Sugli insiemi numerici

Marcello Seri

21 aprile 2007

Indice

1 Introduzione **2**

2 I numeri naturali **4**
2.1 Gi assiomi di Peano 6
2.2 Le operazioni tra numeri naturali 8

3 I numeri interi **13**

4 I numeri razionali **18**
4.1 Breve premessa sui campi 18
4.2 Dagli interi ai razionali 19

5 I numeri reali **23**

6 I numeri complessi **28**

7 Note conclusive **31**

Riferimenti bibliografici **31**

1 Introduzione

"I numeri regnano sull'universo."
Pitagora (Samo, ca. 572 a.C. - Metaponto, ca. 490 a.C.)

Le origini dei numeri naturali vengono normalmente fatte risalireal 2000 a.C., come testimoniato dalla *tavoletta Plimpton 322* babilonese, probabilmente il primo "sussidiario di matematica" della storia, e dalle tavole numeriche, elenchi di numeri utilizzati per calcoli astronomici e di agrimensura risalenti al X secolo a.C..

Tuttavia nelle culture dell'antica Mesopotamia esistevano tabelle per le addizioni e le sottrazioni già durante il regno di Sargon I, intorno al 2350 a.C..

I documenti dell'Antico Egitto più significativi sono il *papiro di Ahmes* o *Ahmose*, dal nome dello scriba che lo compose nel 1650 a.C. circa, e il *papiro di Mosca*, risalente al 1850 a.C. circa. In totale questi papiri presentano 112 problemi con le relative soluzioni (di cui purtroppo mancano le dimostrazioni).
Tuttavia Ahmes ci dice che il suo materiale è tratto da un documento anteriore, e fa risalire l'originale ad Imhotep, medico e architetto del faraone Djoser della III dinastia, e quindi al 2650 a.C. circa.

L'uso di concetti numerici avanzati, è documentato anche nel *Sulvasutra* indiano, di datazione incerta ma comunque anteriore al VI secolo a.C.. Alcuni particolari comuni tra il *Sulvasutra* e gli *Elementi di Euclide* fanno pensare ad una derivazione diretta o ad un comune retaggio. Ad esempio entrambi utilizzano la media geometrica per la quadratura del rettangolo, ossia la costruzione di un quadrato di area equivalente a quella di un rettangolo dato e questo metodo non è né il più semplice né il più istintivo.

In Grecia, da subito il numero ha avuto un posto centrale nella filosofia: dall'*Uno* di Parmenide e Filolao ai numeri triangolari, pentagonali, piani e solidi dei Pitagorici, passando per la concezione platonica del numero come oggetto concreto del mondo delle idee.

Uno scoglio insolubile nella visione della matematica antica, prettamente basata sugli interi, fu la dimostrazione dell'incommensurabilità della diagonale di un quadrato e del suo lato.

Nel frattempo, anche l'oriente poteva già vantarsi di una cultura numerica molto profonda. La più antica testimonianza della matematica cinese risale al periodo degli Stati Combattenti. Si tratta di un manoscritto, il *Chou Pei Suan Ching o Zhoubi suanjing* (Il libro classico dello gnomone e delle orbite circolari del cielo). Oltre ad essere un testo di astronomia, introduce il teorema di Pitagora e alcune regole per le operazioni con le frazioni. La sua

datazione è incerta, ma si ritiene possa essere stato scritto tra il VI e il III secolo a.C., e forse è basato su materiale precedente ignoto. Nel 1984, in tre tombe della dinastia Han vicino Jiangling, nella provincia di Hubei, vennero portate alla luce numerose striscie di bambù, che costituivano una raccolta di argomenti matematici: su una di esse vi era l'intestazione *Suan Shu Shu* (Un libro sull'aritmetica). Vengono datate intorno all'inizio del III secolo AC, e probabilmente sono dunque contemporanee al Chou Pei. Favoriti dal vantaggio di un sistema posizionale, dell'uso dello zero e dei negativi, in pochi secoli i matematici cinesi arrivarono ad avere conoscenze matematiche che l'occidente avrebbe visto solo molto più tardi: ad esempio, già nell'XI secolo il matematico Chia Hsien aveva sviluppato il triangolo di Pascal per l'espansione della potenza n-esima del binomio $(a+b)$ in forma esplicita. Inoltre, sia William Horner che Paolo Ruffini conoscevano, e potrebbero avervi basato i loro metodi, la soluzione cinese per trovare le radici delle equazioni di grado qualunque.

I metodi cinesi di calcolo arrivarono fino in Giappone, dove nel XVII secolo Seki Kowa, vero genio fuori dal tempo, introdusse sia una forma di calcolo detto *yenri* del tutto equivalente a quelli moderni basati su derivate ed integrali che utilizzò per calcolare il volume della sfera, sia il concetto di determinante, nel suo trattato *Kai Fukadai No Ho* del 1683.

Anche i Maya avevano raggiunto un altro grado di rappresentazione dei numeri grazie al quale potevano cimentarsi nelle scienze matematiche e nell'astronomia con risultati a volte sconcertanti. A loro, infatti, viene attribuita anche la scoperta dello zero, molto prima di quando accadde in India.

Nonostante tutto questo, la struttura dei numeri, legata ai cosiddetti numeri primi, è ancora oggi un mistero. Per una prima assiomatizzazione si è dovuta attendere la fine del XIX secolo, quando negli *Aritmetca Principia* il matematico italiano Giuseppe Peano scrisse i cinque postulati che ancora portano il suo nome.

Questo testo vuole essere un breve ma esauriente viaggio nella costruzione dei numeri, a partire dalla definizione dei numeri naturali e delle operazioni elementari fino ad arrivare a definire i numeri complessi dimostrandone le proprietà. Un percorso che corre in poco più di un secolo di storia della matematica ma che tocca argomenti vecchi di millenni.

2 I numeri naturali

"Dio ci ha dato i numeri naturali,
il resto è opera dell'uomo."
Leopold Kronecker (Liegnitz, 1823 - Berlino, 1891)

Quanto vale 1? Che cosa è la "dualità", cioè quella proprietà che caratterizza il 2? Cosa identifica il 3? Sembra una domanda ovvia dalla risposta ancora più ovvia, eppure come rispondereste?

Ci sono vari modi per definire i numeri. Si potrebbe definire 2 come l'elemento che caratterizza *tutti* gli insiemi con due elementi ad esempio. Noi seguiremo una strada diversa. Cerchiamo una via che identifichi i numeri tramite un confronto con una sorta di "metro" fissato. In effetti, per stabilire se due oggetti hanno o meno la stessa lunghezza basta confrontarli, non serve conoscere con precisione la definizione di "lunghezza".

Supponiamo di esser riusciti a definire un numero, ad esempio 42, proprio come un insieme con 42 elementi. Come possiamo definire il 43, cioè un insieme con esattamente 43 elementi? Il modo più ovvio che può venirci in mente, visto che in 42 possiamo già trovare 42 elementi, è definire 43 come l'insieme che contenga i 42 elementi di 42 più 42 stesso.

L'idea che sta dietro a tutta la costruzione, dunque, è che ogni numero corrisponde all'insieme dei suoi predecessori. Sulla base di questo è possibile definire il concetto di successore:

Definizione 2.1. *Dato un insieme x, definiamo* successore $s(x)$ *di x l'insieme ottenuto aggiungendo x stesso agli elementi di x:*

$$s(x) = x \cup \{x\}.$$

Con questa idea di successori e predecessori, se vogliamo che 0 identifichi l'insieme che contiene zero elementi, è inevitabile definire

$$0 = \{\} = \varnothing.$$

Forti di quest'idea, per mantenere la notazione comune risulta naturale definire

$$\begin{aligned}
1 &= s(0) = \{\{\}\} = \{\varnothing\} = \{0\},\\
2 &= s(1) = \{\{\}, \{\{\}\}\} = \{0, \{0\}\} = \{0, 1\},\\
3 &= s(2) = \{\{\}, \{\{\}\}, \{\{\}, \{\{\}\}\}\} = \{0, \{0\}, \{0, \{0\}\}\} = \{0, 1, 2\},\\
4 &= s(4) = \{0, 1, 2, 3\},
\end{aligned}$$

e così via per tutti gli altri numeri.

Su questo "e così via", però, sorge un problema: non abbiamo nessuna garanzia che tale costruzione sui successori possa essere protratta all'infinito restando sempre in uno stesso grande insieme contenitore. D'altra parte non abbiamo ancora definito nemmeno il concetto di "infinitezza". Queste sono due delle ragioni per cui in ZF (teoria assiomatica degli insiemi di Zermelo-Fraenkel) è stato introdotto il seguente postulato.

Assioma 2.1 (dell'infinito)**.** *Esiste un insieme A che contiene 0 ed il successore di ogni suo elemento.*
Nel linguaggio formale di ZF ciò corrisponde a scrivere

$$\exists A : \varnothing \in A \wedge (\forall : a \in A \Longrightarrow a \cup \{a\} \in A)$$

È ragionevole pensare che un insieme del tipo descritto dall'assioma appena enunciato è infinito.

Definizione 2.2. *Un insieme A si definisce* insieme induttivo *se*

(i) $0 \in A$,

(ii) se $x \in A$, *allora* $s(x) \in A$.

L'assioma di infinitezza ci dice che esiste almeno un insieme induttivo A. Basta applicare le proprietà della definizione per osservare che l'intersezione di insiemi induttivi (non vuoti) è ancora un insieme induttivo, dunque l'intersezione degli insiemi induttivi contenuti in A è, a sua volta, un insieme induttivo ω.

Teorema 2.1. *L'insieme ω è un sottoinsieme di ogni insieme induttivo.*

Dimostrazione. Sia B un generico insieme induttivo, come abbiamo detto lo è anche $A \cap B$. Allo stesso tempo $A \cap B \subset A$ dunque è uno degli insiemi che intervengono nella definizione di ω, il che implica che $\omega \subset A \cap B$, quindi $\omega \subset B$. □

Lasciatemi ora scrivere un altro dei postulati di ZF.

