline{K}$ quindi esistono $p, q, r \in K$, $p > 0,\ q > 0,\ r > 0$, tali che $a_n > p$ e $b_n > q$ per n sufficientemente grande e anche, essendo $(b_n)_n$ limitata, $b_n < r$. Essendo K archiemedeo, esisterà un $u \in \mathbb{N}$ tale che $up > r$, quindi $ua_n > up > r > b_n$, sempre da un certo n in poi. Allora l'elemento $[(ua_n)_n]$ è maggiore di $[(b_n)_n]$. □

9 In numeri reali

Definizione 9.1. Un campo ordinato K si dice *completo* se ogni successione di Cauchy in K è convergente.

Poiché abbiamo già visto che una successione convergente è di Cauchy, abbiamo che un campo ordinato è completo esattamente quando tutte e sole le successioni di Cauchy sono convergenti.

Nella sezione precedente si è mostrato come costruire l'ampliamento cantoriano di un campo ordinato. Vediamo ora il:

Teorema 9.2. *Sia K un campo ordinato archimedeo e $\overline{K}$ il suo ampliamento cantoriano. Allora $\overline{K}$ è completo.*

Prima di procedere, forse è meglio mettere in evidenza alcuni dettagli che saranno poi utili nella dimostrazione. Innanzitutto vale:

Lemma 9.3. *Sia $(\alpha_n)_n$ una successione di $\overline{K}$. Le seguenti tre affermazioni sono equivalenti:*

1. $\forall\, \varepsilon > 0,\ \varepsilon \in \overline{K},\ \exists\, n_\varepsilon$ *tale che* $|\alpha_m - \alpha_n| < \varepsilon\ \ \forall\, m, n > n_\varepsilon$ *(cioè $(\alpha_n)_n$ è una successione di Cauchy);*
2. $\forall\, \varepsilon > 0,\ \varepsilon \in K,\ \exists\, n_\varepsilon$ *tale che* $|\alpha_m - \alpha_n| < \varepsilon\ \ \forall\, m, n > n_\varepsilon$*;*
3. $\forall\, k \in \mathbb{N} \setminus \{0\},\ \exists\, n_k$ *tale che* $|\alpha_m - \alpha_n| < 1/k\ \ \forall\, m, n > n_k$.

La dimostrazione è una immediata conseguenza dell'osservazione 7.12. Il vantaggio del precedente lemma è che per trattare successioni di Cauchy, ci si può limitare a scegliere elementi ε che sono in K (o addirittura che sono della forma $1/k$). Analoga considerazione vale per la verifica della convergenza di una successione di $(\alpha_n)_n$.

Se $[(a_n)_n]$ è un elemento non nullo di $\overline{K}$, il suo valore assoluto $|[(a_n)_n]|$ può essere visto come la classe $[(|a_n|)_n]$. Se prendiamo un elemento $[(a_n)_n]$ di $\overline{K}$ e se, fissato un $k \in \mathbb{N}$, consideriamo la successione $(a_{k+n})_n$ allora quest'ultima è anche una successione di Cauchy e vale: $[(a_n)_n] = [(a_{k+n})_n]$ (cioè la classe della successione che si ottiene da $(a_n)_n$ cancellando i primi k elementi conicide con la classe della successione $(a_n)_n$). Più in generale, se $(a_{n_k})_k$ è una sottosuccessione di una successione di Cauchy, anche $(a_{n_k})_k$ è di Cauchy e $[(a_n)_n] = [(a_{n_k})_k]$ in $\overline{K}$.

Dimostrazione. Dobbiamo far veder che una successione di Cauchy $(\alpha_n)_n$ in $\overline{K}$ è convergente. Per come è costruito l'ampliamento cantoriano, abbiamo che α_n (per ogni $n \in \mathbb{N}$) è una classe di successioni di Cauchy, cioè $\alpha_n = [(a_{nk})_k]$, dove $(a_{nk})_k$ è una successione di Cauchy in K. Da questo segue che, fissato un indice $n \in \mathbb{N}$, sarà $|a_{nh} - a_{nk}| < 1/n$ (consideriamo quindi il caso $\varepsilon = 1/n$) per h e k sufficientemente grandi. In base alle osservazioni fatte prima della presente

dimostrazione, possiamo assumere che α_n sia rappresentato da una successione per cui vale:

$$|a_{nk} - a_{nn}| < 1/n \quad \text{per ogni } k \in \mathbb{N}. \tag{2}$$

(infatti, per avere verificata la condizione (2), basta sopprimere quegli elementi—finiti—della successione (a_{nk}) che non verificano la disequazione). Esplicitiamo ora il fatto che $(\alpha_n)_n$ è di Cauchy. Fissato $\varepsilon \in \overline{K}$ (e, anzi, possiamo pensare che ε sia in K), esiste un $n_\varepsilon \in \mathbb{N}$ tale che $|\alpha_m - \alpha_n| < \varepsilon$ per ogni $m, n > n_\varepsilon$. Gli elementi α_m e α_n sono classi di successioni di Cauchy in K, quindi: $|\alpha_m - \alpha_n| = |[(a_{mk})_k] - [(a_{nk})_k]| = [(|a_{mk} - a_{nk}|)_k]$ e se questa classe è minore di ε, ricordando sempre come è definito l'ordinamento di $\overline{K}$, abbiamo che, fissato ε vale:

$$|a_{ml} - a_{nl}| < \varepsilon \quad \text{per } l \text{ abbastanza grande e per ogni } m, n > n_\varepsilon \tag{3}$$

Consideriamo la seguente successione: $(a_{kk})_k$. Si vedrà ora che essa è una successione di Cauchy, quindi dà origine ad un elemento di $\overline{K}$ e che la successione $(\alpha_n)_n$ converge proprio a questo elemento.
Proveremo che, fissato ε, vale:

$$|a_{mn} - a_{nn}| < \varepsilon \quad \text{per } m \text{ e } n \text{ sufficientemente grandi} \tag{4}$$

Da questa disequazione segue facilmente che la successione $(a_{kk})_k$ è di Cauchy, infatti $|a_{kk} - a_{hh}| = |a_{kk} - a_{hk} + a_{hk} - a_{hh}| \leq |a_{kk} - a_{hk}| + |a_{hk} - a_{hh}|$ e la prima diseguaglianza si può limitare usando la formula (4), la seconda usando la (2). Sempre da (4) si ottiene facilmente la convergenza di $(\alpha_n)_n$ a $[(a_{kk})_k]$, infatti la verifica del limite richiede di stimare $|\alpha_n - [(a_{kk})_k]|$. Ma questa espressione può essere così sviluppata:

$$\begin{aligned} |\alpha_n - [(a_{kk})_k]| &= |[(a_{nk})_k] - [(a_{kk})_k]| = |[(a_{nk} - a_{kk})_k]| \\ &= [(|a_{nk} - a_{kk}|)_k] \end{aligned}$$

e da qui la formula (4) permette di ottenere la tesi.
Vediamo allora di verificare la formula (4). Fissiamo un $\varepsilon > 0$ (come detto in precedenza, è sufficiente fissarlo in K). Prendendiamo $l \in \mathbb{N}$ in modo che valga la (3), prendiamo un k arbitrario e consideriamo l'espressione $|a_{nk} - a_{mk}|$. Vale:

$$\begin{aligned} |a_{nk} - a_{mk}| &= |a_{nk} - a_{nl} + a_{nl} - a_{ml} + a_{ml} - a_{mk}| \\ &= |a_{nk} - a_{nl} + a_{ml} - a_{mk} + a_{nl} - a_{ml}| \\ &\leq |a_{nk} - a_{nl}| + |a_{ml} - a_{mk}| + |a_{nl} - a_{ml}| \\ &= |a_{nk} - a_{nn} + a_{nn} - a_{nl}| + |a_{ml} - a_{mm} + a_{mm} - a_{mk}| + |a_{nl} - a_{ml}| \\ &\leq |a_{nk} - a_{nn}| + |a_{nn} - a_{nl}| + |a_{ml} - a_{mm}| + |a_{mm} - a_{mk}| + |a_{ml} - a_{nl}| \\ &< 1/n + 1/n + 1/m + 1/m + \varepsilon \end{aligned}$$

Nell'ultimo passaggio si è usata la formula (2) e anche la formula (3), la quale richiede che m ed n siano sufficientemente grandi. Prendendo ora $k = n$, da

quest'ultima formula si ottiene che $|a_{mn} - a_{nn}| < 2/m + 2/n + \varepsilon$. Siccome K è archimedeo, prendendo m ed n sufficientemente grandi, l'espressione $2/m + 2/n + \varepsilon$ può essere resa arbitrariamente piccola e questo prova la formula (4). □

Osservazione 9.4. Si noti che, a prima vista, può sembrare che, se nella formula (3) si pone $l = n$, si ottiene la formula (4) e quindi in questo modo si potrebbe evitare l'ultima parte della precedente dimostrazione. Il problema è che la formula (3) vale per l abbastanza grande e non è detto quindi che valga per $l = n$.

Teorema 9.5. *Sia K un campo ordinato archimedeo. Ogni elemento dell'ampliamento cantoriano $\overline{K}$ è limite di una successione di Cauchy a coefficienti in K.*

Dimostrazione. Consideriamo un elemento $\alpha \in \overline{K}$, quindi $\alpha = [(a_k)_k]$ e definiamo $\alpha_n = [(a_n, a_n, \ldots)]$, cioè α_n è l'elemento di $\overline{K}$ che nasce dalla successione costante $(a_n, a_n, \ldots)$. Consideriamo $|\alpha_n - \alpha|$. Abbiamo:

$$\begin{aligned} |\alpha_n - \alpha| &= |[(a_n, a_n, \ldots)] - [(a_k)_k]| \\ &= [(|a_n - a_0|, |a_n - a_1|, \ldots, |a_n - a_m|, \ldots)] \end{aligned}$$

e poichè $(a_k)_k$ è di Cauchy, $|a_n - a_m|$ può essere reso arbitrariamente piccolo e questo prova che α_n converge ad α. □

9.1 Il campo $\mathbb{R}$

Si definisce come campo reale l'ampliamento cantoriano del campo $\mathbb{Q}$. Essendo $\mathbb{Q}$ archimedeo, il campo $\mathbb{R}$ è un campo archimedeo completo. In $\mathbb{R}$ vale quindi il fatto che una successione di elementi di $\mathbb{R}$ è convergente se e solo se è una successione di Cauchy (questo risultato è noto come *teorema di Cauchy*). In base ai precedenti risultati, si ha che gli elementi di $\mathbb{R}$ si possono vedere come i limiti delle successioni di Cauchy a coefficienti razionali. Completiamo questa sezione con il seguente risultato:

Teorema 9.6. *Sia A un campo ordinato archimedeo completo. Allora A è isomorfo al campo $\mathbb{R}$ (l'isomorfismo è di campi ordinati). Quindi, a meno di isomorfismi, esiste un solo campo ordinato archimedeo completo.*

Dimostrazione. In base a quanto discusso in conseguenza del teorema 7.14, abbiamo che $\mathbb{Q}$ è un sottocampo di A. Dal fatto che A è archimedeo, segue poi che per ogni $a \in A$ esiste un numero naturale n tale che $n > a$ inoltre si trova facilmente che esiste un intero m tale che $m < a$ (se $a \geq 0$ basta prendere $m = -1$, se $a < 0$ allora sia $k \in \mathbb{N}$ tale che $k > -a$ e quindi $m = -k$). Consideriamo la successione che vale $a_0 = m$, $a_1 = m$ se $m < a < (m + n)/2$ e $a_1 = (m + n)/2$ altrimenti e così via. Si costruisce una successione $(a_k)_k$ che converge ad a (perchè $|a - a_k|$ tende a zero) e quindi $[(a_k)_k]$ è un elemento di $\mathbb{R}$. Costruiamo in questo modo un'applicazione $f : A \longrightarrow \mathbb{R}$ (infatti f è ben definita, perchè se $(b_k)_k$ è un'altra successione che converge ad a, allora la successione $(a_k - b_k)_k$

è infinitesima e quindi $[(a_k)] = [(b_k)_k]$. Se $[(a_k)_k]$ è un qualunque elemento di $\mathbb{R}$ (quindi $(a_k)_k$ è una successione di Cauchy in $\mathbb{Q}$), essendo A completo, esiste $a \in A$ tale che la successione $(a_k)_k$, pensata in A, converge ad a, e da questo segue la suriettività di f. L'iniettività di f segue dall'unicità del limite di successioni. L'applicazione f conserva le somme e i prodotti perché il limite di una somma (di un prodotto) è la somma (il prodotto) dei limiti. Infine si verifica immediatamente che f conserva anche l'ordinamento. Quindi f è un isomorfismo di campi ordinati. □

La conseguenza di quest'ultimo teorema è allora che esiste (a meno di isomorfismi) un unico campo archimedeo ordinato: il campo $\mathbb{R}$.

10 Dedekind

Richiamiamo, brevemente, alcune definizioni relative agli insiemi totalmente ordinati. Sia S un insieme totalmente ordinato e sia A un suo sottoinsieme non vuoto. Si dice che $m \in A$ è *massimo* di A se $a \leq m$ per ogni $a \in A$. Analogamente si dà la definizione di minimo. Si vede immediatamente che se m è massimo (minimo) di A, esso è unico (se m, m' sono due massimi di A, deve essere $m \leq m'$ perché m' è massimo e $m' \leq m$ perché m è massimo). L'insieme A si dice *superiormente limitato* se esiste un $l \in S$ tale che $a \leq l$ per ogni $a \in A$. L'elemento l si dice *limitazione superiore* di A, mentre A si dice *inferiormente limitato* se esiste $l \in K$ tale che $a \geq l$ per ogni $a \in A$. In questo caso l si dice *limitazione inferiore*.

Sia A superiormente limitato e sia L l'insieme di tutte le limitazioni superiori di A. Se L ha minimo, esso si dice *estremo superiore* di A. Analogamente si definisce *l'estremo inferiore* di A.

Se un insieme A ha massimo, allora esso è anche estremo superiore, analogamente, il minimo è estremo inferiore.

Esempio 10.1. I seguenti, semplici esempi, mostrano che massimo, minimo, estremo superiore, estremo inferiore non sempre esistono:

- Nell'insieme $S = \mathbb{N}$ dei numeri naturali (ordinato nel modo usuale) ogni sottoinsieme non vuoto ha minimo (v. teorema 6.15).
- Se S è un insieme totalmente ordinato e $A \subseteq S$ è un insieme finito, esso ha massimo e minimo.
- Sia $S = \mathbb{Z}$ con l'ordinamento usuale. L'insieme $A = \{2n \in \mathbb{Z} \mid n \in \mathbb{Z}\}$ dei numeri pari non è né superiormente, né inferiormente limitato.
- L'insieme $A \subseteq \mathbb{Q}$ dato da $A = \{q \in \mathbb{Q} \mid q < 3\}$ non è inferiormente limitato, è superiormente limitato, non ha massimo, ha estremo superiore, che è 3.
- L'insieme $A = \{q \in \mathbb{Q} \mid q^2 < 2 \text{ o } q < 0\}$ non è inferiormente limitato, è superiormente limitato, non ha massimo e nemmeno estremo superiore (l'estremo superiore è $\sqrt{2}$ se A viene pensato in $\mathbb{R}$).
- L'insieme $A = \{q \in \mathbb{Q} \mid 3 \leq q < 5\}$ è superiormente e inferiormente limitato, ha minimo (il numero 3), non ha massimo, ma ha estremo superiore (il numero 5).

Applichiamo ora le precedenti definizioni al caso specifico dei campi ordinati.

Proposizione 10.2. *Sia ora K un campo ordinato archimedeo. Allora le seguenti condizioni sono equivalenti:*

1. *K è completo (cioè ogni successione di Cauchy ha limite);*
2. *ogni sottoinsieme A di K non vuoto e superiormente limitato ha estremo superiore;*

3. *ogni sottoinsieme A di K non vuoto e inferiormente limitato ha estremo inferiore.*

Dimostrazione. L'equivalenza tra la condizione 2. e 3. è immediata: se A è superiormente limitato, allora l'insieme $A' = \{-a \mid a \in A\}$ è inferiormente limitato e l'estremo superiore di A diventa l'estremo inferiore di A' e viceversa (si noti che qui non si usa l'ipotesi che K sia archimedeo).
Vediamo ora che la completezza comporta l'esistenza di estremo superiore per un insieme A superiormente limitato. Sia l una limitazione superiore di A e sia $a \in A$. Poniamo: $a_0 = a$, $l_0 = l$, $d = |l - a|$. Definiamo ricorsivamente due successioni $(a_n)_n$ e $(l_n)_n$ in questo modo: supposte note a_n e l_n, sia $\alpha = (a_n + l_n)/2$. Se α è maggiorante di A, allora poniamo $a_{n+1} = a_n$ e $l_{n+1} = \alpha$, se invece α non è maggiorante di A, allora esiste un $\beta \in A$ tale che $\alpha < \beta$. In questo secondo caso, poniamo $a_{n+1} = \beta$, $l_{n+1} = l_n$. Si vede subito che vale, per ogni n:

$$a_0 \leq a_1 \leq \cdots \leq a_n \leq l_n \leq \cdots \leq l_1 \leq l_0$$

inoltre $|l_n - a_n| \leq d/2^{n+1}$. Fissiamo $k \in \mathbb{N}$. Allora $|l_k - a_k| \leq d/2^{k+1}$ inoltre, se $m, n > k$ (supponiamo $m < n$), allora $a_k \leq l_n \leq l_m \leq l_k$, quindi $|l_m - l_n| \leq |l_k - a_k| \leq d/2^{k+1}$, pertanto, essendo K archimedeo, $d/2^{k+1}$ può essere reso vicino a zero a piacere e quindi $(l_n)_n$ è di Cauchy. (Analogamente si può vedere che $(a_n)_n$ è di Cauchy, ma questo risultato non è necessario). Sia λ il limite della successione $(l_n)_n$. Verifichiamo che λ è l'estremo superiore di A. Se esistesse $\alpha \in A$ tale che $\alpha > \lambda$, dal fatto che l_n è vicino a λ quanto si vuole, si potrebbe trovare un indice n tale che l_n sta tra λ e α, cioè l_n, che è un maggiorante di A, sarebbe minore di un elemento di A. Questo assurdo prova che λ è un maggiorante di A. Se ci fosse un altro maggiorante di A, $\lambda' < \lambda$, dal fatto che a_n è vicino a l_n quanto si vuole e a sua volta l_n converge verso λ, si troverebbe che ci sono elementi di A che superano λ'. Pertanto non ci possono essere maggioranti di A più piccoli di λ. In altre parole, $\sup(A) = \lambda$.
Vediamo ora che l'esistenza dell'estremo superiore per un insieme non vuoto e superiormente limitato A comporta la completezza. Sia $(a_n)_n$ una successione di Cauchy e consieriamo l'insieme

$$A = \{a \in K \mid a_n < a \text{ solo per finiti } n\}.$$

(in particolare A contiene anche tutti gli a tali che non è mai vero che $a_n < a$). Poichè la successione $(a_n)_n$ è di Cauchy, è limitata e da questo segue che A è superiormente limitato e non vuoto, quindi ammette estremo superiore l. Fissiamo $\varepsilon \in K$, $\varepsilon > 0$. Allora vale: $a_n > l - \varepsilon$ per n sufficientemente grande (infatti, essendo l estremo superiore di A, esiste un $b \in A$ tale che $b > l - \varepsilon$ e quindi prima di b ci sono solo finiti elementi della successione); inoltre anche dopo $l + \varepsilon$ si trovano solo un numero finito di elementi di $(a_n)_n$; per provare questa affermazione, supponiamo che dopo $l + \varepsilon$ ci siano infiniti elementi della successione. Essendo essa di Cauchy, esisterà un n_0 tale che, se $m, n > n_0$, allora $|a_n - a_m| < \varepsilon/2$. Sia $n_1 > n_0$ tale che $a_{n_1} > l + \varepsilon$. Allora $|a_{n_1} - a_m| < \varepsilon/2$, cioè, per ogni $m > n_0$ vale: $a_{n_1} - \varepsilon/2 < a_m < a_{n_1} + \varepsilon/2$ e quindi abbiamo che prima

di $a = a_{n_1} - \varepsilon/2$ ci sono solo finiti elementi della successione, allora $a \in A$ ma questo è assurdo, perché $a > l$. Pertanto abbiamo provato che tutti gli elementi della successione, tranne un numero finito, stanno tra $l - \varepsilon$ e $l + \varepsilon$. Essendo ε arbitrario, questo prova che l è il limite di $(a_n)_n$. □

Vediamo ora brevemente un altro approccio alla costruzione dei numeri reali (partendo sempre dai razionali), dovuta a Richard Dedekind. Ripartiamo dalla tabella 1 e osserviamo che da essa si possono immaginare i seguenti due sottoinsiemi di $\mathbb{Q}$: l'insieme B costituito da tutti i numeri razionali il cui quadrato è maggiore di 2 e l'insieme A dei numeri il cui quadrato è minore di 2 (a cui aggiungiamo anche i numeri negativi). Gli insiemi A e B sono disgiunti, ogni elemento di A è minore di ogni elemento di B e la loro unione è tutto l'insieme $\mathbb{Q}$ dei razionali. Inoltre, assumendo di conoscere già i numeri reali, questi due insiemi individuano in modo abbastanza eviente il numero irrazionale $\sqrt{2}$. Così come, nella costruzione di Cantor, una successione di Cauchy individua un numero reale (che è il numero a cui la successione dovrebbe convergere) e quindi i numeri reali possono essere costruiti partendo dalle successioni di Cauchy, nella costruzione di Dedekind un numero reale è individuato da una coppia di insiemi come A e B con le proprietà indicate sopra. Più precisamente,

Definizione 10.3. Sia K un campo ordinato e siano A e B due insiemi tali che:

1. $A \neq \emptyset$, $B \neq \emptyset$;
2. $K = A \cup B$;
3. Per ogni $a \in A$ e $b \in B$, vale $a < b$.

Allora (A, B) si chiama una *sezione* (o *taglio*) *di Dedekind*.

(Una conseguenza della definizione è che $A \cap B = \emptyset$). Si dice poi che una sezione è di prima specie se A ha massimo o B ha minimo, di seconda specie altrimenti. Non può succedere che A abbia massimo e anche B abbia minimo (se a fosse massimo di A e b minimo di B, considerando $(a+b)/2$ si otterrebbe un elemento in K che non sta in $A \cup B$ e questo contraddirebbe il secondo punto della definizione di sezione). Ad esempio una sezione di Dedekind può essere la seguente: $A = \{a \in \mathbb{Q} \mid a < 4\}$, $B = \{b \in \mathbb{Q} \mid b \geq 4\}$. In questo caso A non ha massimo, B ha minimo; anche la seguente è una sezione di Dedekind: $A' = \{a \in \mathbb{Q} \mid a \leq 4\}$, $B' = \{b \in \mathbb{Q} \mid b > 4\}$. In questo caso A' ha massimo. Le due sezioni "individuano" lo stesso numero (il numero 4). Per evitare questa ambiguità, si può semplificare la definizione precedente, ponendo:

Definizione 10.4. Una *sezione sinistra di Dedekind* è un sottoinsieme $A \subseteq K$ tale che:

1. $A \neq K$, $A \neq \emptyset$;
2. Se $a \in A$ e $a' < a$, allora $a' \in A$;

3. A non ha massimo, cioè per ogni $a \in A$, esiste un $b \in A$ tale che $a < b$.

Una sezione sinistra di Dedekind dà origine ad una sezione di Dedekind (data da $(A, K \setminus A)$) e in questa sezione di Dedekind o $K \setminus A$ ha minimo o né A ha massimo, né $K \setminus A$ ha minimo (in questo caso la sezione si dice che è di *seconda specie* o una *lacuna*).

Indichiamo con $\tilde{K}$ l'insieme delle sezioni sinistre di Dedekind.

Sia $f : K \longrightarrow \tilde{K}$ data da: $f(q) = \{x \in K \mid x < q\}$. L'applicazione f è iniettiva e permette quindi di ritrovare K in $\tilde{K}$ (identificando K con $f(K)$).

