§ 3. GLI INSIEMI NUMERICI

Questo capitolo riprende concetti noti dai corsi del I anno del triennio, aggiunge considerazioni che si possono anche vedere come applicazioni di quanto visto in precedenza sulle strutture algebriche o come possibili spunti per un insegnamento dei numeri, incominciando dai naturali, e delle loro applicazioni. Alcuni approfondimenti saranno contenuti nelle schede integrative.

Un itinerario possibile potrebbe essere il seguente:

- Gli assiomi di Peano; operazioni, potenze, ordinamenti, il principio del minimo; sistemi di numerazione. *Numeri primi e divisibilità*. I numeri cardinali: equipotenza, numeri cardinali, operazioni e loro proprietà, ordinamento; cardinali finiti; insiemi numerabili.
- Calcolo combinatorio: principio di addizione, principio dei cassetti, principio di moltiplicazione, funzioni iniettive e permutazioni, anagrammi, sottoinsiemi di un insieme, coefficienti binomiali ed applicazioni.
- L'anello $\mathbf{Z}$ dei numeri interi: la costruzione come numeri naturali col segno. Divisione euclidea, ideali, quozienti.
- L'azione di $\mathbf{Q}^+$ sulle grandezze [1]. Da $\mathbf{Q}^+$ a $\mathbf{Q}$. IL campo razionale, i suoi gruppi. *Numeri decimali periodici e loro operazioni*.
- Numeri decimali e loro operazioni e ordinamento. Il campo reale e le sue proprietà. Definizione assiomatica come unico campo ordinato completo. Costruzioni del campo reale secondo Dedekind e secondo Cantor.
- Il campo complesso: alcune costruzioni mediante il piano di Argand-Gauss o altri procedimenti elementari.

Naturalmente non c'è spazio per ripercorrere per intero a lezione questo itinerario. Tuttavia, come detto, in buona parte questi argomenti sono stati trattati nei corsi di Algebra, Analisi e Storia della Matematica. Le parti in corsivo sono oggetto di seminari.

[1] I contenuti di questa sezione sono trattati in modo più esteso ed esauriente nel modulo di Geometria.

§ 3.1. I numeri naturali e i numeri cardinali

In queste prime pagine si richiama la definizione secondo Peano dell'insieme **N** = {0, 1, 2, ...} dei numeri naturali, rivisitata con un linguaggio più attuale; successivamente si introducono le operazioni di addizione e moltiplicazione di **N** e le relative relazioni d'ordine e ne sono descritte le proprietà principali.

Assiomi di Peano. L'insieme **N** dei numeri naturali può essere definito mediante gli assiomi di Peano, che, con il linguaggio degli insiemi, tradurremo nel modo seguente:

I. **N** contiene un elemento, indicato con 0.

II. E' definita una funzione iniettiva $\sigma : \mathbf{N} \xrightarrow{1-1} \mathbf{N}$, la cui immagine è $\mathbf{N} \setminus \{0\}$

III. Per ogni $M \subseteq \mathbf{N}$, se $0 \in M$ e se per ogni $n \in M$ anche $\sigma(n) \in M$, allora $M = \mathbf{N}$.

Per ogni $n \in \mathbf{N}$, l'elemento $\sigma(n)$ è detto *successivo* di n. Dalla proprietà II segue che **N** è infinito (si veda la sezione 2).

La proprietà III si chiama *principio d'induzione* e si usa in definizioni e dimostrazioni che coinvolgano una variabile $n \in \mathbf{N}$.

Le *dimostrazioni per induzione* seguono lo schema seguente: si debba provare un'affermazione P(n) che abbia senso per ogni numero naturale.

a) Si dimostra innanzitutto che è vera P(0).
b) Si dimostra che l'essere vera P(n) (*ipotesi induttiva*) implica che è vera $P(\sigma(n))$.

In tal modo l'insieme M dei numeri n per i quali P(n) è vera contiene 0 e per ogni $n \in M$ contiene anche $\sigma(n)$. Dunque, per il principio d'induzione, $M = \mathbf{N}$.

Analogamente, la proprietà III serve per definire nozioni, secondo lo schema seguente (*definizioni ricorsive*): si debba definire una nozione, che denoteremo con D(n), e che abbia senso per ogni numero naturale.

a) Si definisce esplicitamente D(0).
b) Supposta definita D(n), si definisce mediante essa $D(\sigma(n))$.

In tal modo l'insieme M dei numeri n per i quali D(n) è definita contiene 0 e per ogni $n \in M$ contiene anche $\sigma(n)$. Dunque, per il principio d'induzione, $M = \mathbf{N}$.

A volte si parte da un numero n_0 anziché da 0. In tal caso, l'affermazione P(n) sarà provata solo per ogni $n \geq n_0$. Analogamente per le definizioni D(n).

NOTA. In alcuni casi, per dimostrare un'affermazione P(n) si segue uno schema un po' diverso, detto *Il principio d'induzione*:

a) si dimostra P(0)

b) supposto vero P(k) per ogni $k \le n$, si dimostra $P(\sigma(n))$.

Ciò posto, ripercorriamo alcune parti della costruzione di Peano.

ADDIZIONE. Su **N** si può definire ricorsivamente la somma di un numero m con un numero n qualsiasi, nel modo seguente:

$$\text{poniamo: } \begin{cases} m+0=m \\ m+\sigma(n)=\sigma(m+n) \end{cases}$$

In tal modo, per la proprietà III, per ogni $m\in\mathbf{N}$ la *somma* m+n è definita per ogni $n\in\mathbf{N}$. Posto $1=\sigma(0)$, si ottiene subito, per ogni $m\in\mathbf{N}$:

$$\sigma(m)=\sigma(m+0)=m+\sigma(0)=m+1.$$

Chiamiamo *addizione* l'operazione $+:\mathbf{N}^2\to\mathbf{N}$, $+:(m,n)\mapsto m+n$, che associa a una coppia ordinata (m, n) di numeri naturali la loro somma.
Mediante il principio d'induzione di dimostra il seguente risultato:

PROPOSIZIONE 3.1.1. - L'addizione possiede le proprietà seguenti:

a) *associativa*: per ogni $a, b, c\in\mathbf{N}$ risulta: (a+b)+c = a+(b+c);

b) *elemento neutro*: per ogni $a\in\mathbf{N}$ si ha a+0 = 0+a = a;

c) *commutativa*: per ogni $a, b\in\mathbf{N}$ risulta a+b = b+a.

Dimostrazione.

a) L'uguaglianza è vera per c = 0, risultando (a+b)+0 = a+b = a+(b+0).

Supponendola provata per c = n (ipotesi induttiva), dimostriamo che è vera per $c=\sigma(n)$ nel modo seguente:

	(a+b)+c = (a+b)+σ(n) =
(per la definizione di +)	= σ((a+b)+n) =
(per l'ipotesi induttiva)	= σ(a+(b+n)) =
(per la definizione di +)	= a+σ(b+n) =
(ancora per la definizione di +)	= a+(b+σ(n)) = a+(b+c),

come si voleva.

b) Per definizione di + si ha a+0 = a. L'uguaglianza 0+a = a è vera ovviamente per a = 0. Supponendola provata per a = n, se $a=\sigma(n)$ si ha:

$$0+a=0+\sigma(n)=\sigma(0+n)=\sigma(n)=a.$$

c) La dimostrazione della proprietà commutativa è più complessa, occorrendo procedere per induzione rispetto ad entrambi gli addendi. Per b) è vera se a = 0. Sia vera per a = n e dimostriamo che è vera per $a=\sigma(n)$. Per questo procediamo per induzione rispetto a b.

E' vera per definizione di + se b = 0. Sia vera per b = m. Per b = σ(m) si ha allora:

a+b = σ(n)+σ(m) = σ(σ(n)+m) =

(per l'ipotesi induttiva su b) = σ(m+σ(n)) = σ(σ(m+n)) =

(per l'ipotesi induttiva su a) = σ(σ(n+m)) = σ(n+σ(m)) =

(ancora per l'ipotesi induttiva su a) = σ(σ(m)+n) = σ(m)+σ(n) = b+a,

come si voleva.

Si può ora proseguire con analoghi metodi lo sviluppo della teoria.

PROPOSIZIONE 3.1.2. - Ulteriori proprietà dell'addizione.

a) Per ogni a, b∈**N**, se a+b = 0 allora a = b = 0.

b) *Legge di cancellazione*: per ogni a, b, c∈**N**, se a+b = a+c allora b = c.

c) Per ogni a, b∈**N**, una e, se a ≠ b, una sola delle due equazioni: $\begin{cases} a + x = b \\ b + y = a \end{cases}$, nelle incognite x ed y∈**N**, ha una ed una sola soluzione.

Sottrazione. Se risulta a+d = b, si pone b-a = d e d si chiama *differenza* di b ed a. In particolare si ha a-a = 0.

Moltiplicazione. Si definisce ricorsivamente l'operazione di *moltiplicazione* · definendo dapprima il *prodotto* di un m per un n qualsiasi, nel modo seguente (ricordando che σ(n) = n+1):

per ogni m, n∈**N**, poniamo: $\begin{cases} m \cdot 0 = 0 \\ m \cdot (n+1) = m \cdot n + m \end{cases}$.

Di conseguenza, per esempio, m·1 = m·(0+1) = m·0+m = m, ecc. Solitamente il prodotto di m per n si denota con mn, anziché con m·n.

La moltiplicazione è l'operazione che ad ogni coppia (m,n) associa il prodotto $m \cdot n$.

PROPOSIZIONE 3.1.3. - Proprietà della moltiplicazione.

1) *Elemento assorbente*: per ogni a∈**N**, 0·a = a·0 = 0
2) *Elemento neutro*: per ogni a∈**N** si ha a·1 = 1·a = a.
3) *Distributiva* rispetto al +: per ogni a, b, c∈**N** risulta $\begin{cases} (a+b)c = ac + bc \\ a(b+c) = ab + ac \end{cases}$
4) *Associativa*: per ogni a, b, c∈**N** risulta (ab)c = a(bc)
5) *Commutativa*: per ogni a, b∈**N** risulta ab = ba.

6) L'unico elemento dotato di *inverso* è 1, cioè per ogni a, b∈**N**, se a·b = 1 allora a = b = 1.
7) *Legge di annullamento del prodotto*: per ogni a, b∈**N** si ha a·b = 0 se e solo se a = 0 oppure b = 0.

Consideriamo ora il sottoinsieme $\mathbf{N}^+ = \mathbf{N}\setminus\{0\}$: la legge di annullamento del prodotto ha come conseguenza che se a, b∈$\mathbf{N}^+$ anche a·b∈$\mathbf{N}^+$.

PROPOSIZIONE 3.1.4. - Proprietà della moltiplicazione in $\mathbf{N}^+$.

a) *Legge di cancellazione*: per ogni a, b, c∈$\mathbf{N}^+$, se ab = ac allora b = c.

b) Per ogni a, b∈$\mathbf{N}^+$ al massimo una delle due equazioni $\begin{cases} a \cdot x = b \\ b \cdot y = a \end{cases}$, nelle incognite x ed y∈$\mathbf{N}^+$, ha soluzione. Tale soluzione, se esiste, è unica (per la legge di cancellazione).

NOTA. A differenza della analoga proprietà dell'addizione, la proprietà 3.1.5.b della moltiplicazione contiene solo l'affermazione dell'unicità dell'eventuale soluzione.

L'ordine naturale. L'ordine naturale di **N** si può definire a partire dall'addizione, ponendo per ogni a, b∈**N**,

$$a \le b \text{ se esiste } d\in\mathbf{N} \text{ tale che } a+d = b.$$

Le proprietà dell'ordinamento si dimostrano a partire da quelle dell'addizione, in particolare la dicotomia. Dunque, (**N**, ≤) è un *insieme ordinato* e l'ordine è *totale*. Inoltre, poiché per ogni n∈**N** si ha 0+n = n allora 0 ≤ n. Dunque 0 è il *minimo*. Non c'è invece *massimo*, poiché per ogni n∈**N** si ha n < n+1. Inoltre, l'ordine è discreto e compatibile con le operazioni. In particolare, n+1 copre n.
Il seguente risultato è in realtà equivalente al principio d'induzione.

PROPOSIZIONE 3.1.5 (principio del minimo). - Ogni sottoinsieme non vuoto H di **N** possiede il minimo.

Dimostrazione. Se 0∈H allora 0 è il suo minimo. Sia 0∉H e sia M(H) l'insieme dei minoranti stretti di H. Innanzitutto, 0∈M(H). Se per ogni x∈M(H) si avesse anche x+1∈M(H) allora, per il principio d'induzione, M(H) = **N** e H sarebbe vuoto, assurdo. Dunque, esiste x_0∈M(H) tale che x_0+1∈H. Ne segue che x_0+1 è il minimo cercato: infatti ogni altro h∈H è maggiore di x_0, quindi per 3.1.7.b) è anche h ≥ x_0+1.

La proprietà seguente è estremamente importante per la struttura di numeri e polinomi, ed è insegnata anche nella scuola elementare.

PROPOSIZIONE 3.1.6. - Dati due numeri naturali a, b, con $b \neq 0$, esistono due numeri naturali q, r, univocamente determinati, tali che $\begin{cases} a = b \cdot q + r \\ 0 \leq r < b \end{cases}$.

Dimostrazione: se a < b allora q = 0 ed r = a. Se a ≥ b sia $M = \left\{ x \in \mathbf{N} \mid \exists k \in \mathbf{N},\ x = a - b \cdot k \right\}$: non è vuoto perché a∈M, perciò ha minimo r ≥ 0. Allora esiste q tale che $r = a - b \cdot q$, e si ha r < b, altrimenti s = r–b = a-(q+1)b∈M e s < r, assurdo. Se poi si ha anche $a = b \cdot q' + r'$, con per esempio r' < r, allora:

$$b \cdot q + r = b \cdot q' + r' \Rightarrow r - r' = b \cdot \left(q' - q \right), \text{ con q'-q} \geq 1.$$

Ma si ha contemporaneamente $r - r' < r < b \leq b \cdot \left(q' - q \right)$, assurdo. Dunque si ha l'unicità di q ed r.

I numeri q ed r si chiamano rispettivamente *quoziente* e *resto* di a diviso b. Questa "operazione" è detta *divisione euclidea* o *divisione col resto* in **N**.

Dati a, b∈$\mathbf{N}^+$, se esiste q∈**N** tale che a·q = b allora q si dice *quoto* di "b diviso a" e si pone b:a = q. Questa operazione si chiama spesso *divisione esatta* di a per b. In particolare, b:b = 1. Si osservi che si ha la divisione esatta fra a e b se e solo se la divisione euclidea dà resto nullo. In tal caso, il quoto coincide col quoziente. Torneremo più avanti su questo algoritmo.

NOTA. Poiché per ogni a ≠ 0 risulta a·0 = 0, si può definire il quoto di 0 diviso a ponendo 0:a = 0. Non ha senso invece la scrittura 0:0, in quanto per ogni q∈**N** si ha 0·q = 0.

L'ordine dalla divisibilità. Eseguendo una 'traduzione' in notazione moltiplicativa delle nozioni precedenti, introduciamo un ordine in $\mathbf{N}^+$. Definiamo la relazione | (*divide*) in $\mathbf{N}^+$ ponendo:

per ogni a, b∈$\mathbf{N}^+$, a | b se esiste q∈$\mathbf{N}^+$ tale che a·q = b.

Sostituendo ≤ con | e 0 con 1 nella proposizione 3.1.6, mediante le proprietà della moltiplicazione si provano subito le seguenti proprietà:

PROPOSIZIONE 3.1.7. - Proprietà della relazione $|$

a) *Proprietà riflessiva*: per ogni $a \in \mathbf{N}^+$ si ha $a|a$.

b) *Proprietà antisimmetrica*: per ogni $a,b \in \mathbf{N}^+$, se $a|b$ e $b|a$ allora $a = b$.

c) *Proprietà transitiva:* per ogni $a, b, c \in \mathbf{N}^+$, se $a|b$ e $b|c$ allora $a|c$.

d) L'ordine è solo parziale; ha minimo 1 e non ha massimo.

e) Per ogni $a, b \in \mathbf{N}^+$, se $a \mid b$ allora $a \leq b$. Inversamente, se $a < b$ allora b non divide a.

NOTA. Volendo estendere l'ordinamento $\mid$ a tutto $\mathbf{N}$, si deve porre necessariamente $n \mid 0$ per ogni $n \in \mathbf{N}$, in particolare, $0 \mid 0$. Infatti per ogni $n \in \mathbf{N}$ esiste almeno un elemento $q \in \mathbf{N}$, tale che $nq = 0$: è ovviamente $q = 0$ (e non è richiesta l'unicità di q). Pertanto ($\mathbf{N}$, $\mid$) oltre al minimo, uguale ad 1, possiede anche il massimo, lo zero.

Potenze. Per ogni $a \in \mathbf{N}^+$ e per ogni $n \in \mathbf{N}$ si definisce ricorsivamente la *potenza* a^n nel modo seguente:

$$\begin{cases} a^0 = 1 \\ a^{n+1} = a^n \cdot a \end{cases}.$$

In particolare si ha $a^1 = a$. Per le potenze valgono le seguenti proprietà, che si dimostrano per induzione rispetto ad n:

PROPOSIZIONE 3.1.3. - Per ogni $a, b \in \mathbf{N}^+$ e per ogni $m, n \in \mathbf{N}$ si ha:

a) $a^m \cdot a^n = a^{m+n}$

b) $(a^m)^n = a^{mn}$

c) $(ab)^n = a^n b^n$

NOTA. Mentre le prime proprietà dipendono solo dalla definizione di potenza e dalla proprietà associativa della moltiplicazione, la terza dipende in modo essenziale dalla proprietà commutativa: $(ab)^2 = abab = aabb = a^2 b^2$.

Quanto sopra detto per le potenze si può ripetere per l'addizione. Osserviamo che in notazione additiva la potenza di base a ed esponente n si scrive *na* anziché a^n, e si ha:

$$\begin{cases} 0a = 0 \\ (n+1)a = na + a \end{cases}.$$

Il numero *na* si chiama *multiplo naturale* di a.

PROPOSIZIONE 3.1.9. - Altre proprietà di multipli e potenze.

a) Per ogni n, h, k∈**N**, n ≠ 0, si ha h < k se e solo se hn < kn. In particolare, l'unico multiplo di n che sia minore di n è lo zero.

b) Per ogni n, h, k∈$\mathbf{N}^+$, n ≠ 1, si ha h < k se e solo se $n^h < n^k$ (o equivalentemente se e solo se n^h divide "propriamente" n^k). In particolare, l'unica potenza di n che sia minore di n (cioè divisore proprio di n) è 1.