Assioma 2.2 (dell'estensione)**.** *Dato un generico insieme A e dato un generico insieme B, $A = B$ se e solo se, dato un qualsiasi altro C, C è un elemento di A se e solo se C è un elemento di B.*
Nel linguaggio formale di ZF ciò corrisponde a scrivere

$$\forall A, \forall B : A = B \Longleftrightarrow (\forall C : C \in A \Leftrightarrow C \in B),$$

L'assioma dell'estensione ci garantisce che può esistere un solo insieme induttivo contenuto in ogni insieme induttivo, quindi la proprietà di minimalità trovata su ω lo caratterizza univocamente.

Vedremo che l'insieme ω è l'insieme dei *numeri naturali* e la costruzione insiemistica che abbiamo fatto risolve il problema del "e così via" di cui si è parlato prima. Da ora in poi, quindi, identificheremo ω con $\mathbb{N}$.

Per quanto questa costruzione possa sembrare controintuitiva e possa sconvolgere in qualche modo l'idea che ognuno di noi aveva dei numeri naturali, oltre a porre delle basi più solide e a risolvere alcuni problemi delle assiomatiche precedenti, ci permette di recuperare quelli che erano gli *Assiomi di Peano* su cui si basava la teoria aritmetica dei numeri naturali.

2.1 Gi assiomi di Peano

La proprietà più importante dell'insieme $\mathbb{N}$ dei numeri naturali è che si tratta dell'*unico insieme induttivo che è sottoinsieme di ogni insieme induttivo.*

Per essere un insieme induttivo, certamente deve accadere che

(I) $0 \in \mathbb{N}$

dove, come abbiamo visto, $0 = \varnothing$, e che

(II) $n \in \mathbb{N} \Rightarrow s(n) \in \mathbb{N}$

dove $s(n) = n \cup \{n\}$. D'altra parte la minimalità ci dice che se se S è un sottoinsieme induttivo di $\mathbb{N}$, necessariamente $S = \mathbb{N}$, in altri termini

(III) sia $S \subseteq \mathbb{N}$, se $0 \in S$ e $n \in S \Rightarrow s(n) \in S$, allora $S = \mathbb{N}$.

Quindi siamo riusciti a ricavare senza sforzo anche il *Principio di Induzione.*

Per ricostruire l'assiomatica di Peano, a questo punto, dobbiamo dimostrare soltanto altre due proprietà:

(IV) $s(n) \neq 0 \; \forall n \in \mathbb{N}$

(V) se $n, m \in \mathbb{N}$ e se $s(n) = s(m)$, allora $n = m$

Dimostrazione.

(IV) Sappiamo che $0 = \varnothing$ e $s(n) \supset n$ quindi, quale che sia n, $s(n) \supset 0$. D'altra parte l'insieme vuoto non può contenere propriamente altri insiemi, dunque $s(n) \neq 0$.

(V) Per dimostrare questa proprietà, è necessario premettere i due lemmi seguenti:

Lemma 2.2. *Nessun numero naturale è un sottoinsieme di un suo elemento. Cioè*

$$\forall n \in \mathbb{N}, \nexists\, m \in n \text{ tale che } n \subset m$$

Lemma 2.3. *Ogni elemento di un numero naturale è un suo sottoinsieme. Cioè*

$$\forall n \in \mathbb{N}, \forall m \in n, m \subset n$$

Nota 2.1. Un insieme T si dice *transitivo* se accade che $x \in y$ e $y \in T$ implicano $x \in T$. Il secondo lemma ci dice che i numeri naturali sono insiemi transitivi.

Dimostrazione. La dimostrazione del primo lemma è un'applicazione del Principio di Induzione. Sia $S = \{n \in \mathbb{N} : \forall m \in n, n \nsubseteq m\}$ l'insieme di tutti i numeri naturali n che non sono inclusi nei loro elementi.
Poiché 0 non ha elementi, non può essere contenuto nei suoi elementi, dunque $0 \in S$.
Supponiamo ora che $n \in S$. Poiché n è contenuto in se stesso ed appartiene ad S, n non può essere un elemento di n, dunque $s(n)$ non può essere contenuto in n per definizione. Preso un $x \in \mathbb{N}$ tale che $s(n) \subset x$, necessariamente $n \subset x$ e quindi, ricordando che $n \in S$, avremo $x \notin n$, cioè $s(n)$ non può essere un sottoinsieme di n e non può essere sottoinsieme di alcun elemento di n, allora $s(n)$ non può essere sottoinsieme di nessun suo elemento, dunque $s(n) \in S$. Applicando il principio di induzione si ottiene la tesi.

Anche la dimostrazione del secondo lemma è un'applicazione del principio di induzione. Sia ora $S = \{n \in \mathbb{N} : \forall m \in n, m \subset n\}$ l'insieme di tutti i numeri naturali transitivi.
Il fatto che $0 \in S$ è banale.
Supponiamo $n \in S$, sia $x \in s(n)$, di certo $x \in n$ oppure $x = n$. Nel primo caso $x \subset n$ in quanto $n \in S$ e dunque $x \subset s(n)$, nel secondo caso $x \subset s(n)$ per definizione. Dunque ogni elemento di $s(n)$ è un suo sottoinsieme, che significa $s(n) \in S$. Applicando il principio di induzione si ottiene la tesi. □

A questo punto possiamo dimostrare la proprietà (V). Siano m ed n naturali tali che $s(m) = s(n)$. Poiché $n \subset s(n)$, deve accadere anche che $n \subset s(m)$ e dunque anche che $n \in m$ o $n = m$. Allo stesso modo

deve accadere che $m \in n$ o $m = n$.
Supponiamo per assurdo $n \neq m$. Abbiamo che $n \in m$ ed $m \in n$. Il secondo lemma ci dice che n è transitivo, quindi dovrebbe accadere che $n \in n$. Ma questo significa che $n \subset n$ e dunque stiamo contraddicendo il primo lemma. Di conseguenza $n = m$.

□

2.2 Le operazioni tra numeri naturali

A partire dalle proprietà (I)-(V) che, come abbiamo detto, coincidono con gli assiomi di Peano, è possibile definire anche i numeri interi, razionali, reali e complessi e derivare tutte le loro proprietà aritmetiche e analitiche. Cerchiamo innanzitutto di ricostruire le operazioni e le strutture algebriche comunemente associate ai numeri naturali.

La costruzione fatta, alla luce anche di quanto osservato fin qui, conduce in modo naturale alla definizione di una relazione d'ordine totale di "minore o uguale" sui numeri naturali per la quale dati $a, b \in \mathbb{N}$, $a \leq b$ se e solo se $a \subseteq b$. Presupposti gli assiomi di Zermelo-Fraenkel per la teoria degli insiemi (quelli su cui è basato tutto il lavoro in sostanza), non è difficile verificare che '$\leq$' verifica le seguenti proprietà: $\forall a, b, c \in \mathbb{N}$

1. $a \leq a$ (riflessiva)
2. $((a \leq b) \wedge (b \leq a)) \Rightarrow (a = b)$ (antisimmetrica)
3. $((a \leq b) \wedge (b \leq c)) \Rightarrow (a \leq c)$ (transitiva)
4. $(a \leq b) \vee (b \leq a)$ (ordine totale)

Al momento i naturali sembrano essere una struttura molto povera, abbiamo definito soltanto un ordine totale che non sembra troppo comodo ed intuitivo da usare e non ci sono ancora né la somma né il prodotto. C'è ancora un fatto, che potrebbe sfuggire, che ci impedisce di definirle in modo semplice: vorremmo introdurle utilizzando una funzione ricorsiva ma il principio di induzione non basta a garantirci l'esistenza di una tale applicazione. Cerchiamo di dimostrare che possiamo farlo.

Teorema 2.4 (di ricorsione)**.** *Sia x_0 un elemento di un insieme X, se $h : X \to X$ è una funzione, allora esiste una funzione f da $\mathbb{N}$ in X tale che*

(i) $f(0) = x_0$,

(ii) $f(s(n)) = h(f(n))\ \forall n \in \mathbb{N}$.

Dimostrazione. Cominciamo provando l'unicità di tale f.
Supponiamo esistano f e g che verificano le due proprietà e procediamo per induzione.
Per $n = 0$ si ha $f(0) = x_0 = g(0)$.
Supponiamo ora $f(n) = g(n)$, allora $f(s(n)) = h(f(n)) = h(g(n)) = g(s(n))$.

Proviamo ora l'esistenza.
Una funzione da $\mathbb{N}$ in X è per definizione un particolare sottoinsieme di $\mathbb{N}\times X$, cerchiamo di costruire f esplicitamente (come insieme di coppie ordinate). Sia Ω la collezione dei sottoinsiemi A di $\mathbb{N} \times X$ tali che

(a) $(0, x_0) \in A$,

(b) $(n, x) \in A \Rightarrow (s(n), h(x)) \in A$.

Poiché $\mathbb{N} \times X$ soddisfa tali ipotesi, la collezione Ω non è vuota.
Consideriamo l'intersezione f di tutti gli insiemi della collezione Ω. Ovviamente $\forall A \in \Omega,\ f \subset A$. Poiché $(0, x_0)$ appartiene a tutti gli $A \in \Omega$, $(0, x_0) \in \cap_{A\in\Omega} A = f$; d'altra parte se $(n, x) \in f$ allora $(n, x) \in A$ $(\forall A \in \Omega)$, ma per la seconda proprietà di Ω, ogni A contiene anche $(s(n), h(x))$ e quindi $(s(n), h(x)) \in f$. Ma questo vuol dire che $f \in \Omega$.