Esercizio 7. Provare che $A = \{q \in \mathbb{Q} \mid q < 0 \text{ o } q > 0 \text{ e } q^2 < 2\}$ è una sezione sinistra di Dedekind (relativa al campo ordinato $\mathbb{Q}$).

Sull'insieme $\tilde{K}$ si può definire una relazione d'ordine nel seguente modo: siano A e B due sezioni sinistre. Si pone $A < B$ se $A \subset B$.

Esercizio 8. Verificare che:

1. La relazione così definita è una relazione d'ordine totale;
2. L'applicazione $f : K \longrightarrow \tilde{K}$ conserva l'ordine.

Vediamo ora il teorema principale:

Teorema 10.5. *Sia $\mathscr{U} \subseteq \tilde{K}$ un insieme non vuoto e superiormente limitato. Allora $\mathscr{U}$ ha estremo superiore.*

Dimostrazione. Consideriamo l'insieme $A = \cup_{U \in \mathscr{U}} U$. Essendo ogni U un sottoinsieme di K, A è un sottoinsieme di K. Verifichiamo che A è una sezione sinistra di Dedekind. Certamente $A \neq \emptyset$ perché gli U sono non vuoti. Poi $K \setminus A \neq \emptyset$ in quanto $\mathscr{U}$ è superiormente limitato in $\tilde{K}$ da un elemento B (che è una sezione sinistra). Pertanto $U < B$ in $\tilde{K}$ per ogni $U \in \mathscr{U}$, e quindi $U \subset B$ in K per ogni U e quindi $A \subset B$. Essendo $K \setminus B \neq \emptyset$, anche $K \setminus A$ è non vuoto. Se $p, q \in K$, con $p < q$ e se $q \in A$, allora $q \in U$ per un opportuno U e quindi, essendo U sezione sinistra di Dedekind, $q \in U$. Allora $q \in A$. Vediamo infine che A, come sottoinsieme di K, non ha massimo. Sia $p \in A$, allora esiste un $U \in \mathscr{U}$ tale che $p \in U$. Poiché U non ha massimo, esiste un $q \in U$ tale che $p < q$, ma allora $q \in A$ e quindi A non ha massimo. Pertanto $A \in \tilde{K}$. Certamente $U \leq A$ per ogni $U \in \mathscr{U}$, quindi A è una limitazione superiore per $\mathscr{U}$. Se poi X è un'altra limitazione superiore di $\mathscr{U}$, $U \subseteq X$ per ogni U, quindi $\cup U \subseteq X$ e allora $A \subseteq X$, cioè A è il minimo delle limitazioni superiori di $\mathscr{U}$, pertanto A è l'estremo superiore di $\mathscr{U}$. □

Vediamo ora di definire una somma e un prodotto sull'insieme $\tilde{K}$. Definire la somma è facile:
Se $A, B \in \tilde{K}$, definiamo

$$A + B = \{p + q \mid p \in A,\ q \in B\}$$

Si vede facilmente che $(\tilde{K}, +)$ è un gruppo abeliano: la somma è associativa e commutativa perché la somma di K è associativa e commutativa. L'elemento

neutro è dato da $0 = \{p \in K \mid p < 0\}$ (cioè 0 altro non è che $f(0)$, dove f è l'applicazione definita in precedenza che immerge K in $\tilde{K}$).

Esercizio 9. Verificare che vale:

1. Se $A \in \tilde{K}$, allora $-A$ è l'insieme $\{q \in K \mid -q \notin A\}$, a cui va eventualmente tolto il massimo;
2. L'applicazione f precedentemente definita è un omomorfismo di $(K, +)$ in $(\tilde{K}, +)$;
3. Se $A, B, C \in \tilde{K}$ e $A < B$, allora $A + C < B + C$.

In $\tilde{K}$ si può anche definire un prodotto, anche se la sua definizione richiede qualche cautela.
Sia $A \in \tilde{K}$ e assumiamo $A > 0$. Sia $B \in \tilde{K}$. Allora poniamo:

$$A \cdot B = \begin{cases} \{p \cdot q \mid p \in A, p > 0 \text{ e } q \in B,\ q > 0\} \cup \{q \in K \mid q \leq 0\} & \text{se } B > 0; \\ \{p \cdot q \mid p \notin A \text{ e } q \in B\} & \text{se } B \leq 0. \end{cases}$$

Analoga definizione nel caso in cui $A < 0$.

Esercizio 10. Supponiamo che K sia il campo $\mathbb{Q}$ dei razionali. Sia $f : \mathbb{Q} \longrightarrow \tilde{\mathbb{Q}}$ l'applicazione che corrisponde all'applicazione f definita nel caso generale. Verificare che vale:

1. $f(2) + f(3) = f(5)$;
2. $f(2) \cdot f(3) = f(6)$;
3. Se $A = \{q \in \mathbb{Q} \mid q^2 < 2 \text{ o } q < 0\}$, allora $A \cdot A = f(2)$.

L'insieme $\tilde{K}$ con le operazioni di somma e prodotto ora introdotte risulta essere un campo ordinato che contiene una copia isomorfa di K. Inoltre, se K è archimedeo, $\tilde{K}$ risulta essere archimedeo. Quindi in questo caso $\tilde{K}$ è un campo ordinato archimedeo completo (la completezza è conseguenza del teorema 10.5 e della proposizione 10.2). Allora, in conseguenza del teorema 9.6, il campo $\tilde{K}$ altro non è che il campo dei numeri reali costruito precedentemente con l'utilizzo delle successioni di Cauchy.

11 Numeri utili

Dopo aver introdotto due diverse costruzioni di $\mathbb{R}$, ci soffermiamo ora brevemente ad analizzare le possibili caratteristiche che hanno tali numeri reali. I "nuovi" numeri di $\mathbb{R}$, quelli cioè che stanno in $\mathbb{R}$ ma non in $\mathbb{Q}$ si dicono numeri *irrazionali*. Il primo esempio di numero irrazionale che solitamente si incontra è il numero $\sqrt{2}$. La dimostrazione della sua irrazionalità si fa per assurdo. Se fosse $\sqrt{2} = r/s \in \mathbb{Q}$ (con r ed s primi tra loro), allora avremmo $2 = r^2/s^2$, cioè $2s^2 = r^2$. Quindi r^2 è pari. Allora r è pari, quindi $r = 2r'$, quindi $2s^2 = 4r'^2$, allora s^2 è pari, quindi s è pari e questo contraddice il fatto che r ed s sono primi tra loro.
In questo ragionamento si è fatto il passaggio: "se r^2 è pari, allora r è pari". Questo può essere gustificato in vari modi.
Primo modo: Se r fosse dispari, allora sarebbe della forma $2m+1$ e il suo quadrato sarebbe quindi della forma $4m^2+4m+1$ che è anche dispari.
Secondo modo (variante del primo): Se r^2 è pari, allora $r^2 \equiv 0 \bmod 2$ e se non fosse $r \equiv 0 \bmod 2$, allora sarebbe $r \equiv 1 \bmod 2$, ma allora $r^2 \equiv 1^1 = 1 \bmod 2$.
Terzo modo: usando il teorema fondamentale dell'aritmetica, possiamo scomporre r in fattori primi: $r = p_1^{\alpha_1} \cdot \cdots \cdot p_n^{\alpha_n}$. Quindi r^2 si scompone in $p_1^{2\alpha_1} \cdot \cdots \cdot p_n^{2\alpha_n}$ e se 2 è un fattore di r^2, allora deve essere anche un fattore di r.
Questo terzo modo è più generale e dimostra in generale che se un numero primo p divide il quadrato (o il cubo, o la potenza n-ima) di un numero r, allora p divide r.

Esercizio 11. Usare tutti e tre i modi esposti sopra per provare che $\sqrt{3}$ è irrazionale.
Usare il terzo metodo per provare che $\sqrt[5]{23}$ è irrazionale.

I numeri irrazionali, a differenza dei numeri razionali, non sono chiusi rispetto alle operazioni di somma e prodotto, come subito si vede. Ad esempio $\sqrt{2} \cdot \sqrt{2}$ prova che il prodotto di irrazionali può essere razionale. Inoltre somma di un irrazionale con un razionale è un irrazionale, così per il prodotto (a meno che il numero razionale non sia 0) e analogamente per il rapporto (razionale/irrazionale e irrazionale/razionale sono irrazionali). Pertanto, avendo provato che $\sqrt{2}$ è irrazionale, abbiamo subito che, ad esempio $\frac{5}{3+4\sqrt{2}}$ è irrazionale.

I numeri $\sqrt{2}$, $\sqrt{3}$, $\sqrt[5]{23}$, oltre ad essere accomunati dal fatto di essere irrazionali, hanno un'ulteriore caratteristica comune: sono soluzioni di un'equazione polinomiale (rispetivamente $x^2 - 2 = 0$, $x^2 - 3 = 0$, $x^5 - 23 = 0$). Ricordiamo che questi numeri si dicono algebrici, cioè in generale, se K ed L sono campi, con K sottocampo di L si pone:

Definizione 11.1. Un elemento $a \in L$ si dice algebrico su K se esiste un polinomio $f(x) \in K[x]$ non nullo tale che $f(a) = 0$. Un elemento di L che non è algebrico su K si dice trascendente su K.

In particolare, un numero di $\mathbb{R}$ che non è algebrico su $\mathbb{Q}$ si dice numero trascendente.

Richiamiamo brevemente alcune proprietà degli elementi algebrici. Se $a \in L$ à algebrico su K, allora il polinomio monico, di grado minimo possibile che si annulla in a è unico e si dice *polinomio minimo*. Si vede facilmente che il polinomio minimo è irriducibile. Se a è algebrico su K e se il suo polinomio minimo ha grado n, allora a si dice algebrico di grado n. Risulta conveniente riassumere il fatto che L è un campo che contiene K come sottocampo con la notazione $L : K$. In questa situazione, L risulta uno spazio vettoriale su K. La sua dimensione, come spazio vettoriale, si indica con $[L : K]$. Si vede subito che se $[L : K]$ è un numero finito, allora L è un'estensione algebrica di K, cioè ogni elemento di L è algebrico su K. (La dimostrazione è immediata: se $a \in L$ e se $[L : K] = n$, allora $1, a, a^2, \ldots, a^n$ sono $n+1$ elementi di L e quindi linearmente dipendenti su K. Esiste quindi una loro combinazione lineare a coefficienti in K, non tutti nulli, che vale 0. Tale combinazione lineare fornisce un polinomio in $K[x]$ che si annulla in a).

Si ricordi ancora il teorema della torre: se K, L, M sono tre campi tali che $L : K$ e $M : L$, allora $M : K$ e vale $[M : K] = [M : L] \cdot [L : K]$.

Ancora alcuni richiami sugli elementi algebrici. Se abbiamo un'estensione di campi $L : K$ e se $a \in L$ à algebrico su K, allora $K[a]$ (il più piccolo anello che contiene K ed a, che è fatto da elementi della forma $f(a)$ dove f è un polinomio di $K[x]$) risulta essere un campo ed è isomorfo a $K[x]/(m)$, dove m è il polinomio minimo di a su K. Analogamente, se $a_1, \ldots, a_n \in L$ sono algebrici su K, allora anche $K[a_1, \ldots, a_n]$ (il più piccolo anello che contiene K e $a_1, \ldots, a_n$) è un campo. Inoltre vale: Se $a, b \in L$ sono algebrici su K, allora $a+b$, ab, a^{-1} (se $a \neq 0$) sono algebrici su K. La dimostrazione di queste proprietà deriva dalla seguente torre di campi: $K \subseteq K[a] \subseteq K[a, b]$. Se a è algebrico su K, allora $[K[a] : K]$ è finita, poi b è algebrico su K e quindi anche su $K[a]$, quindi $[K[a][b] : K[a]]$ è finita, allora $K[a, b] = K[a][b]$ è un'estensione finita di K, pertanto tutti i suoi elementi sono algebrici su K. Tra i suoi elementi troviamo anche $a + b$, ab, a^{-1} che sono quindi algebrici su K.

Richiamiamo ancora alcune nozioni sui polinomi di $\mathbb{Q}[x]$ e $\mathbb{Z}[x]$. Il lemma di Gauss garantisce che il problema di fattorizzare polinomi non costanti in $\mathbb{Q}[x]$ è equivalente al problema della fattorizzazione in $\mathbb{Z}[x]$, cioè se $f(x) \in \mathbb{Z}[x]$ è un polinomio primitivo (cioè tale che i suoi coefficienti non hanno un fattore comune) e se $f(x) = a(x) \cdot b(x)$ in $\mathbb{Q}[x]$, allora esistono polinomi $a'(x), b'(x) \in \mathbb{Z}[x]$ associati ad $a(x)$ e $b(x)$ rispettivamente, tali che $f(x) = a'(x) \cdot b'(x)$. (Dire che $a(x)$ è associato a $a'(x)$ significa dire che esiste una costante $r \in \mathbb{Q}$ tale che $a'(x) = ra(x)$).

Scoprire se un polinomio $f(x) \in \mathbb{Z}[x]$ ha radici razionali è teoricamente facile: se $f(x) = a_0 + a_1x + \cdots + a_nx^n$ e se p/q è una radice razionale, allora deve succedere che p divide a_0 e q divide a_n. Quindi le eventuali radici razionali vanno ricercate tra un numero finito di possibili frazioni. In particolare, se il polinomio $f(x) \in \mathbb{Z}[x]$ è monico, allora se ha radici razionali, esse devono per forza essere numeri interi.

Vediamo ora qualche ulteriore esempio di numero irrazionale. Tutti i numeri reali algebrici di grado maggiore di 1 sono irrazionali. Infatti, se a è algebrico e il suo polinomio minimo $m(x)$ ha grado $n > 1$, se a fosse razionale, sarebbe una

radice in $\mathbb{Q}$ del polinomio irriducibile $m(x)$. Da qui abbiamo ancora un modo per provare che $\sqrt{2}$ è algebrico su $\mathbb{Q}$: il polinomio minimo di $\sqrt{2}$ su $\mathbb{Q}$ è $x^2 - 2$ che è di grado 2.
Vale:

Proposizione 11.2. *Sia $a \in \mathbb{N}$. Il numero $\sqrt[n]{a}$ o è intero (se $a = k^n$ con $k \in \mathbb{N}$) o è irrazionale.*

Dimostrazione. Se $\alpha = \sqrt[n]{a}$, allora α è zero del polinomio $x^n - a$, che è un polinomio monico a coefficienti interi, quindi se ha una soluzione razionale α, per quanto detto sopra, essa deve essere un numero intero k. Allora $\alpha = k$ e $a = k^n$ altrimenti α è irrazionale. □

Consideriamo ora le funzioni trigonometriche. Vogliamo in particolare avere informazioni sul tipo di numero reale (razionale? algebrico?) che si ottiene calcolando il seno o il coseno di vari angoli. Ricordiamo le seguenti formule:

$$\begin{array}{rcl} \sin(\alpha+\beta) & = & \sin(\alpha)\cos(\beta) + \cos(\alpha)\sin(\beta) \\ \cos(\alpha+\beta) & = & \cos(\alpha)\cos(\beta) - \sin(\alpha)\sin(\beta) \end{array} \tag{5}$$

Da esse si ricava ad esempio che

$$\begin{array}{rcl} \cos(2\alpha) & = & 2\cos^2(\alpha) - 1 \\ \cos(3\alpha) & = & 4\cos^3(\alpha) - 3\cos(\alpha) \end{array} \tag{6}$$

Da queste ultime si ottiene che, ad esempio, $\cos(20^o) = \cos(\pi/9)$ è un numero algebrico. Infatti $\cos(60^o) = \cos(3 \cdot 20^o)$ e quindi $\cos(60^o) = 4cos^3(20^o) - 3\cos(20^o)$. Detto $x = \cos(20^o)$, abbiamo che $4x^3 - 3x - 1/2 = 0$, cioè $8x^3 - 6x + 1 = 0$. Se $\cos(20^o)$ fosse un numero razionale sarebbe uno zero del polinomio $8x^3 - 6x + 1$ ma le eventuali radici razionali di questo polinomio possono essere solo i numeri $\pm 1, \pm 1/2, \pm 1/4, \pm 1/8$ e si vede (per esempio con un conto diretto) che nessuno di questi numeri può essere radice. Si può però approfondire molto di più la conoscenza dei valori delle funzioni trigonometriche.

Definizione 11.3. Si dicono *polinomi di Chebyshev* i polinomi definiti ricorsivamente nel seguente modo: $T_0(x) = 1$, $T_1(x) = x$, $T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x)$

Vale:

$$\begin{array}{rcl} T_2(x) & = & 2x^2 - 1 \\ T_3(x) & = & 4x^3 - 3x \\ T_4(x) & = & 8x^4 - 8x^2 + 1 \\ T_5(x) & = & 16x^5 - 20x^3 + 5x \\ & \ldots & \end{array}$$

Proposizione 11.4. *Vale la seguente relazione: per ogni $n \in \mathbb{N}$*

$$\cos(nx) = T_n(\cos(x))$$

Dimostrazione. La formula si può verificare per induzione. Per $n = 0, 1, 2, 3$ è ovvia o è diretta conseguenza delle formule (5) e (6). Inoltre vale (sempre usando le (5)):

$$\begin{aligned} \cos((n+1)x) &= \cos(nx)\cos(x) - \sin(nx)\sin(x) \\ \cos((n-1)x) &= \cos(nx)\cos(x) + \sin(nx)\sin(x) \end{aligned}$$

Sommando membro a membro si ottiene:

$$\cos((n+1)x) + \cos((n-1)x) = 2\cos(x)\cos(nx)$$

Pertanto $\cos((n+1)x) = 2\cos(x)\cos(nx) - \cos((n-1)x)$ e, per induzione: $\cos((n+1)x) = 2\cos(x)T_n(\cos(x)) - T_{n-1}(\cos(x)) = T_{n+1}(\cos(x))$. □

Da questa formula è facile scoprire che il coseno di ogni angolo della forma $90^o/n$ (cioè $\pi/(2n)$) è un numero algebrico. Infatti, se $\alpha = \pi/(2n)$, allora $\cos(n\alpha) = 0$ e $\cos(\alpha)$ è soluzione del polinomio $T_n(x)$, quindi $\cos(\alpha)$ è algebrico. Di più, se $\cos(\beta)$ è algebrico, allora anche $\cos(m\beta)$ è algebrico. Infatti, sempre dalla proposizione 11.4 abbiamo che $\cos(m\beta) = T_m(\cos(\beta))$. Poiché $\cos(\beta)$ è algebrico, lo è anche $\cos^i(\beta)$ per ogni $i \in \mathbb{N}$ e allora è algebrica ogni combinazione lineare a coefficienti in $\mathbb{Q}$ di $1, \cos(\beta), \cos^2(\beta), \cos^3(\beta), \ldots$. In conclusione abbiamo che è algebrico il coseno di ogni angolo multiplo razionale di $\pi/2$ (o di π, che è ovviamente lo stesso). La relazione $\sin^2(\alpha) + \cos^2(\alpha) = 1$ permette di ottenere che se $\cos(\alpha)$ è algebrico, allora lo è anche $\sin(\alpha)$ e quindi anche $\tan(\alpha)$ (in alternativa, per vedere che se $\cos(\alpha)$ è algebrico, allora lo è anche $\sin(\alpha)$, basta usare la relazione: $\sin(\alpha) = \cos(\pi/2 - \alpha)$).
Resta ancora un punto da chiarire. Per quali multipli razionali di $\pi/2$ il coseno è un numero razionale? Per esempio sappiamo che se $x = 0, \pi/3, \pi/2$ allora $\cos(x)$ vale, rispettivamente, $1, 1/2, 0$ ed è quindi razionale. Lo è anche per gli angoli che si ottengono sommando a 0 o a $\pi/3$ o a $\pi/2$ multipli di $\pi/2$, ma ci possono essere altri angoli, multipli razionali di $\pi/2$, che hanno il coseno razionale?

Vale il seguente risultato (detto anche teorema di Niven):

Proposizione 11.5. *Sia α un angolo compreso tra 0 e $\pi/2$, multiplo razionale di $\pi/2$ e si supponga che il coseno sia razionale. Allora l'angolo vale o 0 o $\pi/3$ o $\pi/2$. Analogamente, il seno vale 0 o $\pi/6$ o $\pi/2$.*

Dimostrazione. Poniamo $F_n(x) = 2T_n(x/2)$. Si verifica facilmente che $F_n(x)$ è un polinomio monico di grado n a coefficienti interi. Vale inoltre:

$$F_n(2\cos(x)) = 2\cos(nx)$$

Si supponga che α sia un multiplo razionale di $\pi/2$, cioè $\alpha = m\pi/(2n)$ e si supponga che $\cos(\alpha)$ sia razionale. Allora $F_n(2\cos(\alpha)) = 2\cos(m\pi/2)$. Pertanto $2\cos(\alpha)$ è uno zero di $F_n(x)$ o di $F_n(x) - 2$ o di $F_n(x) + 2$ (a seconda del valore di $2\cos(m\pi/2)$ che può essere 0 o 1 o -1. Tutti e tre i polinomi sono a coefficienti interi e sono monici, quindi $2\cos(\alpha)$ deve essere un intero ed essendo il coseno limitato tra -1 e 1, allora i possibili valori di $\cos(\alpha)$ possono essere solo

$-1, -1/2, 0, 1/2$ e 1. Assumendo che α sia un angolo tra 0 e $\pi/2$, abbiamo che α può avere solo i valori 0, $\pi/3$ e $\pi/2$. Ricordando che $\sin(\alpha) = \cos(\pi/2 - \alpha)$, si ottiene il risultato per il seno. □

Osservazione 11.6. I risultati ora provati devono essere interpretati nel giusto modo: non stanno a significare che "quasi sempre" il seno e il coseno (e la tangente) sono numeri algebrici: il seno, ad esempio, è una funzione che, in quanto continua, assume tutti i valori dell'intervallo reale $[-1, 1]$, (anzi, è una biiezione tra $[-\pi/2, \pi/2]$ e $[-1, 1]$) e quindi $\sin(x)$ ha gli stessi "tipi" di numeri reali che ci sono in $[-1, 1]$. Quanto abbiamo qui provato mostra semplicemente che per un insieme di angoli molto naturali da considerare, che sono gli angoli del tipo $(p/q)\pi$ (ma che sono un insieme molto piccolo rispetto a tutti gli angoli) il seno, il coseno e la tangente sono numeri algebrici.

Per concludere, vediamo ancora cosa si riesce a dire per quanto riguarda il logaritmo di qualche numero. In questi esempi consideremo il *il logaritmo in base 10* che indicheremo con Log. Iniziamo con un esempio: consideriamo il $\operatorname{Log} 2$. Supponiamo sia un numero razionale p/q. Allora $10^{p/q} = 2$, da cui si ricava che $10^p = 2^q$, cioè $2^p \cdot 5^p = 2^q$. Usando il teorema fondamentale dell'aritmetica, si vede che supporre che $\operatorname{Log}(2)$ sia razionale, porta ad un assurdo. Possiamo essere più precisi:

Proposizione 11.7. *Supponiamo che $r > 0$ sia un numero razionale e che $\operatorname{Log} r$ sia anche un numero razionale. Allora necessariamente $r = 10^m$, con $m \in \mathbb{Z}$ (e quindi $\operatorname{Log} r = m$ è un intero).*

Dimostrazione. Supponiamo che $r = \alpha/\beta$ con α e β numeri naturali, ridotti ai minimi termini e sia $\operatorname{Log}(\alpha/\beta) = p/q$ con p e q numeri interi, ridotti ai minimi termini. Allora otteniamo:

$$10^{\frac{p}{q}} = \frac{\alpha}{\beta}$$

da cui

$$2^p \cdot 5^p = \frac{\alpha^q}{\beta^q}, \text{ quindi } \beta^q 2^p 5^p = \alpha^q$$

Ora usiamo il teorema fondamentale dell'aritmetica e otteniamo che α deve avere i fattori 2 e 5, pertanto $\alpha = 2^m \cdot 5^n \cdot \alpha'$, inoltre β non può avere il fattore 2 o il fattore 5 (perché primo con α), pertanto $\beta^q = \alpha'^p$ e quindi deve valere $mq = p = nq$, da cui $m = n$ ed essendo p e q primi tra loro, si deduce che deve essere $q = 1$. Inoltre, sempre da $\beta^q = \alpha'^q$, si ottiene $\beta = 1$ (sempre perché β è primo con α), quindi $\alpha' = 1$. Si conclude allora che r deve essere un numero naturale della forma $2^m \cdot 5^m = 10^m$. □

Conseguenza della proposizione è che il numero $\operatorname{Log} r$ è irrazionale per ogni r razionale, non potenza di 10. È algebrico o trascendente? La risposta non è banale e si può ottenere facendo ricorso alla risoluzione del settimo problema di Hilbert, data (indipendentemente) nel 1934 da A. Gelfond e T. Schneider. Vale questo teorema:

Teorema 11.8. *Se a è un numero algebrico diverso da* 0 *e da* 1 *e b è un numero algebrico di grado maggiore di* 1*, allora a^b è trascendente.*

Supponiamo allora che r sia razionale e $\operatorname{Log} r$ sia un numero algebrico b, siccome abbiamo visto che b è irrazionale, se b è algebrico, è di grado maggiore di uno, allora 10^b sarebbe trascendente, ma $10^b = r$ che è razionale, e quindi $\operatorname{Log} r$ deve essere trascendente.