Riprendiamo il discorso sui numeri naturali e sul modo di rappresentarli, ossia sui *sistemi di numerazione*. Nella storia ci sono stati vari approcci. Il più antico consiste nel rappresentare i numeri naturali come file finite di *tacche*:

1 = | 2 = || 3 = ||| e così via.

Lo *zero* è l'assenza di tacche. E' un metodo che dal punto di vista teorico permette di capire facilmente le operazioni ed il confronto.

- L'*ordinamento* è evidente: si sovrappongono le due file di tacche e quella che "sporge" è maggiore dell'altra.
- *Addizionare* non è altro che concatenare:

  |||+|||| = |||||||

  e così ogni numero è somma di tanti 1 quante sono le sue tacche.
- *Sottrarre* è eliminare dal minuendo tante tacche quante sono espresse dal sottraendo, purché sia minore o uguale al minuendo:

  ||||| - || = |||
- *Moltiplicare* è addizionare successivamente lo stesso numero di tacche:

  ||| × || = ||+||+|| = ||||||
- *Dividere* è sottrarre successivamente il divisore dal dividendo, finché possibile: il *quoziente* è il numero delle sottrazioni, il *resto* è quel che rimane alla fine.

Le proprietà sono quasi immediate. In particolare, persino uno scoglio concettuale come la divisione per zero è facile: sottrarre zero tacche da un numero dato non lo cambia mai, si può proseguire all'infinito e non si ha un quoziente ed un resto, perciò non ha senso dividere per zero.

Questo metodo si pensa sia stato il primo ad essere utilizzato nella storia della rappresentazione dei numeri: infatti il più antico ritrovamento consiste in un osso di lupo, risalente a 30.000 anni fa circa, con incise una successione di tacche a distanza all'incirca costante l'una dall'altra e con una tacca più lunga in corrispondenza di cinque tacche corte.

Tuttavia, questo approccio non è soddisfacente per un uso pratico: i numeri come tacche diventano presto ingestibili e le esigenze di calcolo e di introduzione di nuovi insiemi di numeri (per misurare e non solo per contare) richiedono una razionalizzazione dei numeri naturali ed una loro diversa rappresentazione. Parliamo allora in generale di sistemi di numerazione.

Per *sistema di numerazione* si intende l'insieme dei simboli e delle regole che consentono di rappresentare graficamente i numeri e di leggerli. Un sistema di numerazione è quindi una sequenza di nomi di numeri, o numerali, utilizzata per *enumerare*, ossia per attribuire ad ogni elemento di un insieme finito un nome, che dipende dall'ordine con il quale prendiamo in considerazione tale elemento.

Gli aspetti di un sistema di numerazione, che vengono valutati per determinarne la "qualità", sono:

1) *Motivazione*: è una proprietà non matematica, che dipende dagli usi, dalle abitudini. A differenza del sistema unario delle tacche, il nostro sistema a base 10 non è particolarmente motivato, se non dal numero delle nostre dita delle mani.
2) *Astrattezza*: proprietà fondamentale, dato che vengono trattati numeri che sono entità astratte.
3) *Organicità*: un sistema è organico se con un metodo semplice e composto da poche regole riesce a rappresentare tutti i numeri (naturali).
4) *Efficienza computazionale*: un sistema è efficiente quando permette, non solo di menzionare i numeri, ma anche di utilizzarli nel calcolo delle comuni operazioni con facilità. Il sistema posizionale da noi utilizzato ha avuto successo grazie alla sua straordinaria efficienza nel calcolo rispetto ai sistemi fino a quel momento utilizzati.

La sequenza dei nomi che costituisce un sistema di numerazione si può pensare che debba essere infinita, data l'infinità dei numeri. Sin dai primi tentativi di enumerazione, l'uomo ha capito la necessità di attribuire nomi ai numeri seguendo regole e non in modo arbitrario, ed ha escogitato nel corso della storia diversi metodi di rappresentazione dei numeri attraverso la scrittura. Dividiamo tali metodi in due categorie principali: i *metodi senza base* e quelli *con base*.

Del primo tipo è il metodo delle tacche, già visto, ma anche il rappresentare ogni numero con un simbolo diverso e senza nessi logici fra i simboli. Quest'ultimo metodo è sicuramente inefficiente perché privo di organicità e perché non permette le fasi di memorizzazione e trasmissione del processo del contare.

Nei metodi con base rappresentiamo numeri che sappiamo essere decomponibili in una somma di q_n unità u_n, q_{n-1} unità u_{n-i}, ..., q_0 unità u_0. Ricordiamo solo i due seguenti:

1) I numeri romani

Questo metodo fu introdotto per evitare di scrivere successivamente più di 3 simboli uguali. Per fare questo furono introdotti simboli per le potenze di 10 ed altri simboli per "unità intermedie", e una notazione sottrattiva. Il suo supporto grafico è costituito da 7 lettere dell'alfabeto latino :

I = 1, V = 5, X =10, L = 50, C = 100 , D = 500 M = 1000.

Per rappresentare un numero venivano scritte le lettere in ordine decrescente dei loro valori, che venivano sommati, ma per evitare la ripetizione di 4 lettere uguali fu inventata la seguente regola: se una lettera di valore inferiore è collocata alla sinistra di una lettera di valore superiore, i due valori vanno sottratti; se è collocata alla destra i due valori vanno sommati. In questo modo otteniamo ad esempio: XL = 40 e LX = 60. L'efficienza computazionale è bassissima e la rappresentazione di numeri altri assai complicata.

2) Rappresentazione di posizione (RP)

La logica che sta alla base di questo metodo è la seguente: stabilita una convenzione per la scrittura, i diversi addendi q_iu_i vengono rappresentati per lo stesso valore di q_i, con lo stesso simbolo e il valore di u_i viene indicato solo attraverso la posizione del corrispondente simbolo per q_i occupata nella stringa di simboli che costituisce la rappresentazione del numero. Questo metodo poteva creare degli errori causati dal dovere lasciare uno spazio vuoto in corrispondenza di un moltiplicatore assente. Questo problema fu risolto con l'introduzione di un simbolo speciale chiamato *zero*, sia all'interno delle sequenze (*zero intercalare*) sia alla fine di esse (*zero finale*). Questo metodo è utilizzato da quasi tutti i popoli, facendo riferimento alla base 10 e usando attualmente i simboli 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 come cifre, combinate secondo le seguenti regole:

- i primi nove interi positivi sono rappresentati da 1, 2, 3, 4, 5, 6, 7, 8, 9
- il successivo di 9 si scrive 10
- il successivo rappresentato da n cifre si scrive nel seguente modo: se l'ultima cifra non è 9 si sostituisce questa con la sua successiva; se l'ultima cifra è 9 si sostituisce 9 con 0 e l'intero rappresentato dalle n-1 prime cifre col suo successivo.

Questo metodo ha origini indo-arabiche ed è usato non tanto per la motivazione dei simboli, quanto per la sua sistematicità e per la sua elevata efficienza computazionale. I sistemi posizionali si sono sviluppati gradualmente, in concomitanza con l'uso di "unità di

ordine superiore" (decine, centinaia, dozzine, lustri...) rese necessarie dall'espansione del sistema dei numerali verso numeri sempre più grandi.

NOTA. Sembra che il metodo posizionale risalga circa al 600 d. C. Circa nel 750 d.C. il persiano al-Khowarizmi tradusse in arabo il libro indiano che spiegava l'aritmetica decimale. Il metodo posizionale fu poi introdotto in Europa da Leonardo Fibonacci, che ne espose le caratteristiche nel suo celebre "Liber Abaci" (1202), traduzione latina del libro arabo di al-Khowarizmi. Nel "Liber Abaci" il termine arabo *as-sifr* fu latinizzato in *zephirum*, da cui deriva l'italiano *zefiro*, corretto in *zeuero*, e infine in *zero.* Da esso derivano anche l'italiano *cifra*, il francese *chiffre*, il tedesco *ziffer,* per indicare tutti i simboli da 0 a 9 e non solo lo zero.

Nella scuola elementare s'imparano le tecniche per eseguire le operazioni sui numeri naturali scritti in base 10. Successivamente, nella scuola media, si impara talora ad usare la base 2, a causa della scrittura binaria usata nell'informatica. Quest'ultima usa solo i simboli 1 e 0, sostituibili con ON/OFF o con V/F (vero o falso). Una tabella di confronto per i primi dodici numeri naturali scritti nei vari sistemi di numerazione è interessante:

tacche		I	II	III	IIII	IIIII	IIIIII	IIIIIII	IIIIIIII	IIIIIIIII	IIIIIIIIII	IIIIIIIIIII	IIIIIIIIIIII
Romani		I	II	III	IV	V	VI	VII	VIII	IX	X	XI	XII
2	0	1	10	11	100	101	110	111	1000	1001	1010	1011	1100
10	0	1	2	3	4	5	6	7	8	9	10	11	12

ESEMPIO 3.1.10. Algoritmo di passaggio dalla base 10 alla base 2: si divide il numero per 2 e si trascrivono quoziente e resto; si ripete col quoziente come dividendo. I resti concatenati in ordine inverso danno il numero in base 2.

numero dec.	547	273	136	68	34	17	8	4	2	1
quoziente	273	136	68	34	17	8	4	2	1	0
resto	1	1	0	0	0	1	0	0	0	1

Il numero in base 2 è allora 1000100011 (= $2^9 + 2^5 + 2 + 1$)

NOTA. Interessante come attività scolastica, interdisciplinare ed interclasse, è anche il confronto dei nomi dei numeri nelle varie lingue, perché può coinvolgere gli insegnanti di lingua straniera e di lingue classiche, gli allievi di provenienza estera; può essere spunto per ricerche su Internet o su enciclopedie su lingue sempre più attuali come lo spagnolo, l'arabo, il russo o il cinese.

I numeri cardinali. Si tratta di un argomento profondo e complesso, forse il cuore della teoria degli insiemi. Qui è accennato solo come possibile approccio ai numeri naturali, poiché riprende, dal punto di vista superiore, quello che gli insegnanti delle scuole dell'infanzia ed elementari propongono ai bambini, mediante figure di oggetti da confrontare: due uova, due conigli, due automobili, ... per formare il concetto di numero 2.

Due insiemi A e B si dicono *equipotenti* se esiste una biiezione $f : A \xrightarrow[su]{1\text{–}1} B$.

Se A è equipotente a B scriviamo per brevità $A \cong B$.

PROPOSIZIONE 3.1.10. - In ogni insieme **U** di insiemi, l'equipotenza è una relazione d'equivalenza.

Dimostrazione. Per ogni A, B, C appartenenti ad **U**, si ha:

- proprietà riflessiva: poiché $id_A : A \xrightarrow[su]{1\text{–}1} A$, allora $A \cong A$.
- proprietà simmetrica: sia $A \cong B$, allora esiste $f : A \xrightarrow[su]{1\text{–}1} B$. Ne segue $f^{-1} : B \xrightarrow[su]{1\text{–}1} A$, quindi $B \cong A$.
- proprietà transitiva: siano $A \cong B$, $B \cong C$; esistono allora $f : A \xrightarrow[su]{1\text{–}1} B$ e $g : B \xrightarrow[su]{1\text{–}1} C$, da cui segue $g \circ f : A \xrightarrow[su]{1\text{–}1} C$ e quindi $A \cong C$.

Le classi d'equivalenza si chiamano *numeri cardinali*. La classe dell'insieme A, ossia il suo numero cardinale, la denoteremo con $|A|$.

Supponiamo ora che l'insieme **U** sia *chiuso* rispetto all'unione, all'intersezione, all'inclusione, al prodotto cartesiano e contenga l'insieme vuoto e l'insieme $\{\varnothing\}$. Poniamo dapprima $0 = |\varnothing|$ e $1 = |\{\varnothing\}|$. Allora, $0 \neq 1$ perché $\varnothing$ e $\{\varnothing\}$ non sono equipotenti.

Definiamo ora le operazioni di *addizione* e *moltiplicazione* in **U**. Siano A e B due insiemi e siano $A' = A \times \{0\}$, $B' = B \times \{1\}$. I due insiemi A' e B' sono equipotenti ad A e B rispettivamente, e sono disgiunti, ossia $A' \cap B' = \varnothing$. Poniamo:

$$|A| + |B| = |A' \cup B'|, \quad |A| \cdot |B| = |A \times B|$$

Le due definizioni sono ben poste. Infatti, siano $C \cong A$, $D \cong B$. Allora sicuramente $C \times D \cong A \times B$. Inoltre, posto $C' = C \times \{0\}$, $D' = D \times \{1\}$, si ha $C' \cup D' \cong A' \cup B'$.

Queste operazioni sono inoltre associative, commutative, la moltiplicazione è distributiva rispetto all'addizione. Inoltre, $0 = |\varnothing|$, ossia lo *zero*, è l'elemento neutro dell'addizione ed è

elemento assorbente della moltiplicazione. Infine, $1 = \left|\{\varnothing\}\right|$, ossia l'*uno*, è l'elemento neutro della moltiplicazione.

Si può anche definire un ordine tra i numeri cardinali. Enunciamo dapprima il seguente teorema:

TEOREMA 3.1.11 (Cantor – Bernstein). - Siano A e B due insiemi. Se esistono $f : A \xrightarrow{1-1} B$ e, allora A e B sono equipotenti.

Osserviamo poi che: dati quattro insiemi A, A', B, B', $A \cong A'$, $B \cong B'$, ed esiste $f : A \xrightarrow{1-1} B$, allora esiste anche $f' : A' \xrightarrow{1-1} B'$. Infatti, siano $\alpha : A \xrightarrow[su]{1-1} A'$, $\beta : B \xrightarrow[su]{1-1} B'$, allora $f' = \beta \circ f \circ \alpha^{-1}$ è iniettiva.

Ne segue la possibilità di definire $|A| \le |B|$ se esiste $f : A \xrightarrow{1-1} B$, e questa è una relazione d'ordine. In più, è *totale*: infatti, si può dimostrare che dati due insiemi A e B, se non esiste $f : A \xrightarrow{1-1} B$ allora esiste $g : B \xrightarrow{1-1} A$; pertanto, se non si ha $|A| \le |B|$, allora necessariamente $|B| \le |A|$.

Concludiamo osservando che se per il nostro insieme universo **U** si ha $A \in \mathbf{U} \Rightarrow \wp(A) \in \mathbf{U}$, allora a partire da **U** si trovano numeri cardinali grandi a piacere. Infatti, un teorema di Cantor afferma che $\forall A,\ A \in \mathbf{U} \Rightarrow |A| < |\wp(A)|$.

Seguendo Dedekind, un insieme A si dice *infinito* se è equipotente ad un suo sottoinsieme proprio. Se non è infinito, si dice *finito*. Ogni insieme equipotente ad A è infinito o finito come A. Pertanto, possiamo parlare di numeri cardinali finiti. Il vuoto è un insieme finito (non è equipotente ad un sottoinsieme proprio perché non ne ha), quindi 0 è un cardinale finito, e così pure 1 è finito. Si ha poi (e non è ovvio!):

a) Somma e prodotto di cardinali finiti sono cardinali finiti.
b) Se n è un cardinale finito, anche n+1 lo è.
c) Se m ed n sono finiti, $n \neq 0$, allora $m+n \neq m$.
d) I numeri cardinali finiti costituiscono un insieme, che denoteremo con **N**, e che chiameremo insieme dei numeri naturali.
e) **N** non è un insieme finito, poiché posto $\sigma(n) = n+1$, si ha $\sigma : \mathbf{N} \xrightarrow{1-1} \mathbf{N} \setminus \{0\}$.

f) La terna $(\mathbf{N}, 0, \sigma)$ soddisfa gli assiomi di Peano e quindi è un modello dei numeri naturali.

Gli insiemi equipotenti ad **N** si dicono *numerabili*. Si può dimostrare che un insieme è infinito se e solo se contiene un sottoinsieme numerabile. Allora ogni numero cardinale infinito è maggiore di $|\mathbf{N}|$. Quest'ultimo numero cardinale si denota con $\aleph_0$ (che si legge Aleph zero).

ESEMPI 3.1.12. – a) L'insieme **Z** degli interi relativi è numerabile.

Una funzione biiettiva da **Z** ad **N** è la seguente:

$f(x) = \begin{cases} 2x & \text{se } x \geq 0 \\ -1-2x & \text{se } x < 0 \end{cases}$. Per esempio,

x	0	1	2	3	…	–1	–2	–3	–4	…
f(x)	0	2	4	6	…	1	3	5	7	…

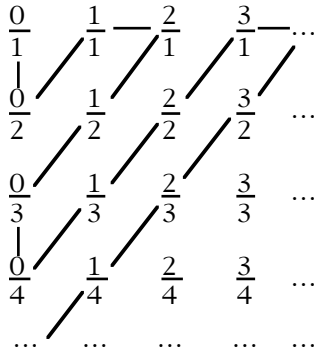
Per dimostrare che è suriettiva, si osservi che per ogni n∈**N**, se n è pari allora $n = 2n' = f(n'),\ n' \geq 0$. Se è dispari, allora $n = 2n' - 1 = -1 - 2(-n') = f(-n'),\ n' > 0$. Per l'iniettività si osservi che l'immagine dei negativi è l'insieme dei dispari, quella dei positivi o nulli è l'insieme dei pari. Se quindi x, y sono tali che f(x) = f(y), allora x ed y sono entrambi ≥ 0 o entrambi < 0.

Ora, sui ≥ 0: 2x = 2y ⇒ x = y; sui negativi, -1-2x = -1-2y ⇒ x = y, perciò f è anche iniettiva.

b) L'insieme **Q** dei numeri razionali è numerabile.

Poiché **Q** contiene **N** allora |**Q**| ≥ $\aleph_0$. Per la disuguaglianza inversa si parte col costruire una funzione iniettiva dall'insieme **N** all'insieme delle frazioni $\frac{m}{n}$, con m ed n numeri naturali e n ≠ 0.