Resta da provare che $\forall n \in \mathbb{N}\ \exists!\, x \in X : (n, x) \in f$. Sia

$$S = \{n \in \mathbb{N} : \exists!\, x \in X \text{ t.c. } (n, x) \in f\},$$

dobbiamo mostrare che $0 \in S$ e che $n \in S \Rightarrow s(n) \in S$.
Procediamo per induzione su n.
Sia $n = 0$, sappiamo già che $(0, x_0) \in f$. Supponiamo per assurdo che esista $(0, y) \in f$ con $y \neq x_0$. Sia $f' = f - \{(0, y)\}$, chiaramente $(0, x_0) \in f'$ e, poiché $s(n) \neq 0$ per ogni n, $(s(n), h(x)) \neq (0, y)$, quindi se $(n, x) \in f'$ allora $(s(n), h(x)) \in f'$. Ma questo implica che $f' \in \Omega$ che è assurdo in quanto $f \nsubseteq f'$. Quindi $0 \in S$.
Supponiamo ora $n \in S$. Sia $x \in X$ l'unico elemento per cui $(n, x) \in f$. Poiché f soddisfa la (b), $(s(n), h(x)) \in f$. Supponiamo per assurdo che anche $(s(n), y) \in f$ con $y \neq h(x)$. Sia, come prima, $f' = f - \{(s(n), y)\}$. Dalla proprietà (IV) segue che $(0, x_0) \neq (s(n), y)$ e quindi, dato che $(0, x_0) \in f$ si ha $(0, x_0) \in f'$. D'altra parte, se $(m, z) \in f' \subset f$, allora $(s(m), h(z)) \in f$.
Si hanno due casi: $n \neq m$ oppure $n = m$. Se $n \neq m$, per la proprietà (V) si ha $(s(m), h(z)) \neq (s(n), y)$ e quindi $(s(m), h(z)) \in f'$. Se, invece, $m = n$ allora

$(m, z) = (n, z) \in f$ ma per ipotesi induttiva esiste un unico $x \in X$ per cui $(n, x) \in f$, dunque $z = x$. Dato che $h(x) \neq y$, $(s(m), h(z)) = (s(n), h(x)) \in f'$. Quindi $f' \in \Omega$ che è assurdo in quanto $f \nsubseteq f'$. Quindi $s(n) \in S$. □

Il teorema di ricorsione è uno strumento molto potente e flessibile. Finalmente possiamo premetterci di definire qualche operazione:

Definizione 2.3 (Somma)**.** *Dato $n \in \mathbb{N}$ si chiama* somma *la funzione $m \mapsto n + m$ definita ricorsivamente da*

(i) $n + 0 = n$

(ii) $n + s(m) = s(n + m)$

Si noti che in base a questa definizione $s(n) = n + 1$ $\forall n \in \mathbb{N}$, infatti $n + 1 = n + s(0) = s(n + 0) = s(n)$.

Lemma 2.5. *La struttura algebrica data da $(\mathbb{N}, +)$ è un monoide abeliano cioè valgono le seguenti proprietà: $\forall a, b, c \in \mathbb{N}$*

(i) $(a + b) + c = a + (b + c)$ *(associativa)*

(ii) $a + 0 = 0 + a = a$ *(elemento neutro)*

(iii) $a + b = b + a$ *(commutativa)*

Dimostrazione. Verifichiamo le tre proprietà.

(i) Per $c = 0$ e $c = 1$ la proprietà è banalmente verificata. Supponiamo ora che sia vera per c e dimostriamo che è vera per $c + 1 = s(c)$. Si ha

$$\begin{aligned}(a + b) + s(c) &= s((a + b) + c) = s(a + (b + c)) = a + s(b + c) = \\ &= a + [(b + c) + 1] = a + [b + (c + 1)] = a + (b + s(c)).\end{aligned}$$

Per il principio di induzione la proprietà risulta dimostrata.

(iii) Prima di tutto dimostriamo che $\forall a \in \mathbb{N}$ si ha $a + 1 = 1 + a$. Se $a = 1$ non ci sono problemi. Supponiamo sia vera per a, si ha

$$s(a) + 1 = (a + 1) + 1 = (1 + a) + 1 = 1 + (a + 1) = 1 + s(a).$$

Pertanto la commutativa vale certamente se uno dei due elementi è 1. Supponiamo valga per un b qualunque e dimostriamo che vale anche per $s(b)$. Si ha

$$\begin{aligned}a + s(b) &= s(a + b) = s(b + a) = b + s(a) = \\ &= b + (a + 1) = b + (1 + a) = (b + 1) + a = s(b) + a.\end{aligned}$$

(ii) Si dimostra banalmente sfruttando le definizioni.

□

Altrettanto facilmente è possibile verificare che:

Teorema 2.6 (Legge di cancellazione della somma)**.**
Comunque si prendano $a, b, c \in \mathbb{N}$, $a = b \iff a + c = b + c$.

La somma induce su $\mathbb{N}$ una relazione d'ordine totale di "minore o uguale", infatti si può definire

$$a \leq b \text{ se e solo se } \exists\, c \in \mathbb{N} \text{ tale che } a + c = b.$$

Si può dimostrare che tale relazione è equivalente a quella già definita in precedenza.

Con questa definizione non è difficile dimostrare che comunque si prendano $a, b, c \in \mathbb{N}$, se $a \leq b$ anche $a + c \leq b + c$. Questa proprietà si chiama *proprietà di monotonia della somma.*

Purtroppo, i numeri naturali non formano un gruppo rispetto all'addizione. Infatti

$$\forall n \in \mathbb{N} \setminus \{0\} \nexists\, n' \in \mathbb{N} \text{ tale che } n + n' = 0.$$

La dimostrazione di questo è fatto è quasi banale. Sappiamo che $n \neq 0$, ovviamente $n' \neq 0$ infatti in quel caso si avrebbe $0 = n + 0 = n$. In quanto non nullo, $\exists\, m \in \mathbb{N}$ tale che $n' = s(m)$, ma questo vuol dire che $0 = n + s(m) = s(n + m)$ che è impossibile per la (IV).

Per il momento lasciamo da parte la somma e cerchiamo di dare una definizione di prodotto.

Definizione 2.4 (Prodotto)**.** *Dato* $n \in \mathbb{N}$ *si chiama* prodotto *la funzione* $m \mapsto n \cdot m$ *definita ricorsivamente da*

(i) $n \cdot 0 = 0$

(ii) $n \cdot s(m) = n \cdot m + n$

Generalmente scriveremo $n \cdot m = nm$.
Si noti che $n \cdot 1 = n \cdot 0 + n = n$.

La moltiplicazione è legata alla somma fin nella definizione, questo legame è evidenziato dalla *proprietà distributiva*, cioè $(a + b)c = ac + bc$.

Dimostrazione. Per $c = 1$ la proprietà è banalmente vera. Supponiamo valga per un generico c e dimostriamo che vale anche per $s(c)$. Si ha

$$\begin{aligned}(a+b)s(c) &= (a+b)c + a + b = ac + bc + a + b = \\ &= ac + a + bc + b = a \cdot s(c) + b \cdot s(c).\end{aligned}$$

La dimostrazione segue per induzione. □

Lemma 2.7. *La struttura algebrica data da* $(\mathbb{N}, \cdot)$ *è un monoide abeliano cioè valgono le seguenti proprietà:* $\forall a, b, c \in \mathbb{N}$

(i) $(ab)c = a(bc)$ *(associativa)*

(ii) $a \cdot 1 = 1 \cdot a = a$ *(elemento neutro)*

(iii) $ab = ba$ *(commutativa)*

Dimostrazione. Verifichiamo le tre proprietà.

(ii) Sappiamo già che $a \cdot 1 = a$. Se $a = 1$, banalmente si ha $1 \cdot 1 = 1$. Supponiamo sia vero per un a generico, allora $1 \cdot s(a) = 1 \cdot a + 1 = a + 1 = s(a)$. Dunque $a \cdot 1 = 1 \cdot a = a$.

(iii) Per $b = 1$ la proprietà è banalmente verificata. Supponiamo valga per b, si ha $a \cdot s(b) = ab + a = ba + a = ba + 1 \cdot a = (b+1)a = s(b) \cdot a$.

(i) Per $c = 1$ la proprietà è banalmente vera. Supponiamo sia vera per per c qualsiasi e verifichiamo che vale per $s(c)$. Dunque $(ab)s(c) = (ab)c + ab = a(bc) + ab = (bc)a + ba = (bc + b)a = a(bc + b) = a(b \cdot s(c))$.

□

Per la moltiplicazione, in modo simile alla somma, vale la *proprietà di monotonia del prodotto*: $\forall a, b, c \in \mathbb{N}$, se $a \leq b$ anche $ac \leq bc$.

Nota 2.2. Presi $a, b \in \mathbb{N}$ con $b \neq 0$ è possibile definire una procedura di *divisione con resto* con cui si possono trovare due numeri naturali q e r tali che $a = bq + r$ con $r < b$, il numero q è chiamato il *quoziente* e r è chiamato il *resto della divisione di a con b*. I numeri q e r sono unicamente determinati da a e b.

3 I numeri interi

"... sebbene essi facciano anche uso delle forme visibili e vi ragionino intorno, non è ad esse a cui pensano, ma alle idee a cui assomigliano."
Platone (Atene, 427 a.C. - Atene, 347 a.C.)

Molte persone credono che i numeri naturali non siano altro che un sottoinsieme dei numeri interi. Come vedremo questo è vero fino ad un certo punto. La prima cosa da fare per poterlo capire è dimostrare il seguente teorema:

Teorema 3.1. *Un monoide abeliano che soddisfa la legge di cancellazione della somma* ($a + b = a + c \Rightarrow b = c$) *può essere immerso in un gruppo abeliano.*

Dimostrazione. Sia $(M, +, 0)$ un monoide abeliano. Cerchiamo innanzitutto di sfruttarlo per definire un gruppo abeliano.
Se ragioniamo un secondo senza rigore (e teniamo a mente l'esempio dei numeri naturali) potrebbe sembrare ragionevole creare una struttura che contenga già tutti gli elementi $a - b$ (in modo da includere anche $0 - b$ e $b - 0$) dove il $-$ è legato a quell'operazione intuitiva di sottrazione che conosciamo sin da bambini (e che potremmo anche definire come "$a - b = c \Leftrightarrow a = b + c$"). Proviamo a muoverci in questa direzione...