Può succedere che a e b siano due numeri irrazionali tali che a^b sia razionale? Una possibile risposta elementare, che non fa uso del teorema precedente, è la seguente: Consideriamo $a = b = \sqrt{2}$. Se a^b è razionale, abbiamo risposto affermativamente alla domanda. Se invece a^b è irrazionale, consideriamo $(a^b)^{\sqrt{2}}$. È della forma irrazionale$^{\text{irrazionale}}$ e vale 2. Quindi la risposta alla domanda che ci siamo posti è affermativa, anche se non sappiamo quale tra $\sqrt{2}^{\sqrt{2}}$ e $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}}$ sia l'esempio giusto. Naturalmente, una volta noto il teorema precedente, abbiamo che $\sqrt{2}^{\sqrt{2}}$ è trascendente e quindi non può essere razionale.

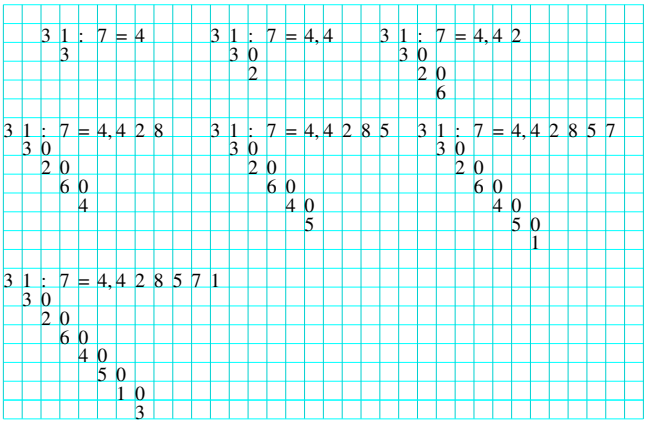

Figura 1: La costruzione della rappresentazione decimale del numero 31/7.

12 Numeri in forma decimale

Come è ben noto, un numero razionale p/q si può scrivere in forma decimale. Pensiamo ad un esempio, che servirà da guida. Eseguiamo nei dettagli la rappresentazione in forma decimale di 31/7 (v. figura 1).

Otteniamo che 31/7 si scrive come $4,428571\ldots$ e notiamo che poi, volendo continuare nella divisione, le cifre decimali si ripetono. Il motivo per cui si ripetono è che il resto che otteniamo all'ultimo passaggio dello schema riportato (cioè 3) è lo stesso resto che otteniamo al primo passaggio.

Il calcolo che abbiamo fatto nella divisione di figura 1 può essere schematizzato, per una frazione generica p/q, nel modo che segue (per comodità, supponiamo di partire da una frazione p/q positiva). Innanzitutto eseguiamo la divisione dell'intero con l'intero q:

$$p = p_0 q + r_0$$

Il resto r_0 soddisfa alla condizione $0 \leq r_0 < q$ e quindi non può più essere diviso per q, però possiamo dividere per q il numero $10\,r_0$, ottenendo:

$$10\,r_0 = a_1 q + r_1 \quad \text{con } 0 \leq r_1 < q,\ 0 \leq a_1 \leq 9$$

Quindi

$$\frac{p}{q} = p_0 + \frac{a_1}{10} + \frac{r_1}{10}$$

Continuando, dividiamo $10\,r_1$ per q, ottenendo:

$$10\,r_1 = a_2 q + r_2 \quad \text{con } 0 \leq r_2 < q,\ 0 \leq a_2 \leq 9$$

e quindi

$$\frac{p}{q} = p_0 + \frac{a_1}{10} + \frac{a_2}{100} + \frac{r_2}{100}$$

e così via, quindi possiamo scrivere

$$\frac{p}{q} = p_0 + \frac{a_1}{10} + \frac{a_2}{100} + \cdots + \frac{a_k}{10^k} + \cdots$$

Il modo usuale di scrivere questa ultima espressione è: $p = p_0, a_1a_2a_3 \ldots a_k \ldots$ e questa si dice rappresentazione decimale di p/q. È chiaro che il numero 10 (la base 10) non riveste un ruolo particolare, per cui analoghe considerazioni si possono fare per una base qualunque. È chiaro inoltre che le divisioni possono andare avanti all'infinito ma ad un certo punto si ripetono, così come accade nell'esempio di figura 1, perchè i resti $r_0, r_1, r_2, \ldots$ che via via costruiamo sono sempre numeri naturali minori di q e quindi, per il principio della piccionaia, devono ripetersi (pertanto anche i quozienti $a_1, a_2, \ldots$ ad un certo punto si ripetono).

Esempio 12.1. Questo esempio vuol mostrare un comportamento "anomalo" dei linguaggi di programmazione (nell'esempio che facciamo, il linguaggio è Java, ma si adatta anche ad altri linguaggi), per mostrare l'effetto di rappresentare numeri in differenti basi. Consideriamo le seguenti righe di codice:

```
double a = 4.35;
System.out.println(100*a);
```

La prima riga definisce una variabile (di tiplo `double`) di nome a alla quale viene assegnato il valore 4.35. La seconda riga semplicemente stampa il valore $100a$. Ci si aspetterebbe quindi che la risposta sia 435 (o, meglio, 435.0). La risposta che invece si ottiene è: 434.99999999999994. Se, per fare un'altra prova, ad a assegnamo invece ad esempio il valore 4.04, il valore che viene stampato in corrispondenza a $100a$ è 404.0, cioè è il valore corretto. La spiegazione è che il calcolatore converte i numeri in base 2. In base 2 il numero 4.35 risulta periodico, precisamente vale:
$4.35_{10} = 100.01011001100110011\ldots_2 = 100.010\overline{0011}_2$, quindi quando viene immagazzinato nella memoria del calcolatore, viene necessariamente troncato e quando si esegue il prodotto di questo numero per 100 il risultato non è più $100 \cdot 4.35$ ma 100 moltiplicato per un numero un po' minore di 4.35, da cui l'errore. Invece il numero 4.04, quando viene rappresentato in base 2, è in forma non periodica e quindi non ci sono troncature.

Se un numero $a = p/q$ si scrive in forma decimale come $p_0, a_1a_2 \ldots a_k \ldots$, è chiaro che, per ogni k vale la disuguaglianza:

$$p_0, a_1a_2 \ldots a_k \leq a < p_0, a_1a_2 \ldots a_k + \frac{1}{10^k}$$

(perché certamente $a_k/(10^k) + a_{k+1}/(10^{k+1}) + \cdots < (a_k + 1)/10^k$).

Quando si converte un numero razionale $a = p/q$ in forma decimale, si ottiene sempre un allineamento decimale periodico (eventualmente del tipo $p_0, a_1a_2 \ldots a_k\, 0\, 0\, 0 \ldots$, cioè in cui è lo zero a ripetersi infinitamente, nel qual caso si parla di allineamento decimale finito e a si indica con $p_0, a_1 \ldots a_k$). Nella

costruzione che si effettua per la conversione, non si potrà mai avere che la cifra 9 è periodica, cioè non si potrà mai avere un allineamento decimale del tipo: $p_0, a_1a_2 \ldots a_k\, 9\, 9\, 9 \ldots$. Per vedere questo, si ricordi la formula della somma di una progressione geometrica:

$$\sum_{i=0}^{n} u^i = \frac{1-u^{n+1}}{1-u} \tag{7}$$

Se avessimo una rappresentazione decimale di un numero $a = p_0, a_1a_2 \ldots a_k \ldots a_n \ldots$ del tipo: $a = p_0, a_1a_2 \ldots a_k\, 9\, 9\, 9 \ldots$, avremmo, per ogni $n > k$:

$$\begin{aligned}
p_0, a_1a_2 \ldots a_k \ldots a_n &= p_0, a_1a_2 \ldots a_k + \frac{9}{10^{k+1}} + \cdots + \frac{9}{10^n} \\
&= p_0, a_1 \ldots a_k + \frac{9}{10^{k+1}} \left(\sum_{i=0}^{n-k-1} \frac{1}{10^i} \right) \\
&= p_0, a_1 \ldots a_k + \frac{9}{10^{k+1}} \frac{1 - \left(\frac{1}{10}^{n-k}\right)}{1 - \frac{1}{10}} \\
&= p_0, a_1 \ldots a_k + \frac{1}{10^k} \left(1 - \frac{1}{10^{n-k}} \right) \\
&= p_0, a_1 \ldots a_k + \frac{1}{10^k} - \frac{1}{10^n}.
\end{aligned}$$

e quindi si dovrebbe avere:

$$p_0, a_1 \ldots a_k + \frac{1}{10^k} - \frac{1}{10^n} \leq a < p_0, a_1 \ldots a_k + \frac{1}{10^k}$$

Poiché questo dovrebbe valere per ogni $n \in \mathbb{N}$, si otterrebbe $p_0, a_1 \ldots a_k + \frac{1}{10^k} \leq a$ contraddicendo la seconda disequazione.

Può comunque tornare utile ammettere anche allienamenti del tipo $a = p_0, a_1a_2 \ldots a_k\, 9\, 9\, 9 \ldots$ (con $a_k < 9$), per essi si fa la convenzione che valgono $p_0, a_1a_2 \ldots (a_k + 1)$ (notazione coerente con il fatto che $p_0, a_1 \ldots a_k + \frac{1}{10^k} - \frac{1}{10^n}$ tende a $p_0, a_1 \ldots (a_k + 1)$ quando n tende all'infinito).

In conclusione, ad ogni allineamento decimale periodico, risulta univocamente associato un numero razionale positivo (e viceversa), analogamente si può associare ad ogni decimale periodico negativo un numero razionale negativo e in questo modo si ottiene una corrispondenza biunivoca tra i numeri razionali e gli allineamenti decimali periodici.

Sull'insieme degli allineamenti periodici (positivi e negativi) si può introdurre un ordinamento e le operazioni di somma e prodotto. Per quanto riguarda l'ordinamento, possiamo dire che dati due numeri in forma decimale periodica $a = p_0, a_1a_2 \ldots a_k \ldots$ e $b = q_0, b_1b_2 \ldots b_k \ldots$, allora $a < b$ se a è negativo e b è positivo o, se entrambi sono positivi, se $p_0 < q_0$ o, se $p_0 = q_0$, allora se $a_1 < b_1$ o, se $a_1 = b_1$, se $a_2 < b_2$ e così via (cioè l'ordinamento è definito usando l'ordinamento lessicografico sulle cifre). Se infine a e b sono entrambi negativi,

allora si pone $a < b$ se $-b < -a$. La somma e il prodotto di due numeri dati con allineamenti periodici possono essere dedotte dalle usuali operazioni di somma e prodotto dei numeri (qualche attenzione va data al fatto che si deve verificare che somma di allineamenti periodici è un allineamento periodico e analogamente per il prodotto). Senza entrare troppo nei dettagli, vediamo alcuni esempi (soltanto per il caso della somma): è chiaro che $1,44444\ldots + 3,22222\ldots$ ha per risutato $4,66666\ldots$ mentre $1,44444\ldots + 3,77777\ldots$ risulta $5,22222\ldots$. Per giustificare questo risultato, si eseguano le seguenti somme di numeri decimali finiti: $1,4 + 3,7$, poi $1,44 + 3,77$, poi $1,444 + 3,777$ ecc. Infine si noti che $1,44444\ldots + 3,55555\ldots$ risulta $4,99999\ldots$ cioè 5 e qui si vede la necessità di trattare il caso dei numeri periodici con periodo 9.

Definendo le operazioni di somma e prodotto sui numeri decimali periodici, si vede che si viene a costruire un campo che è isomorfo al campo $\mathbb{Q}$ dei numeri razionali (e quindi la definizione dei razionali con gli allineamenti decimali può essere vista come una costruzione alternativa del campo $\mathbb{Q}$ (si veda il capitolo 7.1).

Prima di trattare ad una nuova costruzione dei numeri reali, vediamo brevemente come si può passare da un numero razionale scritto nella forma di allineamento periodico alla sua rappresentazione in forma di frazione (cioè come si calcola quella che talvolta viene chiamata la *frazione generatrice* del numero decimale). Un modo per procedere, è utilizzare la formula (7). Forse qualche esempio chiarisce meglio di ogni altra cosa la costruzione:

Esempio 12.2. Sia $a = 1,\overline{3}$. Scrivere a in forma frazionaria.

$$\begin{aligned} 1,33333\ldots &= 1 + \frac{3}{10} + \frac{3}{100} + \frac{3}{1000} + \ldots \\ &= 1 + \frac{3}{10}\left(1 + \frac{1}{10} + \frac{1}{100} + \cdots\right) \\ &= 1 + \frac{3}{10}\left(\sum_{i\geq 0} \frac{1}{10^i}\right) \end{aligned}$$

La somma infinita $\sum_{i\geq 0} \frac{1}{10^i}$ si può calcolare con la formula (7) e un passaggio al limite, ottenendo il valore $\frac{10}{9}$. Pertanto $a = 1 + \frac{3}{10}\frac{10}{9} = \frac{4}{3}$.

Sia $a = 1,24\overline{35}$. Trovare la frazione generatrice di a. Possiamo procedere in modo simile. Vale:

$$\begin{aligned} 1,24353535\ldots &= \frac{124}{100} + \frac{35}{10^4} + \frac{35}{10^6} + \frac{35}{10^8} + \cdots \\ &= \frac{124}{100} + \frac{35}{10^4}\left(1 + \frac{1}{10^2} + \frac{1}{10^4} + \cdots\right) \\ &= \frac{124}{100} + \frac{35}{10000}\left(\sum_{i=0}^{\infty} \frac{1}{100^i}\right) \\ &= \frac{124}{100} + \frac{35}{10000}\frac{1}{1 - \frac{1}{100}} = \frac{124}{100} + \frac{35}{10000}\frac{100}{99} \end{aligned}$$

$$= \frac{12311}{9900}$$

C'è anche un altro modo per calcolare la frazione generatrice, che non richiede l'esplicito calcolo di un limite ed è quindi più elementare. Vediamolo applicato agli esempi di sopra: se $a = 1,\overline{3}$, allora $10\,a = 13,\overline{3}$, quindi $10\,a - a = 12$ (abbiamo fatto in modo che la parte decimale di $10\,a$ e la parte decimale di a si elidano nella differenza). Allora $a = 12/9 = 4/3$. Analogamente, per l'esempio $a = 1,24\overline{35}$, moltiplichiamo a per 10000 ed a $10000\,a$ sottraiamo $100\,a$, così da far canellare le parti decimali. Otteniamo $10000\,a - 100\,a = 12435 - 124 = 12311$, pertanto $9900\,a = 12311$ e quindi ritroviamo (ovviamente) la stessa frazione generatrice di a di prima.

Si può quindi formulare una regola per il calcolo della frazione generatrice di un numero decimale periodico. Prima di enunciarla, è opportuno introdurre un po' di nomenclatura. Si chiama *periodo* di un numero periodico il gruppo delle cifre che si ripetono. Ad esempio il periodo di $3,012401010101\ldots$ è 01. Si chiama *antiperiodo* il gruppo di cifre decimali che precedono il periodo, (potrebbe non essere presente). Nel caso di sopra, l'antiperiodo è 0124. Allora la regola per trovare la funzione generatrice si può enunciare nel modo seguente:

> al numeratore si scrive il numero naturale formato dalla parte intera del numero dato, seguita dall'antiperiodo e dal periodo e al numero così formato va sottratto il numero naturale formato dalla parte intera del numero dato seguita dall'antiperiodo; al denominatore va scritto il numero naturale formato da tante cifre 9 quante sono le cifre del periodo seguite da tante cifre 0 quante sono le cifre dell'antiperiodo.

Esercizio 12. Giustificare la regola sia seguendo il metodo usato nell'esempio 12.2, sia il metodo indicato successivamente.
Se si applica la regola al numero periodico $3,2\overline{0}$, che cosa si ottiene?
Se si applica la regola al numero periodico $4,\overline{9}$ che cosa si ottiene?
Il numero $7,\overline{123}$ può essere riscritto anche nella forma $7,12\overline{312}$. Il calcolo della frazione generatrice nei due casi dà lo stesso risultato?
Quale potrebbe essere il modo migliore per insegnare la regola descritta sopra?

12.1 I numeri reali, in forma di allienamenti decimali

In questo paragrafo, introduciamo brevemente i numeri reali usando gli allineamenti decimali. Per certi versi, questo è il modo più naturale di intendere un numero reale: il numero $\sqrt{2}$ è molto più concreto se pensato come, *circa*, $1,414213\ldots$ piuttosto che come una classe di equivalenza di una sucessione di Cauchy o una sezione (sinistra) di Dedekind. La definizione di numero reale che proproniamo ora è dunque la seguente:

Definizione 12.3. Un numero reale è una terna (σ, p, ϕ) dove σ è il segno ($+$ o $-$), $p \in \mathbb{N}$, ϕ è un'applicazione da $\mathbb{N} \setminus \{0\}$ nell'insieme di cifre $\{0, 1, \ldots, 9\}$.

La definizione è un po' macchinosa, ma esprime sostanzialmente l'idea che un numero reale può essere positivo o negativo, è fatto da una parte intera (p) ed ha infinite cifre decimali (che sono $\phi(1), \phi(2), \phi(3), \ldots$). Dunque per noi ora l'insieme dei numeri reali ha per oggetti gli elementi descritti nella definizione. Indichiamo con $\mathbf{R}$ tale insieme. Si tratta di vedere se $\mathbf{R}$ ha effettivamente le proprietà note dell'insieme dei numeri reali. Prima di tutto diciamo che due numeri reali (σ_1, p_1, ϕ_1) e (σ_2, p_2, ϕ_2) sono uguali se (ovviamente) $\sigma_1 = \sigma_2$, $p_1 = p_2$, $\phi_1 = \phi_2$. Nell'insieme $\mathbf{R}$ ritroviamo l'insieme $\mathbb{Q}$ (i cui elementi sono espressi con gli allineamenti decimali, come definito nel paragrafo precedente). In particolare, richiediamo che valga ancora la convenzione relativa all'allineamento periodico di periodo 9. L'ordinamento che poniamo su $\mathbf{R}$ è definito allo stesso modo dell'ordinamento dell'ordinamento di $\mathbb{Q}$ (sostanzialmente, è l'ordinamento lessicografico sulle cifre decimali). In particolare, l'ordinamento di $\mathbf{R}$ estende quindi quello di $\mathbb{Q}$.

Dobbiamo ora definire le operazioni di somma e prodotto in $\mathbf{R}$. Da un punto di vista "pratico", quanto fa $\sqrt{2} \cdot \sqrt{3}$? Dovremmo moltiplicare $1,4142135\ldots$ per $1.7320508\ldots$. Il prodotto di $1,41$ (che è *circa* $\sqrt{2}$) per 1.73 (che è *circa* $\sqrt{3}$) vale precisamente $2,4393$ e ci si dovrebbe aspettare che questo sia *circa* il valore del prodotto che, d'altro canto, è $\sqrt{6}$ e $\sqrt{6} = 2.449489742\ldots$. Questo esperimento mostra che se approssimiamo $\sqrt{2}$ e $\sqrt{3}$ con 2 cifre decimali, otteniamo il loro prodotto con 1 cifra decimale corretta. Ovviamente, se approssimiamo i due fattori con più cifre decimali, è naturale aspettarsi che anche il loro prodotto meglio approssimi il valore corretto. Nella seguente tabella scriviamo $\sqrt{2}$ e $\sqrt{3}$ con $3, 4, 5, 6, 7$ cifre decimali e vediamo qual è il risultato del prodotto:

$\sqrt{2}$	$\sqrt{3}$	prodotto
1,414	1,732	2,449$\underline{0}$48
1,4142	1,7320	2,449$\underline{3}$9440
1,41421	1,73205	2,449$\underline{4}$824305
1,414213	1,732050	2,449$\underline{4}$87626650
1,4142135	1,7320508	2.449$\underline{4}$8962404580

Si tratta dunque di formalizzare questo procedimento. Consideriamo una successione $(a_n)_n$ di numeri (non negativi) dati con allineamenti decimali:

$$\begin{array}{lcl} a_0 & = & \alpha_{00}, \alpha_{01}\alpha_{02}\alpha_{03}\ldots \\ a_1 & = & \alpha_{10}, \alpha_{11}\alpha_{12}\alpha_{13}\ldots \\ a_2 & = & \alpha_{20}, \alpha_{21}\alpha_{22}\alpha_{23}\ldots \\ \ldots & & \ldots \end{array} \tag{8}$$

e consideriamo la matrice infinita costituita dagli α_{ij} (che, ricordiamo, sono numeri interi e, se il secondo indice è maggiore di 0, sono compresi tra 0 e 9).

Definizione 12.4. Se per ogni $k \geq 0$ la successione di interi $(\alpha_{nk})_n$ fatta con la colonna k–ima è definitivamente costante, allora la successione $(a_n)_n$ si dice *stabilizzata*.

Se in particolare guardiamo la colonna "prodotto" della tabella scritta sopra, vediamo che in effetti la successione di numeri sembra stabilizzarsi: ad esempio

le quarte cifre decimali dei numeri della successione (evidenziate dalla sottolineatura) sono: $0, 3, 4, 4, 4$ e sembra quindi essere (l'inizio di) una successione definitivamente costante (a 4), così la successione delle quinte cifre decimali è $4, 9, 8, 8, 8$ e sembra anch'essa essere definitivamente costante.

Se la successione $(a_n)_n$ è stabilizzata, individua un unico numero reale γ dato da $\gamma_0, \gamma_1\gamma_2\gamma_3\ldots$, dove γ_i è il valore definitivamente costante della successione $(\alpha_{ni})_n$. Per dire che la successione $(a_n)_n$ si stabilizza e individua il numero reale γ, scriveremo $a_n \rightsquigarrow \gamma$.