(si veda la figura seguente). L'insieme di queste frazioni è dunque numerabile.



n	0	1	2	3	4	5	6	7	8	9	10	11	12	…
f(n)	0/1	0/2	1/1	2/1	1/2	0/3	0/4	1/3	2/2	3/1	4/1	3/2	2/3	…

Ogni numero razionale "assoluto" è identificabile con una frazione ridotta ai minimi termini, perciò l'insieme dei numeri razionali assoluti è equipotente ad un sottoinsieme dell'insieme delle frazioni, ed è di conseguenza numerabile a sua volta. Ossia, esiste una funzione biiettiva $g : \mathbf{N} \to \mathbf{Q}^+ \cup \{0\}$.

Con uno scambio eventuale tra lo zero di **Q** e g(0), possiamo ricondurci al caso di $g(0) = 0$.

Si può allora costruire una funzione biiettiva $\Gamma : \mathbf{N} \to \mathbf{Q}$, ponendo, per ogni n∈**N**,

$$\begin{cases} \Gamma(2n) = g(n) \\ \Gamma(2n+1) = -g(n) \end{cases}$$

e ciò prova che **Q** è numerabile.

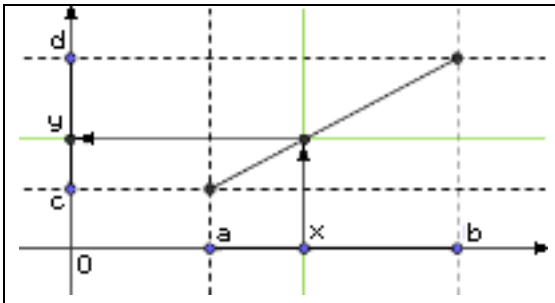
c) L'insieme **R** dei numeri reali non è numerabile.

Poiché **R** contiene **N** allora $|\mathbf{R}| \geq \aleph_0$. Mostriamo che non vale l'uguaglianza. Per cominciare, osserviamo che l'insieme $\{0\} \cup \left\{ \frac{1}{n} \;\middle|\; n \in \mathbf{N}^+ \right\}$ è equipotente ad **N** ed è incluso nell'intervallo $[0,1[$ di **R**. Pertanto, questo intervallo è almeno numerabile. Supponiamo che lo sia, cioè che sia data una $f : \mathbf{N} \xrightarrow[\text{su}]{1\text{-}1} [0,1[$. A meno di uno scambio, supponiamo $f(0) = 0$. Rappresentiamo gli elementi di $[0,1[$ in base 10 come al solito, ossia con numeri decimali del tipo $0, c_1 c_2 c_3 \cdots$ Ognuno di questi numeri è il corrispondente tramite f di un numero naturale. Ma ora mostriamo che non è vero, parafrasando Cantor, costruendo cioè un numero diverso da ogni f(n).

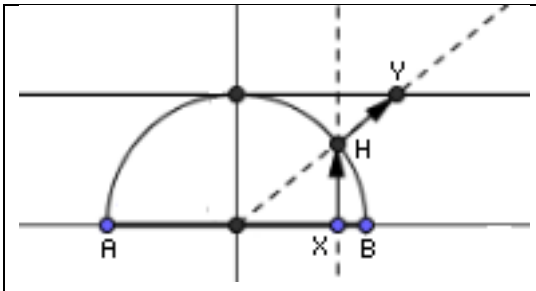
Sia x = $0, c_1 c_2 c_3 \cdots$ il nostro numero da costruire. Per ogni n∈**N**, n > 0, poniamo:

$$c_n = \begin{cases} 2 & \text{se la n-esima cifra decimale di } f(n) \text{ è } 1 \\ 1 & \text{altrimenti} \end{cases}$$

In tal modo, il nostro numero x sarà non nullo, quindi ≠ f(0), e differirà da ogni altro f(n) per la n-esima cifra decimale, ed allora x∉f(**N**). D'altra parte, essendo un numero decimale del tipo 0,… si ha x∈$[0,1[$ = f(**N**), quindi abbiamo una contraddizione. Ne segue che una tale f non esiste, ed allora $[0,1[$ non è numerabile. Ne segue che anche **R** non è numerabile.



d) Due intervalli chiusi e limitati $[a,b]$ e $[c,d]$ di **R** sono equipotenti.
Ne segue anche l'equipotenza di intervalli limitati ma non necessariamente chiusi.
La figura è eseguita col software Geogebra e qualche manipolazione.



e) Un segmento aperto $]A,B[$ è equipotente ad una semicirconferenza aperta di diametro AB e ad una retta.
Ne segue l'equipotenza fra rette e segmenti, e fra **R** ed ogni suo intervallo.

f) **R** ed $\mathbf{R}^2$ sono equipotenti. Lo stesso Peano mostrò infatti che esiste una funzione suriettiva dall'intervallo $[0,1]$ di R al quadrato $[0,1]\times[0,1]$ di $\mathbf{R}^2$. Ne segue che esiste una funzione iniettiva da $[0,1]\times[0,1]$ a $[0,1]$ e, valendo ovviamente il viceversa, i due insiemi sono equipotenti. Ne segue che anche **R** ed $\mathbf{R}^2$ sono equipotenti.

NOTA. Il numero cardinale dell'insieme **R** è denotato con *c* ed è detto *potenza del continuo*.
Tra $\aleph_0$ e *c* ci sono altri numeri cardinali? La risposta non segue dagli altri assiomi della teoria degli insiemi, ma può diventare a sua volta un assioma da aggiungere agli altri: se ne può fare a meno, o si può postulare l'esistenza o postulare la non esistenza (*ipotesi del continuo*), senza per questo cadere in contraddizioni.

Certamente questi esempi sono interessanti ed istruttivi, ma coinvolgono nozioni molto delicate, che non sono trattabili compiutamente a livello elementare. Il concetto di numero cardinale finito è sfuggente; il fatto che i cardinali finiti siano un insieme non è ovvio. Il fatto che non esista l'"insieme di tutti gli insiemi", costringe a considerare un insieme *universo*, i cui elementi siano insiemi, che sia abbastanza grande da contenere tutti i possibili cardinali finiti: esiste? In universi differenti si ottengono numeri cardinali differenti, ma saranno almeno in qualche senso isomorfi?

3.2. – Calcolo combinatorio

In questa sezione vediamo gli insiemi finiti con l'impostazione opposta a quella della sezione precedente: si suppongono noti i numeri naturali e si usano per contare gli elementi di certi insiemi finiti, ossia esploriamo il *calcolo combinatorio* elementare. Il problema generale è la determinazione del numero di elementi di certi insiemi finiti conoscendo il numero d'elementi di certi altri insiemi finiti. Ricordiamo che due insiemi A e B si dicono *equipotenti* se esiste una biiezione $f : A \xrightarrow[su]{1-1} > B$. L'equipotenza possiede le proprietà riflessiva, simmetrica e transitiva. Se A è equipotente a B scriviamo $A \cong B$.

Siano $n \in \mathbf{N}$, $n > 0$, ed $\mathbf{N}_n = \{i \in \mathbf{N} \mid 1 \le i \le n\}$. Sia poi X un insieme. Diremo che X è *finito* se $X = \emptyset$ oppure se esiste $n \in \mathbf{N}$ tale che $\mathbf{N}_n \cong X$.

Ci sono vari modi di introdurre il numero di elementi di un insieme finito, ed ogni autore ha le sue preferenze. A me piace il modo seguente, basato su un lemmma di unicità.

LEMMA 3.2.1. Per ogni $m, n \in \mathbf{N}$, non nulli, se $\mathbf{N}_m$ ed $\mathbf{N}_n$ sono equipotenti allora $n = m$.

Dimostrazione. Procediamo per induzione rispetto ad m. Siano $\mathbf{N}_m$ ed $\mathbf{N}_n$ equipotenti e sia $f : \mathbf{N}_m \xrightarrow[su]{1-1} > \mathbf{N}_n$. Se m = 1, allora n = 1, altrimenti $\mathbf{N}_n = \{k \in \mathbf{N} \mid 1 \le k \le n\} \supset \{f(1)\}$, e viceversa. Sia m > 1 (quindi n > 1), sia vero il lemma per m-1 e dimostriamo che è vero anche per m.

Sia $u = f^{-1}(n) \in \mathbf{N}_m$. Poniamo $g : \mathbf{N}_{m-1} \to \mathbf{N}_n$, $g(k) = \begin{cases} f(k) & k < u \\ f(k+1) & k \ge u \end{cases}$. Allora:

$$\mathrm{im}(g) = \mathrm{im}(f) \setminus \{f(u)\} = \mathbf{N}_n \setminus \{n\} = \mathbf{N}_{n-1}$$

Inoltre, g è iniettiva. Infatti, $\forall h,k \in \mathbf{N}_{m-1}$, se g(h) = g(k) allora:

- Se sono entrambi minori di u, si ha f(h) = f(k) quindi h = k.
- Se sono entrambi maggiori di u, allora f(h+1) = f(k+1) implica h+1 = k+1 ossia h = k.
- Altrimenti, se k < u ≤ h, allora f(k) = f(h+1) implica $k = h+1 > h > k$, assurdo.

Pertanto, $g : \mathbf{N}_{m-1} \xrightarrow[su]{1-1} > \mathbf{N}_{n-1}$.

L'ipotesi induttiva implica allora m-1 = n-1, ossia m = n.

Questo lemma giustifica la seguente definizione. Siano X un insieme ed n un numero naturale non nullo. Se $X = \emptyset$ poniamo $|X| = 0$. Sia $X \neq \emptyset$; se X è equipotente ad $\mathbf{N}_n$ poniamo $|X| = n$. Chiameremo $|X|$ *numero di elementi* di X.

PROPOSIZIONE 3.2.2. Sia X un insieme finito, |X| = n.

a) Ogni insieme Y equipotente ad X ha lo stesso numero n di elementi.

b) Per ogni $A \subseteq X$ si ha $|A| \leq n$.

Dimostrazione. a) Se X è vuoto, anche Y è vuoto, quindi |X| = |Y| = 0. Sia X non vuoto; |X| = n significa che esiste $f : \mathbf{N}_n \xrightarrow{1-1 \atop su} X$. X ≅ Y significa che esiste $g : X \xrightarrow{1-1 \atop su} Y$, allora $g \circ f : \mathbf{N}_n \xrightarrow{1-1 \atop su} Y$ e quindi |Y| = n.

b) Se X = ø allora A = ø. Sia X ≠ ø; |X| = n significa che esiste $f : \mathbf{N}_n \xrightarrow{1-1 \atop su} X$. Consideriamo l'immagine $f^{-1}(A) \subseteq \mathbf{N}_n$ di A rispetto alla biiezione inversa. Allora $|A| = |f^{-1}(A)|$ e $f^{-1}(A)$ è costituito da numeri naturali distinti compresi tra 1 ed n, quindi sono al massimo n. Pertanto, |A| ≤ n.

Qui vedremo alcuni problemi classici in una formulazione che fa uso della teoria degli insiemi. Ciascuno di essi fornisce lo strumento per risolvere il problema successivo.

PROBLEMA I. Siano A e B insiemi finiti, e sia $A \cap B = \varnothing$. Calcolare $|A \cup B|$.

TEOREMA 3.2.3. - In queste ipotesi si ha $|A \cup B| = |A| + |B|$.

Dimostrazione. Poniamo |A| = k, |B| = n. Se k = 0 oppure n = 0 allora è banale. Altrimenti esistono $\varphi : \mathbf{N}_k \xrightarrow{1-1 \atop su} A$, $\psi : \mathbf{N}_n \xrightarrow{1-1 \atop su} B$. Definiamo ora una funzione $\Phi : \mathbf{N}_{k+n} \xrightarrow{1-1 \atop su} A \cup B$ ponendo, per ogni $i \in I_{k+n}$,

$$\Phi(i) = \begin{cases} \varphi(i) & \text{se } i \leq k \\ \psi(i-k) & \text{se } i > k \end{cases}$$

Poiché φ e ψ sono funzioni e $A \cap B = \varnothing$, anche Φ è una funzione ed è anche una biiezione.

COROLLARIO 3.2.4 – a) **Principio di addizione.** - Siano $A_1, \ldots, A_r$ insiemi finiti a due a due disgiunti. Allora $\left|\bigcup_{i=1}^{r} A_i\right| = \sum_{i=1}^{r} |A_i|$.

b) **Principio dei cassetti:** se A è un insieme con n elementi e $\wp = \{C_1, \ldots, C_m\}$ è una partizione di A con m < n blocchi, allora esiste $i \in \{1, 2, \ldots, r\}$ tale che $|C_i| > 1$.

Dimostrazione. a) Per induzione su r, se r = 2 è vero per il teorema 3.3.3. Supponiamo il teorema vero per r (≥ 2) e proviamo che di conseguenza è vero per r+1.

Posto $B = \bigcup_{i=1}^{r} A_i$, si ha $B \cap A_{r+1} = \varnothing$ e $|B| = \sum_{i=1}^{r} |A_i|$, dunque per il teorema 3.3.3 si ha $|B \cup A_{r+1}| = \sum_{i=1}^{r} |A_i| + |A_{r+1}| = \sum_{i=1}^{r+1} |A_i|$.

b) Se in un insieme A con n elementi consideriamo una partizione $\wp = \{C_1, \ldots, C_m\}$, allora A è unione disgiunta delle componenti $C_1, \ldots, C_m$. Ne segue $|A| = \left|\bigcup_{i=1}^{m} C_i\right| = \sum_{i=1}^{m} |C_i|$. In particolare, poiché ogni componente ha almeno un elemento, allora $|A| = \sum_{i=1}^{m} |C_i| \geq \sum_{i=1}^{m} 1 = m = |\wp|$. Di conseguenza, n > m implica che per almeno uno dei "cassetti" sia $|C_i| > 1$.

COROLLARIO 3.2.5. Siano A e B insiemi finiti. Se esiste $f : A \xrightarrow{su} B$ allora $|A| \geq |B|$.

Dimostrazione. Consideriamo la relazione di equivalenza $\Re_f$ in A, associata ad f, secondo la quale sono in relazione due elementi x ed y se f(x) = f(y). Essendo f suriettiva esiste una biiezione F tra l'insieme quoziente $A/\Re_f$, che è una partizione di A, e il codominio B, che associa ad ogni classe $[a]_{\Re_f}$ l'elemento $f(a)$. Dunque, $|A/\Re_f| = |B|$. Per quanto precede, però, $|A| \geq |A/\Re_f|$, perciò $|A| \geq |B|$.

COROLLARIO 3.2.6. Siano |A| = k, |B| = n, $C \subseteq A$, |C| = r.

a) $|A \setminus C| = k-r$.

b) Sia $C = A \cap B$, allora $|A \cup B| = k+n-r$.

Dimostrazione. a) La coppia $\{C, A \setminus C\}$ è una partizione di A, quindi per il principio di addizione si ha $|A| = |C| + |A \setminus C|$, da cui segue |A\C| = |A|-|C| = k-r.

b) La terna $\{C, A \setminus C, B \setminus C\}$ è una partizione di A∪B, quindi

$$|A \cup B| = |A \cap B| + |A \setminus C| + |B \setminus C| = r + (k - r) + (n - r) = k + n - r$$

Denotiamo con A×B il prodotto cartesiano di A per B, cioè l'insieme di tutte le coppie ordinate (a, b), con a∈A e b∈B.

PROBLEMA II. Siano A e B insiemi finiti. Calcolare |A×B|.

TEOREMA 3.2.7. Si ha |A×B| = |A| · |B|.

Dimostrazione. Se A oppure B è vuoto allora è banale. Altrimenti osserviamo che $A \times B = \bigcup_{a \in A} \left(\{a\} \times B \right)$, e che tutti gli insiemi $\{a\} \times B$ sono a due a due disgiunti ed equipotenti a B. Infatti, $a \neq a' \Rightarrow (a, b) \neq (a', b')$ per tutti i b, b'∈B, quindi $\left(\{a\} \times B \right) \cap \left(\{a'\} \times B \right) = \varnothing$. Inoltre, per ogni a∈A, la funzione $f_a : B \to \{a\} \times B,\ f_a : b \mapsto (a, b)$, risulta biiettiva, perciò $\{a\} \times B$ è equipotente a B. Per il corollario 3.3.4 si ha quindi:

$$|A \times B| = \left| \bigcup_{a \in A} \left(\{a\} \times B \right) \right| = \sum_{a \in A} |\{a\} \times B| = \sum_{a \in A} |B| = |A| \cdot |B|$$

perché somma di $|A|$ addendi uguali a $|B|$.

Il prodotto cartesiano degli insiemi $A_1, A_2, \ldots, A_n$, $n > 2$ è definito induttivamente: $A_1 \times \ldots \times A_n = (A_1 \times \ldots \times A_{n-1}) \times A_n$. I suoi elementi sono detti *liste* o *n-uple ordinate*, e denotati con $(a_1, a_2, \ldots, a_n)$.

COROLLARIO 3.2.8. Il principio di moltiplicazione. Se A_1, ..., A_k sono insiemi finiti, allora $|A_1 \times \ldots \times A_k| = \prod_{i=1}^{k} |A_i|$.

Dimostrazione. Procediamo per induzione rispetto a k. Per k = 2 l'asserto è il teorema 3.3.7. Sia k ≥ 3, allora si ha $A_1 \times \ldots \times A_k = (A_1 \times \ldots \times A_{k-1}) \times A_k$. Per ipotesi induttiva, $|A_1 \times \ldots \times A_{k-1}| = \prod_{i=1}^{k-1} |A_i|$ e, per il teorema 3.3.7, si ottiene:

$$|A_1 \times \ldots \times A_k| = |(A_1 \times \ldots \times A_{k-1}) \times A_k| = \left(\prod_{i=1}^{k-1} |A_i| \right) \cdot |A_k| = \prod_{i=1}^{k} |A_i|$$

NOTA. Il *principio di moltiplicazione* afferma che se per la lista $(a_1, a_2, \ldots, a_n)$ ci sono: n_1 possibilità per a_1, n_2 possibilità per a_2, e così via, in tutto ci sono $n_1 \cdot n_2 \cdot \ldots \cdot n_k$ liste distinte. In particolare, se A_1, ... , A_k sono tutti uguali ad un insieme A con n elementi, ci sono in tutto n^k liste distinte (k = lunghezza della lista, n = numero di scelte per ogni casella).

PROBLEMA III. Siano A e B insiemi finiti non vuoti. Calcolare $|B^A|$, ovvero il numero di funzioni f:A→B.

TEOREMA 3.2.9. Risulta $|B^A| = |B|^{|A|}$.