Consideriamo le coppie ordinate $(a, b) \in M \times M$. Su questo insieme definiamo la relazione

$$(a, b) \sim (c, d) \text{ se } a + d = b + c.$$

Tornando al ragionamento non rigoroso, abbiamo detto in sostanza che due coppie (a, b) e (c, d) sono equivalenti se $a - b = c - d$. Verifichiamo che si tratta di una relazione di equivalenza:

- *Proprietà riflessiva*: $\forall (a, b) \in M \times M$, per la proprietà commutativa $a + b = b + a$, dunque $(a, b) \sim (b, a)$;
- *Proprietà simmetrica*: se $(a, b) \sim (c, d)$, banalmente $(c, d) \sim (a, b)$;
- *Proprietà transitiva*: siano $(a, b) \sim (c, d)$ e $(c, d) \sim (e, f)$, questo vuol dire che $a + d = b + c$ e $c + f = d + e$, quindi $a + d + c + f = b + c + d + e$, poiché vale la legge di cancellazione della somma $a + f = b + e$, cioè $(a, b) \sim (e, f)$.

Consideriamo l'insieme $G = (M \times M)/\sim$, con classi di equivalenza

$$[(a,b)] = [(a,b)]_\sim = \{(m,n) : (a,b) \sim (m,n)\} \in (M \times M)/\sim,$$

e definiamo la seguente operazione:

$$[(a,b)] \oplus [(c,d)] = [(a+c, b+d)].$$

Dobbiamo ora verificare che sia ben definita, cioè indipendente dal particolare rappresentante scelto per le classi $[(a,b)]$ e $[(c,d)]$. Se $[(a,b)] = [(a',b')]$ e $[(c,d)] = [(c',d')]$, si ha direttamente che $[(a+c, b+d)] = [(a'+c', b'+d')]$.

La proiezione canonica $\pi : (M \times M, +, (0,0)) \to (P, \oplus, [(0,0)])$, dove $+$ denota la somma componente per componente, è un epimorfismo, quindi $(P, \oplus, [(0,0)])$ è un monoide perché immagine omomorfa di un monoide.

Inoltre, possiamo osservare che

$$[(a,b)] \oplus [(b,a)] = [(a+b, b+a)] = [(0,0)],$$

dunque esiste l'inverso. Questo vuol dire che $(P, \oplus, [(0,0)])$ è un *gruppo*. Indicheremo l'inverso $[(b,a)] \in P$ di $[(a,b)] \in P$ con $-[(a,b)]$.

Si consideri, ora, l'applicazione $i : M \to P$ definita $a \mapsto [(a,0)]$. È facile verificare che i è un monomorfismo per le strutture

$$i : (M, +, 0) \to (P, \oplus, [(0,0)]).$$

Identificando le strutture isomorfe, possiamo dire che $(M, +, 0)$ è una *sotto-struttura* di P. □

Se poniamo $M = \mathbb{N}$ e $P = \mathbb{Z}$, abbiamo dimostrato che il monoide abeliano $(\mathbb{N}, +, 0)$ è una sottostruttura del gruppo abeliano $(\mathbb{Z}, \oplus, [(0,0)])$.

A questo punto possiamo pensare di introdurre in $\mathbb{Z}$ un'operazione di moltiplicazione $\odot$ in modo simile a quanto già fatto nella dimostrazione: presi $[(a,b)]$ e $[(c,d)]$ in P, definiamo

$$[(a,b)] \odot [(c,d)] = [(ac+bd, ad+bc)].$$

Anche questa volta dobbiamo verificare che sia ben definita, ma se $[(a,b)] = [(a',b')]$ e $[(c,d)] = [(c',d')]$, si ha direttamente che $[(ac+bd, ad+bc)] = [(a'c'+b'd', a'd'+b'c')]$.

Grazie alle proprietà della somma e del prodotto in $\mathbb{N}$, si può facilmente verificare che $(\mathbb{Z}, \odot, [(1,0)])$ è un *monoide abeliano* e che vale la proprietà distributiva del prodotto $\odot$ rispetto alla somma $\oplus$.

Sia, ora, $j : \mathbb{N} \to \mathbb{Z}$ definita $j : n \mapsto [(n, 0)]$, è questione di pochi calcoli osservare che j è un monomorfismo per le strutture $j : (\mathbb{N}, +, \cdot, 0, 1) \to (\mathbb{Z}, \oplus, \odot, [(0, 0)], [(1, 0)])$. Allora se si identificano le strutture isomorfe, si può dire che $(\mathbb{N}, +, \cdot, 0, 1)$ è una *sottostruttura* di $(\mathbb{Z}, \oplus, \odot, [(0, 0)], [(1, 0)])$.

Presa una classe $[(m, n)] \in \mathbb{Z}$ sono possibili due casi

(1) $n \leq m$, quindi $\exists k \in \mathbb{N}$ tale che $m = n + k$. In questo caso si ha

$$[(m, n)] = [(k, 0)] = i(k).$$

(2) $m < n$, quindi $\exists h \in \mathbb{N} \setminus \{0\}$ tale che $n = m + h$. Allora

$$[(0, h)] = [(m, n)] = -[(n, m)] = -[(h, 0)] = -i(h).$$

Questo vuol dire che $\forall x \in \mathbb{Z}$, $x \in \mathbb{N}$ oppure $-x \in \mathbb{N}$ dove $-x$ denota l'opposto di x, cioè l'inverso di x nel gruppo additivo $(\mathbb{Z}, \oplus, [(0, 0)])$.

NOTA 3.1. Il formalismo di considerare $\mathbb{Z}$ come insieme quoziente $(\mathbb{N} \times \mathbb{N})/\sim$ ci è servito solo per introdurre le operazioni e verificarne le proprietà. A questo punto i numeri interi non negativi verranno denotati come i naturali e gli interi negativi come naturali preceduti dal segno $-$, in accordo con quanto osservato.

In base a quanto detto fin qui, la relazione d'ordine $\leq$ su $\mathbb{Z}$ può essere definita

$$a \leq b \iff b - a \in \mathbb{N}.$$

È facile verificare che tale relazione (come per i naturali) è un *ordine totale compatibile con le operazioni*, cioè soddisfa $\forall a, b, c \in \mathbb{Z}$, $\forall d > 0 \in \mathbb{Z}$ le seguenti proprietà:

(i) $a < b \implies a + c < b + c$;

(ii) $a < b \implies ad < bd$;

(iii) $a < b \implies a(-d) < b(-d)$.

Di conseguenza si possono ricavare le regole dei segni nel prodotto e quindi la legge di annullamento del prodotto che dice

$$ab = 0 \iff (a = 0) \vee (b = 0).$$

Si può anche definire l'operazione *valore assoluto*: $|n| = \max\{n, -n\}$.

Purtroppo nemmeno $(\mathbb{Z}, \cdot, 1)$ è un gruppo moltiplicativo ma, come anche per $\mathbb{N}$, vale il seguente teorema:

Teorema 3.2 (Teorema del quoziente e del resto)**.** *Siano $a, b \in \mathbb{Z}$ con $b \neq 0$, allora esistono e sono unici $q, r \in \mathbb{Z}$ tali che $a = bq + r$ con $0 \leq r < |b|$.*

Avremmo già potuto definire le *potenze* in $\mathbb{N}$, ma non ci sarebbero servite a molto. Le introdurremo ora cercando di considerare il caso generale.

Consideriamo un monoide $(M, \cdot, \mathbb{1})$. Sappiamo dal Teorema 2.4 che, per ogni $a \in M$, esiste ed è unica la funzione $\phi_a : \mathbb{N} \to M$ definita con lo schema ricorsivo $\phi_a(0) = \mathbb{1}$, $\phi_a(n+1) = a \cdot \phi_a(n)$ $\forall n \in \mathbb{N}$. Denoteremo la *potenza* $\phi_a(n)$ con a^n in cui chiameremo a *base* ed n *esponente*. Le potenze ad esponente in $\mathbb{N}$ soddisfano le seguenti proprietà:

(i) $a^0 = \mathbb{1}$, $a^{m+n} = a^m \cdot a^n$;

(ii) ϕ_a è l'unico morfismo $\psi : (\mathbb{N}, +, 0) \to (M, \cdot, \mathbb{1})$ tale che $\psi(1) = a$;

(iii) $(a^m)^n = a^{mn}$;

(iv) Se $f : (M, \cdot, \mathbb{1}) \to (S, \cdot, v)$ è un morfismo di monoidi allora $f(a^n) = f(a)^n$;

(v) Se a, b commutano (cioè $a \cdot b = b \cdot a$) allora $a^n \cdot b^m = b^m \cdot a^n$ e anche $(a \cdot b)^n = a^n \cdot b^n$

Tutte queste proprietà, che si possono facilmente dimostrare per induzione, provano che $\phi_a : (\mathbb{N}, +, 0) \to (M, \cdot, \mathbb{1})$ è un morfismo di monoidi. Tale ϕ_a, se al posto di M avessimo un gruppo G, può essere estesa ad un morfismo di gruppi $\Phi_a : (\mathbb{Z}, +, 0) \to (G, \cdot, \mathbb{1})$ in modo che valgano le proprietà appena elencate per ogni $m, n \in \mathbb{Z}$. Osserviamo inoltre che se $a \in G$, denotando l'inverso di a con a', si ha immediatamente che

(vi) $(a')^n = (a^n)'$ $\forall n \in \mathbb{N}$.