Lemma 12.5. *Sia $(a_n)_n$ una successione di numeri reali (elementi di $\mathbf{R}$) non negativi, non decrescente (cioè $a_n \leq a_{n+1}$ per ogni n) e superiormente limitata (da un numero $M \in \mathbf{R}$). Allora $(a_n)_n$ è stabilizzata, cioè $a_n \rightsquigarrow \gamma$ e inoltre $a_n \leq \gamma \leq M$.*

Dimostrazione. Supponiamo che la successione $(a_n)_n$ sia sempre rappresentata dalla formula (8). Ogni a_n è minore di M, pertanto ogni numero decimale $\alpha_{n0}, \alpha_{n1}\alpha_{n2}\ldots\alpha_{nk}$ è minore di M. La successione $\alpha_{00}, \alpha_{01}, \alpha_{02}, \ldots$ è una successione di numeri naturali non decrescenti e superiormente limitata (da M), quindi deve stabilizzarsi. Supponiamo ora che si siano stabilizzate le cifre fino alla k–ima e vediamo che si deve stabilizzare anche la $k+1$–ima. Quindi supponiamo che esista un n_k sufficientemente grande per cui si abbia

$$a_n = \gamma_0, \gamma_1 \ldots \gamma_k \alpha_{n\,k+1}\alpha_{n\,k+2}\ldots$$

per ogni $n > n_k$. Allora i numeri $\gamma_0, \gamma_1 \ldots \gamma_k\alpha_{n\,k+1}$ hanno la parte intera e le prime k cifre decimali tutte uguali per ogni $n > n_k$ e sono non decrescenti e quindi la $k+1$–ima cifra decimale deve stabilizzarsi ad un valore γ_{k+1}. Inoltre $\gamma_0, \gamma_1 \ldots \gamma_{k+1} \leq M$. Questo prova che $a_n \rightsquigarrow \gamma$. Resta da vedere che $a_n \leq \gamma$. Ma se esistesse un m tale che $a_m > \gamma$, allora avremmo (assumendo che in a_m si siano stabilizzate le prime k cifre): $\gamma_0, \gamma_1 \ldots \gamma_k\alpha_{m\,k+1}\ldots > \gamma_0, \gamma_1 \ldots \gamma_k\gamma_{k+1}\ldots$ e dovrebbe essere $\alpha_{m\,k+1} > \gamma_{k+1}$, ma allora, scelto un $m_1 > m$ tale che a_{m_1} abbia stabilizzato anche la cifra $k+1$, necessariamente al valore γ_{k+1}, avremmo $a_m > a_{m_1}$ e questo contraddirebbe il fatto che $(a_n)_n$ è non decrescente. □

Una conseguenza del lemma è la possibilità di definire le operazioni di somma e prodotto sull'insieme $\mathbf{R}$.

Partiamo da due numeri reali non negativi in forma decimale:

$$a = p, \alpha_1\alpha_2\ldots, \qquad b = q, \beta_1\beta_2\ldots$$

e consideriamo i numeri razionali in forma decimale ottenuti da a e b troncando le cifre dopo n:

$$a^{(n)} = p, \alpha_1 \ldots \alpha_n\, 0\, 0\, 0\, \ldots, \qquad b^{(n)} = q, \beta_1 \ldots \beta_n\, 0\, 0\, 0 \ldots$$

Si osservi che le successioni di numeri razionali:

$$\left(a^{(n)} + b^{(n)}\right)_n \text{ e } \left(a^{(n)} \cdot b^{(n)}\right)_n$$

(che si sanno calcolare in quanto si tratta di fare somme e prodotti di numeri razionali) sono non decrescenti e limitate superiormente (la prima è limitata superiormente da $p+1+q+1 = p+q+2$, la seconda da $(p+1)(q+1)$) e quindi, per il lemma, sono stabilizzate. Allora individuano due numeri reali, σ, π:

$$a^{(n)} + b^{(n)} \rightsquigarrow \sigma, \qquad a^{(n)} \cdot b^{(n)} \rightsquigarrow \pi$$

In questo modo abbiamo definito una somma e un prodotto tra gli elementi non negativi di $\mathbf{R}$. In modo simile, anche se con qualche ulteriore precauzione, si può estendere la somma e il prodotto a tutti gli elementi di $\mathbf{R}$. Si tratta poi di verificare che con queste operazioni $\mathbf{R}$ diventa un campo ordinato, verifica che, per essere completata, richiederebbe molti conti tediosi ma del tutto naturali (che quindi omettiamo). Vediamo invece che $\mathbf{R}$ è archimedeo: fissiamo due elementi $a, b \in \mathbf{R}$ $a > 0$, $b > 0$. Sia $b = b_0, b_1 b_2 \ldots$. Supponiamo che $b_i = 0$ per ogni $i < k$ e $b_k \neq 0$ (e quindi $b_k > 0$). Allora la cifra di posto k di $b + b$ sarà o $b_k + b_k$ (se $b_k + b_k \leq 9$) e tutte le cifre prima sono 0 oppure la cifra di posto $k-1$ di $b+b$ sarà 1. Se la $k-1$–ima cifra di $b+b$ è zero, calcoliamo $b+b+b$ e procediamo così finché non otteniamo che tale cifra è non nulla. Procedendo in questo modo possiamo quindi ottenere un multiplo nb grande quanto vogliamo, in particolare possiamo ottenere $nb > a$.

Per completare la costruzione dei numeri reali seguendo l'approccio proposto in questo paragrafo, dobbiamo ancora far vedere che il campo $\mathbf{R}$ così costruito è completo. Ricordando la proposizione 10.2, si deve far vedere, per esempio, che ogni sottoinsieme di $\mathbf{R}$, non vuoto e superiormente limitato, ammette estremo superiore. Omettiamo qui la dimostrazione (che ricalca ragionamenti già fatti).

Possiamo quindi finalmente concludere che l'insieme $\mathbf{R}$ qui costruito è un campo ordinato archimedeo completo, quindi $\mathbf{R} = \mathbb{R}$.

La rappresentazione dei numeri reali in forma decimale permette di dimostrare facilmente un risultato molto importante relativo alla cardinalità di $\mathbb{R}$. Si ricordi (Definizione 6.19) che un insieme si dice infinito numerabile se è in biiezione con $\mathbb{N}$.

Teorema 12.6. *L'insieme $\mathbb{R}$ dei numeri reali è un insieme infinito ma non numerabile.*

Dimostrazione. Si noti che $\mathbb{R}$ è in biiezione con l'intervallo aperto $]0,1[$ (la funzione $\tan(2\pi x - \pi)$ può dare un esempio di biiezione), mentre, banalmente, l'insieme $\mathbb{N}$ è in biiezione con $\mathbb{N} \setminus \{0\}$, quindi per provare che $\mathbb{R}$ non è numerabile, basta provare che l'intervallo $]0,1[$ non è in biiezione con $\mathbb{N} \setminus \{0\}$. Supponiamo ci sia allora un'applicazione biiettiva tra $\mathbb{N} \setminus \{0\}$ e l'intervallo, quindi possiamo elencare gli elementi di $]0,1[$ con $a_1, a_2, \ldots$ I numeri $a_1, a_2, \ldots$ possono essere scritti in forma decimale ed elencati nel seguente modo:

$$\begin{array}{rcl} a_1 & = & 0.\alpha_{11}\alpha_{12}\alpha_{13}\ldots \\ a_2 & = & 0.\alpha_{21}\alpha_{22}\alpha_{23}\ldots \\ a_3 & = & 0.\alpha_{31}\alpha_{32}\alpha_{33}\ldots \\ \ldots & & \ldots \end{array}$$

Consideriamo allora il numero reale d dato da:

$$d = 0.\delta_1\delta_2\delta_3\ldots$$

dove la cifra δ_1 è un numero naturale diverso da α_{11} e da 9, δ_2 è un numero naturale diverso da α_{22} e da 9, e, in generale, δ_i è scelto diverso da α_{ii} e 9. Pertanto d è un numero reale incluso nell'intervallo $]0, 1[$, quindi deve essere uno dei numeri a_k ma non può esserlo perché la k-ima cifra decimale di d e di a_k sono diverse. □

La dimostrazione ora esposta, di solito indicata con il nome di "metodo diagonale di Cantor" è stata pubblicata da Cantor nel 1891.

13 Frazioni continue

Consideriamo un numero razionale, ad esempio $\frac{73}{30}$. Abbiamo visto come rappresentarlo in forma decimale: si esegue la divisione euclidea tra i due numeri interi dati dal numeratore e denominatore $73 = 2 \cdot 30 + 13$ dove il resto $r = 13$ soddisfa alla condizione $0 \leq r < 30$ e quindi non può più essere diviso per 30. Allora si moltiplica per la base 10 e il risultato si divide nuovamente per 30. Proseguendo in questo modo si ottiene, come visto, la rappresentazione della frazione in forma decimale. Ora seguiamo un percorso simile. Dalla divisione otteniamo $73/30 = 2+13/30$. La frazione $13/30$ si può anche scrivere $1/(30/13)$ e da questa scrittura otteniamo la frazione $30/13$ in cui il numeratore è più grande del denominatore e quindi può essere ulteriormente diviso. Possiamo allora scrivere $30 = 2 \cdot 13 + 4$ e quindi $30/13 = 2 + 4/13$. Otteniamo allora la seguente espressione per $30/13$:

$$\frac{30}{13} = 2 + \frac{1}{2 + \frac{4}{13}} \tag{9}$$

Naturalmente si può andare avanti ancora. Riassumiamo i risultati:

$$\frac{30}{13} \;=\; 2 + \frac{13}{30} \;=\; 2 + \frac{1}{2 + \frac{4}{13}} \;=\; 2 + \frac{1}{2 + \frac{1}{3 + \frac{1}{4}}}$$

Se volessimo ancora continuare con le divisioni, dovremmo scrivere $1/4 = 1/(4/1)$, e quindi dovremmo effettuare la divisione di 4 per 1 comporta $4 = 4 \cdot 1 + 0$. Oltre quindi non si potrebbe andare. L'ultima espressione che abbiamo ottenuto nella formula (9) si dice *frazione continua*. I numeri $2, 2, 3, 4$, cioè i numeri interi che sono sommati alle varie frazioni, si dicono i *termini* della frazione continua. Riassumiamo le divisioni euclidee che abbiamo effettuato:

$$\begin{aligned} 73 &= 2 \cdot 30 + 13 \\ 30 &= 2 \cdot 13 + 4 \\ 13 &= 3 \cdot 4 + 1 \\ 4 &= 4 \cdot 1 + 0 \end{aligned}$$

Se proviamo ora a calcolare il massimo comun divisore di 73 e 30 ci accorgiamo che dobbiamo effettuare proprio le stesse divisioni elencate qui sopra. Vi è quindi uno stretto legame tra la conversione di un numero razionale a/b in frazione continua e l'algoritmo di Euclide per il calcolo del massimo comun divisore tra i numeri a e b. In particolare, il calcolo che abbiamo seguito per convertire un numero razionale in frazione continua deve terminare dopo un numero finito di passi.

Generalizzando l'esempio, possiamo quindi affermare che dato un qualunque numero razionale a/b (che assumiamo positivo) esistono dei numeri naturali

$q_0, q_1, \ldots, q_n$ tali che

$$\frac{a}{b} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}} \tag{10}$$

Per semplificare la notazione, si scrive anche:

$$\frac{a}{b} = q_0 + \frac{1}{q_1+}\,\frac{1}{q_2+}\cdots\frac{1}{q_{n-1}+}\,\frac{1}{q_n} \tag{11}$$

Consideriamo ora la formula (10) (o la (11)) per alcuni valori di n. Per avere risultati più generali, conviene ora assumere che $q_0, q_1, \ldots$ siano variabili, non necessariamente numeri naturali. Se $n = 1$ o $n = 2$ otteniamo, rispettivamente:

$$q_0 + \frac{1}{q_1} = \frac{q_0 q_1 + 1}{q_1}, \qquad q_0 + \frac{1}{q_1+}\,\frac{1}{q_2} = \frac{q_0 q_1 q_2 + q_0 + q_2}{q_1 q_2 + 1}$$

Se $n = 3$, invece:

$$q_0 + \frac{1}{q_1+}\,\frac{1}{q_2+}\,\frac{1}{q_3} = \frac{q_0 q_1 q_2 q_3 + q_0 q_1 + q_0 q_3 + q_2 q_3 + 1}{q_1 q_2 q_3 + q_1 + q_3}$$

Ovviamente si può continuare. Indichiamo con $[q_0, q_1, \ldots, q_n]$ il numeratore che si ottiene da (10). Dai tre casi specifici trattati, abbiamo:

$$\begin{aligned} [q_0] &= q_0 \\ [q_0, q_1] &= q_0 q_1 + 1 \\ [q_0, q_1, q_2] &= q_0 q_1 q_2 + q_0 + q_2 \\ [q_0, q_1, q_2, q_3] &= q_0 q_1 q_2 q_3 + q_0 q_1 + q_0 q_3 + q_2 q_3 + 1. \end{aligned} \tag{12}$$

(la prima uguaglianza è stata aggiunta perché sarà utile in futuro). Si osserva che, nei tre casi trattati, il denominatore che si ottiene dalla conversione di (10) (o (11)) in frazione, vale $[q_1, \ldots, q_n]$. Questo è vero in generale, in quanto, come si vede osservando la formula (11), si ha:

$$q_0 + \frac{1}{q_1+}\,\frac{1}{q_2+}\cdots\frac{1}{q_{n-1}+}\,\frac{1}{q_n} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2+}\cdots\cfrac{1}{q_n}} \tag{13}$$

Pertanto il numeratore di $q_1 + \frac{1}{q_2+}\cdots\frac{1}{q_n}$ vale $[q_1, \ldots, q_n]$ e questo diventa il denominatore di $q_0 + \frac{1}{q_1+}\cdots\frac{1}{q_n}$. Quindi:

$$q_0 + \frac{1}{q_1+}\,\frac{1}{q_2+}\cdots\frac{1}{q_{n-1}+}\,\frac{1}{q_n} = \frac{[q_0, q_1, \ldots, q_n]}{[q_1, q_2, \ldots, q_n]} \tag{14}$$

Sempre da (13) si ottiene quindi:

$$\frac{[q_0, q_1, \ldots, q_n]}{[q_1, q_2, \ldots, q_n]} = q_0 + \frac{1}{\dfrac{[q_1, q_2, \ldots, q_n]}{[q_2, \ldots, q_n]}}$$

da cui si ricava la formula:

$$[q_0, q_1, \ldots, q_n] = q_0[q_1, \ldots, q_n] + [q_2, \ldots, q_n] \tag{15}$$

che permette di definire ricorsivamente l'espressione $[q_0, q_1, \ldots, q_n]$. La formula vale per $n \geq 2$, ma, se per $n = 1$ poniamo $[q_2, \ldots, q_n] = 1$, vediamo che la formula vale anche per $n = 1$.

Esempio 13.1. Consideriamo la frazione continua data da

$$3 + \frac{1}{4+}\,\frac{1}{3+}\,\frac{1}{5+}\,\frac{1}{6}$$

In questo esempio, $[q_0, \ldots, q_n]$ vale $[3, 4, 3, 5, 6]$. Quindi $[5, 6] = 5 \cdot [6] + 1 = 5 \cdot 6 + 1 = 31$, allora $[3, 5, 6] = 3 \cdot [5, 6] + [6] = 3 \cdot 31 + 6 = 99$, continuando: $[4, 3, 5, 6] = 4 \cdot [3, 5, 6] + [5, 6] = 4 \cdot 99 + 31 = 427$ e $[3, 4, 3, 5, 6] = 3 \cdot [4, 3, 5, 6] + [3, 5, 6] = 3 \cdot 427 + 99 = 1380$. Analogamente si trova che $[q_1, q_2, \ldots, q_n]$ vale $[4, 3, 5, 6] = 427$, quindi la frazione continua considerata vale $\frac{1380}{427}$. Naturalmente, se partiamo da quest'ultima frazione e calcoliamo come visto con le divisioni successive la frazione continua, torniamo all'espressione scritta all'inizio dell'esempio.

Le formule (12) mostrano una regolarità nelle espressioni $[q_0, \ldots, q_n]$ che potrebbe essere utile per un calcolo più rapido. La regola è stata formulata da Eulero. Si devono considerare le coppie di elementi consecutivi, cioè della forma q_i, q_{i+1}. La regola di Eulero dice che per calcolare $[q_0, \ldots, q_n]$ si deve calcolare il prodotto $q_0 \cdots q_n$ a cui vanno sommati tutti i prodotti $q_0 \cdots q_n$ a cui vanno tolte, in tutti i modi, tutte le coppie consecutive, poi vanno sommati ancora tutti i prodotti $q_0 \cdots q_n$ a cui vanno tolte in tutti i modi due coppie consecutive a cui vanno sommati i prodotti $q_0 \cdots q_n$ a cui vanno tolte in tutti i modi tre coppie consecutive e così via. Se n è dispari e quindi $n + 1$ è pari, si conviene che all'ultimo passaggio, quando si tolgono tutte le $(n+1)/2$ coppie consecutive al prodotto $q_0 \cdots q_n$, si debba scrivere il valore 1.

Esempio 13.2. Se $n = 3$ otteniamo:

$$\begin{aligned}[q_0, q_1, q_2, q_3] &= q_0q_1q_2q_3 + \cancel{q_0q_1}q_2q_3 + q_0\cancel{q_1q_2}q_3 + q_0q_1\cancel{q_2q_3} + \cancel{q_0q_1}\cancel{q_2q_3} \\ &= q_0q_1q_2q_3 + q_2q_3 + q_0q_3 + q_2q_3 + 1\end{aligned}$$

Se $n = 4$ otteniamo:

$$\begin{aligned}[q_0, q_1, q_2, q_3, q_4] &= q_0q_1q_2q_3q_4 + \cancel{q_0q_1}q_2q_3q_4 + q_0\cancel{q_1q_2}q_3q_4 + q_0q_1\cancel{q_2q_3}q_4 + \\ &\quad + q_0q_1q_2\cancel{q_3q_4} + \cancel{q_0q_1}\cancel{q_2q_3}q_4 + \cancel{q_0q_1}q_2\cancel{q_3q_4} + q_0\cancel{q_1q_2}\cancel{q_3q_4} \\ &= q_0q_1q_2q_3q_4 + q_2q_3q_4 + q_0q_3q_4 + q_0q_1q_4 + q_4 + q_2 + q_0\end{aligned}$$

La regola di Eulero si dimostra per induzione. Se $n = 1, 2, 3$ è vera perché è confermata dalle formule (12). Supponiamo sia vera per $n > 3$ e vediamo che vale per $n + 1$. Useremo la formula (15). Consideriamo lo sviluppo di $[q_2, \ldots, q_n]$ con la formula di Eulero. È la somma di tutti i fattori $q_2 \cdots q_n$ a cui vengono tolte k coppie consecutive (con $k = 1, 2, \ldots$). Questi sono esattamente i fattori di $q_0 \cdots q_n$ a cui vengono tolte $k + 1$ coppie consecutive tali che la prima coppia sia sempre costituita da $q_0 q_1$. Poi consideriamo $q_0[q_1, \ldots, q_n]$ e sviluppiamo $[q_1, \ldots, q_n]$ con la formula di Eulero. Otteniamo la somma di tutti i fattori di $q_0 \cdot q_1 \cdots q_n$ a cui vengono tolte k coppie consecutive con l'accortezza di non togliere mai la prima coppia $q_0 q_1$ (con $k = 1, 2, \ldots$). In questo modo, ricordando la formula (15),vediamo che $[q_0, \ldots, q_n]$ si ottiene proprio nel modo stabilito dalla formula di Eulero.

Una conseguenza della formula di Eulero è che $[q_0, \ldots, q_n]$ non cambia se i termini vengono scritti in ordine opposto:

$$[q_0, q_1, \ldots, q_n] = [q_n, q_{n-1}, \ldots, q_0]$$

Da questo fatto segue subito che, analogamente alla formula (15), abbiamo anche:

$$[q_0, q_1, \ldots, q_n] \quad = \quad q_n[q_0, \ldots, q_{n-1}] + [q_0, \ldots, q_{n-2}] \tag{16}$$

13.1 Convergenti

Consideriamo una frazione continua:

$$q_0 + \frac{1}{q_1+}\,\frac{1}{q_2+}\cdots\frac{1}{q_n} \tag{17}$$

Da essa si possono ottenere le seguenti frazioni continue:

$$q_0, \quad q_0 + \frac{1}{q_1}, \quad q_0 + \frac{1}{q_1+}\,\frac{1}{q_2}, \cdots$$

(ottenute prendendo i primi addendi della frazione continua iniziale). Queste frazioni continue si dicono i *convergenti* di (17). Il convergente m-imo (con $m \leq n$) vale:

$$q_0 + \frac{1}{q_1+}\,\frac{1}{q_2+}\cdots\frac{1}{q_m} = \frac{[q_0, \ldots, q_m]}{[q_1, \ldots, q_m]}$$

L'uguaglianza deriva dalla formula (14). Poniamo

$$A_m = [q_0, \ldots, q_m], \qquad B_m = [q_1, \ldots, q_m]$$

I primi valori per A_m e B_m sono: $A_0 = q_0$, $A_1 = q_0q_1 + 1$, $B_0 = 1$, $B_1 = q_1$. Dalla formula (16) segue quindi:

$$A_m = q_mA_{m-1} + A_{m-2}, \qquad B_m = q_mB_{m-1} + B_{m-2} \tag{18}$$

Proposizione 13.3. *Vale la seguente relazione:*

$$A_mB_{m-1} - B_mA_{m-1} = (-1)^{m-1} \tag{19}$$

Dimostrazione. Poniamo $C_m = A_mB_{m-1} - B_mA_{m-1}$. Vale: $C_1 = A_1B_0 - B_1A_0 = 1$, inoltre, usando le relazioni (18), abbiamo:

$$\begin{aligned} C_m &= (q_mA_{m-1} + A_{m-2})B_{m-1} - (q_mB_{m-1} + B_{m-2})A_{m-1} \\ &= A_{m-2}B_{m-1} - B_{m-2}A_{m-1} \;=\; -C_{m-1} \end{aligned}$$

da questa relazione, abbiamo quindi $C_m = -C_{m-1} = C_{m-2} = \cdots = \pm C_1$ (se m è pari, il segno vale $-$, se m è dispari, il segno vale $+$), quindi $C_m = (-1)^{m-1}$. □

Una conseguenza della proposizione 13.3 è che A_m e B_m non possono avere fattori comuni (sia se i $q_0, q_1, \ldots$ sono pensati come variabili, sia nel caso in cui siano numeri interi) perché un fattore comune ad A_m e B_m dovrebbe dividere anche 1. In particolare, la frazione A_m/B_m è sempre ridotta ai minimi termini (per ogni $m = 0, 1, \ldots, n$). Dalla formula (19), dividendo per B_mB_{m-1}, si ottiene:

$$\frac{A_m}{B_m} - \frac{A_{m-1}}{B_{m-1}} = \frac{(-1)^{m-1}}{B_mB_{m-1}} \tag{20}$$

Supponiamo ora di partire da un numero razionale a/b e costruire la frazione continua associata che avrà la forma (17) dove q_0 è un numero intero e $q_1, q_2, \ldots$ sono numeri naturali non nulli. Dalla formula (18) segue che $B_0, B_1, B_2, \ldots$ sono numeri naturali strettamente crescenti. Vediamo ora come si posizionano sulla retta reale i convergenti A_m/B_m.

Proposizione 13.4. *Sia a/b un numero razionale e siano A_0/B_0, A_1/B_1, $\ldots, A_n/B_n = a/b$ i convergenti della frazione continua ottenuta da a/b. Allora vale:*

$$\frac{A_0}{B_0} < \frac{A_2}{B_2} \cdots < \frac{A_n}{B_n} = \frac{a}{b} < \cdots < \frac{A_3}{B_3} < \frac{A_1}{B_1}.$$

Dimostrazione. Dalla formula (20) segue che, se m è dispari, $(-1)^{m-1}$ vale 1, quindi $A_m/B_m = A_{m-1}/B_{m-1} + \varepsilon$, dove $\varepsilon = 1/(B_m B_{m-1})$ è un numero positivo, quindi $A_{m-1}/B_{m-1} < A_m/B_m$. Viceversa, se m è pari, $A_m/B_m < A_{m-1}/B_{m-1}$. Supponiamo ora m dispari. Sempre da (20) abbiamo che

$$\frac{A_m}{B_m} - \frac{A_{m-1}}{B_{m-1}} = \frac{1}{B_m B_{m-1}} \quad \text{e} \quad \frac{A_{m-1}}{B_{m-1}} - \frac{A_{m-2}}{B_{m-2}} = \frac{-1}{B_{m-1} B_{m-2}}.$$

Sommando membro a membro, otteniamo:

$$\frac{A_m}{B_m} - \frac{A_{m-2}}{B_{m-2}} = \frac{B_{m-2} - B_m}{B_m B_{m-1} B_{m-2}}$$

Poiché, per (18), $B_m - B_{m-2} = q_m B_{m-1}$, otteniamo:

$$\frac{A_m}{B_m} - \frac{A_{m-2}}{B_{m-2}} = -\frac{q_m}{B_m B_{m-2}}$$

e quindi, se m è dispari, $A_{m-2}/B_{m-2} < A_m B_m$. Similmente si prova che $A_{m-2}/B_{m-2} > A_m B_m$ se m è pari. □

Esempio 13.5. Consideriamo il numero razionale 323/224. Espresso in frazione continua, diventa:

$$\frac{323}{224} = 1 + \frac{1}{2+}\,\frac{1}{3+}\,\frac{1}{1+}\,\frac{1}{4+}\,\frac{1}{5}$$

quindi i suoi termini sono 1, 2, 3, 1, 4, 5 e i suoi convergenti sono:

$$1,\ \tfrac{3}{2},\ \tfrac{10}{7},\ \tfrac{13}{9},\ \tfrac{62}{43},\ \tfrac{323}{224},$$

i cui valori, in cifre decimali, sono approssimativamente:

$$1.000,\ 1.5000,\ 1.4286,\ 1.4444,\ 1.4419,\ 1.4420$$

e, come si vede facilmente, oscillano a destra e a sinistra del valore finale che è 323/224.