Dimostrazione. Sia $A = \{a_1, a_2, \dots, a_k\}$. Ogni f:A→B si può rappresentare mediante la tabella

x	f(x)
a_1	$f(a_1)$
a_2	$f(a_2)$
...	...
a_k	$f(a_k)$

, ossia, in definitiva, mediante la lista $(f(a_1), f(a_2), \dots, f(a_r))$. Quest'ultimo oggetto è un elemento del prodotto cartesiano B^k. Inversamente, dato un qualunque elemento $(b_1, b_2, \dots, b_k) \in B^k$, la tabella

x	y
a_1	b_1
a_2	b_2
...	...
a_k	b_k

definisce una funzione f:A→B. Allora la corrispondenza Φ che ad ogni funzione f:A→B associa la lista $(f(a_1), f(a_2), \dots, f(a_r)) \in B^k$ è una biiezione da B^A a B^k. Quest'ultimo ha $|B|^k = |B|^{|A|}$ elementi, quindi risulta proprio $|B^A| = |B|^{|A|}$.

ESEMPI 3.2.10.

3.3.10.A. - Quante parole di 3 lettere si possono scrivere con l'alfabeto $\{a, c, g, t\}$?

Ogni parola è una lista di lettere. Nel nostro caso, le lettere sono tre, e per ciascuna ci sono 4 possibilità, quindi $4 \cdot 4 \cdot 4 = 4^3 = 64$ parole.

3.2.10.B. - Sia |A| = n. Quante operazioni diverse, ossia funzioni $* : A \times A \to A$, si possono definire su A?

Poiché $|A \times A| = n^2$, le operazioni possibili sono $n^{(n^2)}$. Per esempio, se n = 2, ci sono $2^4 = 16$ operazioni distinte.

COROLLARIO 3.2.11. Sia U un insieme finito, |U| = n; allora $|\wp(U)| = 2^n$.

Dimostrazione. Sia X⊆U; definiamo la seguente funzione associata ad X, detta *funzione caratteristica* di X: $\varepsilon_X : U \to \{0,1\}$, $\varepsilon_X : x \mapsto \begin{cases} 0 & \text{se } x \notin X \\ 1 & \text{se } x \in X \end{cases}$.

Definiamo ora la funzione $\varepsilon : \wp(U) \to \{0,1\}^U$, $\varepsilon : X \mapsto \varepsilon_X$. Tale funzione è una biiezione, e allora dal teorema 3.3.8 segue l'asserto.

PROBLEMA IV. Siano A e B due insiemi finiti non vuoti. Calcolare il numero delle funzioni iniettive $f : A \xrightarrow{1-1} B$.

Se $|A| = k$ e $|B| = n$ tale numero si denota con $D_{n,k}$ e viene anche chiamato *numero delle disposizioni senza ripetizioni* di n oggetti a k a k. Il problema si può porre anche per $|A| = 0$: in tal caso fra A e B vi è solo la *funzione vuota*, che è iniettiva. Pertanto $D_{n,0} = 1$ per ogni $n \geq 0$.

LEMMA 3.2.12. Siano A e B insiemi finiti. Se esiste $f : A \xrightarrow{1-1} B$ allora $|A| \leq |B|$.

Dimostrazione. Poiché f è iniettiva allora la co-restrizione di f ad f(A) $\subseteq$ B è biiettiva da A ad f(A). Pertanto, A è equipotente ad f(A). Allora, $|A| = |f(A)| \leq |B|$.

TEOREMA 3.2.13. Risulta $D_{n,k} = \begin{cases} 0 & \text{se } k > n \\ \prod_{i=0}^{k-1}(n-i) & \text{se } 0 \leq k \leq n \end{cases}$.

Dimostrazione. Sia $|B| = n$. Se $|A| = k > n$, allora per il lemma si ha $D_{n,k} = 0$. Sia $k \leq n$. Ogni $f : A \xrightarrow{1-1} B$ si può rappresentare mediante la lista $(f(a_1), f(a_2), \ldots, f(a_r))$, dove gli elementi sono tutti distinti. Allora, mentre $f(a_1)$ è un elemento qualunque di B, $f(a_2) \in B \setminus f(a_1)$, che ha n-1 elementi, $f(a_3) \in B \setminus \{f(a_1), f(a_2)\}$, che ha n-2 elementi, e così via. La conclusione segue ora dal principio di moltiplicazione.

Poniamo 0! = 1, e per ogni n > 0 poniamo n! = (n-1)!·n. Il simbolo n! si legge "n *fattoriale* ".

PROPOSIZIONE 3.2.13. – a) Sia X un insieme finito non vuoto, $|X| = n$. Sia S_X l'insieme delle permutazioni su X. Allora $|S_X| = n!$

b) Risulta $D_{n,k} = \dfrac{n!}{(n-k)!}$ per ogni $0 \leq k \leq n$.

Dimostrazione. a) Le permutazioni di X sono biiezioni da X a se stesso, perciò ce ne sono $D_{n,n}$. Quest'ultimo numero coincide proprio con n!

b) Si ha $D_{n,k} = \dfrac{D_{n,k} \cdot (n-k)!}{(n-k)!} = \dfrac{n!}{(n-k)!}$.

Anagrammi. - Sia X un insieme finito non vuoto, |X| = n. Permutarlo è come dire riordinarlo in modo differente. Ciò si può fare in n! modi diversi.

Se una parola di lunghezza n non ha lettere ripetute, ci sono quindi n! *anagrammi* (prescindendo dal loro significato in italiano).

Se ci sono lettere con frequenza maggiore di 1?

Nei 120 anagrammi della parola *babbo*, le sei permutazioni delle tre *b* non mutano la parola. Pertanto, ogni anagramma si trova ripetuto 6 volte. In tutto quindi ci sono 20 anagrammi distinti.

Nella parola *mamma* oltre alle sei permutazioni delle tre *m*, anche le due della *a* non mutano la parola.
Allora ogni anagramma si trova ripetuto $6 \cdot 2 = 3! \cdot 2! = 12$ volte.
In tutto ci sono quindi $120/12 = 10$ anagrammi distinti.

Per una parola di n lettere che presenta due sole lettere distinte di frequenze k ed n-k, gli anagrammi distinti sono dunque $\frac{n!}{k! \cdot (n-k)!}$.

PROBLEMA V. Sia X un insieme finito con n elementi. Trovare il numero $C_{n,k}$ di sottoinsiemi di X aventi k elementi. Tale numero è anche chiamato numero delle *combinazioni senza ripetizione* di n oggetti a k a k.

NOTA: nel linguaggio comune, *combinazione* è spesso usata al posto di lista o n-upla ordinata.

TEOREMA 3.2.15. Si ha $C_{n,0} = 1$, e, per $0 \le k < n$, $C_{n,k} = \frac{n!}{k! \cdot (n-k)!} = D_{n,k}/k!$

Dimostrazione. Ordiniamo l'insieme X di n elementi in un ordine totale fissato, $X = \{x_1, x_2, \ldots, x_n\}$.

Ad ogni sottoinsieme Y associamo una parola w(Y) di lunghezza n, tale che se $x_i \in Y$ allora la i-esima lettera è V, altrimenti è F. Per esempio, al sottoinsieme vuoto è associata la parola con n lettere F, mentre ad X quella con n lettere V. Sia k il numero di lettere V e quindi n-k quello delle lettere F. Ogni sottoinsieme con k elementi ha associata una parola con lo stesso numero di lettere V e quindi un anagramma di w(Y). Inversamente, ad ogni tal anagramma è associato univocamente il sottoinsieme formato dagli elementi di X corrispondenti alle posizioni delle sue lettere V.

Poiché il numero di tali anagrammi è $\frac{n!}{k!\cdot(n-k)!}$, allora $C_{n,k} = \frac{n!}{k!\cdot(n-k)!} = D_{n,k}/k!$.

RIASSUNTO.

Sia X un insieme con n elementi.

- Se $k > n$, allora $C_{n,k} = 0$;
- se $0 \le k \le n$, $C_{n,k} = \frac{n!}{k!\cdot(n-k)!} = \frac{D_{n,k}}{k!}$.

Poniamo $\binom{n}{k} = C_{n,k} = \frac{n!}{k!\cdot(n-k)!}$. Questo simbolo si chiama *coefficiente binomiale*, ed è una frazione apparente, ossia un **numero intero**.

PROPOSIZIONE 3.2.16. Siano n, k due numeri interi ≥ 0 e sia $k \le n$.

a) $\binom{n}{0} = \binom{n}{n} = 1$.

b) $\binom{n}{k} = \binom{n}{n-k}$.

c) $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ (formula di Stiefel)

Dimostrazione. Sia X un insieme con n elementi.

a) $\binom{n}{0}$ è il numero di sottoinsiemi di X con 0 elementi, ossia vuoti, e ce n'è uno solo. Analogamente, di sottoinsiemi di X con n elementi c'è solo X.

b) Per ogni sottoinsieme di X con k elementi c'è il complementare con n-k elementi. Pertanto,

$$\binom{n}{k} = \binom{n}{n-k}.$$

c) Si fissi un elemento x di X. Ogni sottoinsieme Y di X con k elementi è di uno dei due tipi seguenti:

- Y non contiene x: è un sottoinsieme con k elementi di X\{x}, che ha n-1 elementi; di questi Y quindi ce ne sono $\binom{n-1}{k}$;
- Y contiene x: allora Y\{x} è un sottoinsieme con k-1 elementi di X\{x}, che ha n-1 elementi; di questi Y quindi ce ne sono $\binom{n-1}{k-1}$

In totale quindi ci sono $\binom{n-1}{k} + \binom{n-1}{k-1}$ sottoinsiemi Y con k elementi.

Le proprietà a) e c) consentono di costruire un noto triangolo, detto in Italia "Triangolo di Tartaglia", in Francia "Triangolo di Pascal", in Germania "Triangolo di Stifel" e così via, ma era noto anche a cinesi e indiani di vari secoli prima. Perciò è preferibile chiamarlo *triangolo aritmetico*. Il termine all'incrocio della riga n-esima con la colonna k–esima è $\binom{n}{k}$, ed è ottenuto sommando i termini $\binom{n-1}{k-1}$ ed $\binom{n-1}{k}$, che lo sovrastano nella riga precedente. Gli zeri sono omessi per semplicità.

n \ k	0	1	2	3	4	5	6	7	2^n
0	1								$1 = 2^0$
1	1	1							$2 = 2^1$
2	1	2	1						$4 = 2^2$
3	1	3	3	1					$8 = 2^3$
4	1	4	6	4	1				$16 = 2^4$
5	1	5	10	10	5	1			$32 = 2^5$
6	1	6	15	20	15	6	1		$64 = 2^6$
7	1	7	21	35	35	21	7	1	$128 = 2^7$

La somma dei termini della riga n-esima dà il numero di sottoinsiemi di un insieme con n elementi, che sappiamo essere 2^n. La somma dei termini paralleli alla diagonale secondaria è la *successione di Fibonacci*

1 1 2 3 5 8 13 21 34 …

Questa successione è definita da $\begin{cases} f(0) = 0 \\ f(1) = 1 \\ f(n+2) = f(n) + f(n+1) \end{cases}$.

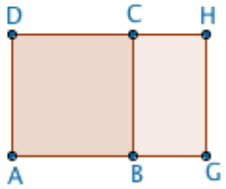
Essa per n→+∞ tende a +∞, tuttavia la successione dei rapporti f(n+1)/f(n) tende ad un limite finito γ.
Si ha infatti:

$$\gamma = \lim_{x\to\infty} \frac{f(n+2)}{f(n+1)} = \lim_{x\to\infty} \frac{f(n+1)+f(n)}{f(n+1)} = \lim_{x\to\infty} \left(1 + \frac{f(n)}{f(n+1)}\right) = \lim_{x\to\infty} \left(1 + \frac{1}{\frac{f(n+1)}{f(n)}}\right) = 1 + \frac{1}{\gamma}.$$

Pertanto, γ deve essere finito ed è la soluzione positiva dell'equazione:

$$x^2 - x - 1 = 0 \Rightarrow \gamma = \frac{1+\sqrt{5}}{2} \approx 1{,}618$$

ossia il celebre *numero aureo* dell'architettura greca.



Il rettangolo aureo:

ABCD è un quadrato e AG:AD = AD:BG, ossia i rettangoli AGHD e BGHC sono simili. Allora si ricava AG:AD = γ

COROLLARIO 3.2.17. - *Formula di Newton* - Siano x e y due numeri reali ed n∈**N.**

Allora $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$.

Dimostrazione. Se n = 0 oppure n = 1 il risultato è immediato.

Sia n ≥ 2: $(x+y)^n = (x+y)(x+y)\cdots(x+y)$, e lo sviluppo del secondo membro è la somma dei monomi ottenuti scegliendo un termine da ogni fattore x+y, dunque ogni tal monomio è del tipo $x^{n-k}y^k$, ed è ottenuto scegliendo y da k degli n fattori x+y ed x dagli altri n-k. Pertanto per ognuno degli $\binom{n}{k}$ insiemi di k fattori x+y vi è un monomio $x^{n-k}y^k$; riducendo i termini simili, il coefficiente di questo monomio diviene $\binom{n}{k}$.

NOTA. Posto x = y = 1, dalla formula di Newton si riottiene il numero 2^n di sottoinsiemi di un insieme con n elementi.

Esempio 3.2.18. a) Il numero di possibili sestine nel superenalotto si ottiene considerando che da un insieme di n = 90 numeri sostanzialmente se ne estraggono k = 6, distinti. Allora il numero cercato è:

$$C_{90,6} = \binom{90}{6} = \frac{90!}{6!\cdot 84!} = \frac{90\cdot 89\cdot 88\cdot 87\cdot 86\cdot 85}{6\cdot 5\cdot 4\cdot 3\cdot 2\cdot 1} = 622.614.630.$$

b) Le applicazioni dei coefficienti binomiali sono numerose, non solo in Algebra ed in Combinatoria, ma anche in altre discipline. Per esempio, se in una specie animale le nascite di maschi e femmine hanno la stessa probabilità e se ogni nascita non influenza le altre, qual è la probabilità che di otto figli di una coppia, cinque siano femmine e tre maschi? E quella che le femmine siano almeno cinque?

Secondo la formula di Bernoulli, la probabilità di cinque femmine e tre maschi è $\binom{8}{5}\cdot\left(\frac{1}{2}\right)^5\cdot\left(\frac{1}{2}\right)^3 = \binom{8}{3}\cdot\left(\frac{1}{2}\right)^8 = \frac{8\cdot 7\cdot 6}{3\cdot 2\cdot 1\cdot 256} = \frac{7}{32} = 0,21875 \approx 21,9\%$. La probabilità che almeno cinque siano femmine, oltre al caso precedente, comprende anche sei, sette od otto femmine, quindi, ricordando che $\binom{n}{k} = \binom{n}{n-k}$, si ottiene:

$$\frac{1}{256}\cdot\left(\binom{8}{3}+\binom{8}{2}+\binom{8}{1}+\binom{8}{0}\right) = \frac{56+28+8+1}{256} = \frac{93}{256} \approx 36,3\%$$

3.3. I numeri interi (relativi)

All'Università s'insegna a passare dai numeri naturali all'anello dei numeri interi relativi. Il procedimento che si segue è la simmetrizzazione del monoide commutativo regolare (**N**, +, 0). Questa costruzione di **Z**, pur così astratta, presenta alcuni vantaggi: le definizioni e le dimostrazioni sono dirette e generali e non è necessario esaminare sottocasi. Essa consente di definire in **Z** anche la moltiplicazione e l'ordinamento a partire da quelli di **N**, ma non in modo abbastanza naturale.
Si ottiene l'anello **Z** e, da questo, col procedimento generale del campo dei quozienti di un dominio d'integrità, si passa al campo razionale **Q**.
Nei corsi d'Algebra della scuola secondaria questa via non viene però mai seguita, ma si costruiscono i "numeri razionali assoluti", poi i "numeri reali assoluti" ed infine si passa a introdurre i numeri (reali) negativi e la struttura di campo ordinato (che non viene però quasi mai nominata).
Nel seguito presento una possibile via per costruire direttamente **Z** a partire da **N**, che serve da modello per il passaggio da razionali e reali "assoluti" a razionali e reali "relativi".

L'impossibilità di eseguire sempre la sottrazione nell'insieme **N** dei numeri naturali ha portato alla costruzione dei numeri *interi relativi*, o semplicemente dei *numeri interi*.
Elementarmente, si possono definire coppie formate da un *segno,* + oppure -, e da un numero naturale: +7, -12, -35, +35.

Le coppie +0 e -0 si considerano coincidenti e individuano un numero intero che si denota solo con 0.

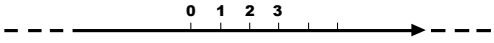
L'insieme ottenuto si denota con:

$$\mathbf{Z} = \{0, +1, -1, +2, -2, +3, -3, \ldots\}.$$

Per comodità, il segno + di solito non si scrive.
Chiamiamo *negativi* i numeri col segno - e *positivi* quelli col +.

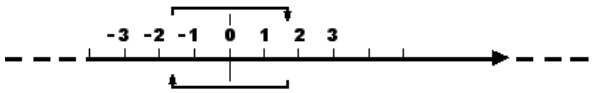
"Identifichiamo" gli interi positivi e lo zero con i numeri naturali.

Rappresentazione geometrica. Sia data una retta r, su cui siano fissati un *punto* O, una *unità di misura* u ed un *orientamento*. Possiamo distribuire i numeri naturali 0, 1, 2, ... sulla semiretta positiva, facendoli corrispondere ai multipli del segmento unità di misura.



Sull'altra semiretta collochiamo i numeri negativi.

L'effetto del segno – è quello di scambiare, con una rotazione di 180° intorno ad O, la semiretta positiva con quella negativa.



Perciò, per ogni x∈**Z**, -(-x) = x.

Ordinamento. Definiamo l'*ordine* ≤ in **Z**:

- Lo zero è maggiore di ogni numero negativo e minore di ogni positivo.
- Sui positivi l'ordine coincide con quello naturale di **N**:

  $+3 < +5$ perché $3 < 5$
- Sui negativi l'ordine è opposto, perché il segno – opera una simmetria rispetto all'origine: $-5 < -3$ perché $3 < 5$

L'ordine ≤ è totale ed è una *estensione* di quello di **N**: sui numeri positivi coincide infatti con quello di **N**.