Quindi possiamo definire, per $a \in G$ gruppo ed $m \in \mathbb{Z}$, l'applicazione $\Phi_a(m) = a^m$ se $m > 0$ e $\Phi_a(m) = (a^{|m|})'$ se $m < 0$.

Nota 3.2. Per semplicità continueremo ad indicare $\Phi_a(m)$ con a^m sia nel caso $m \geq 0$ che ne caso $m < 0$. Quindi $\Phi_a(-1) = a' = a^{-1}$, inoltre $a^{-n} = (a^n)^{-1} = (a^{-1})^n$ per ogni $k \in \mathbb{Z}$.

Nota 3.3. Nel caso in cui si trattasse di notazione additiva, scriveremo na al posto di a^n e parleremo di *multipli*, ma le proprietà sono dello stesso tipo:

(i)' $0a = 0$, $(m+n)a = ma + na$;

(ii)' $n(ma) = (nm)a$;

(iii)' $f(na) = nf(a)$ per ogni morfismo tra gruppi f;

(iv)' $n(a+b) = na + nb$.

Tirando le somme, abbiamo visto che $(\mathbb{Z}, +, 0)$ è un gruppo abeliano, $(\mathbb{Z}, \cdot, 1)$ è un monoide abeliano e valgono la distributiva del prodotto rispetto alla somma e la legge di annullamento del prodotto. Questo vuol dire che $(\mathbb{Z}, +, \cdot, 0, 1)$ è un *anello commutativo unitario integro*. Essendo $\mathbb{Z}$ evidentemente diverso dall'anello banale $\{0\}$, la struttura $(\mathbb{Z}, +, \cdot, 0, 1)$ è un *dominio di integrità commutativo* (o più brevemente un dominio commutativo). Vedremo che questo è essenziale nella costruzione dei numeri razionali.

4 I numeri razionali

4.1 Breve premessa sui campi

"Il secondo argomento è quello detto di Achille. Eccolo: il più lento corridore non sarà mai raggiunto nella sua corsa dal più veloce. Infatti sarà necessario che l'inseguitore proceda fin donde si è mosso il fuggitivo, quindi è necessario che il corridore più lento si trovi sempre un pò più innanzi."
Aristotele[1] (Stagira, 384 a.C. - Calcide, 7.3.322 a.C.)

Supponiamo di avere un campo $(K, +, \cdot, \mathbb{0}, \mathbb{1})$, cioè una struttura per cui K è un gruppo abeliano rispetto alla somma $+$, $K^* = K \setminus \{\mathbb{0}\}$ è un gruppo abeliano rispetto al prodotto $\cdot$ e vale la proprietà distributiva del prodotto rispetto alla somma.

Se $(a, b) \in K \times K^*$, possiamo considerare gli elementi $a/b = ab^{-1}$ detti *quozienti* (o frazioni) di *numeratore* a e *denominatore* b. Non è difficile verificare che $\forall a, c \in K$, $\forall b, d \in K^*$, $\forall m \in \mathbb{Z}$ valgono le seguenti proprietà:

(i) $a/b = c/d \iff ad = bc$;

(ii) $a/b = \mathbb{1} \iff a = b$;

(iii) $a/b = \mathbb{0} \iff a = \mathbb{0}$;

(iv) $a/b + c/d = (ad + bc)/bd$;

(v) $(a/b)(c/d) = (ac)/(bd)$;

(vi) Se $a \neq \mathbb{0}$, si ha $(a/b)^{-1} = (b/a)$;

(vii) $-(a/b) = (-a)/b = a/(-b)$;

(viii) $m(a/b) = (ma)/b$.

Si dice che F è *sottocampo* di K se $F \subseteq K$ è un campo rispetto alle restrizioni delle operazioni di K ad F.

Se D è un sottoanello di K, allora il più piccolo sottocampo di K contenente D, detto *sottocampo generato da* D, risulta essere

$$F = \{ab^{-1} : a \in D, b \in D^*\}.$$

[1] Questo passo è tratto dalla "Fisica" di Aristotele. Si tratta del "paradosso di Achille e la Tartaruga" ideato da Zenone di Elea, filosofo greco vissuto tra il 495 a.C e il 430 a.C.

Dimostrazione. Sia F il sottocampo generato da D. Chiaramente se $a, b \in D$ e $b \neq 0$ dobbiamo avere $ab^{-1} \in F$. Innanzitutto verifichiamo che l'insieme

$$\{ab^{-1} : a \in D, b \in D^* = D \setminus \{\mathbb{0}\}\}$$

è un sottocampo di K:

$$\begin{aligned} ab^{-1} + cd^{-1} &= ab^{-1}dd^{-1} + cbb^{-1}d^{-1} = (ad + bc)(bd)^{-1} \\ (ab^{-1})(cd^{-1}) &= acb^{-1}d^{-1} = ac(bd)^{-1} \\ 0 &= 0b^{-1} \\ 1 &= aa^{-1} \\ -ab^{-1} &= (-a)b^{-1} \\ (ab^{-1})^{-1} &= ba^{-1} \text{ se } a \neq \mathbb{0} \end{aligned}$$

Poiché F è generato da D, non può esistere un sottocampo di F diverso da F che contenga D. Poiché l'insieme $\{ab^{-1}\}$ contiene D come sottoinsieme di elementi $a1^{-1} = a$, è chiaro che $F = \{ab^{-1} : a \in D, b \in D^*\}$. □

Osserviamo che

$$ab^{-1} = cd^{-1} \iff ad = bc,$$

basta moltiplicare entrambi i lati della prima uguaglianza per bd o entrambi i lati della seconda per $(bd)^{-1}$.

4.2 Dagli interi ai razionali

"Succede invece che l'infinito sia il contrario di ciò che dicono,
perché non è ciò fuori del quale non c'è nulla,
ma ciò fuori del quale c'è sempre qualcosa."
Aristotele (Stagira, 384 a.C. - Calcide, 7.3.322 a.C.)

Possiamo estendere l'idea usata per passare dai numeri naturali ai numeri interi per ricostruire anche il campo dei razionali. Anche questa volta partiamo da un fatto generale:

Teorema 4.1. *Ogni dominio commutativo D può essere immerso in un campo F.*

Dimostrazione. Abbiamo visto che se D può essere immerso in un campo F, gli elementi della sua minima estensione di campo sono ottenuti dalle coppie $(a, b) \in D \times D^*$. Dunque, l'idea è di fare in modo che (a, b) giochi il ruolo di ab^{-1}.

Ovviamente, poiché $D \neq 0$, $D \neq \varnothing$. Consideriamo sulle coppie ordinate $(a, b) \in D \times D^*$ una relazione $\sim$ definita

$$(a, b) \sim (c, d) \Longleftrightarrow ad = bc.$$

Verifichiamo che si tratta di una relazione di equivalenza:

- *Proprietà riflessiva*: $\forall (a, b) \in D \times D^*$, per la proprietà commutativa $ab = ba$, dunque $(a, b) \sim (b, a)$;
- *Proprietà simmetrica*: se $(a, b) \sim (c, d)$, banalmente $(c, d) \sim (a, b)$;
- *Proprietà transitiva*: siano $(a, b) \sim (c, d)$ e $(c, d) \sim (e, f)$, questo vuol dire che $ad = bc$ e $cf = de$, quindi $(ad)f = (bc)f = b(de)$, poiché vale la legge di cancellazione della somma $af = be$, cioè $(a, b) \sim (e, f)$.

Inoltre se $(a, b) \sim (a', b')$ e $(c, d) \sim (c', d')$, si ha $(ad+bc, bd) \sim (a'd'+b'c', b'd')$ e $(ac, bd) \sim (a'c', b'd')$. Infatti

- le scritture hanno senso, in quanto se $(a, b), (c, d), (a', b'), (c', d') \in D \times D^*$, allora i prodotti $bd, b'd, bd', b'd'$ sono certamente non nulli in quanto $b, b', d, d' \neq \mathbb{0}$ e D dominio di integrità;
- per ipotesi sappiamo che $ab' = ba'$ e $cd' = dc'$ quindi $ab'dd' + cd'bb' = ba'dd' + dc'bb'$ da cui $(ad + bc)b'd' = (a'd' + b'c')bd$;
- per ipotesi sappiamo che $ab' = ba'$ e $cd' = dc'$ quindi $ab'cd' = ba'dc'$ da cui $(ac)(b'd') = (bd)(a'c')$.

Consideriamo il quoziente $(D \times D^*)/\sim$, con classi di equivalenza

$$[(a, b)] = [(a, b)]_\sim = \{(m, n) : (a, b) \sim (m, n)\} \in (D \times D^*)/\sim .$$

Per quanto osservato, è naturale definire le seguenti operazioni:

$$\begin{aligned} [(a, b)] \oplus [(c, d)] &= [(ad + bc, bd)] \\ [(a, b)] \odot [(c, d)] &= [(ac, bd)] \end{aligned}$$

Bastano pochi calcoli, a questo punto, per verificare che la struttura che abbiamo costruito è un anello commutativo dove, qualunque sia $b \in D^*$, l'elemento $[(0, b)]$ è lo zero e $[(b, b)] = [(1, 1)]$ è l'unità. Inoltre $\forall (a, b) \in D^* \times D^*$ si ha $[(a, b)] \odot [(b, a)] = [(ab, ab)] = [(1, 1)]$. Dunque ogni elemento non nullo è invertibile e quindi la struttura che abbiamo è un campo che per il momento denotiamo con $\mathcal{Q}(D)$.