13.2 Frazioni continue infinite

Innanzitutto ricordiamo una definizione: la *parte intera* di un numero α è quel numero intero q_0 tale che $\alpha' = \alpha - q_0$ sia compreso tra 0 e 1 (1 escluso). Ad esempio la parte intera di $3,524$ è 3, la parte intera di $-3,524$ è -4.

Fino ad ora abbiamo considerato frazioni continue ottenute a partire da numeri razionali e si è visto che sono sempre finite (cioè i termini $q_0, q_1, \ldots$ sono in numero finito). La costruzione seguita per ottenere una frazione continua a partire da un numero razionale è basata sull'algoritmo euclideo di divisione. Se riprendiamo l'esempio considerato nella sezione 13 (lo sviluppo in frazione continua del numero razionale $73/30$), vediamo che al primo passo calcoliamo la parte intera di $73/30$ (che è $q_0 = 2$) e quindi possiamo scrivere $73/30 = 2 + \alpha'$ dove $0 \leq \alpha' < 1$ (nell'esempio, $\alpha' = 13/30$). Essendo $\alpha' < 1$, il suo reciproco sarà più grande di 1, pertanto sarà costituito da una parte intera q_1 (che nel nostro esempio vale 2) e possiamo quindi scrivere $1/\alpha' = q_1 + \alpha''$ dove $0 \leq \alpha'' < 1$. Mettendo assieme i dati finora calcolati, otteniamo:

$$\frac{73}{30} = 2 + \frac{1}{2 + \alpha''}$$

e così via. In questa variante, la costruzione non richiama più esplicitamente l'algoritmo di Euclide e possiamo quindi ripeterla per un qualunque numero reale α. Riassumiamola:
1) Scriviamo $\alpha = q_0 + \alpha'$ dove $q_0 \in \mathbb{Z}$ è la parte intera di α e $0 \leq \alpha' < 1$.
2) Se α' vale 0 ci fermiamo, altrimenti consideriamo il suo reciproco ($\alpha_1 = 1/\alpha'$) che è maggiore di 1 e quindi è della forma $q_1 + \alpha''$, dove q_1 è la parte intera di α_1 (e, essendo $\alpha_1 > 1$, $q_1 \in \mathbb{N} \setminus \{0\}$) e $0 \leq \alpha'' < 1$.
3) Se $\alpha'' = 0$ ci fermiamo, altrimenti consideriamo il suo reciproco $\alpha_2 = 1/\alpha''$ e quindi sarà $\alpha_2 = q_2 + \alpha'''$ con $q_2 \in \mathbb{N} \setminus \{0\}$ e $0 \leq \alpha''' < 1$, e così via.

Veniamo così a costruire le seguenti frazioni continue che hanno tutte per valore α:

$$q_0 + \frac{1}{\alpha_1}, \quad q_0 + \cfrac{1}{q_1 + \cfrac{1}{\alpha_2}}, \qquad q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\alpha_3}}}, \quad \cdots$$

Se ci fermiamo dopo n passi, otteniamo:

$$\alpha = q_0 + \frac{1}{q_1+}\,\frac{1}{q_2+}\,\cdots\frac{1}{q_n+}\,\frac{1}{\alpha_{n+1}} \tag{21}$$

dove, come detto, $q_0, q_1, \ldots, q_n$ sono numeri interi, con $q_1, \ldots, q_n > 1$.

Osservazione 13.6. Se il numero α da cui partiamo è razionale, la costruzione, come è noto, deve fermarsi e in effetti ciò accade perché ad un certo passo i otterremo $\alpha_i = q_i + 0$ (cioè α_i sarà un numero intero). Se invece il numero da cui partiamo è irrazionale, non potrà mai succedere che un α_i sia intero (perché vorrebbe dire che α è uguale ad una frazione continua finita ma quest'ultima

è sempre un numero razionale) e quindi si può continuare con la costruzione all'infinito.
Infine, nel caso che α sia razionale e quindi ottenibile come frazione continua finita con termini $q_0, q_1, \ldots, q_n$, si potrà sempre assumere che q_n sia maggiore di 1 (infatti, se q_n fosse 1, avremmo che la frazione continua si può ottenere con i termini $q_0, q_1, \ldots, (q_{n-1}+1)$).

Anche se α è un numero irrazionale, la frazione continua data da (21) è una frazione continua finita, quindi per essa valgono tutti quei risultati ottenuti nei paragrafi precedenti. In particolare possiamo considerare i convergenti:

$$\frac{A_0}{B_0} = q_0, \quad \frac{A_1}{B_1} = q_0 + \frac{1}{q_1}, \quad \frac{A_2}{B_2} = q_0 + \frac{1}{q_1 +}\,\frac{1}{q_2}, \cdots \tag{22}$$

ed essi soddisfano alle condizioni (18) e (19). La formula (21) si può anche esprimere, usando la formula (14),

$$\alpha = \frac{[q_0, q_1, \ldots, q_n, \alpha_{n+1}]}{[q_1, \ldots, q_n, \alpha_{n+1}]}$$

Usando la (16), otteniamo che il numeratore di sopra vale: $\alpha_{n+1}A_n + A_{n-1}$ e il denominatore vale $\alpha_{n+1}B_n + B_{n-1}$, pertanto:

$$\alpha = \frac{\alpha_{n+1}A_n + A_{n-1}}{\alpha_{n+1}B_n + B_{n-1}} \tag{23}$$

Come si diceva, la costruzione dei convergenti partendo da un numero irrazionale α può proseguire all'infinito, si viene così a costruire una successione di numeri razionali $A_0/B_0, A_1/B_1, A_2/B_2, \ldots$ che è strettamente legata con il numero α. Più precisamente, vale:

Teorema 13.7. *La successione $(A_n/B_n)_n$ dei convergenti di un numero irrazionale α converge ed ha per limite il numero α stesso.*

Dimostrazione. Per verificare che il limite della successione $(A_n/B_n)_n$ vale α, dobbiamo stimare il valore di $|\alpha - A_n/B_n|$. Usando la formula (23) e la formula (19) abbiamo:

$$\begin{aligned}\left|\alpha - \frac{A_n}{B_n}\right| &= \left|\frac{\alpha_{n+1}A_n + A_{n-1}}{\alpha_{n+1}B_n + B_{n-1}} - \frac{A_n}{B_n}\right| \\ &= \left|\frac{A_{n-1}B_n - B_{n-1}A_n}{B_n(\alpha_{n+1}B_n + B_{n-1})}\right| = \left|\frac{\pm 1}{B_n(\alpha_{n+1}B_n + B_{n-1})}\right|\end{aligned}$$

Ovviamente il ± 1, essendo dentro al valore assoluto, può essere omesso, inoltre $\alpha_{n+1} > q_{n+1}$ (si ricordi che q_{n+1} è la parte intera di α_{n+1}), allora otteniamo:

$$\left|\alpha - \frac{A_n}{B_n}\right| < \frac{1}{B_n B_{n+1}}. \tag{24}$$

I numeri $B_0, B_1, \ldots$ sono una successione di numeri naturali positivi strettamente crescenti (come si vede subito, per esempio dalla formula (18)), quindi, scegliendo n sufficientemente grande, la frazione $1/(B_n B_{n+1})$ può essere resa piccola quanto si vuole e questo prova che la successione dei convergenti tende al limite α. □

14 Ancora sulle frazioni continue infinite

Si è visto che partendo da un numero irrazionale α si ottiene una frazione continua infinita i cui termini sono numeri interi $q_0, q_1, q_2, \ldots$ (con $q_i > 1$ se $i = 1, 2, \ldots$). Ci si può ora chiedere se vale anche il viceversa, se cioè, fissata una successione di numeri interi positivi (tranne il primo, che può essere anche negativo o nullo) si può dare un significato alla frazione continua che da essi si può scrivere. Vale il:

Teorema 14.1. *Siano $q_0, q_1, q_2, \ldots \in \mathbb{Z}$, con $q_1, q_2, \ldots > 1$ Consideriamo le frazioni continue finite corrispondenti, esprimibili con la formula (22). Allora la successione $(A_n/B_n)_n$ ha un limite finito α e la frazione continua associata ad α ha per termini proprio $q_0, q_1, \ldots$*

Prima di passare alla dimostrazione, richiamiamo un ben noto risultato sulle successioni reali monotone crescenti: se $(a_n)_n$ è una successione monotona crescente e superiormente limitata, allora essa è convergente (la dimostrazione è immediata, considerando l'insieme A fatto dagli elementi della successione. L'insieme A non è vuoto ed è superiormente limitato, quindi, per la completezza di $\mathbb{R}$, ammette estremo superiore. Si verifica facilmente che tale estremo superiore è il limite di $(a_n)_n$). Un risultato del tutto analogo vale per le successioni monotone decrescenti inferiormente limitate. Passiamo ora alla dimostrazione del teorema:

Dimostrazione. Consideriamo i convergenti di indice pari: $A_0/B_0, A_2/B_2, \ldots$. Essi formano una successione crescente (come conseguenza della proposizione 13.4) ed è superiormente limitata (per esempio da A_1/B_1), quindi converge ad un numero reale α'. Analogamente la successione dei convergenti di indice dispari è monotona decrescente e inferiormente limitata e converge ad un numero α''. Inoltre, dalla formula (20), si ottiene che $\alpha' - \alpha''$ diventa piccolo a piacere e quindi $\alpha' = \alpha''$. Sia quindi α il limite comune delle due successioni. Vediamo ora che se partiamo dal numero reale α e costruiamo la frazione continua ad esso associata, otteniamo una frazione continua i cui termini sono proprio $q_0, q_1, \ldots$. Poiché α è il limite della successione crescente dei convergenti di indice pari, abbiamo che $A_0/B_0 < \alpha$ e poiché è il limite della successione decrescente dei convergenti di indice dispari, abbiamo che $\alpha < A_1/B_1$, quindi $q_0 < \alpha < q_0 + 1/q_1$ ed essendo $1/q_1 < 1$, abbiamo che la parte intera di α vale proprio q_0. Se scriviamo ora $\alpha = q_0 + 1/\alpha_1$, usando il convergente A_2/B_2, abbiamo:

$$q_0 + \frac{1}{q_1 + \frac{1}{q_2}} < q_0 + 1/\alpha_1 < q_0 + \frac{1}{q_1}$$

da cui, cancellando q_0 e passando ai reciproci:

$$q_1 < \alpha_1 < q_1 + \frac{1}{q_2}$$

essendo $1/q_2 < 1$, abbiamo che q_1 è proprio la parte intera di α_1. Procedendo in questo modo vediamo che, partendo dal numero α, si ottiene la frazione continua infinita i cui termini sono $q_0, q_1, \ldots$ □

Il teorema ora dimostrato stabilisce una corrispondenza biunivoca tra numeri irrazionali e frazioni continue infinite. In particolare, ogni numero irrazionale è individuato da una e una sola successione di numeri interi $q_0, q_1, \ldots$ con $q_i > 1$ se $i = 1, 2, \ldots$. I numeri razionali sono invece individuati, come abbiamo visto, da una successione finita $q_0, \ldots, q_n$ di numeri interi, anche ora con $q_i > 1$ per $i = 1, 2, \ldots$ e con l'ulteriore condizione che q_n non sia l'unità. Le frazioni continue possono dunque essere utilizzate per fornire una nuova costruzione dei numeri reali, anche se non è banale capire come, partendo da esse, si possano esprimere le operazioni di somma e prodotto.

14.1 Costruzione di numeri trascendenti

Una delle applicazioni delle frazioni continue è che permettono di trovare "facilmente" numeri trascendenti. I risultati che qui esporremo sono dovuti a Liouville, che nel 1844 ha trovato i primi esempi di numeri trascendenti.

Abbiamo innanzitutto bisogno del seguente risultato:

Proposizione 14.2. *Sia $\alpha \in \mathbb{R}$ algebrico su $\mathbb{Q}$, di grado n. Allora α non è radice multipla del suo polinomio minimo.*

Dimostrazione. Sia $f(x) \in \mathbb{Q}[x]$ il polinomio minimo di α (quindi è irriducibile, di grado n). Se fosse $f(x) = (x-\alpha)^e f_1(x)$ con $e > 1$ (e $f_1(x) \in \mathbb{R}[x]$), avremmo che $f'(x)$, il derivato di $f(x)$, sarebbe un polinomio a coefficienti in $\mathbb{Q}[x]$ che ammette α come radice, ma questo è assurdo perché $f'(x)$ ha grado $n-1$. □

Il seguente teorema (di Liouville) permetterà di ottenere infiniti esempi di numeri trascendenti.

Teorema 14.3. *Sia α un numero algebrico di grado $n > 1$. Allora esiste un numero reale $C > 0$ tale che*

$$\left|\alpha - \frac{p}{q}\right| > \frac{C}{q^n}$$

per ogni numero intero p e q, con $q > 0$.

Dimostrazione. Sia $f(x) \in \mathbb{Q}[x]$ il polinomio minimo (di grado n) di α. Moltiplicando per il comune denominatore dei coefficienti di f, possiamo assumere che f sia a coefficienti interi (ora non necessariamente monico) $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ ($a_i \in \mathbb{Z}$). Sia $f(x) = (x-\alpha) f_1(x)$ con $f_1(x) \in \mathbb{R}[x]$. La conseguenza della proposizione 14.2 è che $f_1(\alpha) \neq 0$, allora, per continuità della funzione $f_1(x)$, esiste un $\delta > 0$ tale che $f_1(x) \neq 0$ per ogni $x \in [\alpha - \delta, \alpha + \delta]$. Siano $p, q \in \mathbb{Z}$, $q > 0$ arbitrari e supponiamo che valga: $|\alpha - (p/q)| \leq \delta$. Da $f(x) = (x-\alpha) f_1(x)$ otteniamo

$$\begin{aligned} \frac{p}{q} - \alpha &= \frac{f(\frac{p}{q})}{f_1(\frac{p}{q})} \\ &= \frac{a_0 q^n + a_1 q^{n-1} p + \cdots + a_n p^n}{q^n f_1(\frac{p}{q})} \end{aligned}$$

Il numeratore dell'ultima frazione è un intero non nullo (se fosse zero, avremmo $\alpha = p/q$ e α sarebbe algebrico di grado 1). Pertanto il numeratore, in valore assoluto, vale almeno 1. Sia M il minimo della funzione $|f_1(x)|$ nell'intervallo $[\alpha-\delta, \alpha+\delta]$ (esiste per il teorema di Weierstrass e non è nullo per come è stato definito δ). Pertanto, dalla disugaglianza di sopra, supponendo che $|\alpha - p/q| \leq \delta$, otteniamo:

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{1}{Mq^n}.$$

(ricordare che q è positivo). Se invece $|\alpha - p/q| > \delta$, allora, essendo q intero positivo, sarà anche $|\alpha - p/q| > \delta/(q^n)$. Se scegliamo quindi C un numero positivo, minore di $1/M$ e δ, abbiamo che, per arbitrari p e $q > 0$, vale:

$$\left|\alpha - \frac{p}{q}\right| > \frac{C}{q^n}.$$

□

Il significato del teorema di Liouville è che per approssimare un numero algebrico con un numero razionale p/q si commette un errore che è almeno dell'ordine di $1/(q^n)$. Se riusciamo a trovare quindi un numero reale che si riesce ad approssimare meglio con i numeri razionali, quel numero non può essere algebrico.

Definizione 14.4. Un numero reale α si dice *numero di Liouville* se per ogni $m \in \mathbb{N}$, $m \geq 1$, esistono due interi p e q con $q > 1$ tali che:

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^m}. \tag{25}$$

Teorema 14.5. *Un numero di Liouville è trascendente.*

Dimostrazione. Supponiamo che α sia algebrico di grado n e sia $C > 0$ come nel teorema di Liouville. Scegliamo $r \in \mathbb{N}$ tale che $2^r > 1/C$. Sia $m \geq r + n$ e siano p e q gli interi relativi ad m, come nella definizione di numero di Liouville. Allora vale:

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^m} < \frac{1}{q^r} \cdot \frac{1}{q^n} < \frac{1}{2^r}\frac{1}{q^n} < \frac{C}{q^n}.$$

e questo contraddice il teorema 14.3. □

Con l'utilizzo della rappresentazione dei numeri reali con le frazioni continue, è facile costruire numeri di Liouville. Scriviamo un numero α come una frazione continua:

$$\alpha = q_0 + \frac{1}{q_1+}\,\frac{1}{q_2+}\,\cdots$$

dove $q_0, q_1, q_2, \ldots$ sono da scegliere in modo che α soddisfi alla condizione di non essere algebrico. Scegliamo q_0, q_1 e q_2 arbitrariamente e prendiamo, per $m > 1$:

$$q_{m+1} > B_m^{m-2}$$

Allora vale (usando la disequazione (24)):

$$\left|\alpha - \frac{A_m}{B_m}\right| < \frac{1}{B_m B_{m+1}} < \frac{1}{B_m(q_{m+1}B_m + B_{m-1})} < \frac{1}{B_m^2 q_{m+1}} < \frac{1}{q_m^m}$$

e quindi, se i termini di α soddisfano alla condizione imposta, α è un numero di Liouville. Naturalmente, la scelta dei termini q_{m+1} può essere fatta in infiniti modi.

Esempio 14.6. Esempio di costruzione di un numero di Liouville:
Fissiamo i primi termini q_0, q_1, q_2 di una frazione continua α, per esempio $q_0 = 0, q_1 = 1, q_2 = 2$ e quindi i primi tre convergenti sono: $A_0/B_0 = 0/1$, $A_1/B_1 = 1/1$, $A_2/B_2 = 3/2$. Scegliamo $q_3 > B_2^0 = 1$, quindi, per esempio, $q_3 = 2$, allora $B_3 = q_3 B_2 + B_1$, quindi $B_3 = 2 \cdot 2 + 1 = 5$, scegliamo $q_4 > B_3 = 5$, quindi, ad esempio, $q_4 = 6$. Allora $B_4 = 6 \cdot 5 + 2 = 32$, e allora scegliamo $q_5 > 32^2 = 1024$, per esempio $q_5 = 1025$ e così via. In questo modo costruiamo induttivamente i termini:

$$q_0 = 0,\ q_1 = 1,\ q_2 = 2,\ q_3 = 2,\ q_4 = 6,\ q_5 = 1025,\ \ldots$$

che danno un numero α trascendente.

Si chiama *costante di Liouville* il numero:

$$c = \sum_{k=1}^{+\infty} \frac{1}{10^{k!}}$$

È un numero di Liouville, come segue dalle seguenti considerazioni. Poniamo

$$p_m = \sum_{k=1}^{m} 10^{m!-k!} = 10^{m!} \sum_{k=1}^{m} 10^{-k!}; \qquad q_m = 10^{m!}$$

Allora

$$\begin{aligned}
\left|c - \frac{p_m}{q_m}\right| &= \sum_{k=1}^{+\infty} \frac{1}{10^{k!}} - \frac{p_m}{q_m} = \sum_{k=1}^{+\infty} \frac{1}{10^{k!}} - \sum_{k=1}^{m} \frac{1}{10^{k!}} = \sum_{k=m+1}^{+\infty} \frac{1}{10^{k!}} \\
&= \frac{1}{10^{(m+1)!}} + \frac{1}{10^{(m+2)!}} + \frac{1}{10^{(m+3)!}} + \cdots \\
&< \frac{1}{10^{(m+1)!}} + \frac{1}{10^{(m+1)!} \cdot 10} + \frac{1}{10^{(m+1)!} \cdot 10^2} + \cdots \\
&= \frac{1}{10^{(m+1)!}} \left(\sum_{k=0}^{+\infty} \frac{1}{10^k}\right) = \frac{10}{9} \left(\frac{1}{10^{m!}}\right) \cdot \left(\frac{1}{10^{m!}}\right)^m < \frac{1}{q_m^m}.
\end{aligned}$$

e quindi c è un numero di Liouville.

Naturalmente ci sono molti numeri trascendenti che non sono numeri di Liouville. Il primo numero non artificiosamente costruito che si provò essere

trascendente è la costante di Nepero e (la dimostrazione risale a Hermite, 1873). Nel 1882 Lindemann pubblicò una dimostrazione, basata anche sul precedente lavoro di Hermite, della trascendenza di π. Nel frattempo Cantor (nel 1874) aveva dimostrato che "la maggior parte" dei numeri reali è trascendente (cioè aveva provato che i numeri algebrici sono un sottoinsieme numerabile di $\mathbb{R}$, mentre $\mathbb{R}$ non è numerabile). Probabilmente torneremo sull'argomento.