Il successivo. La funzione σ ("*successivo di*") si prolunga da **N** a **Z** ponendo ∀m, n∈**N**:

$$\sigma(-m) = -n \Leftrightarrow \sigma(n) = m$$

Si ha così: $\sigma : \mathbf{Z} \xrightarrow[\text{su}]{1\text{–}1} \mathbf{Z}$. In particolare, si ha $0 = \sigma(-1)$. Inoltre, esiste σ^{-1}.

Valore assoluto e segno. Ad ogni intero x associamo un intero $|x| \geq 0$, ed un altro intero $\text{sign}(x) \in \{-1, 1\}$, definiti da:

$$|x| = \begin{cases} x & \text{se } x \geq 0 \\ -x & \text{se } x < 0 \end{cases}, \quad \text{sign}(x) = \begin{cases} 1 & \text{se } x > 0 \\ -1 & \text{se } x < 0 \end{cases}.$$

$|x|$ è il *valore assoluto* di x; sign(x) è il *segno* di x ed è definito solo per $x \neq 0$.

Operazioni. Le *operazioni* in **Z** sono costruite in modo che sui numeri positivi coincidano con quelle di **N**, ed inoltre siano compatibili con il segno.

In particolare, $\forall a \in \mathbf{Z}, \forall n \in \mathbf{N}$, si potrebbe definire l'*addizione* nel modo ricorsivo seguente:

$$\begin{cases} a + 0 = a \\ a + \sigma(n) = \sigma(a + n) \end{cases} \qquad \begin{cases} a + (-1) = \sigma^{-1}(a) \\ a + (-\sigma(n)) = \sigma^{-1}(a + (-n)) \end{cases}$$

Ma questa definizione è incomprensibile. Pare più intuitivo ragionare geometricamente: σ è una traslazione di una unità nel verso positivo, mentre σ^{-1} è una traslazione di una unità nel verso negativo. Allora $a+n=\sigma^{n}(a)$, $a+(-n)=\sigma^{-n}(a)$. Ossia, aggiungere n ad a significa spostarsi verso destra a partire da a di n unità; sommare -n ad a significa spostarsi invece verso sinistra a partire da a di n unità.

Ora si può definire la *sottrazione*: ∀a, b∈**Z**, a-b = a+(-b). Questa è ora una operazione in **Z**, sempre possibile.

Poi si definisce la *moltiplicazione*:

$$\begin{cases} a\cdot 0=0 \\ a\cdot\sigma(n)=a\cdot n+a \end{cases} \qquad \begin{cases} a\cdot(-1)=-a \\ a\cdot(-n)=(-a)\cdot n \end{cases}$$

In alternativa, ricaviamo la *regola dei segni*

·	+	−
+	+	−
−	−	+

ricordando la funzione del segno – come inversione dell'ordine sulla retta, e poi definiamo il prodotto di due interi non nulli come prodotto dei loro *valori assoluti* (eseguita come fossero numeri naturali) e dei loro *segni*.

Ne ricaviamo la *legge d'annullamento del prodotto*:

∀a, b∈**Z**, a·b = 0 ⇒ a = 0 oppure b = 0

Le due operazioni + e · hanno le proprietà associativa e commutativa; hanno gli elementi neutri (0 per l'addizione ed 1 per la moltiplicazione), ed ogni elemento x ha l'opposto –x, tale che x + (-x) = 0.

Inoltre, come in **N**, la moltiplicazione è *distributiva* rispetto all'addizione:

∀a, b, c∈**Z**: (a+b)·c = a·c + b·c

Potremmo riassumere queste proprietà dicendo che con queste operazioni **Z** diventa un *dominio d'integrità*.

Elementi invertibili. Dalla definizione di prodotto e dalle proprietà di **N** si ricava:

$$\mathbf{Z}^{*}=\{x\in\mathbf{Z}\mid \exists y\in\mathbf{Z},\ x\cdot y=1\}=\{1,-1\}$$

Questo *gruppo* coincide col gruppo moltiplicativo dei segni.

La divisione col resto. Come in **N**, dati due interi a, b, con $b \neq 0$, esistono due interi q ed r tali che $a = b \cdot q + r$, con $|r| < |b|$.

Non sono unici, in generale; lo sono se si impone $r \geq 0$.

Esempi:

$$\begin{array}{r|l} 11 & -7 \\ \hline 4 & -1 \end{array} \qquad \begin{array}{r|l} -11 & -7 \\ \hline 3 & 2 \end{array} \qquad \begin{array}{r|l} -11 & 7 \\ \hline 3 & -2 \end{array}$$

La divisibilità. Si può procedere come in **N**, ma c'è la complicazione dei segni: ogni numero $a \in \mathbf{Z}$ è infatti divisore anche del suo opposto: $a = (-1)\cdot(-a)$.

Per esempio, un numero p è *primo* se ha per divisori solo 1, -1, p, -p.

Conviene però pensare ogni numero negativo come ottenuto moltiplicando il suo opposto (che è positivo) per -1. In tal modo, i conti si svolgono sempre con numeri positivi.

Valgono allora in **Z** il *teorema fondamentale dell'aritmetica*, *l'algoritmo euclideo* e l'esistenza del *MCD* e del *mcm* e la loro unicità se scelti positivi.

In **Z** c'è in più un vantaggio non piccolo: *l'identità di Bézout*: per ogni a, $b \in \mathbf{Z}$ non nulli esistono x, $y \in \mathbf{Z}$ tali che $a \cdot x + b \cdot y = MCD(a,b)$.

Con queste proprietà, **Z** diventa un *dominio euclideo* e quindi un *dominio ad ideali principali*.

Proprietà che collegano l'ordine alle operazioni e lo trasformano in un *anello ordinato*: $\forall a,b,c \in \mathbf{Z}$,

- $a \leq b \Leftrightarrow a+c \leq b+c$
- $c > 0$: $a \leq b \Rightarrow a \cdot c \leq b \cdot c$
- $c < 0$: $a \leq b \Rightarrow a \cdot c \geq b \cdot c$

NOTA. Un altro modo di definire l'ordine in **Z** consiste nel porre:

$x \leq y$ se $y - x$ è positivo.

Si dimostra che questa è una relazione d'ordine totale, e che coincide con quella definita in precedenza.

Questo modo di definire i numeri interi fa uso della visione geometrica, ossia in realtà sembra presupporre i numeri reali. Inoltre, le dimostrazioni sono spesso difficili. Tuttavia, la costruzione è abbastanza intuitiva e questo è lo scopo del primo approccio con i numeri relativi.

Inoltre, i numeri negativi si possono giustificare con le temperature invernali, le perdite finanziarie ecc. oltre che con l'esigenza di poter eseguire sempre la sottrazione.

3.4. I numeri razionali assoluti e relativi

La costruzione qui presentata riprende la parte vista nel capitolo dei numeri naturali e ricalca in parte la via seguita nella scuola secondaria. La differenza principale è nella definizione della relazione d'equivalenza tra le frazioni, che nella scuola media è: moltiplicando o dividendo (ove possibile) numeratore e denominatore della frazione $\frac{a}{b}$ per uno stesso numero k, si ottiene una frazione equivalente a quella data. Inoltre, la relazione d'ordine è ottenuta riducendo due frazioni allo stesso denominatore (il mcm dei denominatori) e poi confrontando i nuovi numeratori.

Dal monoide moltiplicativo $\left(\mathbf{N}^+, \cdot, 1\right)$ dei numeri naturali non nulli possiamo ottenere per simmetrizzazione il gruppo moltiplicativo $\left(\mathbf{Q}^+, \cdot, 1\right)$ dei razionali assoluti. I suoi elementi si denotano comunque con $\frac{a}{b}$, e come rappresentanti delle classi si scelgono a, b in modo che MCD(a,b) = 1 (frazione ridotta ai *minimi termini*), dato che in ogni classe c'è una sola frazione di questo tipo.

Si definisce poi l'addizione, dapprima tra le frazioni ponendo $\frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + b \cdot c}{b \cdot d}$ e, poiché anche questa operazione risulta compatibile con la relazione d'equivalenza ~, in seguito si estende anche tra le classi di frazioni. Si aggiunge la classe $0 = \left\{ \frac{0}{b} \;\middle|\; b \in \mathbf{N}^+ \right\}$, che diventa l'elemento neutro di + e che è elemento assorbente per la moltiplicazione. Poniamo $\overline{\mathbf{Q}} = \mathbf{Q}^+ \cup \{0\}$, l'insieme *dei razionali assoluti*. $\left(\overline{\mathbf{Q}}, +, 0\right)$ è un monoide commutativo regolare.

L'ordine in $\overline{\mathbf{Q}}$ è definito dapprima ponendo $\frac{a}{b} \le \frac{c}{d} \Leftrightarrow a \cdot d \le b \cdot c$ e poi, essendo tale relazione compatibile con l'equivalenza ~, si passa alle classi di frazioni.

Si tratta di un ordine *denso*, ossia tra due suoi elementi ce n'è sempre un altro; si ha infatti, per ogni x ed y distinti, con x < y, si ha $x < \frac{x+y}{2} < y$.

Non è invece un ordine *completo*, ossia esistono dei sottoinsiemi non vuoti privi di *estremo superiore*. Un esempio è $\left\{ x \in \overline{\mathbf{Q}} \;\middle|\; x^2 \le 2 \right\}$, dato che non esistono razionali col quadrato uguale a 2.

Per estendere l'insieme $\overline{\mathbf{Q}}$ dei razionali assoluti, si può ora simmetrizzare il monoide commutativo regolare additivo $\left(\overline{\mathbf{Q}},+,0\right)$, oppure ripetere quanto visto nel passare da **N** a **Z**.

Nel primo caso, i numeri razionali relativi sono ottenuti come coppie ordinate di razionali assoluti, ossia di elementi di $\overline{\mathbf{Q}}$. Come nel caso di (**N**, +, 0), la relazione ~ diventa: (a,b) ~ (c,d) se a+d = b+c. L'operazione di addizione tra coppie di *razionali assoluti* è definita da:

$$(a,b)+(c,d) = (a+c, b+d)$$

ed è compatibile con la relazione d'equivalenza ~. Il suo elemento neutro è la coppia (0, 0); l'opposta della classe [a,b] è [b,a]. Il gruppo quoziente è denotato con **Q**.

Le classi del tipo $[a,0]$ costituiscono un sottomonoide isomorfo a $\left(\overline{\mathbf{Q}},+,0\right)$. Identifichiamo [a, 0] con a. Si ha così la seguente proprietà:

ogni elemento di **Q** o appartiene a $\overline{\mathbf{Q}}$ o è l'opposto di un elemento di $\overline{\mathbf{Q}}$.

Infatti, dato [a,b]∈**Q**, se a ≥ b si ha [a, b] = [a-b, 0], risultando a+0 = b+(a-b).
Se invece a < b, essendo a+(b-a) = b+0, si ha [a, b] = [0, b-a] = -[b-a, 0].
Chiamiamo ora *positivi* gli elementi di $E = \mathbf{Q}^- \cup \{0\} \cup \left(\left(A \cap \mathbf{Q}^+\right)\cdot\left(C \cap \mathbf{Q}^+\right)\right) = \left\{x \in \mathbf{Q} \mid x = [a,0], a \neq 0\right\}$ e negativi i loro opposti. Questo sottoinsieme è chiuso rispetto all'addizione ed alla moltiplicazione e per ogni elemento x∈**Q** non nullo, uno ed uno solo tra x e –x è positivo. L'ordinamento in **Q** è definito allora ponendo: x < y se y-x è positivo. Si tratta di un ordine totale, in cui i positivi sono tutti e soli i numeri maggiori di zero. Esso estende l'analogo ordine di $\overline{\mathbf{Q}}$. In alternativa si può dire che l'ordine ≤ in **Q** è definito da:

- x ≤ y se x è negativo ed y è positivo o nullo;
- x ≤ y se x ed y sono entrambi positivi e x ≤ y come razionali assoluti;
- x ≤ y se sono entrambi negativi e –y ≤ -x come razionali assoluti.

L'ordine è poi *denso*, perché dati x ed y distinti, x < y, si ha $x < \frac{x+y}{2} < y$; non è completo perché non lo è in $\overline{\mathbf{Q}}$.
Resta da estendere la moltiplicazione, con una certa casistica:

- Se a e b sono entrambi positivi, si moltiplicano come in $\mathbf{Q}^+$ e si ha un numero positivo.
- Se a è negativo, b positivo, allora $a \cdot b = -\left(\left(-a\right)\cdot b\right)$, che è negativo perché opposto di un positivo.
- Se a è positivo, b negativo, allora $a \cdot b = -\left(a \cdot \left(-b\right)\right)$, che è negativo.
- Se sono entrambi negativi, allora $a \cdot b = \left(-a\right)\cdot\left(-b\right)$, che è positivo.

- Se uno dei due è = 0, il prodotto è = 0.

Questa moltiplicazione risulta associativa, commutativa, ha 1 per elemento neutro, è distributiva rispetto al + e ogni elemento non nullo ha l'inverso; infine, ristretta a $\overline{\mathbf{Q}}$, coincide con quella di $\overline{\mathbf{Q}}$. Alla fine, la struttura che si ottiene è detta *campo razionale* **Q**.

In alternativa a questo metodo, che sarebbe poco comprensibile in una scuola, si può ricorrere all'aggiunta dei segni + e - davanti ai razionali assoluti, e poi procedere come per **Z** dicendo che i numeri col + sono i *positivi* e quelli col – i *negativi*, mentre +0 = -0 = 0 non ha segno.

Si definiscono le due funzioni *valore assoluto* e *segno* come in **Z**.

L'o*rdinamento* è definibile come abbiamo visto per **Z**.

Il *prodotto* si ottiene come prodotto dei moduli (che sono positivi e quindi identificabili con gli elementi di $\mathbf{Q}^+$) e dei segni con la regola consueta.

L'*addizione* è più complicata, perché qui non c'è il successivo. Allora si devono distinguere vari casi, a seconda dei valori assoluti e dei segni degli addendi.

Dimostrare le proprietà dell'addizione non è ovvio, ma nella scuola secondaria ecc. ecc.

Si definiscono infine la *sottrazione* tra elementi di **Q** ponendo: $x - y = x + (-y)$, e la *divisione esatta* ponendo, se $y \neq 0$, $x : y = x \cdot y^{-1}$.

Razionali come operatori su grandezze. Ora vediamo una costruzione alternativa, che tenta di formalizzare quel che sui numeri razionali imparano gli alunni delle scuole elementari, e che forse è più intutiva e naturale.

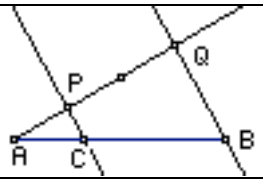
Come visto nel modulo di Elementi di Geometria, i segmenti costituiscono una classe di grandezze. I segmenti si possono trasportare come segmenti OP di una prefissata semiretta avente origine in un punto O. Rispetto alla somma i segmenti costituiscono un monoide regolare ordinato. Il segmento degenere OO, ossia il punto O, è l'elemento neutro.

Su questo monoide $(\Sigma,+,O)$ i numeri naturali agiscono innanzi tutto come *multipli interi*: $\forall n \in \mathbf{N}$, $\forall OP \in \Sigma$, si pone: $nOP = \begin{cases} O & \text{se } n = 0 \\ (n-1)OP + OP & \text{se } n > 0 \end{cases}$.

Con le simmetrie rispetto alle rette tratteggiate, si ottiene $AA' = 2AB$, $AB' = 3AB$, $AH = 4AB$.

I numeri naturali positivi agiscono anche come *sottomultipli*, ossia

$$\forall n \in \mathbf{N}^+, \forall OP \in \Sigma, \ \frac{1}{n}OP = OC \Leftrightarrow nOC = OP$$

	Tracciata una semiretta per A, preso su di essa un punto P, si costruisca il segmento AQ = nAP. La parallela per P a BQ interseca AB nel punto C tale che nAC = AB. In figura è n = 3.

Possiamo quindi definire l'azione della *frazione* $\frac{m}{n}$, con $n \neq 0$, ponendo per ogni segmento AB (o anche solo sui segmenti OP):

$$\frac{m}{n}AB = \frac{1}{n}\left(mAB\right)$$

La definizione è ben posta, perché se AB = A'B' allora $\frac{m}{n}AB = \frac{m}{n}A'B'$. Inoltre, si ha:

$$m\left(\frac{1}{n}AB\right) = \frac{1}{n}\left(mAB\right) = \frac{m}{n}AB$$

Abbiamo definito quindi delle *funzioni* sul monoide dei segmenti, funzioni che denoteremo con le frazioni stesse.

Tra le funzioni è definita "a monte" l'uguaglianza: date $f, g : X \to Y$ si ha

$$f = g \Leftrightarrow \forall x \in X,\ f\left(x\right) = g\left(x\right).$$

Nel nostro caso quindi per ogni coppia di frazioni $\frac{m}{n}, \frac{p}{q}$ si ha $\frac{m}{n} = \frac{p}{q} \Leftrightarrow \forall AB,\ \frac{m}{n}AB = \frac{p}{q}AB$.

Per ottenere una condizione aritmetica si applicherà la definizione di questa azione, ottenendo: $(m \cdot q)OP = (n \cdot p)OP$, ossia $m \cdot q = n \cdot p$.

Ne segue, in definitiva, $\frac{m}{n} = \frac{p}{q} \Leftrightarrow m \cdot q = n \cdot p$, e questa è la consueta equivalenza tra le frazioni. In particolare, si ha $\forall k \neq 0,\ \frac{m}{n} = \frac{m \cdot k}{n \cdot k}$. Ciascuna di queste funzioni è rappresentabile mediante una qualunque delle infinite frazioni equivalenti, fra le quali di norma scegliamo $\frac{0}{1}$ per la funzione nulla e $\frac{m}{n}$, $MCD\left(m, n\right) = 1$, negli altri casi. Tali frazioni sono dette "ridotte ai minimi termini".