Sia ora $j : D \to \mathcal{Q}(D)$ l'applicazione definita da $j(a) = [(a, 1)]$. Si prova facilmente che j è un monomorfismo. Osserviamo che

- $\forall[(a,b)] \in \mathcal{Q}(D)$ si ha $[(a,b)] = [(a,1)] \odot [(1,b)] = [(a,1)] \odot [(b,1)]^{-1} = j(a) \odot j(b)^{-1} = j(a)/j(b)$;
- Se $[(a,b)] = j(c)/j(d)$ allora $j(a)/j(b) = j(c)/j(d)$, quindi $j(a) \odot j(d) = j(b) \odot j(c)$ da cui $j(ad) = j(bc)$, ovvero $[(ad,1)] = [(bc,1)]$ che vuol dire $ad = bc$, o meglio $[(a,b)] = [(c,d)]$.

Questo significa che la rappresentazione di un elemento di $\mathcal{Q}(D)$ come quoziente $j(a)/j(b)$, dove $(a,b) \in D \times D^*$, è unica.

NOTA 4.1. Se D non avesse l'unità, scriveremmo $j(a) = [(ab,b)]$ per qualche (e quindi $\forall$) $b \in D^*$; da cui $[(a,b)] = [(ab,b)][(b,b^2)] = [(ab,b)][(b^2,b)]^{-1} = j(a)/j(b)$.

In altre parole, abbiamo detto che possiamo rappresentare gli elementi di $\mathcal{Q}(D)$ come ab^{-1} dove $a, b \in D, b \neq \mathbb{0}$. Per le osservazioni fatte nella precedente sottosezione, $F = \mathcal{Q}(D)$. □

In virtù della dimostrazione appena fatta, possiamo definire l'insieme dei numeri razionali

$$\mathbb{Q} = \mathcal{Q}(D) = \left\{ \frac{m}{n} : m \in \mathbb{Z}, n \in \mathbb{Z}^* \right\}.$$

La struttura data da $(\mathbb{Q}, +, \cdot, 1, 0)$ è un campo.

Chiaramente, considerando il monomorfismo $j : (\mathbb{Z}, +, \cdot, 0, 1) \mapsto (\mathbb{Q}, +, \cdot, 0, 1)$ definito $j : n \mapsto n/1$ ed identificando le strutture isomorfe, possiamo considerare $(\mathbb{Z}, +, \cdot, 0, 1)$ come sottostruttura $(\mathbb{Q}, +, \cdot, 0, 1)$.

Su $\mathbb{Q}$ possiamo definire una relazione d'ordine $\leq$, che affonda le sue radici nella relazione tra gli interi, come segue:

$$a/b \leq c/d \iff ((bd > 0) \wedge (ad \leq bc)) \vee ((bd < 0) \wedge (ad \geq bc)).$$

TEOREMA 4.2.
$\mathbb{Q}$ è totalmente ordinato, inoltre

$$\forall a/b,\ c/d \in \mathbb{Q},\ \exists\, e/f \in \mathbb{Q} \text{ tale che } a/b \leq e/f \leq c/d.$$

Dimostrazione. Il primo punto è banale e segue dalle definizioni.
Per il secondo punto basta considerare $e/f = (ad + bc)/2bd$. □

Siamo riusciti ad ottenere un insieme numerico chiuso anche rispetto all'inverso del prodotto (quoziente); cosa succede per quanto riguarda le potenze? Le potenze non sono altro che prodotti, quindi $\mathbb{Q}$, $\mathbb{Z}$ ed $\mathbb{N}$ sono chiusi rispetto alla potenza con esponente in $\mathbb{N}$. In particolare, in $\mathbb{Q}$ abbiamo anche le potenze negative che corrispondono agli inversi delle potenze positive. Ma l'operazione inversa della potenza, è ben definita in $\mathbb{Q}$?

L'operazione di cui parliamo è la cosiddetta *estrazione di radice*, che potremmo rudimentalmente definire come:

$$y = \sqrt[n]{x} \iff x = y^n.$$

Ovviamente, se n è pari, la x deve essere positiva.

Consideriamo $n = 2$ ed $x = 4$, possiamo dire senza problemi che $y = 2$. Ma se $x = 2$? Già i pitagorici avevano scoperto che $\sqrt{2}$ è un numero *irrazionale*, cioè non appartenente all'insieme dei razionali (ma, come vedremo, appartenente a quello dei reali).

Dimostrazione. Supponiamo $\sqrt{2}$ razionale. Dunque esistono due interi a e b tali che $\frac{a}{b} = \sqrt{2}$. Senza perdere di generalità, supponiamo a e b primi tra loro (in caso non lo fossero basta fare le opportune semplificazioni e chiamare in modo appropriato il numeratore e il denominatore ottenuti). Se eleviamo tutto al quadrato, otteniamo $\frac{a^2}{b^2} = 2$ dunque $a^2 = 2b^2$ pari. Questo vuol dire che a^2 è pari e quindi anche a deve esserlo. Allora esiste un intero k tale che $a = 2k$. Sostituendo nell'equazione di prima otteniamo che $2b^2 = (2k)^2$ e quindi $b^2 = 2k^2$. Per lo stesso ragionamento di prima esiste h per cui $b = 2h$. Ma questo vuol dire che a e b non sono primi tra loro che è assurdo. □

Cerchiamo quindi di estendere i razionali in modo da includere tutti questi "irrazionali".

5 I numeri reali

Ora, in ogni caso in cui c'è una sezione (A_1, A_2) che non è prodotta da un numero razionale, allora noi creiamo un nuovo numero irrazionale a che riteniamo completamente definito da questa sezione; diremo che questo numero a corrisponde a questa sezione oppure che produce questa sezione.
Julius W. R. Dedekind (Braunschweig, 6.2.1831 - Braunschweig, 12.2.1916)

Ci sono essenzialmente due strade per costruire i numeri reali: il metodo di completamento per tagli di Dedekind e il metodo di Cantor delle successioni. Il primo è logicamente più semplice mentre il secondo presenta un modo pratico per approssimare i numeri reali oltre ad essere più vantaggioso per definire le operazioni algebriche. È per questo che la nostra attenzione si rivolgerà al metodo di Cantor.

Sia K un campo ordinato. Diamo innanzitutto alcune definizioni:

Definizione 5.1. *Una* successione nulla *in K è una successione di elementi di K definita:*

$$\{a_n \in K \,|\, \forall \epsilon > 0 \text{ in } K, \exists\, n_0 \in \mathbb{N} : \forall n > n_0,\ |a_n| < \epsilon\}\,.$$

Recuperando le notazioni usuali dell'analisi, diciamo che 'a_n converge a 0 per n che tende a ∞' e scriviamo '$a_n \underset{n\to\infty}{\longrightarrow} 0$' o equivalentemente '$\lim_{n\to\infty} a_n = 0$'.

Una condizione necessaria per la convergenza di una serie è la *Criterio di Cauchy*:

Teorema 5.1 (Criterio di Cauchy)**.** *Se una serie a_n converge ad a, allora la serie $c_{m,n} = a_m - a_n$ converge a 0.*

Più esplicitamente vuol dire che dato $\epsilon > 0$, esiste n_0 tale che $|a_m - a_n| < \epsilon$ per ogni $m, n > n_0$. La dimostrazione segue dalla disuguaglianza triangolare.

Definizione 5.2. *Una successione $\{a_n\}$ è una* successione di Cauchy *se $|a_m - a_n| \to 0$.*

Definizione 5.3. *Ogni campo ordinato si dice* completo *se ogni successione di Cauchy è convergente.*

Per il Criterio di Cauchy, infatti, ogni serie convergente è di Cauchy. Il viceversa, però, non è sempre vero (ad esempio basta considerare le successioni di numeri in $\mathbb{Q}$ che convergono a π, $\sqrt{2}$ oppure al numero aureo ϕ). Ci proponiamo ora di dimostrare che se anche un campo ordinato non è necessariamente completo, possiamo sempre costruire un suo completamento.

Teorema 5.2. *Sia K un campo ordinato, allora esistono un campo completo ordinato $\tilde{K}$ ed una immersione d'ordine $\lambda : K \to \tilde{K}$ tali che ad ogni immersione d'ordine $f : K \to L$ in un campo ordinato completo L corrisponda un'unica immersione d'ordine $f' : \tilde{K} \to L$ tale che $f = \lambda \circ f'$.*

Dimostrazione. Sia R l'insieme delle successioni di Cauchy in K. Ovviamente $R \subseteq K^{\mathbb{N}}$ insieme di tutte le successioni in K. $K^{\mathbb{N}}$ è un anello commutativo unitario, prodotto diretto di K, ed R è chiaramente un suo sottoanello (anche lui commutativo e unitario).

L'insieme $\mathfrak{n}$ di tutte le successioni nulle è un ideale in R.
Siano, infatti, $\{a_n\} \in R$ e $\{b_n\} \in \mathfrak{n}$, poiché $\{a_n\}$ è di Cauchy, esisterà un certo n_0 per cui $|a_m - a_n| < \mathbb{1}$ per ogni $m, n > n_0$, quindi $|a_m| < |a_{n_0}| + \mathbb{1}$ per ogni $m > n_0$. Segue che $|a_m| \leq M = \max\{|a_1|, |a_2|, \ldots, |a_{n_0-1}|, |a_{n_0}| + \mathbb{1}\}$ e quindi ogni successione di Cauchy è limitata. D'altra parte sappiamo che $b_n \to 0$, quindi per ogni $\epsilon > \mathbb{0}$ fissato si ha che $b_n < \frac{\epsilon}{M}$ per ogni $n > n_1 \geq n_0$. Ne consegue che $|a_n b_n| < \epsilon$ per $n > n_1$, cioè che $a_n b_n \to 0$. Quindi $\{a_n b_n\} \in \mathfrak{n}$.