Ci sono numeri che hanno "belle" rappresentazioni quando scritti sotto forma di frazioni continue. Ne richiamiamo qui alcuni:

$$\begin{aligned} e &= 2+\frac{1}{1+}\frac{1}{2+}\frac{1}{1+}\frac{1}{1+}\frac{1}{4+}\frac{1}{1+}\frac{1}{1+}\frac{1}{6+}\cdots \\ \tanh(1) &= 0+\frac{1}{1+}\frac{1}{3+}\frac{1}{5+}\frac{1}{7+}\cdots \\ \tan(1) &= 1+\frac{1}{1+}\frac{1}{1+}\frac{1}{3+}\frac{1}{1+}\frac{1}{5+}\frac{1}{1+}\frac{1}{7+}\cdots \end{aligned}$$

15 Numeri irrazionali algebrici di grado 2

Cerchiamo ora la frazione continua che corrisponde al numero irrazionale $\sqrt{2}$. Procedendo come abbiamo visto nella sezione 13.2, abbiamo che $\sqrt{2} = 1+1/\alpha_1$, quindi il primo termine q_0 della frazione continua di $\sqrt{2}$ è 1. Ricavando α_1 dall'uguaglianza di sopra, abbiamo che $\alpha_1 = \sqrt{2}+1$ e quindi la parte intera di α_1 vale 2, cioè $q_1 = 2$. Allora $\alpha_1 = 2+1/\alpha_2$. Risolvendo questa uguaglianza rispetto ad α_2, otteniamo che $\alpha_2 = \sqrt{2}+1$, quindi $\alpha_2 = \alpha_1$. Queste informazioni allora ci bastano per scrivere la frazione continua associata a $\sqrt{2}$:

$$\sqrt{2} = 1+\frac{1}{2+}\frac{1}{2+}\frac{1}{2+}\cdots$$

In modo analogo si trova che la frazione continua associata ad altre radici quadratiche di numeri interi. Ecco i primi esempi:

$$\begin{aligned} \sqrt{3} &= 1+\frac{1}{1+}\frac{1}{2+}\frac{1}{1+}\frac{1}{2+}\frac{1}{1+}\frac{1}{2+}\frac{1}{1+}\frac{1}{2+}\cdots \\ \sqrt{5} &= 2+\frac{1}{4+}\frac{1}{4+}\frac{1}{4+}\frac{1}{4+}\frac{1}{4+}\frac{1}{4+}\frac{1}{4+}\frac{1}{4+}\cdots \\ \sqrt{6} &= 2+\frac{1}{2+}\frac{1}{4+}\frac{1}{2+}\frac{1}{4+}\frac{1}{2+}\frac{1}{4+}\frac{1}{2+}\frac{1}{4+}\cdots \\ \sqrt{7} &= 2+\frac{1}{1+}\frac{1}{1+}\frac{1}{1+}\frac{1}{4+}\frac{1}{1+}\frac{1}{1+}\frac{1}{1+}\frac{1}{4+}\cdots \\ \sqrt{8} &= 2+\frac{1}{1+}\frac{1}{4+}\frac{1}{1+}\frac{1}{4+}\frac{1}{1+}\frac{1}{4+}\frac{1}{1+}\frac{1}{4+}\cdots \\ \sqrt{10} &= 3+\frac{1}{6+}\frac{1}{6+}\frac{1}{6+}\frac{1}{6+}\frac{1}{6+}\frac{1}{6+}\frac{1}{6+}\frac{1}{6+}\cdots \\ \sqrt{11} &= 3+\frac{1}{3+}\frac{1}{6+}\frac{1}{3+}\frac{1}{6+}\frac{1}{3+}\frac{1}{6+}\frac{1}{3+}\frac{1}{6+}\cdots \end{aligned}$$

$$\begin{aligned}
\sqrt{12} &= 3+\frac{1}{2+}\frac{1}{6+}\frac{1}{2+}\frac{1}{6+}\frac{1}{2+}\frac{1}{6+}\frac{1}{2+}\frac{1}{6+}\cdots\\
\sqrt{13} &= 3+\frac{1}{1+}\frac{1}{1+}\frac{1}{1+}\frac{1}{1+}\frac{1}{6+}\frac{1}{1+}\frac{1}{1+}\frac{1}{1+}\cdots\\
\sqrt{14} &= 3+\frac{1}{1+}\frac{1}{2+}\frac{1}{1+}\frac{1}{6+}\frac{1}{1+}\frac{1}{2+}\frac{1}{1+}\frac{1}{6+}\cdots\\
\sqrt{15} &= 3+\frac{1}{1+}\frac{1}{6+}\frac{1}{1+}\frac{1}{6+}\frac{1}{1+}\frac{1}{6+}\frac{1}{1+}\frac{1}{6+}\cdots\\
\sqrt{17} &= 4+\frac{1}{8+}\frac{1}{8+}\frac{1}{8+}\frac{1}{8+}\frac{1}{8+}\frac{1}{8+}\frac{1}{8+}\frac{1}{8+}\cdots\\
\sqrt{18} &= 4+\frac{1}{4+}\frac{1}{8+}\frac{1}{4+}\frac{1}{8+}\frac{1}{4+}\frac{1}{8+}\frac{1}{4+}\frac{1}{8+}\cdots\\
\sqrt{19} &= 4+\frac{1}{2+}\frac{1}{1+}\frac{1}{3+}\frac{1}{1+}\frac{1}{2+}\frac{1}{8+}\frac{1}{2+}\frac{1}{1+}\cdots
\end{aligned}$$

Come si vede, in tutti questi esempi i termini delle frazioni continue si ripetono periodicamente.
Consideriamo ancora l'esempio:

$$\alpha = \frac{4-\sqrt{2}}{3}$$

Per costruire la frazione continua associata ad α, consideriamo le seguenti espressioni:

$$\alpha = q_0 + \frac{1}{\alpha_1}, \quad \alpha_1 = q_1 + \frac{1}{\alpha_2}, \quad \alpha_2 = q_2 + \frac{1}{\alpha_3}, \quad \alpha_3 = q_3 + \frac{1}{\alpha_4}, \quad \cdots$$

dove, come al solito, q_0 è la parte intera di α, q_1 è la parte intera di α_1 e così via. Si trova che vale:

$$q_0 = 0,\ q_1 = 6,\ q_2 = 4,\ q_3 = 8,$$

inoltre

$$\alpha_2 = \frac{4+3\sqrt{2}}{2}$$

e si vede che $\alpha_4 = \alpha_2$. Pertanto abbiamo che i termini si ripetono: $q_4 = q_2$, $q_5 = q_3$, $q_6 = q_2$, $q_7 = q_3$, ... quindi anche ora la frazione continua di α è periodica (la differenza rispetto agli esempi precedenti, è che in questo caso compare un "antiperiodo"):

$$\alpha = 0+\frac{1}{6+}\frac{1}{4+}\frac{1}{8+}\frac{1}{4+}\frac{1}{8+}\cdots$$

Formalizziamo ora la definizione di frazione continua periodica.

Definizione 15.1. Sia $\alpha = q_0 + 1/(q_1+)\,1/(q_2+)\,\ldots$ un numero irrazionale, se esistono due numeri naturali k_0 e h tali che, per ogni $k \geq k_0$ vale:

$$q_{k+h} = q_k$$

la frazione continua si dice *periodica*.

In alanogia con i numeri decimali periodici, i termini $q_0, q_1, \ldots$ si scrivono: $q_0, q_1, \ldots, q_{k_0-1}, \overline{q_{k_0}, q_{k_0+1}, \ldots, q_{k_0+h-1}}$.
Vale il seguente risultato (dimostrato da Lagrange, nel 1770):

Teorema 15.2. *Se la frazione continua associata ad un numero reale α è periodica, allora α è un numero algebrico di grado 2 e viceversa, le frazioni continue associate a numeri algebrici di grado 2 sono periodiche.*

Dimostrazione. Vediamo solo la dimostrazione che se la frazione continua di α è periodica, allora α è algebrico di grado 2. Per la dimostrazione del viceversa si rimanda ad esempio a Kinchin o Davenport [@@@]. Sia $k \geq k_0$. Consideriamo le due frazioni continue:

$$q_k + \frac{1}{q_{k+1}+} \frac{1}{q_{k+2}+} \cdots, \qquad q_{k+h} + \frac{1}{q_{k+h+1}+} \frac{1}{q_{k+h+2}+} \cdots$$

come conseguenza della periodicità si ha che sono uguali. Quindi, ricordando l'espressione (21), abbiamo che

$$\alpha_k = \alpha_{k+h}, \quad k \geq k_0$$

Allora, dalla formula (23) abbiamo che

$$\alpha = \frac{\alpha_k A_{k-1} + A_{k-2}}{\alpha_k B_{k-1} + B_{k-2}} = \frac{\alpha_{k+h} A_{k+h-1} + A_{k+h-2}}{\alpha_{k+h} B_{k+h-1} + B_{k+h-2}} = \frac{\alpha_k A_{k+h-1} + A_{k+h-2}}{\alpha_k B_{k+h-1} + B_{k+h-2}} \quad (26)$$

Pertanto otteniamo:

$$\frac{\alpha_k A_{k-1} + A_{k-2}}{\alpha_k B_{k-1} + B_{k-2}} = \frac{\alpha_k A_{k+h-1} + A_{k+h-2}}{\alpha_k B_{k+h-1} + B_{k+h-2}}$$

e questa equazione, quando esplicitata rispetto ad α_k, risulta essere un'equazione di secondo grado in α_k. Quindi α_k è radice di un'equazione di secondo grado a coefficienti interi e pertanto α_k è algebrico di grado 2 o 1. Se però fosse algebrico di grado 1 sarebbe razionale e quindi anche α lo sarebbe, contro l'ipotesi. Consideriamo ora la prima delle equazioni di (26):

$$\alpha = \frac{\alpha_k A_{k-1} + A_{k-2}}{\alpha_k B_{k-1} + B_{k-2}}$$

da essa possiamo ricavere α_k in funzione di α, ottenendo un'espressione della forma $\alpha_k = (r\alpha + s)/(t\alpha + u)$ dove r, s, t, u sono numeri interi. Allora se α_k soddisfa un'equazione di secondo grado a coefficienti interi, lo fa anche α. Quindi α è algebrico di grado 2. □

16 Numeri "costruibili"

La geometria euclidea introduce i concetti di *punto*, *retta*, *piano* come concetti primitivi, che non vanno quindi ulteriormente spiegati. Il loro significato si chiarisce dal modo in cui essi interagiscono tra loro. Si può però costruire un modello della geometria euclidea ove i concetti di retta, punto e piano si possono definire e questo modello richiede l'utilizzo dei soli assiomi di Zermelo Fraenkel: il piano è, per definizione, l'insieme $P = \mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ (ol al caso, il piano complesso $\mathbb{C}^2 = \mathbb{C} \times \mathbb{C}$), i punti del piano sono, per definizione, le coppie ordinate $(x, y) \in P$ (con $x \in \mathbb{R}$, $y \in \mathbb{R}$), le rette sono, per definizione, gli insiemi

$$r = \{(x, y) \in P \mid \exists\, a, b, c \in \mathbb{R} :\ a, b \text{ non entrambi nulli t.c. } ax + by + c = 0\}$$

In questo modo si fornisce un modello per la geometria euclidea e quelli che sono gli assiomi diventano teoremi. Ad esempio l'assioma che afferma che per due punti distinti $A = (x_1, y_1)$ e $B = (x_2, y_2)$ passa una e una sola retta si dimostra provando che il sistema

$$\begin{cases} ax_1 + by_1 + c &= 0 \\ ax_2 + by_2 + c &= 0 \end{cases}$$

ha un'unica soluzione (a, b, c), a meno di un fattore di proporzionalità. In questo modello della geometria euclidea necessitiamo dei numeri reali (costruiti, in uno dei modi visti, a partire dai numeri razionali, a loro volta ottenuti dagli interi, quindi dai naturali, quindi dagli assiomi ZF), necessitiamo di insiemi, come le coppie ordinate (per definire i punti) e le coppie ordinate si possono definire grazie all'assioma ZF3; o insiemi descritti da formule (come per le rette) che sono ammissibili in quanto rispettano l'assioma di separazione (ZF4). Accidentalmente, vediamo che si possono trovare anche altri modelli per interpretare gli (alcuni degli) assiomi della geometria euclidea. I punti potrebbero per esempio essere i punti della superficie di una sfera e le rette potrebbero essere i cerchi massimi. Il discorso potrebbe portare molto lontano, ma qui non approfondiamo ulteriormente questo argomento, quanto piuttosto vogliamo vedere come si possano ottenere i numeri (alcuni numeri) con costruzioni geometriche effettuate, per esempio, con strumenti come la riga e il compasso.

Secondo Wikipedia:

> Eseguire una costruzione con riga e compasso significa tracciare segmenti ed angoli servendosi esclusivamente di una riga e di un compasso idealizzati, ossia non graduati, senza quindi la possibilità di far riferimento alle tacche della riga per prendere misure o di ripetere una data apertura che il compasso aveva avuto in precedenza.

Le regole del gioco per la costruzione di figure geometriche nel piano con riga e compasso che useremo sono le seguenti:

R1 Se sono noti due punti del piano A e B, si può tracciare la retta che li congiunge;

R2 dati tre punti del piano A, B, C, si può tracciare la circonferenza centrata in A e con raggio BC.

Con queste due regole, partendo da alcuni punti noti del piano, si possono ottenerne altri nei seguenti tre modi:

C1 Intersezione di due rette che sono state tracciate;

C2 Intersezione di una retta e una circonferenza;

C3 Intersezione di due circonferenze.

Ad esempio, supponiamo di avere due punti A e B del piano e vogliamo cotruire il punto C che sia il punto di mezzo del segmento AB. In base alla regola **R2** possiamo tracciare la circonferenza centrata in A e di raggio AB. Poi, sempre per **R2**, possiamo tracciare la circonferenza centrata in B e di raggio AB. Le due circonferenze si incontrano in due punti E ed F. Grazie alla regola **R1**, possiamo tracciare la retta per i punti E ed F. Sempre per **R1** possiamo tracciare la retta per i punti A e B. Grazie alla condizione **C1** otteniamo infine il punto C.

Osservazione 16.1. La regola **R2** è in apparenza più permissiva rispetto alla definizione di costruzione con riga e compasso che abbiamo dato, perché consente di ottenere un'apertura per il compasso dalla distanza di due punti B e C e trasportarla, per tracciare una circonferenza centrata in A. Se anche però sostituissimo al posto di **R2** la regola

R2' Dati due punti A e B del piano, si può tracciare la circonferenza centrata in A e con raggio AB

le costruzioni ottenibili sarebbero le stesse. Questo risultato segue da una costruzione presente negli Elementi di Euclide che mostra come trasportare un segmento AB su una retta passante per due punti C e D trovando su tale retta un punto E tale che AB sia congruente a CE. Il disegno di figura 2 mostra la possibile costruzione.

Molte figure si possono costruire con riga e comasso (e molte altre no). Vediamo ora alcune costruzioni possibili (e probabilmente, per la maggior parte, ben note):

1. Dato un segmento AB, costruire il suo asse;
2. Data una retta (ottenuta congiungendo due punti A e B) e un punto P su di essa, tracciare la retta passante per P e ortogonale alla retta data;
3. Data una retta (ottenuta congiungendo due punti A e B) e un punto P esterno ad essa, tracciare la retta passante per P e parallela alla retta data;
4. Dato un segmento AB, disegnare il triangolo equilatero con lato AB;

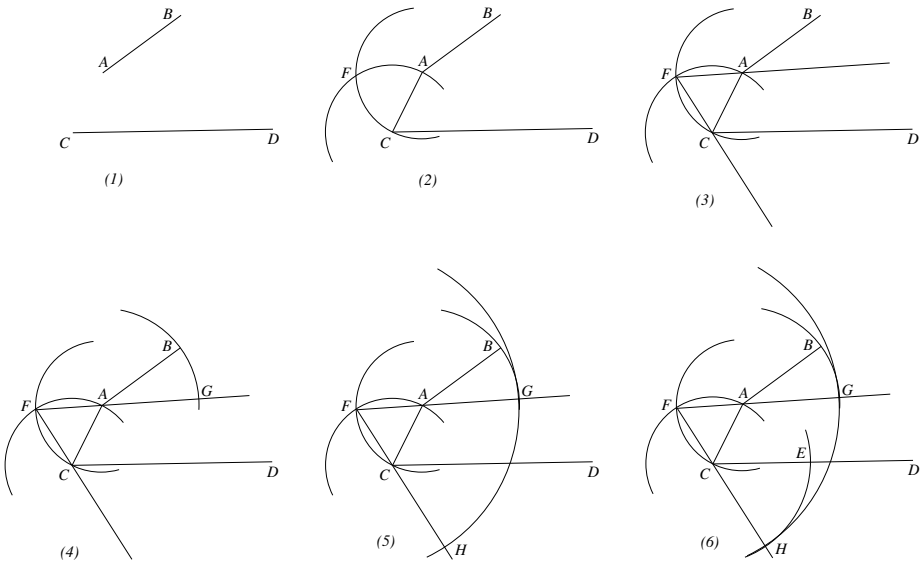

Figura 2: Il segmento AB viene trasportato sulla retta CD. (2): puntanto il compasso prima in A, con apertura AC e poi in C, con apertura CA, si determina il punto F. (3): Si tracciano le rette FA e FC. (4): puntando il compasso in A con apertura AB si traccia un arco di circonferenza, trovando il punto G. (5): Puntando il compasso in F, con apertura FG, si traccia un arco di circonferenza, trovando il punto H. (6): puntando il compasso in C, con apertura CH, si trova il punto E. Poiché AB è congruo a AG, FG è congruo a FH, FA è congruo a FC, abbiamo che CH è congruo ad AB. Infine il segmento CE risulta congruo al segmento AB.

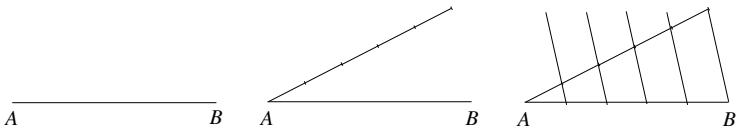

Figura 3: Divisione del segmento AB in n parti uguali (nell'esempio, 5 parti). Si traccia una nuova semiretta passante per A, su di essa si riportano n volte un segmento; l'ultimo estremo di questi segmenti va congiunto con B e poi si mandano le rette parallele a questa retta da ognuno degli estremi dei segmenti.

5. Dato un segmento AB, disegnare il quadrato con lato AB;
6. Dato un segmento AB, disegnare un esagono regolare con lato AB;
7. Dato un segmento AB, disegnare un ottagono regolare con lato AB;
8. Dato un segmento AB, dividerlo in 3, $4, \ldots, n$ parti uguali;
9. Dato un angolo (cioè dati tre punti A, B, C tali che la semiretta AB e la semiretta AC individuano un angolo), dividerlo in due angoli congruenti (cioè: bisecare un angolo);
10. Dato un angolo (come sopra, attraverso tre punti A, B, C) e data una retta individuata da due punti D, E, costruire un angolo congruente all'angolo dato, in modo che abbia vertice in D e sia delimitato dalla semiretta DE.
11. Dato un triangolo ABC e data una retta individuata da due punti D ed E, costruire un triangolo congruente ad ABC in modo che abbia un vertice in D e un lato sulla retta DE;
12. Dato un triangolo ABC e data una retta individuata da due punti D ed E, costruire un triangolo DEF simile al triangolo ABC in modo che $AB : DE = AC : DF = BC : EF$.

Richiamiamo velocemente solo la costruzione relativa alla divisione di un segmento in n parti uguali: un modo di procedere è usare il teorema di Talete (v. figura 3).

16.1 Le costruzioni impossibili

Supponiamo ora di avere un insieme finito di punti $\mathscr{P}_0$ del piano. Precisando quanto detto con le condizioni **C1**, **C2**, **C3**, volgiamo vedere cosa sigifica dire che un punto Q è costruibile con riga e compasso, partendo dall'insieme $\mathscr{P}_0$.

Definizione 16.2. Si dice che il punto Q è *costruibile da $\mathscr{P}_0$ con riga e compasso in un passo* se Q è ottenuto in uno dei seguenti tre modi:

1. come intersezione di due rette passanti per punti di $\mathscr{P}_0$;

2. come intersezione di una retta passante per due punti di $\mathscr{P}_0$ e una circonferenza centrata in un punto di $\mathscr{P}_0$ e con raggio la congiungente due punti di $\mathscr{P}_0$.

3. come intersezione di due circonferenze con centri in due punti di $\mathscr{P}_0$ e raggi ottenuti dalle congiungenti due punti di $\mathscr{P}_0$.

Invece si dice che Q è *costruibile da $\mathscr{P}_0$ con riga e compasso* se esistono dei punti P_1, P_2, ..., P_n tali che P_i è costruibile con riga e compasso in un passo a partire da $\mathscr{P}_0 \cup \{P_1, P_2, \ldots, P_{i-1}\}$ e $P_n = Q$.

Per poter fare una qualche costruzione, bisogna che $\mathscr{P}_0$ abbia almeno due punti (altrimenti non abbiamo la possibilità di tracciare né rette né circonferenze). Se A_0 e A_1 sono dunque due punti dati da cui partiamo, possiamo assumere che il segmento A_0A_1 sia unitario (indichiamolo con u) e possiamo rapportare tutti gli altri segmenti che otteniamo a questa unità di misura. Partendo dai due punti A_0 e A_1, possiamo tracciare la retta passante per A_0 e A_1, puntanto il compasso in A_1 con apertura A_1A_2, possiamo trovare sulla retta un nuovo punto A_2, poi puntando il compasso in A_2 con la stessa apertura, possiamo trovare un punto A_3 e così via. Se fissiamo un'orientazione alla retta per A_0 e A_1, vediamo che le coordinate di A_2, A_3, ecc. sono $2u$, $3u$, ecc. insomma, possiamo cotruire i numeri naturali e quindi anche i numeri interi. Il fatto che abbiamo una costruzione per dividere in un numero arbitrario di parti un segmento, comporta che possiamo costruire sulla retta per A_0 e A_1 tutti i numeri razionali. Poi possiamo cotruire la retta passante per A_0 e ortogonale alla retta per A_0 e A_1; anche su di essa possiamo fissare un'orientazione e costruire tutti i punti razionali. In questo modo abbiamo fissato un sistema di assi cartesiani ortogonali nel piano e vediamo che, con le costruzioni con riga e compasso, possiamo trovare per lo meno tutti i punti a coordinare razionali. Vediamo quali altri punti sono ottenibili.

Partendo da $\mathscr{P}_0$, insieme finito di punti che contiene almeno due punti A_0 ed A_1, sia K_0 il più piccolo campo (sottocampo di $\mathbb{R}$) che contiene le coordinate dei punti di $\mathscr{P}_0$. (se $\mathscr{P}_0 = \{A_0, A_1\}$, per le considerazioni appena fatte, abbiamo che $K_0 = \mathbb{Q}$).

Lemma 16.3. *Sia Q un punto costruibile con riga e compasso in un passo a partire da $\mathscr{P}_0$. Sia K il più piccolo campo che contiene K_0 e le coordinate di Q. Allora vale:*

$$[K : K_0] = 1 \text{ } o \text{ } 2.$$

Dimostrazione. Se $U = (x_0, y_0)$ e $V = (x_1, y_1)$ sono due punti di $\mathscr{P}_0$, (quindi $x_0, y_0, x_1, y_1 \in K_0$) la retta passante per essi ha equazione: $(x - x_0)(y_1 - y_0) = (y - y_0)(x_1 - x_0)$ e quindi è della forma $ax + by + c = 0$, dove $a, b, c \in K_0$. Analogamente si vede che una circonferenza centrata in un punto di $\mathscr{P}_0$ e con raggio la distanza tra due punti di $\mathscr{P}_0$ è della forma $x^2 + y^2 + \alpha x + \beta y + \gamma = 0$ con $\alpha, \beta, \gamma \in K_0$. Il punto Q può essere ottenuto in tre modi: come intersezione

di due rette r ed s ciascuna passante per due punti di $\mathscr{P}_0$; in questo caso il punto di intersezione si ottiene risolvendo il sistema:

$$\begin{cases} a_1x + b_1y + c_1 &= 0 \\ a_2x + b_2y + c_2 &= 0 \end{cases}$$

(dove i coefficienti stanno in K_0) la cui soluzione si ottiene con operazioni che non fanno uscire dal campo K_0. In questo caso, le coordinate di Q sono quindi in K_0 e pertanto $[K : K_0] = 1$. Il punto Q può essere ottenuto come soluzione di un sistema della forma:

$$\begin{cases} ax + by + c &= 0 \\ x^2 + y^2 + \alpha x + \beta y + \gamma &= 0 \end{cases}$$

In questo caso la soluzione del sistema si ottiene risolvendo un'equazione di secondo grado della forma $Ax^2 + Bx + C = 0$ con $A, B, C \in K_0$. Se il polinomio $Ax^2 + Bx + C$ è riducibile in K_0, le soluzioni stanno ancora in K_0, altrimenti, se il polinomio è irriducibile, sia ξ una sua soluzione in $\mathbb{R}$ (la soluzione certamente esiste in $\mathbb{R}$ perché si assume che il punto Q esista), allora le coordinate di Q sono elementi di $K_0[\xi]$, dove ξ è algebrico, di grado 2 su K_0. Quindi, in questo caso, $[K : K_0] = 2$. Infine, il caso in cui Q sia intersezione di due circonferenze è analogo al precedente (sottrarendo membro a membro le equazioni delle due circonferenze, ci si riconduce al caso precedente). □

Sia ora Q un punto costruibile con riga e compasso a partire da $\mathscr{P}_0$. Quindi abbiamo la sequenza di punti $P_1, P_2, \ldots, P_n = Q$, ciascuno costruibile in un passo a partire dai precedenti. Sia K_i il più piccolo campo che contiene K_0 e le coordinate dei punti $P_1, \ldots, P_i$. Sia poi $K = K_n$. Allora vale:

Teorema 16.4. *Siano $x, y \in K$ le coordinate di Q, allora sia $[K_0(x) : K_0]$, sia $[K_0(y) : K_0]$ sono potenze di 2.*

Dimostrazione. Consideriamo la torre di campi:

$$K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = K$$

allora, per il lemma 16.3 abbiamo che per ogni $i = 1, 2 \ldots, n$, $[K_{i-1} : K_i]$ è una potenza di 2, pertanto, per il teorema della torre, $[K : K_0]$ è un prodotto di potenze di 2, quindi è a sua volta una potenza di 2. Consideriamo ora il campo $K_0(x)$. Poiché $K_0 \subseteq K_0(x) \subseteq K$, sempre per il teorema della torre, abbiamo $[K : K_0] = [K : K_0(x)] \cdot [K_0(x) : K_0]$, quindi $[K_0(x) : K_0]$ deve essere una potenza di 2. Il caso di $K_0(y)$ si fa in modo del tutto analogo. □

Conseguenze del precedente teorema sono i seguenti due teoremi di Wantzel (1837):