L'addizione è definita "punto per punto": per ogni coppia di frazioni $\frac{m}{n}, \frac{p}{q}$ si ha:

$$\forall AB,\ \left(\frac{m}{n} + \frac{p}{q}\right)AB = \frac{m}{n}AB + \frac{p}{q}AB$$

Questa addizione è compatibile sia con la congruenza di segmenti, sia con l'equivalenza delle frazioni. Si ha poi: $\forall AB,\ \left(\frac{m}{n} + \frac{p}{q}\right)AB = \frac{m \cdot q + n \cdot p}{n \cdot q}AB$. Questa uguaglianza si dimostra per passi, provando dapprima che $\forall AB,\ \left(\frac{m}{n} + \frac{h}{n}\right)AB = \frac{m + h}{n}AB$ e poi:

$$\forall AB,\ \left(\frac{m}{n} + \frac{p}{q}\right)AB = \left(\frac{m \cdot q}{n \cdot q} + \frac{p \cdot n}{q \cdot n}\right)AB = \frac{m \cdot q}{n \cdot q}AB + \frac{p \cdot n}{q \cdot n}AB = \frac{m \cdot q + n \cdot p}{n \cdot q}AB$$

Ne segue l'usuale regola per sommare le frazioni, $\frac{m}{n}+\frac{p}{q}=\frac{m\cdot q+n\cdot p}{n\cdot q}$, e si dimostra che è compatibile con l'equivalenza di frazioni.

Tra le funzioni è definita anche la composizione. Si ha proprio:

$$\left(\frac{m}{n}\circ\frac{p}{q}\right)AB=\frac{m}{n}\left(\frac{p}{q}AB\right)=\frac{m\cdot p}{n\cdot q}AB$$

Con un poco di pazienza ed applicando la definizione di queste frazioni, si arriva a dimostrare l'uguaglianza di cui sopra, compatibile con l'azione di Γ. Allora possiamo porre:

$$\frac{m}{n}\cdot\frac{p}{q}=\frac{m\cdot p}{n\cdot q}$$

e questa identità è compatibile con l'uguaglianza di frazioni.

Alcune proprietà di queste operazioni sono immediate: per l'addizione (punto per punto) valgono le stesse proprietà del monoide dei segmenti, ossia la commutatività e l'associatività, ed inoltre le frazioni $\frac{0}{n}$, tutte equivalenti fra loro, sono l'elemento neutro. La moltiplicazione, ossia la composizione, è associativa, ha l'identità (che è la classe delle frazioni $\frac{n}{n}$) come elemento neutro ed è distributiva a sinistra rispetto all'addizione, ma, di più, è commutativa e quindi è distributiva anche a destra.

Infine, ogni funzione $\frac{m}{n}$, $m\neq 0$, è biiettiva, in quanto $\forall AB,\ CD=\frac{m}{n}AB\Leftrightarrow AB=\frac{n}{m}CD$. L'inversa è la frazione $\frac{n}{m}$, e ciò è compatibile con l'equivalenza di frazioni.

Riassumendo, abbiamo una classe $\overline{Q}$ di funzioni definite sui segmenti e rappresentate da frazioni. In questo insieme di funzioni abbiamo un'addizione che costituisce un monoide commutativo regolare, una moltiplicazione che è commutativa, associativa, distributiva rispetto all'addizione, ha la funzione nulla per elemento assorbente e, esclusa quest'ultima, forma un gruppo.

Per concludere la costruzione manca solo l'ordinamento. È noto che è possibile confrontare sempre due segmenti, stabilendo chi è il maggiore, se non sono uguali. Si può dimostrare che date due funzioni $\frac{m}{n},\frac{p}{q}$, se si ha $\frac{m}{n}AB\leq\frac{p}{q}AB$ per un dato segmento AB, allora ciò vale per ogni altro segmento, quindi si può porre in questo caso $\frac{m}{n}\leq\frac{p}{q}$. La relazione vale per ogni altra rappresentazione delle due funzioni mediante frazioni. Questa è inoltre una relazione d'ordine totale tra le nostre funzioni, e si può tradurre aritmeticamente così: si ha

$\frac{m}{n} \le \frac{p}{q} \Leftrightarrow m \cdot q \le n \cdot p$. In particolare, si ha $\frac{m}{n} \le \frac{p}{n} \Leftrightarrow m \le p$, e da qui, con qualche passaggio si ricava la formula precedente. Tale ordine è compatibile con l'addizione e la moltiplicazione, ed inoltre è *denso*, ossia tra due frazioni distinte ce ne sono infinite altre.

Questo percorso per costruire i razionali *assoluti* è come detto una possibile razionalizzazione di quanto gli scolari apprendono nella scuola elementare. Esso ha tuttavia varie difficoltà.

- Il monoide di partenza, $(\Sigma, +, O)$ è sostanzialmente $(\mathbf{R}^+ \cup \{0\}, +, 0)$, e se si conoscono già i numeri reali, i razionali si trovano come il particolare sottoinsieme formato dai multipli naturali di 1 e dai loro quozienti.
- L'azione sui segmenti presuppone una buona conoscenza del piano euclideo.
- Si opera di fatto sul quoziente dell'insieme dei segmenti rispetto alla relazione di congruenza, il che è difficile anche per studenti universitari.
- Alle spalle vi è il concetto di funzione, sia pure mimetizzato; la sua mancata esplicitazione vanifica la naturalezza delle definizioni di equivalenza di frazioni, di addizione, moltiplicazione ed ordinamento tra frazioni e poi tra razionali assoluti. Pertanto, alla fine le regole per sommare, moltiplicare e confrontare si rischia comunque di darle in modo astratto ed imperativo.
- In teoria si potrebbero usare altre classi di grandezze al posto dei segmenti. Tuttavia, per esempio le usatissime *torte* (ossia gli angoli di dato vertice) hanno grosse difficoltà: sia concettuali, per esempio il non poter definire con chiarezza e semplicità che cosa sia la somma di due fette maggiori della metà, sia operative, come il non potere agevolmente trovare i sottomultipli: come costruire in modo esatto un terzo di un sesto della torta? Dalla teoria di Galois sappiamo che non è possibile farlo con riga e compasso. Peggio ancora l'usare **N** stesso come insieme di grandezze: chi è la metà di 3?

Proseguendo su questa via, l'estensione dei razionali assoluti al campo razionale, ossia l'introduzione dei numeri negativi, comporta poi altre difficoltà, legate alla giustificazione del segno negativo –. Si può pensare di usare una generalizzazione degli operatori su grandezze, dove le grandezze sono i segmenti, sui quali agisce il gruppo Γ delle isometrie. L'idea più naturale è usare segmenti orientati al posto dei segmenti. Tuttavia, pensare che così semplicemente si risolva il problema è illusorio, in quanto $\vec{AB}$ e $\vec{BA}$ si corrispondono con una rotazione di ampiezza un angolo piatto, ossia con un'isometria diretta. Allora dovremo rinunciare all'azione dell'intero gruppo Γ e limitarci solo al sottogruppo T delle traslazioni. In tal caso, le classi sono i *vettori* del piano, ma la

somma naturale dei vettori è quella con la regola del parallelogramma. Ci sono quindi alcune modifiche da fare.

Si pone intanto $-\vec{AB} = \vec{BA}$. Si definisce poi $\left(-\frac{m}{n}\right)\vec{AB} = \frac{m}{n}\vec{BA} = \frac{m}{n}(-\vec{AB})$. Allora il segno – è una funzione sui vettori, detta *opposto*, che commuta con le frazioni e che, sommata con l'identità, dà la funzione nulla. Più in generale, $\frac{m}{n} + \left(-\frac{m}{n}\right) = \frac{0}{1}$. Allora, la funzione opposto coincide con la funzione $-\frac{1}{1}$, opposta dell'identità.

L'equivalenza di frazioni non cambia, perché è l'uguaglianza delle funzioni corrispondenti. L'insieme di queste funzioni si denota con **Q**. La *regola dei segni* nella moltiplicazione è semplicemente frutto della definizione, in quanto, per ogni $\vec{AB}$:

$$-(-\vec{AB}) = -\vec{BA} = \vec{AB}.$$

La moltiplicazione non crea perciò difficoltà, o almeno non dovrebbe ....

L'addizione è invece complicata da una notevole casistica, come noto anche agli allievi in terza media.

Non sono sicuro che questa impostazione auspicabile. Infatti, vedo varie difficoltà:

- I razionali costruiti come funzioni sui vettori del piano o dello spazio comunque presuppongono la conoscenza del piano o dello spazio euclidei, ossia, in definitiva, dei numeri reali.
- Il cambiare l'insieme delle grandezze su cui lavorare (i segmenti orientati del piano sotto l'azione delle traslazioni, gli analoghi oggetti dello spazio ...) porta a costruire funzioni diverse e quindi un campo razionale "diverso": l'isomorfismo è allora da dimostrare.
- Le costruzioni e le dimostrazioni sono ugualmente complicate rispetto ad altre impostazioni. Se alcune parti si possono considerare concettualmente più semplici, ciò avviene a spese dei prerequisiti, che sono più onerosi.

Proprietà del campo razionale. Il percorso universitario, come ricordato, prevede la costruzione di **Q** come campo dei quozienti dell'anello degli interi. Si ha infatti:

TEOREMA 3.4.1. Dato un dominio d'integrità $(A, +, \cdot, 1_A)$, esiste un campo $Q(A)$ contenente un sottoanello A' isomorfo ad A e tale che ogni elemento di $Q(A)$ è del tipo $a \cdot b^{-1},\ a, b \in A'$. Tale campo è poi l'unico, a meno d'isomorfismi, con questa proprietà.

Dimostrazione. Partiamo dall'insieme F delle coppie ordinate (a,b) di elementi di A, con $b \neq 0_A$: chiameremo *frazioni* queste coppie e le indicheremo con $\frac{a}{b}$. Definiamo tra le frazioni le due operazioni seguenti: $\frac{a}{b}+\frac{c}{d}=\frac{a\cdot d+b\cdot c}{b\cdot d}$, $\frac{a}{b}\cdot\frac{c}{d}=\frac{a\cdot c}{b\cdot d}$.

La definizione è corretta perché $bd \neq 0_A$ in quanto A è un dominio d'integrità. È un esercizio provare che l'insieme F delle frazioni è un monoide commutativo rispetto ad entrambe queste operazioni. Vediamo solo la proprietà associativa dell'addizione:

$$\left(\frac{a}{b}+\frac{c}{d}\right)+\frac{e}{f}=\frac{a\cdot d+b\cdot c}{b\cdot d}+\frac{e}{f}=\frac{\left(a\cdot d+b\cdot c\right)\cdot f+\left(b\cdot d\right)\cdot e}{\left(b\cdot d\right)\cdot f}=\frac{a\cdot d\cdot f+b\cdot c\cdot f+b\cdot d\cdot e}{b\cdot d\cdot f}$$

$$\frac{a}{b}+\left(\frac{c}{d}+\frac{e}{f}\right)=\frac{a}{b}+\frac{c\cdot f+d\cdot e}{d\cdot f}=\frac{a\cdot\left(d\cdot f\right)+b\cdot\left(c\cdot f+d\cdot e\right)}{\left(b\cdot d\right)\cdot f}=\frac{a\cdot d\cdot f+b\cdot c\cdot f+b\cdot d\cdot e}{b\cdot d\cdot f}$$

Gli elementi neutri sono rispettivamente $\frac{0_A}{1_A}$ e $\frac{1_A}{1_A}$.

Definiamo ora in questo insieme di frazioni la seguente relazione ~:

$$\frac{a}{b}\sim\frac{a'}{b'}\Leftrightarrow a\cdot b'=b\cdot a'.$$

Si verifica facilmente che questa relazione è di equivalenza. Vediamo solo la proprietà transitiva: siano $\frac{a}{b}\sim\frac{a'}{b'}$, $\frac{a'}{b'}\sim\frac{a''}{b''}$. Allora: $\frac{a}{b}\sim\frac{a'}{b'}\Leftrightarrow a\cdot b'=b\cdot a'$, $\frac{a'}{b'}\sim\frac{a''}{b''}\Leftrightarrow a'\cdot b''=b'\cdot a''$. Ne segue: $\begin{cases}a\cdot b'=b\cdot a'\\ a'\cdot b''=b'\cdot a''\end{cases}\Rightarrow a\cdot b'\cdot a'\cdot b''=b\cdot a'\cdot b'\cdot a''$, da cui semplificando per b', che è $\neq 0_A$ segue: $a\cdot a'\cdot b''=b\cdot a'\cdot a''$. Ora, se $a' \neq 0_A$ segue $a\cdot b''=b\cdot a''\Rightarrow\frac{a}{b}\sim\frac{a''}{b''}$; se $a' = 0_A$ segue $a = a'' = 0_A$ e di nuovo $\frac{a}{b}\sim\frac{a''}{b''}$.

Di più, questa relazione è compatibile con le due operazioni. Siano infatti $\frac{a}{b}\sim\frac{a'}{b'}$, $\frac{c}{d}\sim\frac{c'}{d'}$. Allora, per la moltiplicazione si ha subito:

$$\begin{cases}a\cdot b'=b\cdot a'\\ c\cdot d'=d\cdot c'\end{cases}\Rightarrow a\cdot b'\cdot c\cdot d'=b\cdot a'\cdot d\cdot c'\Rightarrow\frac{a\cdot c}{b\cdot d}\sim\frac{a'\cdot c'}{b'\cdot d'}$$

Per l'addizione è più complicato:

$$\left(a\cdot d+b\cdot c\right)\cdot\left(b'\cdot d'\right)=a\cdot d\cdot b'\cdot d'+b\cdot c\cdot b'\cdot d'=\left(a\cdot b'\right)\cdot d\cdot d'+\left(c\cdot d'\right)\cdot b\cdot b'=$$

$$=\left(b\cdot a'\right)\cdot d\cdot d'+\left(d\cdot c'\right)\cdot b\cdot b'=\left(a'\cdot d'+c'\cdot b'\right)\cdot\left(b\cdot d\right),$$

quindi $\frac{a}{b}+\frac{c}{d}=\frac{a\cdot d+b\cdot c}{b\cdot d}\sim\frac{a'\cdot d'+b'\cdot c'}{b'\cdot d'}=\frac{a'}{b'}+\frac{c'}{d'}$.

Si ha $\left[\frac{0_A}{1_A}\right]=\left\{\frac{0_A}{b}\;\middle|\; b\neq 0_A\right\}$ e $\left[\frac{1_A}{1_A}\right]=\left\{\frac{b}{b}\;\middle|\; b\neq 0_A\right\}$, come si vede subito.

Consideriamo quindi la struttura quoziente F/~ : essa è un monoide rispetto ad entrambe le operazioni, con elementi neutri rispettivamente $\left[\frac{0_A}{1_A}\right]$ e $\left[\frac{1_A}{1_A}\right]$, ma, di più ogni suo elemento $\left[\frac{a}{b}\right]$ ha l'opposto $\left[\frac{-a}{b}\right]$ e, se a $\neq 0_A$, ha anche l'inverso moltiplicativo, $\left[\frac{b}{a}\right]$. Infine, la moltiplicazione quoziente è distributiva rispetto all'addizione quoziente; infatti si ha

$$\left(\frac{a}{b}+\frac{c}{d}\right)\cdot\frac{e}{f}=\frac{a\cdot d+b\cdot c}{b\cdot d}\cdot\frac{e}{f}=\frac{a\cdot d\cdot e+b\cdot c\cdot e}{b\cdot d\cdot f},\quad \frac{a}{b}\cdot\frac{e}{f}+\frac{c}{d}\cdot\frac{e}{f}=\frac{a\cdot e\cdot d\cdot f+c\cdot e\cdot b\cdot f}{b\cdot f\cdot d\cdot f},$$

e le due frazioni ottenute sono equivalenti, dato che

$$\left(a\cdot d\cdot e+b\cdot c\cdot e\right)\cdot\left(b\cdot f\cdot d\cdot f\right)=\left(a\cdot e\cdot d\cdot f+c\cdot e\cdot b\cdot f\right)\cdot\left(b\cdot d\cdot f\right),$$

come si vede eseguendo le due moltiplicazioni.

Allora, la struttura quoziente è un campo, che si denota con Q(A). Il sottoinsieme $\left\{\left[\frac{a}{1_A}\right]\,\middle|\, a\in A\right\}$ costituisce un sottoanello di Q(A), come si verifica facilmente, e la funzione Φ:A→Q(A), definita da $\Phi(a)=\left[\frac{a}{1_A}\right]$, è un monomorfismo di anelli. Inoltre, per ogni $\left[\frac{a}{b}\right]\in Q(A)$ si ha $\left[\frac{a}{b}\right]=\left[\frac{a}{1_A}\right]\cdot\left[\frac{1_A}{b}\right]=\left[\frac{a}{1_A}\right]\cdot\left[\frac{b}{1_A}\right]^{-1}$. Per questa ragione Q(A) è detto *campo dei quozienti di A*.

Si può anche dimostrare che per ogni campo K che contenga un sottoanello A' isomorfo ad A, l'intersezione di tutti i sottocampi contenenti A' è un sottocampo costituito dai quozienti degli elementi di A', ed è isomorfo a Q(A), quindi Q(A) è in questo senso il campo "generato" da A. Perciò è unico.

NOTA. Se l'anello A è *fattoriale*, ossia se ha senso parlare di MCD ed mcm, gli elementi di Q(A) di norma si rappresentano mediante frazioni $\frac{a}{b}$ *ridotte ai minimi termini*, ossia tali che $MCD(a,b)=1_A$.

In un anello $(A,+,\cdot,1_A)$ il periodo di 1_A nel gruppo additivo (A, +) si chiama *caratteristica* di A. Per esempio **Z** ha caratteristica infinita (e però si usa dire che ha caratteristica *zero*), mentre $\mathbf{Z}_m$ ha caratteristica m. Nel caso dei dominii d'integrità e dei campi la caratteristica o è zero o è un numero primo. Per il campo **Q** la caratteristica è 0, dato che contiene **Z**. Si ha:

TEOREMA 3.4.2. Ogni campo K di caratteristica 0 contiene un sottocampo isomorfo al campo razionale.

Dimostrazione. Ogni sottocampo di K contiene 1_K, quindi anche l'intersezione K_0 di tutti i sottocampi lo contiene. Poiché la caratteristica è 0, il sottogruppo ciclico additivo $\langle 1_k\rangle$ generato da 1_K, costituito dai suoi

multipli interi, è isomorfo al gruppo additivo di Z. Ma $\langle 1_k \rangle$ è chiuso anche rispetto al prodotto, dato che, per la proprietà distributiva della moltiplicazione rispetto all'addizione, per ogni m,n∈Z risulta: $(m1_A)\cdot(n1_A) = (mn)1_A$, quindi è un sottoanello ed è isomorfo all'anello Z. Allora l'insieme K_0 dei quozienti $\frac{m1_A}{n1_A}$, (n ≠ 0), è un sottocampo di K ed è incluso in ogni altro sottocampo di K. Si verifica infine che facendo corrispondere al numero razionale $\frac{m}{n}$ l'elemento $\frac{m1_A}{n1_A}$ di K_0 si ottiene una funzione ben definita (frazioni equivalenti hanno lo stesso corrispondente) ed è un monomorfismo di anelli, la cui immagine K_0 risulta isomorfa al dominio, che è **Q.**

Sia (K, +, ·) un campo. Denotiamo con 0 ed 1 i suoi elementi neutri. Sia poi data in K una relazione d'ordine totale ≤ tale che, per ogni a, b, c∈K si abbia:

a) $a \le b \Rightarrow a+c \le b+c$

b) $\begin{cases} ac \le bc & \text{se } c > 0 \\ ac \ge bc & \text{se } c < 0 \end{cases}$.