Diciamo che $\mathfrak{n}$ è un ideale massimale in R.
Di certo $\mathfrak{n} \neq R$, in quanto la successione costante $\mathbb{1}, \mathbb{1}, \ldots$ non è una successione nulla. D'altra parte se $\{a_n\}$ è una successione di Cauchy non nulla, per definizione esiste $p \in K$, $p > \mathbb{0}$, tale che per ogni n esiste un $n' > n$ per cui $|a_{n'}| > p$. Dal fatto che a_n è di Cauchy sappiamo che esiste n_0 per cui $|a_m - a_n| < \frac{p}{2}$ per ogni $m, n > n_0$. Preso un qualunque $n > n_0$, consideriamo $n' > n$ come prima in modo che $a_n \geq |a_{n'}| - |a_n - a_{n'}| > \frac{p}{2}$, questo implica che a_n^{-1} è una successione limitata per $n > n_0$. Se definiamo

$$b_n = \begin{cases} \mathbb{1} & \text{per } n \leq n_0 \\ a_n^{-1} & \text{per } n > n_0 \end{cases}$$

otteniamo una successione $\{b_n\}$ di Cauchy per cui $\{a_n b_n\}$ converge ad $\mathbb{1}$, cioè $\{a_n\}\{b_n\} \equiv \mathbb{1} \mod \mathfrak{n}$. In altre parole, ogni elemento non appartenente all'ideale (cioè non nullo) è invertibile, questo in aggiunta al fatto che R è un anello commutativo unitario, ci garantisce che $R/\mathfrak{n}$ è un campo e dunque $\mathfrak{n}$ è massimale.

Ricapitolando, il quoziente $R/\mathfrak{n}$ è un campo che indichiamo con $\tilde{K}$ mentre chiameremo λ l'omomorfismo naturale $K \to R \to R/\mathfrak{n}$ ottenuto mappando $a \in K$ nella classe delle sequenze costanti $a, a, \ldots$. Come ogni omomorfismo tra campi, è anche un'immersione, quindi possiamo identificare K con la sua immagine in $\tilde{K}$.

È chiaro come poter estendere l'ordine in $\tilde{K}$: dato $\alpha \in \tilde{K}$, rappresentato da una successione di Cauchy $\{a_n\}$, necessariamente o si tratta di una successione nulla, o esistono $\epsilon > \mathbb{0}$ ed n_0 tali che $a_n > \epsilon$ per ogni $n > n_0$. oppure

esiste n_1 tale che $a_n < -\epsilon$ per $n > n_1$. In ogni caso, le successioni che rappresentano α godono della stessa proprietà, quindi poniamo rispettivamente $\alpha = \mathbb{0}$, $\alpha > \mathbb{0}$ o $\alpha < \mathbb{0}$.

Comunque presi due elementi di $\tilde{K}$, c'è sempre un elemento di K compreso tra i due. Consideriamo α e β in $\tilde{K}$ definiti rispettivamente da $\{a_n \in K\}$ e $\{b_n \in K\}$ e tali che non rappresentino elementi di K, senza perdita di generalità possiamo assumere $\mathbb{0} < \alpha < \beta$ (cioè $\alpha - \beta < 0$ dove $\alpha - \beta$ è definita da $\{a_n - b_n\}$), se fossero uno positivo e l'atro negativo il nostro elemento di K sarebbe lo $\mathbb{0}$. Poiché sia α che β sono di Cauchy, sono successioni limitate e possimo scegliere n_1 ed n_2 tali che $|a_n - a_m| < \varepsilon$ e $|b_{n'} - b_{m'}| < \varepsilon$ per $\varepsilon > \mathbb{0}$ fissato, $m, n > n_1$ ed $m', n' > n_2$. Fissiamo $n_0 > max\{n_1, n_2\}$ per cui esiste $\epsilon > \mathbb{0}$ tale che $a_n - b_n < -\epsilon$ per ogni $n > n_0$. Le successioni $\{a_n : n > n_0\}$ e $\{b_n : n > n_0\}$ sono limitate in K, possiamo quindi considerare $A = \max_{n>n_0} a_n$ e $B = \min_{n>n_0} b_n$. Posto $\gamma = \{a, a, a, \dots\}$ con $a = \frac{A+B}{2}$, da un certo N in poi si avrà $\alpha < \gamma < \beta$ e γ corrisponde ad $a \in K$.

Ora, data una sequenza di Cauchy $\{\alpha_n\} \in \tilde{K}$, o α_n è costante da un certo n in poi quindi è il limite di una qualche successione di Cauchy in K e dunque converge, oppure contiene un'infinità di termini distinti. Omettendo le ripetizioni, possiamo assumere che tutti gli α_n siano distinti. Per ogni n, scegliamo $a_n \in K$ tale che $\alpha_n < a_n < \alpha_{n+1}$, la successione $\{a_n\}$ è una successione in K con limite α in $\tilde{K}$; chiaramente $\lim \alpha_n = \lim a_n = \alpha$ quindi $\tilde{K}$ è completo.

Sia $f : K \to L$ un'immersione d'ordine in un campo completo L. Ogni elemento α di $\tilde{K}$ si ottiene come limite di una successione di Cauchy $\{a_n\}$ in K, non è difficile rendersi conto che $f(a_n)$ è una successione di Cauchy in L e dunque ha un qualche limite b. Ogni altra successione di Cauchy che tende ad α differisce da a_n di una successione nulla, quindi anche la sua immagine tende a b. In altre parole, b dipende solo da α, per cui potremmo porre $f'(\alpha) = b$. Si verifica facilmente che f' è un'immersione d'ordine ed è l'unica per cui $f = \lambda \circ f'$. □

Il campo $\tilde{K}$ si chiama *completamento di K*. Se consideriamo $K = \mathbb{Q}$, allora $\mathbb{R} = \tilde{K}$.

Ci sono alcune proprietà che caratterizzano i numeri reali ed è interessante precisare. Cominciamo da una definizione.

Definizione 5.4. *Un campo ordinato K si dice* archimedeo *se*

$$\forall a, b \in K,\ a > \mathbb{0},\ \exists\, n \in \mathbb{N} \text{ tale che } na > b.$$

Nella definizione assiomatica dei numeri reali, tale proprietà è conosciuta con il nome di *assioma di Eudosso-Archimede*.

Si verifica facilmente che i numeri razionali sono archimedei e, per la densità di $\mathbb{Q}$ in $\mathbb{R}$, lo stesso vale per i reali.

Dimostrazione. Siano $\alpha, \beta \in \mathbb{R}$ con $\alpha > 0$. Se $\alpha \geq \beta$, di certo $2\alpha > \beta$. Supponiamo $0 < \alpha < \beta$, banalmente $0 < \frac{\alpha}{\beta} < 1$ ed esiste $a = \frac{m}{n} \in \mathbb{Q}$ tale che $m, n \in \mathbb{N}$ e $0 < a < \alpha/\beta$. A maggior ragione deve valere che $0 < 1/n < \alpha/\beta$, da cui $n\alpha > \beta$. □

Cerchiamo di capire in che consiste l'importanza di questa proprietà.

Teorema 5.3. *Ogni sottocampo ordinato di $\mathbb{R}$ è archimedeo, e viceversa ogni campo ordinato archimedeo ha un isomorfismo d'ordine con $\mathbb{R}$.*

Dimostrazione. Poiché $\mathbb{Q}$ è denso in $\mathbb{R}$, è denso in ogni sottocampo di $\mathbb{R}$ ed in base alla dimostrazione precedente anche tali sottocampi devono essere archimedei.

D'altra parte, sia K un campo ordinato archimedeo, mostriamo che $\mathbb{Q}$ è denso in K. Siano $\alpha, \beta \in K$ tali che $\alpha < \beta$, allora $1/(\beta - \alpha) > 0$ e per ipotesi esiste $n > 1/(\beta - \alpha)$. Applicando di nuovo l'ipotesi possiamo trovare $m \in \mathbb{N}$ tale che $(m+1)/n \geq \beta$. Si scelga il più grande m per cui $(m+1)/n \geq \beta > m/n$; ricordando che $\beta - \alpha > 1/n$, si ha $\alpha < \beta - 1/n \leq m/n$, quindi $\alpha < m/n < \beta$, che implica che $\mathbb{Q}$ è denso in K.

Inoltre per ogni $\alpha \in K$ ed ogni $n \in \mathbb{N}$, abbiamo verificato che esiste $m = m(n) \in \mathbb{Z}$ tale che $m/n < \alpha \leq (m+1)/n$. Chiaramente le frazioni $m(n)/n$ per $n \in \mathbb{N}$ formano una successione che converge ad α, dunque una successione di Cauchy. Sia α' il limite di questa successione in $\mathbb{R}$, allora la mappa definita $\alpha \mapsto \alpha'$ è ben definita da K in $\mathbb{R}$ ed, in effetti, è un immersione d'ordine (come si può verificare con una ragionevole quantità di calcoli ed osservazioni). □

Chiaramente nessuno sottocampo proprio di $\mathbb{R}$ può essere completo, ne consegue che

Teorema 5.4. *Ogni campo ordinato archimedeo è isomorfo ad $\mathbb{R}$.*

In ogni insieme parzialmente ordinato l'estremo superiore (minimo dei maggioranti), se esiste, è unico. Un insieme si dice superiormente limitato se ammette un maggiorante, si noti che i maggioranti non sono necessariamente unici. Un'altra proprietà che caratterizza i numeri reali è la *superiore limitatezza*: *ogni sottoinsieme non vuoto superiormente limitato ha estremo superiore.* Tale proprietà è conosciuta nella definizione assiomatica dei reali come *assioma di Dedekind o di completezza.*

Dimostrazione. Basta mostrare che ogni campo ordinato K che ammette la proprietà di superiore limitatezza è archimedeo.