Teorema 16.5. *Sia dato un cubo $\mathcal{C}$ di lato l. Non si può costruire, con riga e compasso, il lato di un cubo di volume doppio del volume di $\mathcal{C}$.*

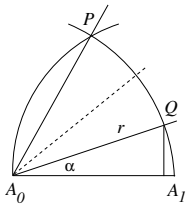

Figura 4: La trisezione di un angolo

Dimostrazione. Possiamo assumere di avere due punti nel piano, A_0 e A_1, tali che il segmento A_0A_1 sia congruo al segmento l. Poniamo $\mathscr{P}_0 = \{A_0, A_1\}$ e costriamo il sistema di assi cartesiani come visto in precedenza. Assumiamo quindi che il cubo $\mathcal{C}$ abbia volume 1 e quindi il cubo di volume doppio ha volume 2, pertanto la lunghezza del suo lato è $\sqrt[3]{2}$. In particolare il campo K_0 risulta quindi essere il campo $\mathbb{Q}$. Il problema allora diventa quello di trovare, sulla retta orientata A_0, A_1, un punto Q di ascissa $\sqrt[3]{2}$. Ma per il teorema 16.4, $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}]$ dovrebbe essere una potenza di 2, ma il polinomio minimo si $\sqrt[3]{2}$ su $\mathbb{Q}$ è $x^3 - 2$ che è di grado 3. □

Teorema 16.6. *In generale non è possibile trovare una costruzione con riga e compasso per trisecare un angolo.*

Dimostrazione. Basta chiaramente trovare un angolo che non si può trisecare con riga e compasso. Consideriamo l'angolo $\pi/3$. Se fissiamo, al solito, l'insieme $\mathscr{P}_0 = \{A_0, A_1\}$, l'angolo $\pi/3$ può essere facilmente costruito con riga e compasso: puntiamo il compasso in A_0 con apertura A_0, A_1 e tracciamo un arco, puntiamo poi il compasso in A_1 con apertura A_1, A_0 e tracciamo un secondo arco che incontra il primo in un punto P, allora la semiretta A_0, P e la semiretta A_0, A_1 formano l'angolo $\pi/3$. Se siamo in grado di trisecarlo, riusciamo a costruire una semiretta r con origine in A_0 tale che l'angolo delimitato da r e dalla semiretta A_0, A_1 sia $\alpha = \pi/9$. Indichiamo con Q il punto di intersezione di r con la circonferenza centrata in A_0 e di raggio A_0A_1 (v. figura 4). Allora l'ascissa di Q vale $\cos(\alpha)$ (assumendo che la lunghezza del segmento A_0A_1 sia l'unità). Dalla formula (6) abbiamo che

$$\cos(3\alpha) = \frac{1}{2} = 4\cos^3(\alpha) - 3\cos(\alpha)$$

quindi $\cos(\alpha)$ è uno zero del polinomio $8Y^3 - 6Y - 1$ che è irriducibile su $\mathbb{Q}$ (se fosse riducibile, avrebbe una soluzione razionale, ma questo non è possibile). In particolare, $[\mathbb{Q}[\cos(\alpha)] : \mathbb{Q}] = 3$ e non è una potenza di 2, come richiesto dal teorema 16.4. □

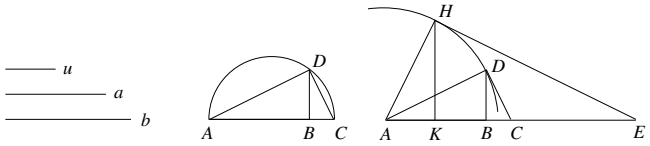

Figura 5: Calcolo del prodotto di $a \cdot b$ con il primo teorema di Euclide

17 Ancora sui numeri costruibili e le costruzioni possibili

Vediamo ora una veloce carellata su alcune possibili costruzioni con riga e compasso. Innanzitutto vediamo quali operazioni si possono eseguire con riga e compasso. Dati due segmenti AB e CD (di lunghezza, rispetto ad una fissata unità di misura, l_1 e l_2 rispettivamente), si può banalmente costruire un segmento di lunghezza $l_1 + l_2$ o $l_1 - l_2$ (in quest'ultimo caso, assumendo $l_1 \geq l_2$). Vediamo ora il prodotto: dati come sopra due segmenti AB e CD, come si può costrire un segmento di lunghezza $l_1 \cdot l_2$? Vi sono molte soluzioni possibili. Nella figura 5 è indicato come procedere per calcolare il prodotto di due segmenti di lunghezza a e b usando il primo teorema di Euclide, sapendo che u è l'unità di misura. Si costruisce il triangolo rettangolo ACD in modo che AB sia di lunghezza a e AC sia di lunghezza b. Puntando il compasso in A e con raggio AD si traccia un arco che incontra la retta ortogonale al AC e passante per K (dove K è scelto in modo che AK sia di lungheza u) nel punto H. Si congiunge A con H e di traccia la retta ortogonale ad AH passante per H. Tale ortogonale incontra la retta AC in E. Il segmento AE ha lunghezza ab. Infatti, per il I teorema di Euclide, $AB \cdot AC = AD^2$ ma $AD^2 = AH^2 = AK \cdot AE$ e da questo segue che $ab = u \cdot AE$, cioè $AE = ab$.

Un'analoga costruzione per il prodotto si può fare usando il secondo teorema di Euclide.

Esercizio 13. Dati, come sopra, due segmenti di lunghezza a e b e data l'unità di misura u, costruire, usando il primo teorema di Euclide, il rapporto a/b. Trovare poi un'analoga costruzione usando il secondo teorema di Euclide.

Esercizio 14. Utilizzare il teorema di Talete per costruire, anche in questo caso, il prodotto e il rapporto di due segmenti di lunghezza a e b.

Ricordare che il teorema della tangente e della secante (v. figura 6) afferma che, data una circonferenza, se AD è una retta tangente in D alla circonferenza e se AC è una retta secante alla circonferenza nei due punti B e C, allora vale la proporzione $AB : AD = AD : AC$.

Esercizio 15. Usando il teorema della tangente e della secante, costruire ancora una volta il prodotto e il rapporto di due segmenti dati.

Vediamo ora come si può costruire la radice quadrata di un segmento, trovare cioè, partendo da un segmento di lunghezza a, un altro segmento di lunghezza

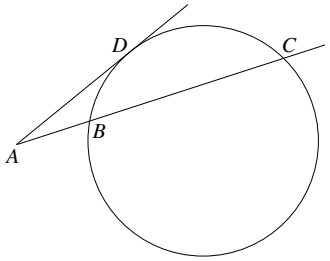

Figura 6: Il teorema della tangente e della secante.

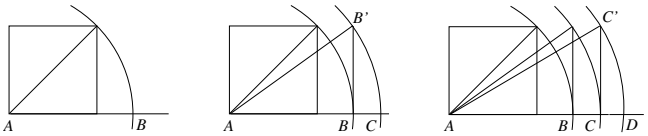

Figura 7: Calcolo di $\sqrt{2}, \sqrt{3}, \sqrt{4}, \ldots$ con il teorema di Pitagora.

b tale che $b^2 = a$. La figura 7 mostra come utilizzare il teorema di Pitagora per calcolare $\sqrt{2}, \sqrt{3}, \sqrt{4}, \ldots$. Partendo da un quadrato di lato unitario, la lunghezza della sua diagonale vale $\sqrt{2}$, quindi il segmento AB vale anche $\sqrt{2}$. Mandando da B una verticale e fermandosi all'altezza del quadrato, si determina un punto B'. Per il teorema di Pitagora, il segmento $AB' = AC$ vale $\sqrt{3}$. Analogamente, mandando da C una verticale fino in C', si determina un segmento AC' di lunghezza $\sqrt{4}$ e così via. Naturalmente vi sono modi molto più efficienti per calcolare le radici quadrate di segmenti.

Esercizio 16. Usare il primo teorema di Euclide, il secondo teorema di Euclide e il teorema della secante e della tangente per calcolare, dato un segmento di lunghezza a, un segmento di lunghezza $\sqrt{a}$.

17.1 Uno strumento per il calcolo del prodotto di due numeri

Descriviamo qui brevemente un possibile strumento atto a calcolare il prodotto di due numeri (basato sul II teorema di Euclide). Consideriamo una retta sulla quale abbiamo fissato un un punto denotato con 0 che divide la retta in due semirette (a e b) e su entrambe le semirette abbiamo messo una scala graduata; inoltre abbiamo tracciato un'altra semiretta t passante per 0 e ortogonale alla prima retta (v. figura 8). La semiretta t va intesa come una "rotaia" su cui va fatto scorrere un perno T attorno al quale può ruotare un sistema di due semirette c e d fissate rigidamente tra loro in modo da formare sempre un angolo retto. Le due semirette possono quindi ruotare attorno a T e T può muoversi in su e in giù lungo la semiretta t. Questo semplice strumento è in grado di

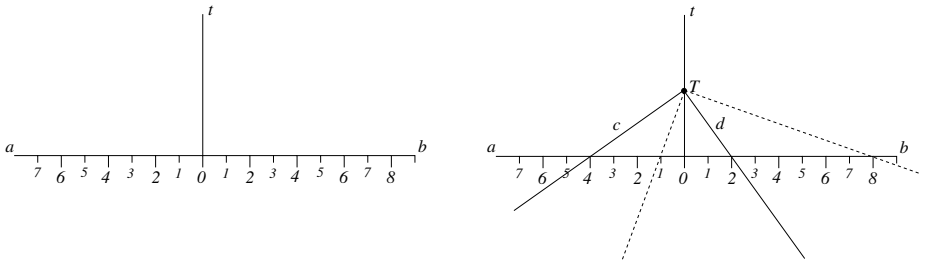

Figura 8: Una macchina per il calcolo del prodotto

calcolare il prodotto di numeri. Supponiamo di voler calcolare il prodotto di 4×2. Posizioniamo le due semirette c e d in modo che la semiretta c passi per il punto 4 della scala graduata di a, mentre la semiretta d passi per il punto 2 della scala di b. Per ottenere questa posizione, il punto T deve essere portato ad una opportuna altezza sulla semiretta t. Fatto ciò, tenendo fissa l'altezza di T, muoviamo la semiretta c in modo che vada a passare per il punto 1 della scala graduata di a (nella figura 8 è la retta tratteggiata di sinistra). Conseguentemente, ruotando attorno a T, anche la semiretta d deve spostarsi (ricordiamo che sono fissate tra loro in modo da formare un angolo retto). La semiretta d quindi (raffigurata dalla semiretta tratteggiata di destra) incontra la semiretta b in un punto che, letto sulla scala graduata di b, è il prodotto di 4×2. La spiegazione del perché si ottenga il prodotto è immediata, non appena si ricordi il II teorema di Euclide: abbiamo infatti due traingoli rettangoli con angolo retto in T e altezza relativa all'ipotenusa sempre $0T$. Nel primo triangolo rettangolo, la proiezione dei due cateti sull'ipotenusa è data da due segmenti di lughezza 4 e 2. Quindi il prodotto 4×2 vale $0T^2$. Nel secondo triangolo rettangolo, le proiezioni dei cateti sono lunghe 1 e, diciamo, x e deve essere $1 \times x = 0T^2$, quindi $x = 4 \times 2$. L'utilità pratica dello strumento è evidente a tutti.

17.2 Poligoni regolari

La costruzione di un poligono regolare di N lati con riga e compasso non è sempre possibile. Se $N = 3, 4, 6, 8$ la costruzione è molto semplice. Se $N = 9$ possiamo vedere subito che non è possibile: se fosse possibile, saremmo in grado di costruire con riga e compasso l'angolo di $2\pi/9$. Ma allora sarebbe facile bisecarlo e quindi saremmo in grado di costruire con riga e compasso l'angolo $\pi/9$ che, abbiamo visto, non è possibile (teorema 16.6). Per caratterizzare i poligoni regolari costruibili con riga e compasso, abbiamo bisogno di definire i primi di Fermat:

Definizione 17.1. Un numero naturale si dice *primo di Fermat* se è un numero primo e della forma

$$2^{2^n} + 1.$$

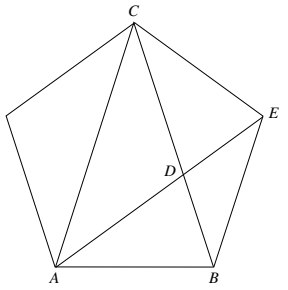

Figura 9: Il pentagono regolare e alcune sue diagonali.

I primi di Fermat noti sono 3, 5, 17, 257, 65537 (ottenuti per, rispettivamente, $n = 0, 1, 2, 3, 4$). Non sono noti altri valori di n per cui $2^{2^n}+1$ sia primo. Il seguente teorema (di Gauss-Wantzel) caratterizza i poligoni regolari che sono costruibili:

Teorema 17.2. *Un poligono regolare di N lati è costruibile con riga e compasso se e solo se la scomposizione in fattori primi di N è della forma $N = 2^k p_1 p_2 \cdots p_r$, dove $k \in \mathbb{N}$ e $p_1, \ldots, p_r$ sono primi di Fermat distinti.*

Il poligono regolare con 5 lati (il pentagono) merita qualche parola. È un poligono costruibile con riga e compasso. Dalla figura 9 si può vedere (con un conteggio di angoli: l'angolo $A\hat{C}B$ e $A\hat{E}B$ sono congruenti, essendo angoli alla circonferenza che insistono sulla stessa corda AB e valgono 36^o), che i triangoli BDE e ACD sono isosceli, da cui segue che i triangoli ABC e ABD sono simili. Pertanto vale: $CB : AB = AB : BD$ e quindi, essendo $AB = CD$, abbiamo: $CB : CD = CD : BD$. Il rapporto tra la lunghezza di CB e la lunghezza di CD si chiama *rapporto aureo* (o sezione aurea o numero di Fidia o divina proporzione...). Detto d la lunghezza della diagonale AC (o BC) del pentagono e l il lato, abbiamo:

$$\frac{d}{l} = \frac{l}{d-l}$$

Se poniamo $\phi = d/l$, si ottiene:

$$\phi^2 - \phi - 1 = 0, \quad \text{cioè} \quad \phi = \frac{1+\sqrt{5}}{2}$$

(scartando per ϕ la soluzione negativa). Dato quindi il lato l di un pentagono, si può costruire, con riga e compasso, la sua diagonale (e quindi tutto il pentagono), se non altro perché sappiamo costruire $\sqrt{5}$, quindi sappiamo calcolare $(1+\sqrt{5})/2$ e moltiplicare questo numero per l. Ci sono comunque altri modi "più eleganti" per costruire un pentagono regolare. Ad esempio si vedano le figure 10 e 11.

Dall'equazione $\phi^2 - \phi - 1 = 0$ si ottiene anche:

$$\phi = 1 + \frac{1}{\phi}$$

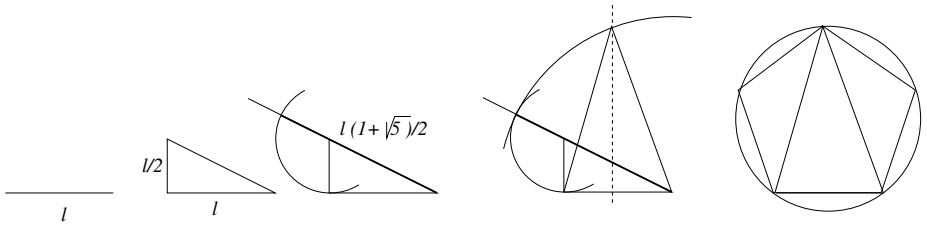

Figura 10: Una possibile costruzione del pentagono regolare: partendo dal lato l, si costruisce il triangolo rettangolo che ha cateti lunghi rispettivamente l e $l/2$, allora la sua ipotenusa è $(l\sqrt{5})/2$. Se ad essa si aggiunge un segmento lungo $l/2$, si ottiene la diagonale del pentagono. Dal lato e dalla diagonale del pentagono, è facile completare la figura.

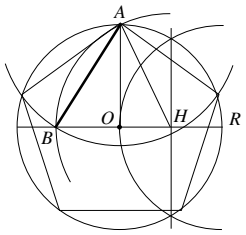

Figura 11: La costruzione probabilmente più nota del pentagono regolare: si traccia una circonferenza e un suo diametro, poi si trova H, il punto di mezzo del raggio OR. Puntando il compasso in H con apertura AH, si trova il punto B. Il segmento AB risulta essere il lato del pentagono regolare inscritto nella circonferenza.

e da questa segue immediatamente un modo per scrivere ϕ in frazione continua:

$$\phi \;=\; 1+\frac{1}{\phi} \;=\; 1+\frac{1}{1+\dfrac{1}{\phi}} \;=\; \cdots \;=\; 1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cdots}}}$$

Osservazione 17.3. Il numero ϕ è una costante ben nota: si chiama *numero aureo* o *costante di Fidia* o *divina proporzione* o *sezione aurea* o *rapporto aureo*... è un numero conosciuto fin dall'antichità e compare in molti campi, non solo della matematica.

Osservazione 17.4. Il fatto che alcune figure geometriche non siano realizzabili con riga e compasso ha stimolato la ricerca di altri strumenti per la loro costruzione. Molti sono gli strumenti che sono stati costruiti. A tal proposito, si segnala ad esempio il sito: `http://www.macchinematematiche.org/` (collegato anche con la collezione delle "Macchine Matematiche", ospitata presso

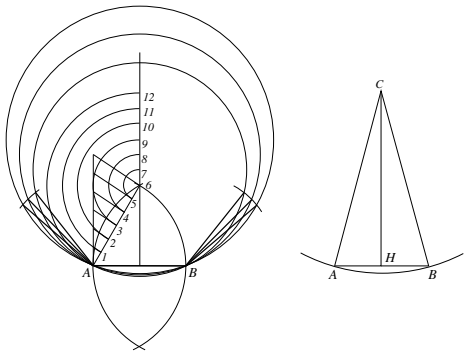

Figura 12: Come costruire con riga e compasso un poligono regolare di n lati (con lato assegnato), ovvero il teorema di Gauss-Wentzel è... sbagliato.

il laboratorio delle macchine matematiche dell'Università di Modena e Reggio Emilia).

17.3 Costruzione di poligoni "quasi" regolari

Vi sono varie costruzioni per ottenere, con riga e compasso, poligoni regolari di n lati, con n qualunque. Spesso si trovano nei libri di disegno geometrico. In rete si trovano anche moltissimi filmati esplicativi. Il problema è che le costruzioni sono *sbagliate* e non può che essere così, a meno che non sia sbagliato il teorema di Gauss-Wantzel... Ciò nonostante, anche in quelle costruzioni c'è qualcosa di buono. Analizziamone una (v. figura 12). In questo caso si suppone dato il lato AB e si vuole costruire un poligono regolare di n lati (sempre di lato AB). La costruzione proposta è la seguente: si traccia l'asse del lato AB. In questo modo si ottiene il punto 6 (intersezione delle due circonferenze di raggio AB e centro A e B). Si congiunge A con 6 e B con 6 (ottenendo un triangolo equilatero). Si divide il lato che congiunge i punti A e 6 in 6 parti uguali (per esempio con Talete, come in figura). Si ottengono così i punti 1, 2, 3, 4, 5. Puntando il compasso nel punto 6 si riportano sull'asse di AB i punti $5, 4, \ldots, 1$ ottenendo, rispettivamente, i punti $7, 8, \ldots, 11$ (e 12, immagine di A). I punti $6, 7, \ldots, 12$ sono i candidati dei centri delle circonferenze che inscrivono un poligono regolare di lato AB con, rispettivamente, $6, 7, \ldots, 12$ lati. Il punto 6 è effettivamente il centro della circonferenza di raggio AB che inscrive il poligono regolare di 6 lati, semplicemente perché l'esagono regolare è inscritto nella circonferenza che ha per raggio proprio il lato dell'esagono. Vediamo ora cosa si può dire del punto 12. Consideriamo allora un dodecagono regolare di lato AB di lunghezza l inscritto in una circonferenza di centro C. Allora l'angolo $A\hat{C}B$ vale $\pi/6$ e quindi l'angolo $A\hat{C}H$ vale $\pi/12$. Per le formule di bisezione, abbiamo che $\tan(\pi/12) = 2 - \sqrt{3}$, e quindi si trova che l'altezza CH del triangolo ABC vale $l + l\sqrt{3}/2$. L'altezza del triangolo che ha per base AB della figura 12 è la somma del segmento AB

e dell'altezza del triangolo equilatero di base AB, quindi vale effettivamente $l + l\sqrt{3}/2$. In altre parole, il punto 12 è effettivamente il centro del dodecagono regolare di lato AB. Il problema sono gli altri centri. Il ragionamento che ha portato alla costruzione della figura 12 è quindi il seguente: il punto 6 è il centro dell'esagono regolare di lato AB, il punto 12 è il centro del dodecagono regolare di lato AB, i centri dei poligoni regolari di $7, 8, \ldots, 11$ lati devono essere dei punti tra il punto 6 e il punto 12. *Assumiamo che siano equidistanti tra loro, cioè assumiamo che il segmento con estremi* 6 *e* 12 *sia diviso in sei parti uguali dai punti* $7, 8, \ldots, 11$. Questa assunzione non è corretta. Possiamo però cercare di capire qual è l'errore che si commette. Prendiamo il punto n (con $n = 6, 7, \ldots$) sull'asse del segmento AB e consideriamo il triangolo isoscele che ha per base AB e vertice il punto n. L'altezza di tale triangolo vale: $l\sqrt{3}/2 + l(n-6)/6$ (è composta dall'altezza del triangolo equilatero di base AB e vertice 6 e del segmento che va dal punto 6 al punto n). Quindi la tangente di metà dell'angolo al vertice del triangolo equilatero con vertice n vale $3/(3\sqrt{3} + n - 6)$ (anziché $\tan(\pi/n)$). Il lato l_v del poligono regolare inscritto nella circonferenza con centro in n e passante per i punti A e B vale:

$$l_v = l \left(\frac{3\sqrt{3} + n - 6}{3} \right) \tan\left(\frac{\pi}{n}\right)$$

Al variare di n la seguente tabella fornisce il rapporto l_v/l (la tabella considera anche poligoni con un numero di lati maggiore di 12):

n	l_v/l	n	l_v/l
6	1	13	1.0020...
7	0.9946...	14	1.0039...
8	0.9935...	15	1.0058...
9	0.9943...	16	1.0075...
10	0.9960...	17	1.0091...
11	0.9979...	18	1.0107...
12	1	19	1.0121...

Come si vede, nel caso in cui n valga 6 o 12, il rapporto vale 1, cioè, come detto, il poligono approssimato coincide con il poligono regolare corrispondente. Negli altri casi l'errore massimo è di circa 1% (nel caso di un poligono di 18 lati). Pertanto i poligoni non risultano del tutto regolari, ma l'errore che si commette è trascurabile (e probabilmente inferiore all'errore che si commette nel puntare il compasso nei punti della costruzione). Ad esempio, se prendiamo il lato di 5 cm e disegnamo un ettagono con il metodo approssimato, il lato "vero" dell'ettagono è più lungo di meno di 3 decimi di millimetro.

Un'altra costruzione di poligoni "regolari" con riga e compasso è proposta nel filmato:
`https://www.youtube.com/watch?v=C8AXFj8jlC4`
ma su questa costruzione è meglio stendere un pietoso velo di silenzio.

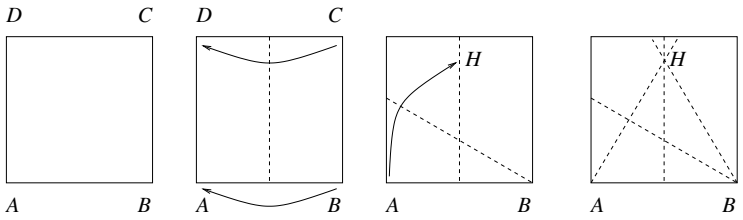

Figura 13: Costruzione di un triangolo equilatero.