La quaterna (K, +, ·, ≤) si dice *campo ordinato.* E' facile provare che per il campo ordinato (K, +, ·, ≤) si ha:

i) $-1 < 0 < 1$

ii) K ha caratteristica 0, quindi contiene il campo razionale.

iii) Posto $K^+ = \{x \in K \mid x > 0\}$, allora K^+ è chiuso rispetto a somma e prodotto e, per ogni $x \neq 0$, fra x e -x uno ed uno solo appartiene a K^+.

Inversamente, se K ha un sottoinsieme K^+ chiuso rispetto a somma e prodotto e, per ogni $x \neq 0$, fra x e -x uno ed uno solo appartiene a K^+, (insieme dei *positivi*) allora si può ordinare in modo totale ponendo: $x < y$ se $y - x \in K^+$. Valgono allora le proprietà a), b) di compatibilità con le operazioni.

Il campo ordinato (K, +, ·, ≤) si dice *archimedeo* se per ogni $x, y \in K^+$, $x < y$, esiste un multiplo intero kx di k che sia maggiore di y.

Sia ora $\emptyset \neq A \subseteq K$. Un elemento b∈K si dice *maggiorante* di A se per ogni a∈A si ha $a \le b$. Il minimo dei maggioranti, se esiste, è detto *estremo superiore* di A e denotato con sup(A). Il campo ordinato (K, +, ·, ≤) si dice *completo* se per ogni sottoinsieme non vuoto A che possieda maggioranti esiste in K il sup(A).

Nel campo **Q** si osserva che per ogni numero razionale $\frac{m}{n}$, se $m \cdot n > 0$ allora ogni frazione equivalente ad $\frac{m}{n}$ ha la stessa proprietà. Ne segue che l'insieme di queste frazioni definisce un sottoinsieme, $\mathbf{Q}^+$, che risulta avere le caratteristiche per essere l'insieme dei positivi. Ne segue che il campo razionale si può ordinare totalmente. La struttura $\left(\mathbf{Q}, +, \cdot, \leq\right)$ è dunque un campo ordinato. È poi archimedeo, perché dati due numeri positivi $x = \frac{h}{k}$, $y = \frac{m}{n}$, con $x < y$, si ha:

$$x \cdot \left(k \cdot m\right) = h \cdot m > \frac{h \cdot m}{n} > \frac{m}{n} = y .$$

Però non è completo. Infatti il sottoinsieme $\{x \in \mathbf{Q}^+ \mid x^2 < 2\}$ non ha in **Q** l'estremo superiore.

NOTA. Come detto, in ogni campo ordinato K il sottocampo minimo sottocampo K_0 è isomorfo a **Q**. L'isomorfismo che fa corrispondere al numero razionale $\frac{m}{n}$ l'elemento $\frac{m1_A}{n1_A}$ di K_0 è compatibile anche con l'ordinamento, nel senso che se $\frac{m}{n} \leq \frac{p}{q}$ in **Q** allora $\frac{m1_A}{n1_A} \leq \frac{p1_A}{q1_A}$ in K, e viceversa.

Per chi vuole approfondire facoltativamente i numeri razionali, esaminiamo ora separatamente i due gruppi additivo e moltiplicativo di **Q**.

3.4.3 **Il gruppo additivo** (**Q**, +).

1) È abeliano, ma non ciclico. Infatti, dato un suo qualunque elemento $\frac{m}{n}$, $MCD(m,n) = 1$, i primi che dividono il denominatore sono in numero finito, quindi esiste un primo p non divisore di n. Ne segue che per ogni k∈Z, non può essere $k \cdot \frac{m}{n} = \frac{1}{p}$, quindi il sottogruppo ciclico $\left\langle \frac{m}{n} \right\rangle$ non coincide con **Q**.

2) Lo stesso argomento dimostra che (**Q**, +) non si è generato da un $S \subseteq \mathbf{Q}$ finito: l'insieme Π dei primi che dividono almeno uno dei denominatori degli elementi di S è finito, quindi esiste un primo $p \notin \Pi$. Come sopra, $\frac{1}{p}$ non è combinazione lineare a coefficienti interi degli elementi di S, quindi S non genera **Q**.

3) Una proprietà curiosa di (**Q**, +) è la *ciclicità locale*: ogni sottogruppo H generato da un insieme finito S di elementi è ciclico. Basterà verificarlo per due generatori, poi procedere per induzione. Siano $\frac{h}{k}, \frac{r}{s}$ i due generatori di H e sia $n = mcm\left(k, s\right)$. Allora posto $n = k \cdot p = s \cdot q$, si ha $\frac{h}{k} = \frac{ph}{n} = ph \cdot \frac{1}{n}$, e

analogamente $\frac{r}{s} = \frac{qr}{n} = qr \cdot \frac{1}{n}$. Ossia, $H = \left\langle \left\{ \frac{h}{k}, \frac{r}{s} \right\} \right\rangle \leq \left\langle \frac{1}{n} \right\rangle$, che è ciclico e quindi anche il suo sottogruppo H lo è.

4) Il solo elemento di (**Q**, +) ad avere periodo finito è lo zero; tutti gli altri hanno periodo infinito.

5) Una proprietà notevole di (**Q**, +) è la *divisibilità*: per ogni $\frac{m}{n} \in \mathbf{Q}$, per ogni $k \in \mathbf{N}^+$ esiste x∈**Q**, tale che $k \cdot x = \frac{m}{n}$. Ovviamente, è $x = \frac{m}{k \cdot n}$. Non è una proprietà comune: infatti, oltre a (**Q**, +) è posseduta solo dai gruppi moltiplicativi $\mathbf{C}_{p^\infty} = \left\{ z \in \mathbf{C} \;\middle|\; \exists h \in \mathbf{N},\ z^{p^h} = 1 \right\}$, dove **C** denota il campo complesso e p un primo qualsiasi, e dai prodotti diretti di copie di **Q** per copie di questi gruppi. In particolare, lo stesso gruppo additivo reale (**R**, +), che è a sua volta divisibile, è prodotto diretto di *c* copie di **Q**, dove c denota la potenza del continuo.

6) Il gruppo (Q, +) possiede sottogruppi notevoli. Uno di essi è naturalmente (Z, +). Sia ora p un numero primo. Denotiamo con $\mathbf{Q}_p$ l'insieme degli elementi che, ridotti ai minimi termini, hanno al denominatore una potenza di p. È un sottogruppo, contiene 1 e quindi contiene Z. Nel gruppo quoziente Q/Z, i quozienti $\mathbf{Q}_p$/Z hanno proprietà notevoli: ogni elemento ha periodo potenza di p, non solo, ma gli elementi di periodo divisore di p^n sono tutti e soli quelli del tipo $\frac{m}{p^n} + \mathbf{Z}$, $0 \leq m < p^n$, e formano un sottogruppo ciclico, generato da $\frac{1}{p^n} + \mathbf{Z}$. Tale sottogruppo contiene tutti i sottogruppi $\left\langle \frac{1}{p^k} + \mathbf{Z} \right\rangle$, k < n, ed è incluso in tutti quelli con k > n. Non ci sono altri sottogruppi oltre a questi, perciò i sottogruppi formano una catena ascendente: $\langle 0 \rangle = \left\langle \frac{1}{p^0} + \mathbf{Z} \right\rangle < \left\langle \frac{1}{p} + \mathbf{Z} \right\rangle < \left\langle \frac{1}{p^2} + \mathbf{Z} \right\rangle < \left\langle \frac{1}{p^3} + \mathbf{Z} \right\rangle < \cdots$ Si tratta in definitiva di un gruppo isomorfo al già citato $\mathbf{C}_{p^\infty} = \left\{ z \in \mathbf{C} \;\middle|\; \exists h \in \mathbf{N},\ z^{p^h} = 1 \right\}$.

7) Tornando a (**Q**, +) ed ai sottogruppi $\mathbf{Q}_p$, chiamiamo *fratti semplici* gli elementi di questi sottogruppi. Ne segue che ogni numero razionale è somma di un numero finito di fratti semplici. Sia infatti dato x∈**Q**. Se x è intero, non c'è nulla da provare. Sia $x = \frac{m}{p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}}$, r ≥ 1, ridotta ai minimi termini. Se r = 1, non c'è nulla da provare. Per induzione, sia r > 1, allora cerchiamo u, v∈**Z**, tali che:

$$x = \frac{m}{p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}} = \frac{u}{p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_{r-1}^{\alpha_{r-1}}} + \frac{v}{p_r^{\alpha_r}} = \frac{u \cdot p_r^{\alpha_r} + v \cdot p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_{r-1}^{\alpha_{r-1}}}{p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}}$$

In definitiva, abbiamo *l'equazione diofantea lineare*:

$$u\cdot\left(p_r^{\alpha_r}\right)+v\cdot\left(p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdots p_{r-1}^{\alpha_{r-1}}\right)=m$$

nelle incognite u, v, i cui coefficienti sono coprimi. Una tale equazione ha sempre infinite soluzioni. Scelta una di esse, $(\bar{u},v_r)$, per l'ipotesi induttiva esistono $v_1,\ldots,v_{r-1}$ tali che

$$x=\frac{\bar{u}}{p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdots p_{r-1}^{\alpha_{r-1}}}+\frac{v_r}{p_r^{\alpha_r}}=\frac{v_1}{p_1^{\alpha_1}}+\frac{v_2}{p_2^{\alpha_2}}+\ldots+\frac{v_{r-1}}{p_{r-1}^{\alpha_{r-1}}}+\frac{v_r}{p_r^{\alpha_r}},$$

come si voleva. La scomposizione non è unica, naturalmente. Per esempio,

$$\frac{5}{12}=\frac{5}{2^2\cdot 3}=\frac{3}{2^2}+\frac{-1}{3}=\frac{-1}{2^2}+\frac{2}{3}.$$

La differenza tra due scomposizioni di x è una r-upla di interi. Ne segue che nel quoziente **Q/Z** la scomposizione è unica, ossia **Q/Z** è *somma diretta* dei suoi sottogruppi $\mathbf{Q}_p/\mathbf{Z}$.

8) Come in ogni campo, per ogni a∈**Q**, la funzione $f_a:x\mapsto a\cdot x$, è un *endomorfismo* del gruppo additivo, dato che

$$\forall x,y\in\mathbf{Q},\ f_a(x+y)=a\cdot(x+y)=a\cdot x+a\cdot y=f_a(x)+f_a(y).$$

Se a ≠ 0, f_a è un *automorfismo,* avendo come inversa $f_{1/a}$. Dunque, $\mathrm{Aut}(\mathbf{Q},+)$ contiene un sottogruppo isomorfo a $(\mathbf{Q}^*,\cdot)$. Ci sono altri automorfismi? Vediamo: sia f un automorfismo, allora poniamo $a=f(1)$.

Ne segue subito

$$f(2)=f(1+1)=f(1)+f(1)=2\cdot f(1)=2a=a\cdot 2.$$

Più in generale, per ogni intero n si ha f(n) = a·n. Inoltre,

$$a=f(1)=f\left(n\cdot\frac{1}{n}\right)=f\left(\underbrace{\frac{1}{n}+\ldots+\frac{1}{n}}_{n}\right)=\underbrace{f\left(\frac{1}{n}\right)+\ldots f\left(\frac{1}{n}\right)}_{n}=n\cdot f\left(\frac{1}{n}\right)\Rightarrow f\left(\frac{1}{n}\right)=a\cdot\frac{1}{n}$$

Ne segue $f\left(\frac{m}{n}\right)=m\cdot f\left(\frac{1}{n}\right)=m\cdot\frac{1}{n}\cdot a=a\cdot\frac{m}{n}$ e, in definitiva, $f=f_a$. Ossia, $\mathrm{Aut}(\mathbf{Q},+)\cong(\mathbf{Q}^*,\cdot)$.

3.4.4. Il gruppo moltiplicativo $(\mathbf{Q}^*,\cdot)$.

1) Il gruppo moltiplicativo $(\mathbf{Q}^*,\cdot)$ è scomponibile nel *prodotto diretto* dei due sottogruppi $\{1,-1\}$ e $\mathbf{Q}^+$. Questo perché, come si insegna alle scuole medie, ogni numero razionale non nullo è costituito da un segno e da un valore assoluto, che lo individuano perfettamente. Le due funzioni *segno* e *valore assoluto* sono definite da:

$$\mathrm{sign}(x)=\begin{cases}+1 & \text{se } x>0\\ -1 & \text{se } x<0\end{cases},\quad |x|=\mathrm{abs}(x)=\begin{cases}x & \text{se } x>0\\ -x & \text{se } x<0\end{cases}$$

e sono entrambe *endomorfismi* del gruppo $\left(\mathbf{Q}^*,\cdot\right)$, in quanto:

$$\forall x, y \in \mathbf{Q}^*, \begin{cases} \operatorname{sign}\left(x \cdot y\right) = \operatorname{sign}\left(x\right) \cdot \operatorname{sign}\left(y\right) \\ \left|x \cdot y\right| = \left|x\right| \cdot \left|y\right| \end{cases}$$

Il nucleo di ciascuna è l'immagine dell'altra e si ha $\forall x \in \mathbf{Q}^*,\ x = \operatorname{sign}\left(x\right) \cdot \left|x\right|$.

2) Gli elementi di $\left(\mathbf{Q}^*,\cdot\right)$ aventi periodo finito sono solo 1 e -1. La struttura di $\left(\mathbf{Q}^*,\cdot\right)$ è nota se è noto il sottogruppo $\mathbf{Q}^+$. Quest'ultimo non è divisibile: tradotto in notazione moltiplicativa, non è vero che per ogni $\frac{m}{n} \in \mathbf{Q}^+$, per ogni $k \in \mathbf{N}^+$ esista $x \in \mathbf{Q}^+$, tale che $x^k = \frac{m}{n}$. Basta considerare $k = \frac{m}{n} = 2$, perché, come ben noto, l'equazione $x^2 = 2$ è impossibile in $\mathbf{Q}^+$. In particolare, quindi, $\left(\mathbf{Q}^+,\cdot\right)$ non è isomorfo a $\left(\mathbf{Q},+\right)$, come invece avviene per il campo reale.

3) Ora esaminiamo proprio $\left(\mathbf{Q}^+,\cdot\right)$. Innanzi tutto, non è finitamente generato, e la dimostrazione è come quella per $\left(\mathbf{Q},+\right)$. In particolare, non è ciclico.

4) $\left(\mathbf{Q}^+,\cdot\right)$ non è neppure localmente ciclico: infatti, il sottogruppo generato per esempio da 2 e da 3 contiene tutte e sole le frazioni del tipo $2^m \cdot 3^n$, con m, n∈**Z**, e poiché si ha $\left(2^m \cdot 3^n\right) \cdot \left(2^p \cdot 3^q\right) = 2^{m+p} \cdot 3^{n+q}$, è isomorfo al prodotto diretto del gruppo additivo **Z** con se stesso, che non è ciclico. Questo esempio, però, suggerisce qualche idea.

5) Consideriamo i sottogruppi ciclici di $\left(\mathbf{Q}^+,\cdot\right)$ generati dai primi: si ha: $\left\langle p \right\rangle = \left\{p^\alpha \mid \alpha \in \mathbf{Z}\right\}$.

Ciò posto, sia $x = \frac{{p_1}^{\alpha_1} \cdot {p_2}^{\alpha_2} \cdots {p_r}^{\alpha_r}}{{q_1}^{\beta_1} \cdot {q_2}^{\beta_2} \cdots {q_s}^{\beta_s}}$, ridotta ai minimi termini. Allora $x = {p_1}^{\alpha_1} \cdot {p_2}^{\alpha_2} \cdots {p_r}^{\alpha_r} \cdot {q_1}^{-\beta_1} \cdot {q_2}^{-\beta_2} \cdots {q_s}^{-\beta_s}$, quindi $x \in \left\langle p_1 \right\rangle \cdots \left\langle p_r \right\rangle \left\langle q_1 \right\rangle \cdots \left\langle q_s \right\rangle$, e la fattorizzazione è unica. Pertanto, $\left(\mathbf{Q}^+,\cdot\right)$ è la somma diretta dei sottogruppi generati dai primi, quindi è isomorfo alla somma diretta di $\aleph_0$ copie del gruppo ciclico $\left(\mathbf{Z},+\right)$.

Nota. Anche il gruppo $\left(\mathbf{Z}[x],+\right)$ dei polinomi a coefficienti interi in una indeterminata è isomorfo alla somma diretta di $\aleph_0$ copie del gruppo ciclico $\left(\mathbf{Z},+\right)$. Un isomorfismo esplicito è costruibile dalla tabella seguente: $\begin{array}{c|ccccccc} p & 2 & 3 & 5 & 7 & 11 & \dots \\ \hline x^k & x^0 & x^1 & x^2 & x^3 & x^4 & \dots \end{array}$. Allora al polinomio $3-5x^3+6x^4$ corrisponde il numero razionale positivo $2^3\cdot 7^{-5}\cdot 11^6 = \dfrac{2^3\cdot 11^6}{7^5}$. Inversamente, al numero razionale $\dfrac{21}{20} = 2^{-2}\cdot 3^1\cdot 5^{-1}\cdot 7^1$ corrisponde il polinomio $-2+x-x^2+x^3$. Pertanto, i gruppi $\left(\mathbf{Q}^+,\cdot\right)$ e $\left(\mathbf{Z}[x],+\right)$ sono isomorfi. In definitiva, poiché $\left(\{1,-1\},\cdot\right)$ è isomorfo al gruppo $\left(\mathbf{Z}_2,+\right)$ e $\left(\mathbf{Q}^+,\cdot\right)$ è isomorfo a $\left(\mathbf{Z}[x],+\right)$ e si ha $\mathbf{Q}^* \cong \mathbf{Q}^+ \times \{1,-1\}$, allora $\mathbf{Q}^* \cong \mathbf{Z}[x]\times \mathbf{Z}_2$.