Siano $\alpha, \beta \in K$, $\alpha > \mathbb{0}$. Supponiamo $n\alpha > \beta$ falso per ogni $n \in \mathbb{N}$, allora $n\alpha \leq \beta$ per ogni n. Questo vuol dire che $\{\alpha, 2\alpha, 3\alpha, \dots\}$ è limitato superiormente da β e, per ipotesi, ammette un estremo superiore γ. Ma $\gamma - \alpha < \gamma$ quindi per qualche n si avrà $n\alpha > \gamma - \alpha$ e di conseguenza $(n+1)\alpha > \gamma$ che contraddice la definizione di γ. Segue che esiste n per cui $n\alpha > \beta$. □

6 I numeri complessi

"La matematica è la regina delle scienze e
la teoria dei numeri è la regina della matematica"
Carl Friedrich Gauss (Braunschweig, 30.4.1777 - Gottinga, 23.2.1855)

Consideriamo l'equazione polinomiale a coefficienti reali $3x^2 + 1 = 0$. Possiamo tentare di trovare soluzioni in $\mathbb{R}$, sta di fatto che non le troveremo mai. Basterebbe definire in qualche modo $\sqrt{-1}$ per riuscire a risolvere almeno l'equazione presa in esame, ma nel passaggio dai razionali ai reali abbiamo ottenuto una chiusura per l'operazione di radice solo per reali positivi o nulli... la radice di un numero negativo esiste soltanto quando è una radice dispari.

Questo fatto può anche essere espresso in termini di chiusura algebrica.

Definizione 6.1. *Un campo F è detto* algebricamente chiuso *se ogni polinomio di grado positivo a coefficienti in F ha almeno una radice in F (cioè un elemento x tale che il valore del polinomio in x è l'elemento neutro dell'addizione in F).*

Il controesempio che abbiamo visto illustra che $\mathbb{R}$ non è algebricamente chiuso.

Vogliamo dunque estendere il campo dei reali in modo da includere le soluzioni di tutti i polinomi di grado maggiore o uguale ad 1. Ormai è diventata una procedura naturale quella di considerare coppie di numeri, siano dunque (a, b) e (c, d) coppie ordinate in $\mathbb{R} \times \mathbb{R}$; su tali coppie definiamo le seguenti operazioni:

$$\begin{aligned} (a, b) \oplus (c, d) &= (a + c, b + d), \\ (a, b) \odot (c, d) &= (ac - bd, bc + ad). \end{aligned}$$

Non è difficile osservare che la struttura data da $(\mathbb{R}\times\mathbb{R}, \oplus, \odot, (0, 0), (1, 0))$ è un campo in cui l'inverso della somma è banalmente $(-a, -b)$ mentre, se $(a, b) \neq (0, 0)$, l'inverso del prodotto è

$$(a, b)^{-1} = \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right).$$

Consideriamo ora l'applicazione $j : \mathbb{R} \to \mathbb{R} \times \mathbb{R}$ definita da $j(a) = (a, 0)$. Si verifica facilmente che j è un monomorfismo per le strutture $j : (\mathbb{R}, +, \cdot, 0, 1) \mapsto (\mathbb{R} \times \mathbb{R}, \oplus, \odot, (0, 0), (1, 0))$ e dunque, identificando le strutture isomorfe, si può asserire che $(\mathbb{R}, +, \cdot, 0, 1)$ è una sottostruttura di $(\mathbb{R}\times\mathbb{R}, \oplus, \odot, (0, 0), (1, 0))$. Definiamo il campo complesso $\mathbb{C}$ come $\mathbb{C} = \mathbb{R}\times\mathbb{R}$

dotato delle operazioni $\oplus$ e $\odot$ che, per comodità, indicheremo rispettivamente con $+$ e $\cdot$. Recuperiamo l'intuizione avuta all'inizio della sezione riguardo alla radice di -1 e consideriamo l'elemento $(0,1)$ elevato al quadrato:

$$(0,1)^2 = (0,1) \cdot (0,1) = (-1,0) = j(-1).$$

Per definizione di radice, come inversa della potenza, $(0,1)$ rappresenta $\sqrt{-1}$. Generalmente, l'elemento $(0,1)$ viene indicato con i e chiamato *unità immaginaria*.
Possiamo considerare

$$a = a \cdot 1 = j(a)j(1) = j(a)(1,0) = (a,0)(1,0) = (a,0)$$

e parallelamente

$$a(0,1) = j(a)(0,1) = (0,a).$$

Posto $i = (0,1)$ (dunque $i^2 = -1$) le rappresentazioni $(a,b) \in \mathbb{C}$ ed

$$a + ib \in \mathbb{R}(i) \equiv \mathbb{R}[x]/(x^2+1)$$

sono equivalenti:

- $(a,b) = (a,0) + (0,b) = a(1,0) + b(0,1) = a + ib$;
- $(a,b) + (c,d) = a + ib + c + id = (a+c) + i(b+d) = (a+c, b+d)$;
- $(a,b)(c,d) = (a+ib)(c+id) = ac + ibc + ida + i^2bd =$
  $= (ac - bd) + i(ad + bc) = (ac - bd, ad + bc)$.

In altre parole, la funzione $k : (\mathbb{C}, \oplus, \odot, (0,0), (1,0)) \to (\mathbb{R}(i), +, \cdot, 0, 1)$ definita da $k(a,b) = a + ib$ è un isomorfismo tra i campi $\mathbb{C}$ e $\mathbb{R}(i)$. Quindi possiamo rappresentare i numeri complessi più comodamente che con le coppie ordinate di reali (a,b) tramite la forma algebrica $a + ib$ per cui valgono le proprietà algebriche del calcolo polinomiale.

Ci sono vari modi di rappresentare i numeri complessi, oltre quelli già visti esiste una forma trigonometrica ed una esponenziale. Inoltre si può facilmente verificare che $\mathbb{C}$ è uno spazio vettoriale complesso ad una dimensione (come tutti i campi) ma è anche uno spazio vettoriale reale a due dimensioni, questo significa che $[\mathbb{C} : \mathbb{R}] = 2$, cioè che il campo complesso è un'estensione finita del campo reale.

Osserviamo che in questa estensione si perde l'ordinamento, o meglio vale il teorema seguente:

Teorema 6.1. *I numeri complessi non possono essere ordinati in modo compatibile con le operazioni aritmetiche.*

Quindi non ha senso chiedersi, ad esempio, se i è maggiore o minore di 1.

Dimostrazione. Siano a e b due numeri complessi. Supponiamo $a < b$ e moltiplichiamo a destra e a sinistra per i due volte:

$$i \cdot i \cdot a < i \cdot i \cdot b.$$

Dato che, per definizione, $i^2 = -1$ si ottiene

$$-a < -b.$$

Sommiamo ad entrambi i membri l'espressione $(a + b)$:

$$(a + b) - a < (a + b) - b,$$

applicando l'associativa e sommando gli opposti otteniamo

$$b < a.$$

Dunque abbiamo $a < b$ e $b < a$ che è assurdo. □

Veniamo ora al teorema chiave. Abbiamo esteso i reali ad un nuovo campo, però abbiamo anche perso la relazione d'ordine. Ci aspettiamo un risultato che valga questa perdita!

Teorema 6.2. *Il campo complesso* $\mathbb{C}$ *è* algebricamente chiuso.

La prima dimostrazione corretta di questo teorema fu data da Gauss nella sua tesi di laurea nel 1799. Non daremo dimostrazioni del teorema in quanto non ne esiste una puramente algebrica semplice.

7 Note conclusive

Il campo dei numeri complessi, come anche tutti gli altri spazi visti in questo percorso, svolge un ruolo fondamentale non solo in vari campi della matematica, ma anche della fisica e dell'ingegneria. Le innumerevoli proprietà che lo caratterizzano si sono rivelate risolutive in una enorme quantità di situazioni, mostrando l'utilità delle estensioni di campo anche in situazioni in cui si ottengono nuove proprietà al prezzo di altre, come nel nostro caso con la perdita dell'ordinamento.

Anche la costante i appare in ogni dove, spesso accompagnata da π e dal numero di Nepero e e ricopre un ruolo fondamentale in moltissime applicazioni. Una famosa identità dimostrata da Eulero verso la metà dal 1700, e da molti indicata come la *più bella equazione della matematica*, le lega assieme in modo inaspettato:

$$e^{i\pi} + 1 = 0.$$

In questa formula è racchiuso un pò tutto il percorso che abbiamo fatto. A partire dallo 0, attraverso l'unità e poi tra gli irrazionali trascendenti ed i numeri immaginari. È strano, o almeno curioso, pensare che l'esponenziale di un numero trascendente per uno immaginario non sia altro che un intero e, forse, può farci rendere conto di quanto siano complicate queste strutture a prima vista così semplici e di come cose intuitive e spesso facilmente comprensibili possano generare una tale complessità. È per questo che mi piace concludere con questa citazione:

> "*Una goccia che si spande nell'acqua, le fluttuazioni delle popolazioni animali, la linea frastagliata di una costa, I ritmi della fibrillazione cardiaca, l'evoluzione delle condizioni meteorologiche, la forma delle nubi, la grande macchia rossa di Giove, gli errori dei computer, le oscillazioni dei prezzi, ... Sono fenomeni apparentemente assai diversi, che possono suscitare la curiosità di un bambino o impegnare per anni uno studioso, con un solo tratto in comune: per la scienza tradizionale, appartengono al regno dell'informe, dell'imprevedibile, dell'irregolare. In una parola al caos. Ma da due decenni, scienziati di diverse discipline stanno scoprendo che dietro il caos c'è in realtà un ordine nascosto, che dà origine a fenomeni estremamente complessi a partire da regole molto semplici.*"
>
> James Gleick (New York City, 1.8.1954 -)

Riferimenti bibliografici

[Coh89] P. M. Cohn. *Algebra - Vol. 2*. John Wiley & Sons, 1989.

[Gle00] James Gleick. *Caos*. Rizzoli, 2000.

[Hal98] Paul Richard Halmos. *Naive Set Theory*. Springer-Verlag, 1998.

[Jac85] Nathan Jacobson. *Basic Algebra I*. Freeman & Co, 1985.

[WP] Wikipedia (http://www.wikipedia.org). Web site.