18 Costruzioni geometriche con le regole dell'origami

Abbiamo visto che, partendo da alcuni punti del piano, si possono costruire altri punti ottenuti come intersezione di due rette passanti per due punti noti, o come intersezione di una retta passante per due punti noti e una circonferenza con centro in un punto noto e raggio la distanza tra due punti noti o, infine, come intersezione di due circonferenze centrate in punti noti e con raggi distanze tra altri punti dati. Siamo poi stati in grado di capire chi sono i possibili punti ottenibili con queste regole, in un numero finito di passi, partendo da un insieme finito di punti dati (v. teorema 16.4). Naturalmente vi sono altri modi per costruire punti. Un modo che vogliamo approfondire qui riguarda quello relativo all'origami, termine che, come dice Wikipedia, è derivato dal giapponese *oru* (piegare) e *kami* (carta).

Prima di dare una trattazione precisa delle regole che possono definire la piegatura di un foglio di carta, trattiamo alcuni esempi, al fine di prendere un po' di dimestichezza con il problema.

Esempio 18.1. Supponiamo di avere un foglio quadrato di carta. Vogliamo ottenere, con opportune piegature, un triangolo equilatero che ha per lato il lato del quadrato. Pieghiamo il quadrato in modo da mandare il punto B nel punto A e contemporaneamente il punto C nel punto D (quindi in modo da far combaciare la retta AD con la retta BC). Otteniamo così una piegatura verticale che è l'altezza (e mediana e bisettrice) relativa alla base del triangolo equilatero che stiamo cercando. Pieghiamo ora il foglio in modo da mandare il punto A sulla linea tratteggiata nel punto H lasciando fisso il punto B, veniamo così a determinare la linea tratteggiata obliqua. Il punto H è il vertice del triangolo equilatero cercato (perché, per costruzione, $AB = BH$). Eseguiamo allora le pieghe che passano per A e H e per B e H e abbiamo così determinato il triangolo equilatero (v. figura 13).

Esempio 18.2. Partiamo ancora da un foglio di carta quadrato. Sul lato AB vogliamo costruire un punto X tale che AX sia medio proporzionale tra AB e BX (quindi tale che AB/AX sia il numero aureo). Piegando a metà, come prima, il quadrato, determiniamo il punto E. Eseguiamo una piega che passa per

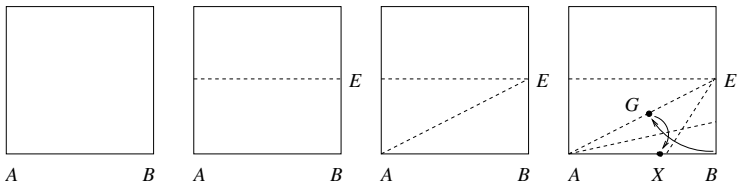

Figura 14: Costruzione del rapporto aureo.

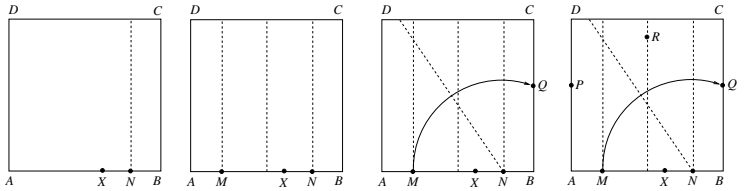

Figura 15: Costruzione di un pentagono regolare.

A ed E e poi una piega che passa per E e manda B in un punto G sulla piega AE. Infine facciamo una piega che passa per A e manda G in un punto X sul lato AB (v. figura 14). Se l è il lato del quadrato, abbiamo: $BE = l/2$, $AE = (l\sqrt{5})/2$, $AG = AE - BE = l(\sqrt{5} - 1)/2$, infine $BX = AB - AG = l(3 - \sqrt{5})/2$. Da questi dati, si vede subito che $AB \cdot BX = AX^2$.

Abbiamo visto, nella sezione 17, che la costruzione del rapporto aureo è importante per la costruzione, con riga e compasso, del pentagono regolare. Vediamo ora come, sulla base dei risultati dell'esempio 18.2, sia possibile ottenere un pentagono regolare con le piegature della carta.

Esempio 18.3. Anche in questo caso supponiamo di avere un foglio di carta quadrato e supponiamo di aver trovato la sezione aurea del lato AB (determinata dal punto X, ottenuto come nell'esempio precedente). Piegando il lato BC in modo da mandare il punto B nel punto X troviamo il punto medio N del segmento XB. Piegando il foglio in modo da mandare il punto B in A troviamo sia l'asse del segmento AB, sia un punto M su AB tale che AM sia congruo a BN. Il segmento MN è il lato del pentagono regolare che andiamo a determinare. Pieghiamo la carta in modo da lasciare fisso N e mandare M su un punto Q del lato BC. Ripiegando lungo l'asse otteniamo il punto P sul lato AD. Infine il punto R può essere deerminato facilmente piegando il foglio in modo da lasciare R fisso e mandare M sull'asse di AB. Il pentagono regolare cercato è dato dai punti $MNPRQ$, come si può verificare facilmente (v. figura 15)

Per concludere questa carellata di esempi, consideriamo ancora due ulteriori costruzioni: la trisezione di un angolo e un diverso modo di ottenere il pentagno regolare.

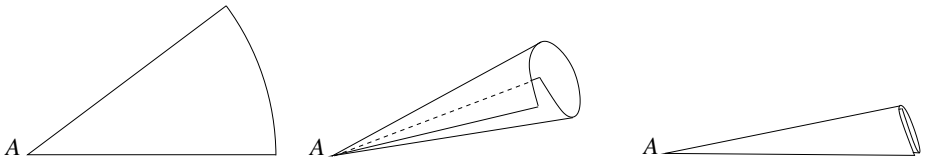

Figura 16: Possibile trisezione di un angolo.

Per quanto riguarda la trisezione, prendiamo un angolo (di carta) di vertice A e pieghiamo i due lati contemporaneamente, in modo da cercare di effettuare due pieghe che passano per A e tali che i lembi di carta si sovrappongano perfettamente. Riaprendo il foglio, si otterranno due pieghe che dovrebbero trisecare l'angolo (v. figura 16).

Infine, prendiamo una striscia di carta abbastanza lunga e sottile e facciamo un semplice noto. Poi tiriamo lievemente i due estremi, in modo che il nodo si stringa sempre di più e diventi sempre più piatto. Alla fine, quando saremo riusciti ad appiattire del tutto il nodo, abbiamo ottenuto un pentagono regolare.

Fino a qui abbiamo sviluppato qualche esempio per cercare di individuare le possibili regole che determinano le piegature della carta. Notiamo che nei primi esempi le costruzioni sono state molto più precise, usando essenzialmente due regole: si sono determinate piegature imponendo che una retta vada a sovrapporsi ad un'altra retta o che un punto vada a cadere su una retta e contemporaneamente un altro punto rimanga sulla piega da determinare. Negli ultimi due esempi la determinazione delle pieghe è stata molto più imprecisa: ha richiesto di procedere per tentativi ed errori, finché non si otteneva il risultato voluto. Gli ultimi due esempi potremmo dire che corrispondono in qualche modo al voler trasportare, con le tacche su un righello, le distanze quando si effettuano costruzioni con riga e compasso. Così come abbiamo scartato questa possibilità nel definire le costruzioni ammissibili con riga e compasso, altrettanto faremo adesso, fornendo una serie di possibili costruzioni da poter effettuare con le piegatura della carta che non richiedono di ottenere il risultato per successive approssimazioni. Ci sono varie (anche non equivalenti) regole che si usano dare quando si vuole trattare l'origami in modo sistematico. Qui abbiamo scelto una collezione di sette costruzioni, sei dovute al matematico H. Huzita (formulate nel 1992) e un'ulteriore dovuta al matematico K. Hatori, dette anche *assiomi di Huzita Hatori*. Servono ad ottenere, da una collezione di punti e rette (pieghe) nuovi punti (come intersezione di due rette) e nuove rette. Gli assiomi sono i seguenti:

Assiomi di Huzita Hatori

H_1 Dati due punti P_1 e P_2, esiste un'unica piegatura che passa per P_1 e P_2;

H_2 Dati due punti P_1 e P_2, esiste un'unica piegatura che porta P_1 in P_2;

H_3 Date due rette l_1 e l_2, esiste una piegatura che porta l_1 su l_2;

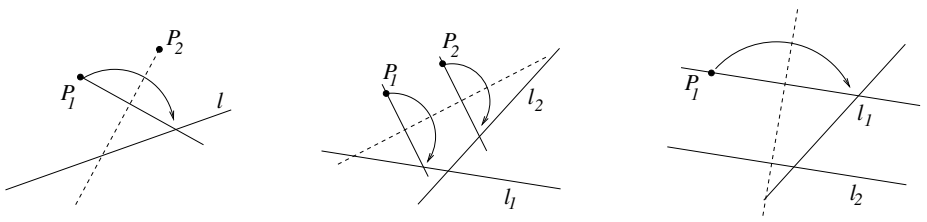

Figura 17: Gli assiomi H_5, H_6 e H_7 (la linea tratteggiata indica la piegatura).

H_4 Dato un punto P_1 e una retta l_1, esiste un'unica piegatura ortogonale ad l_1 che passa per P_1;

H_5 Dati due punti P_1 e P_2 e una retta l, se esiste una piegatura passante per P_2 che porta P_1 su l, tale piegatura può essere costruita;

H_6 Dati due punti P_1 e P_2 e due rette l_1 e l_2, se esiste una piegatura che porta P_1 su l_1 e P_2 su l_2, allora la piegatura può essere costruita;

H_7 Dato un punto P_1 e due rette l_1 ed l_2, esiste una piegatura ortogonale ad l_2 che porta P_1 su l_1.

Il primo assioma quindi dice che esiste sempre la retta per due punti. Il secondo assioma dice che si può trovare l'asse del segmento P_1P_2. Il terzo assioma dice che si possono bisecare angoli (nell'assioma si dice "esiste una piegatura" e non "esiste un'unica piegatura" perché due rette formano 4 angoli (a due a due opposti al vertice e ci sono quindi due possibilità per bisecarli). Il quarto assioma dice che da un punto si può sempre mandare la perpendicolare ad una retta. Nella figura 17 sono infine raffigurati gli ultimi tre assiomi.

Così come abbiamo visto succede per le costruzioni con riga e compasso, anche per quanto riguarda le costruzioni con le regole dell'origami, bisogna assumere che all'inizio siano dati alcuni punti, da cui partire. Come nel caso della riga e compasso, anche ora assumiamo che inizialmente siano dati due punti A_0 e A_1. Da essi si può costruire (con H_1) la retta x che li congiunge, si può costruire (con H_4) la retta y ortogonale alla retta A_0A_1 passante per A_0, si può assumere che il segmento che ha per estremi A_0 e A_1 sia unitario, con l'assioma H_5 si può mandare il punto A_1 in un punto sulla retta y e in questo modo si costruisce un sistema di assi cartesiani ortogonali, rispetto a cui riferire i punti del piano. Naturalmente sull'asse x si possono trovare tutti i punti a coordinate intere (con H_5 si manda il punto A_0 in un punto A_2 sull'asse x lasciando fisso il punto A_1, quindi A_2 ha ascissa 2, e così via). Applicando due volte l'assioma H_4 si vede che, dato un punto P e una retta l, si può costruire una retta passante per P e parallela ad l e in questo modo possiamo usare il teorema di Talete per dividere un segmento in n parti uguali (come nel caso delle costruzioni con riga e compasso), pertanto possiamo assumere che sull'asse x (e analogamente sull'asse y) siano costruibili tutti i punti a coordinate razionali.

Soffermiamoci ora ad analizzare le costruzioni che si possono effetture con i soli assiomi H_1–H_5. Vediamo intanto che ognuna delle costruzioni richieste da essi si può anche effettuare con riga e compasso. Per quanto riguarda i primi 4 assiomi, il risultato è evidente e lo abbiamo già evidenziato quando li abbiamo commentati. Per quanto riguarda H_5, consideriamo il punto Q della retta l in cui P_1 viene mandato dalla piegatura. Sia R il punto di mezzo del segmento P_1Q. Allora la piegatura stessa risulta essere l'asse del segmento P_1Q e quindi passa per R. Inoltre il punto R si trova sulla circonferenza passante per P_1 e P_2 con diametro P_1P_2 (in quanto P_1R e P_2R sono ortogonali). Pertanto la piegatura passante per P_2 e che manda P_1 su l può essere costruita con riga e compasso nel seguente modo: si traccia la circonferenza con diametro P_1P_2 e passante per P_1 e P_2. Si traccia la perpendicolare ad l passante per P_1, sia S il punto d'incontro di tale perpendicolare con l. Si trova il punto di mezzo del segmento P_1S. Da esso si manda la retta parallela ad l. Sia R un punto d'incontro di tale parallela con la circonferenza per P_1 e P_2. La retta P_2R è la piegatura cercata.

In questo modo abbiamo mostrato che tutte le costruzioni che si possono fare con gli assiomi H_1–H_5 si possono fare anche con riga e compasso.

Ora vedremo che vale anche il viceversa. Abbiamo bisogno di alcune premesse. Innanzitutto si ricordi che i punti di una parabola possono essere definiti come tutti i punti del piano equidistanti da un punto fisso F (detto fuoco) e da una retta d (detta direttrice).

Lemma 18.4. *Sia Q un punto di una parabola con fuoco F e direttrice d. Sia R il punto su d tale che $FQ = QR$. Allora la retta tangente alla parabola in Q è l'asse del segmento FR.*

Dimostrazione. A meno di cambiamenti di coordinate, l'equazione della parabola è $y = ax^2$ (con $a \in \mathbb{R}$). In questo caso il suo fuoco ha coordinate $F = (0, 1/(4a))$ mentre la direttrice ha equazione $y = -1/(4a)$. Se quindi $Q = (x_0, ax_0^2)$ è un punto della parabola, il punto R ha coordiante $(x_0, -1/(4a))$, la retta tangente alla parabola in Q ha equazione $y = 2ax_0x - ax_0^2$ e il risultato segue facilmente da questi dati. □

Supponiamo siano ora dati un punto F e una retta d del piano. L'assioma H_5 permette di trovare punti della parabola con fuoco F e direttrice d. Infatti, sia T un ulteriore punto del piano e, con l'assioma H_5, si costruisca la retta t per T che manda F su d, in un punto R. Allora la retta t è l'asse del segmento FR. Da R si mandi la perpendicolare a d che incontra t in un punto Q. Il punto Q è un punto della parabola inoltre, per il lemma precedente, la retta t è tangente alla parabola in Q. Riuscire a tracciare punti di una parabola permette di trovare radici quadrate di numeri (costruibili). Fissiamo infatti una parabola che, come nel lemma precedente, assumiamo avere equazione $y = ax^2$. Partiamo da un punto $T = (\alpha, \beta)$ e supponiamo stia sulla retta tangente alla parabola nel punto $Q = (x_0, y_0)$. Poiché tale retta, come visto nel lemma, ha equazione $y = 2ax_0x - ax_0^2$, abbiamo che deve essere $\beta = 2ax_0\alpha - ax_0^2$. Se scegliamo $\alpha = 0$, abbiamo che $x_0^2 = -\beta/a$, quindi $x_0 = \sqrt{-\beta/a}$, questo mostra

che l'ascissa del punto Q (e del punto R) è la radice quadrata del numero $-\beta/a$. Supponiamo di avere un numero r (per esempio dato come ascissa di un punto) di cui vogliamo calcolare la radice quadrata. Allora prendiamo la parabola con coefficiente $a = 1/4$ e quindi il suo fuoco è il punto $F = (0, 1)$ mentre la direttrice è la retta $y = -1$. Prendiamo il punto $T = (0, -r/4)$ e costruiamo, con H_5, il punto R su d trasformato di F con la piegatura che passa per T. In base ai conti precedenti, l'ascissa di R vale $\sqrt{r}$.

Conseguenza di queste considerazioni è il seguente:

Teorema 18.5. *Dati due punti A_0 e A_1 nel piano, tutti i punti che si possono costruire, a partire da essi, con riga e compasso, si possono anche costruire con le cinque regole H_1–H_5 dell'origami. Viceversa, tutti i punti che si possono costruire con le regole H_1–H_5 dell'origami, si possono anche costuire con riga e compasso.*

Dimostrazione. Si è già visto che H_1–H_5 sono ottenibili con construzioni con riga e compasso, vediamo quindi il viceversa. Assumiamo H_1–H_5, come abbiamo visto nella sezione 16, i nuovi punti che si ottengono nelle costruzioni con riga e compasso nascono in tre modi possibili: o come intersezione di due rette, o come intersezione di una retta e di una circonferenza o come intersezione di due circonferenze. Inoltre le rette sono costruite quando si conoscono due punti per cui devono passare. La regola H_1 comporta che il punto intersezione di due rette si può costruire anche con le regole dell'origami. L'intersezione di una retta e una circonferenza o di due circonferenze comporta, una volta fissato un sistema di assi cartesiani, la soluzione di un'equazione di secondo grado che a sua volta richiede saper calcolare la radice quadrata di un numero. Poiché abbiamo visto che, grazie ad H_5, si possono calcolare le radici quadrate, abbiamo che si riescono a trovare, con i primi cinque assiomi dell'origami, i punti di intersezione di una retta con una circonferenza e di due circonferenze. □

Osservazione 18.6. Vi è un modo geometrico di calcolare, con H_5, l'intersezione di una retta ed una circonferenza. Partiamo da una circonferenza di centro C e passante per un punto P con una retta r. Sulla retta CP si costruisce il punto Q simmetrico a P rispetto a C. Si costruisce la perpendicolare al r passante per Q e si trova il punto H. Sulla retta QH si costruisce il punto R simmetrico di Q rispetto ad H. Si costruisce la retta s parallela ad r e passante per R. Con H_5 si trova la retta passante per P e tale che riflette Q in un punto Q' di s. La retta s, la retta r e la retta QQ' si incontrano in un punto A che è un punto di incontro della circonferenza di centro C e raggio CP con la retta r. L'altro punto B di incontro della circonferenza con r si trova in modo analogo o si sfrutta il fatto che è simmetrico di A rispetto alla retta ortogonale ad r passante per C. (v. figura 18, (1)).
Analogamente si può calcolare l'intersezione di due circonferenze. Supponiamo siano C_1 e C_2 i due centri di due circonferenze passanti per i punti R_1 e R_2 rispettivamente. Usando la costruizione precedente, possiamo assumere che il punto R_1 sia tale che la retta R_1C_1 sia perpendicolare alla retta C_1C_2 e analogamente R_2 sia tale che la retta R_2C_2 sia anche perpendicolare a C_1C_2. Congiungiamo

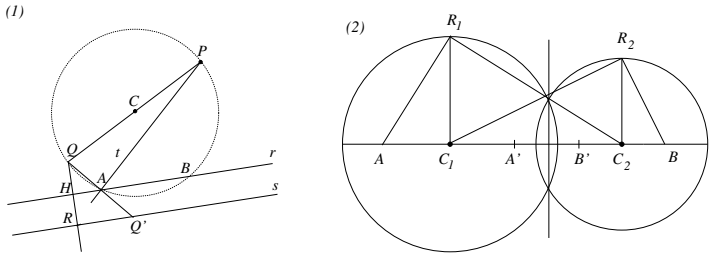

Figura 18: Calcolo dei punti di intersezione di una retta e una circonferenza e di due circonferenze con gli assiomi H_1–H_5.

R_1 con C_2 e mandiamo da R_1 la retta perpendicolare a R_1C_1 e sia A il punto d'incontro di tale retta con la retta C_1C_2. Analogamente congiungiamo R_2 con C_1 e costruiamo il triangolo rettangolo C_1R_2B. Infine costruiamo i punti A' simmetrico di A, rispetto a C_1, e B', simmetrico di B, rispetto a C_2. Si può vedere che la retta ortogonale alla retta C_1C_2 e passante per il punto di mezzo M del segmento $A'B'$ passa per i due punti d'incontro delle due circonferenze. Se proviamo questo, allora abbiamo che i punti d'incontro delle due circonferenze si possono ottenere con la costruzione precedente (v. figura 18, (2)). Sia r_1 il raggio della prima circonferenza, r_2 il raggio della seconda circonferenza, d la distanza dei due centri, a la lunghezza del segmento C_1A e b la lunghezza del segmento C_2B. Per il secondo teorema di Euclide vale $ad = r_1^2$ e $bd = r_2^2$. Inoltre la lunghezza di C_1M vale $a + (d - a - b)/2$ mentre la lunghezza di C_2M vale $b + (d - a - b)/2$. Consideriamo ora due triangoli rettangoli di cateto, rispettivamente, C_1M e C_2M e ipotenusa relativa r_1 e r_2. Usando il teorema di Pitagora si vede che gli altri due cateti dei due triangoli rettangoli sono congruenti. Questo prova che la verticale, passante per M, incontra le due circonferenze nei due punti d'intersezione delle due circonferenze.

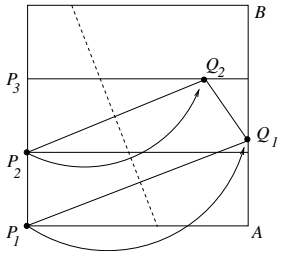

Figura 19: Calcolo di $\sqrt[3]{2}$

19 Gli assiomi H_6 e H_7

L'assioma H_6 aggiunge altre possibilità alle costruzioni che si possono fare con le regole dell'origami e che non sono possibili con riga e compasso. Esso può essere reinterpretato (alla luce di quanto discusso in conseguenza del lemma 18.4) osservando che esso permette, quando possibile, di trovare una retta che sia tangente contemporaneamente a due parabole (il punto P_1 e la retta l_1 sono il fuoco e la direttrice della prima parabola, il punto P_2 e la retta l_2 sono il fuoco e la direttrice della seconda parabola). Infatti tale tangente, per il lemma 18.4 è proprio la retta t della piegatura.

Questa osservazione ha importanti conseguenze perché permette di vedere che con le regole dell'origami si riescono a trovare le soluzioni reali di equazioni di terzo grado. Consideriamo le seguenti due parabole:

$$\left(y - \frac{1}{2}a\right)^2 = 2bx \quad \text{e} \quad y = \frac{1}{2}x^2$$

Se a e b sono numeri costruibili con le regole dell'origami, il fuoco e la direttrice di ciascuna di queste due parabole sono costruibili. Supponiamo che una retta tangente ad entrambe le parabole abbia coefficiente angolare μ e passi per i punti (x_0, y_0) della prima parabola e per il punto (x_1, y_1) della seconda. Con qualche conto analitico si vede che la retta è tangente alle parabole quando μ soddisfa l'equazione:

$$\mu^3 + a\mu + b = 0$$

quindi trovare una retta tangente alle due parabole vuol dire trovare una soluzione a questa equazione di terzo grado (che è un'equazione generica, in quanto ogni equazione di terzo grado, in una variabile, può essere trasformata in una in cui il coefficiente della seconda potenza della variabile non compare).

Il problema della duplicazione del cubo, non risolvibile con riga e compasso, comporta risolvere un'equazione di terzo grado della forma: $x^3 - 2 = 0$. Con le regole dell'origami (e in particolare, grazie a H_6), questo può esser fatto. Un modo per prodedere è il seguente: si parte da un quadrato e si divide un lato (diciamo il lato AB) in tre parti uguali tracciando due rette orizzontali. Si determinano così tre punti P_1, P_2 e P_3 sul lato opposto al lato AB (v. figura 19).

Si piega poi il quadrato in modo da mandare contemporaneamente il punto P_1 sul lato AB (in Q_1) e il punto P_2 sulla retta orizzontale, passante per P_3 (nel punto che chiamiamo Q_1). Si può verificare che il rapporto $\overline{Q_2B}/\overline{Q_2A}$ vale $\sqrt[3]{2}$.

Accenniamo ora brevemente alla costruzione relativa alla trisezione di un angolo. Come si è visto nel teorema 16.6, trisecare un angolo comporta saper risolvere un'equazione di terzo grado, operazione che, abbiamo visto, con H_6 è possibile. La costruzione può essere trovata facilmente in internet. Una possibile fonte può essere l'articolo sul sito:
`http://matematica.unibocconi.it/articoli/la-geometria-degli-origami`
dove si trova anche una dimostrazione matematica della costruzione.

Per quanto riguarda l'assioma H_7, si può vedere che esso è conseguenza degli assiomi precedenti, quindi non ci sono ulteriori costruzioni che sono ottenibili da esso e non già dagli altri.