6) Ogni permutazione sull'insieme dei primi si prolunga ad un automorfismo di $\left(\mathbf{Q}^+,\cdot\right)$. Pertanto si ha che $\mathrm{Aut}\left(\mathbf{Q}^+,\cdot\right)$ contiene il gruppo simmetrico su $\aleph_0$ oggetti. Inoltre, anche l'associare ad un elemento il suo inverso è un automorfismo. Lo studio di $\mathrm{Aut}\left(\mathbf{Q}^+,\cdot\right)$ appare dunque non elementare.

NOTA. Come forse già visto a suo tempo, il campo razionale ha solo l'automorfismo banale

3.5. DAI NUMERI RAZIONALI AI NUMERI REALI

Una delle ragioni che hanno portato a cercare estensioni dell'insieme **N** è la necessità di potere eseguire sempre la sottrazione e la divisione, ossia, equivalentemente, risolvere le equazioni $a + x = b$ e $a \cdot x = b$. Il problema è risolto dalla costruzione del campo razionale **Q**, se si eccettua la divisione per zero. Tuttavia, altri problemi, anche di origine geometrica, non hanno soluzioni razionali.

Il primo di essi deriva dalla applicazione del teorema di Pitagora ai triangoli notevoli, in particolare al mezzo quadrato e al mezzo triangolo equilatero. Nel primo caso, preso come unità di misura un cateto, l'ipotenusa ha come misura un numero il cui quadrato è 2; nel secondo, presa l'ipotenusa come unità di misura, un cateto misura ½, ma il doppio dell'altro è un numero che al quadrato dà 3. Denotata con x la lunghezza incognita, nel primo caso abbiamo la condizione $x^2 = 2$, nel secondo $x^2 = \frac{3}{4}$, o equivalentemente, moltiplicando ambo i membri per 4, $(2x)^2 = 3$.

Un altro esempio concerne la *sezione aurea* di un segmento scelto come unità di misura. Più precisamente, si cerca un rettangolo con la base uguale al nostro segmento e tale che, ritagliatovi un quadrato di lato uguale all'altezza, resti un rettangolo simile a quello di partenza. Detta x l'altezza, abbiamo la condizione: $1 : x = x : (1 - x)$, ossia $x^2 = 1 - x$. Con un poco di manipolazioni algebriche, ossia sommando $x + \frac{1}{4}$ ai due membri e poi moltiplicando per 4, possiamo scrivere $(2x + 1)^2 = 5$.

Ebbene, nessuno di questi problemi ha soluzioni razionali. Di qui la necessità di cercare estensioni del campo razionale.

LEMMA 3.5.1. Sia p un numero primo. Non esiste un numero razionale il cui quadrato sia p.

Dimostrazione. Ricordiamo la proprietà euclidea: un numero primo p, ogni volta che divide un prodotto, divide almeno uno dei fattori. Ricordiamo poi che i due numeri razionali non nulli x e –x hanno lo stesso quadrato, ed uno dei due è positivo. Ragioniamo allora con un numero razionale positivo $x = \frac{m}{n}$, con MCD(m,n) = 1. Supponiamo si abbia $x^2 = p$. Allora, $m^2 = p \cdot n^2$, quindi dato che p è primo e divide il prodotto $m \cdot m$, divide m. Ossia, esiste m' tale che $m = p \cdot m'$. Allora si ha l'uguaglianza $p^2 \cdot m'^2 = p \cdot n^2$, che per la legge di cancellazione implica $p \cdot m'^2 = n^2$. Ma allora p divide anche n^2, e di conseguenza p

divide anche n. Allora p è un divisore comune di m ed n, in contrasto con l'ipotesi MCD(m,n) = 1. Allora per ogni razionale non nullo x si ha $x^2 \neq p$.

I problemi da cui siamo partiti non hanno quindi soluzione razionale: infatti, 2, 3 e 5 sono primi e una soluzione razionale x al problema porterebbe a trovare un razionale di cui essi sarebbero il quadrato.

Problemi di questo tipo si chiamano equazioni di secondo grado a coefficienti razionali. Esse hanno la forma: $a \cdot x^2 + b \cdot x + c = 0$, con $a \neq 0$. Non è detto che abbiano soluzioni: per esempio:

- $x^2 - 4 = 0$ ha due soluzioni: 2 e -2.
- $x^2 - x = 0$ ha due soluzioni: 0 e 1
- $x^2 + 2x + 1 = 0$ ha la sola soluzione -1.
- $x^2 - 2 = 0$ non ha soluzione, perché 2 è primo.
- $x^2 + 4 = 0$ non ha soluzioni: infatti, dalle proprietà dell'ordinamento di **Q** segue, per ogni $x \in \mathbf{Q}$, $x^2 \geq 0$ per cui $4 + x^2 \geq 4 > 0$ per ogni $x \in \mathbf{Q}$.

Come vedere se le soluzioni ci sono? Osserviamo innanzitutto che l'equazione $a \cdot x^2 + b \cdot x + c = 0$ si può riscrivere così:

$$\left(x + \frac{b}{2a}\right)^2 - \frac{\Delta}{4a^2} = 0,$$

dove $\Delta = b^2 - 4ac$ è detto *discriminante*. Se Δ è un quadrato in **Q** ed $h \in \mathbf{Q}$ è tale che $h^2 = \Delta$, l'equazione ha per soluzioni $\frac{-b \pm h}{2a}$.

Pertanto, se potessimo risolvere l'equazione *binomia* $x^2 - k = 0$ per ogni $k \in \mathbf{Q}$, potremo risolvere tutte le equazioni di secondo grado in **Q**, ma questo non è possibile, come visto.

Generalizziamo ancora: una *equazione algebrica di grado n ≥ 1* è del tipo:

$$a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \ldots + a_1 \cdot x + a_0 = 0, \text{ con } a_n \neq 0.$$

I numeri razionali a_0, a_1, ... sono detti *coefficienti*; a_0 è detto *termine noto*, a_n è detto *coefficiente direttore*.

Possiamo moltiplicare i due membri per il mcm dei denominatori dei coefficienti, ottenendo così una equazione a coefficienti interi e con le stesse soluzioni. Possiamo infine raccogliere a fattor comune il MCD dei nuovi coefficienti, ed ottenere così una equazione a coefficienti interi coprimi e con le stesse soluzioni. Diciamo *primitiva* quest'ultima equazione.

A questo punto, un teorema insegnato anche a scuola come *regola di Ruffini* afferma che le eventuali radici razionali di questa equazione a coefficienti interi e col termine noto diverso da zero sono della forma p/q, dove p è un divisore (positivo o negativo) del termine noto, mentre q è un divisore (positivo) del coefficiente direttore.

Esempi 3.5.2 .

1) $3x^2 + 4x + 1 = 3(x + 1)(x + \frac{1}{3})$.

2) $x^4 + x^2 + 1$ non ha ovviamente radici, ma è uguale a $(x^2+x+1)(x^2-x+1)$.

3) $x - 2$ è irriducibile, pur avendo una radice.

4) L'equazione $5x^3 - 24x^2 + 1 = 0$ ha i coefficienti interi. Le eventuali radici razionali sono da ricercarsi nell'insieme $\left\{1,\ -1,\ \frac{1}{5},\ -\frac{1}{5}\right\}$. Si verifica così che $-\frac{1}{5}$ è l'unica radice razionale.

Un altro problema nasce dalla geometria, in particolare dalla misura, denotata usualmente con π, della lunghezza di una circonferenza di diametro unitario. Archimede la stimò in circa $3{,}14\ \left(= 3 + \frac{1}{10} + \frac{4}{100}\right)$ e trovò la semplicissima frazione $\frac{22}{7}$ per esprimerla. Tuttavia, questa non è la lunghezza esatta. Essa comincia con 3.14159, ma queste cifre decimali non bastano, e non bastano neppure le $2{,}7 \cdot 10^{12}$ cifre calcolate di recente in Francia. Si tratta infatti di un numero non razionale.

La via migliore per risolvere le equazioni algebriche passa attraverso l'Analisi Matematica e la Geometria. La costruzione del campo reale **R** avviene innanzitutto per esigenze geometriche: il rapporto fra la diagonale del quadrato ed il lato, o fra la circonferenza rettificata ed il diametro, non sono esprimibili mediante frazioni, cioè si tratta di grandezze *incommensurabili*. Di qui nasce, per opera di Eudosso di Cnido e poi di Archimede, la costruzione della teoria delle grandezze e quindi dei numeri reali assoluti (che si dovrebbe studiare all'inizio del II anno del liceo scientifico) e che abbiamo visto nel modulo di Elementi di Geometria. Aggiungendo i segni, si arriva poi al campo **R** dei numeri reali.

Il campo dei numeri reali si può definire anche per postulati. Abbiamo visto la nozione di campo ordinato e quella di completezza.

Si osservi che dati un campo ordinato K ed un sottoinsieme $A \neq \emptyset$ con estremo superiore, se $\sup(A) \notin A$, allora per ogni $\varepsilon \in K$, $\varepsilon > 0$ esiste un elemento di A maggiore di $\sup(A) - \varepsilon$, perché altrimenti anche $\sup(A) - \varepsilon$ sarebbe un maggiorante di A.

Una proprietà equivalente alla completezza è la seguente. Siano A e B due sottoinsiemi di K non vuoti; essi si dicono *separati* se per ogni $a \in A$ e $b \in B$ si ha $a \leq b$. Un elemento x_0 tale che $a \leq x_0 \leq b$ per ogni $a \in A$ e $b \in B$ è detto *elemento di separazione* fra A e B. Il campo ordinato $(K, +, \cdot, \leq)$ si dice *continuo* se ogni coppia di sottoinsiemi separati ha elementi di separazione in K. Si ha:

- completezza $\Rightarrow$ continuità: $x_0 = \sup(A)$
- continuità $\Rightarrow$ completezza: $\sup(A)$ = elemento di separazione fra A e qualunque insieme di suoi maggioranti.

In un campo ordinato e completo K vale la seguente proprietà (già vista per i monoidi nel modulo di Elementi di Geometria):

TEOREMA 3.5.3 (Legge di Archimede): per ogni $a, b \in K$ tali che $0 < a < b$, esiste $n \in \mathbf{N}$ tale che $na > b$.

Dimostrazione. Osserviamo dapprima che, identificato con **Q** il sottocampo minimo K_0 di K, si ha $\frac{1}{2} < 1$, quindi $0 < \frac{1}{2} \cdot a < 1 \cdot a = a$. Ciò posto, sia falso il teorema. Allora, l'insieme A dei multipli interi na di a possiede b come maggiorante, quindi, per la completezza di K, possiede l'estremo superiore sup(A). Se sup(A) è un multiplo na di a, allora $(n+1) \cdot a > n \cdot a$, assurdo. Perciò $\sup(A) \notin A$. Allora per ogni $\varepsilon > 0$ esiste un multiplo na di a tale che $\sup(A) - na < \varepsilon$. Preso quindi $\varepsilon = a/2 < a$, si ha $(n+1)a = na + a > na + \varepsilon \geq \sup(A)$, assurdo in ogni caso.
Dunque, b non è un maggiorante di A, quindi esiste un multiplo na di a, tale che $na > b$.

OSSERVAZIONE. Si ha anche che ogni elemento $x \in K$ è estremo superiore dell'insieme dei "razionali", ossia degli elementi di K_0, minori di x.

Un *isomorfismo* tra due campi ordinati H e K è una biiezione $f: H \to K$ tale che, per ogni $a, b \in H$, $\begin{cases} f(a+b) = f(a) + f(b) \\ f(a \cdot b) = f(a) \cdot f(b) \\ a \leq b \Leftrightarrow f(a) \leq f(b) \end{cases}$. In sostanza, due campi isomorfi sono sostanzialmente lo stesso campo scritto con simboli diversi. Si può allora dimostrare la seguente proposizione, di cui non si riporta la dimostrazione, ma che deriva dall'osservazione precedente.

TEOREMA 3.5.4. Tutti i campi ordinati completi sono isomorfi tra loro.

Chiamiamo *campo reale* **R** un campo ordinato e completo, che per il teorema precedente è unico a meno di isomorfismi. Questo tuttavia non prova la sua esistenza, ma occorre darne una costruzione. La più classica è quella di **Dedekind**, che chiama *numero reale* ogni *sezione* di **Q**, cioè ogni partizione {A, B} di sottoinsiemi non vuoti e separati di **Q** tali che A∪B = **Q**. Si identificano quelle partizioni con lo stesso elemento separatore, che può appartenere ad A o a B.

Chiamiamo positivo un numero reale {A, B} se 0∈A ma non ne è l'estremo superiore; negativo se 0∈B e non ne è l'estremo inferiore. Negli altri casi, 0 separa A e B e identifichiamo {A, B} con 0.

Le operazioni sono un poco artificiose, ma non troppo. Definiti in modo ovvio somma e prodotto di sottoinsiemi di **Q**, si pone per ogni {A, B}, {C, D}

Addizione: {A, B}+{C, D} = {A+C, B+D}

Moltiplicazione: se sono positivi, {A, B}·{C, D} = {E, F}, dove:

$$E = \mathbf{Q}^- \cup \{0\} \cup \left(\left(A \cap \mathbf{Q}^+\right)\cdot\left(C \cap \mathbf{Q}^+\right)\right),\ F = B\cdot D$$

Se uno di essi è nullo, il risultato si pone = 0.

Ci sono vari altri casi da esaminare, se uno o entrambi sono negativi.

Comunque, con questo metodo si arriva a dimostrare che ogni elemento ha l'opposto e, se non è nullo, ha l'inverso. Inoltre si ottiene l'ordine completo compatibile con le operazioni.

In questa costruzione i numeri *irrazionali* sono le sezioni {A, B} tali che sup(A) non esiste in **Q**, mentre i numeri razionali corrispondono alle altre sezioni.

Nella scuola superiore a volte si fa uso di questa costruzione, sia pure semplificata.

Una costruzione molto elegante, ma assai poco comprensibile, è quella di **Cantor**, rivisitata con nozioni di teoria degli anelli.

Si chiama *successione di Cauchy* ogni successione f in **Q** tale che

$$\forall\ \varepsilon\in\mathbf{Q},\ \varepsilon > 0,\ \exists\ n_\varepsilon\in\mathbf{N} \text{ tale che } |f(n) - f(m)| < \varepsilon\ \forall\ m, n > n_\varepsilon.$$

Si prova che le successioni di Cauchy, con le operazioni *punto per punto*, formano un anello commutativo S. Dato u∈**Q**, una successione di Cauchy f *converge ad u* se

$$\forall\ \varepsilon\in\mathbf{Q},\ \varepsilon > 0,\ \exists\ n_\varepsilon\in\mathbf{N} \text{ tale che } |f(n)-u| < \varepsilon\ \forall\ n > n_\varepsilon.$$

Le successioni convergenti a 0 formano un *ideale massimale* I di S. L'anello quoziente S/I è quindi un campo. Con una opportuna relazione d'ordine, tale campo risulta ordinato e completo e quindi i suoi elementi f+I sono i *numeri reali*. I numeri razionali corrispondono

ai laterali f+I, dove f converge ad un u∈**Q**, gli irrazionali sono i laterali di I determinati dalle successioni non convergenti.

Nella scuola media e nelle applicazioni si fa uso della costruzione mediante i numeri decimali e le loro operazioni.

Chiamiamo *numero decimale* ogni successione di cifre 0, 1, ... , 9, precedute da un segno, + o - e con intercalata una virgola. Un numero decimale x ha quindi la forma:

$$x = x_0,x_1x_2\ldots\ldots, \text{ dove } x_0\in\mathbf{Z} \text{ e } x_i\in\{0, 1, \ldots, 9\} \text{ per ogni } i > 0.$$

Il numero decimale x si chiama *periodico* se esistono r, p > 1 e una sequenza finita di p cifre $a_1a_2\ldots a_p$ tali che

$$x = x_0,x_1x_2\ldots\ldots x_ra_1a_2\ldots a_pa_1a_2\ldots a_pa_1a_2\ldots a_p\ldots\ldots$$

Se p è il minimo intero positivo per cui si ha questa ripetizione, si usa scrivere $x = x_0,x_1x_2\ldots\ldots x_r\,\overline{a_1a_2\ldots a_p}$. In tal caso, il numero naturale $a_1a_2\ldots a_p$ si chiama *periodo* p(x) di x. Il numero naturale $x_0\cdot 10^r+x_1x_2\ldots\ldots x_r$ si dice *antiperiodo* ap(x) di x.

Di solito il periodo 0 non si scrive ed il numero si dice *decimale finito.*

Ciò posto, diremo *equivalenti* due numeri decimali x ed y se sono periodici e tali che

$$p(x) = 0,\ p(y) = 9,\ ap(x) = ap(y)+1.$$

Per esempio, 32,75 = 32,750000000000..... = 32,7499999.....

Ogni altro numero decimale è posto equivalente solo a se stesso.

Chiamiamo ora *numero reale* ogni classe d'equivalenza di numeri decimali.

E' noto dalla scuola media che i numeri razionali corrispondono ai decimali periodici.

Ma come definire le operazioni fra numeri decimali?

Siano dati i due numeri razionali x = 1/3 ed y = 12/7. Ad essi possiamo associare i numeri decimali periodici

$$x' = 0{,}333333333333\ldots,\ y' = 1{,}714285714285714285\ldots$$

La loro somma è s = x+y = 43/21, corrispondente ad s' = 2,047619047619047619...

E' possibile ricavare s' da x' ed y' senza ricorrere alle frazioni generatrici?

Consideriamo le due successioni seguenti:

$a_0=0$	$a_1=0{,}3$	$a_2=0{,}33$	$a_3=0{,}333$	$a_4=0{,}3333$	$a_5=0{,}33333$ ...
$b_0=1$	$b_1=0{,}4$	$b_2=0{,}34$	$b_3=0{,}334$	$b_4=0{,}3334$	$b_5=0{,}33334$ ...

Esse sono formate da decimali finiti tali che per ogni indice n∈**N** si ha:

$$a_n \le x' \le b_n \text{ e } b_n-a_n = 10^{-n}$$

(l'ordinamento indicato con ≤ è quello lessicografico solito, corrispondente per altro a quello delle frazioni generatrici. Le operazioni fra decimali finiti si danno per note).

I numeri a_0, a_1, ... si dicono *approssimazioni per difetto* di x': a meno di 10^0 (una unità), 10^{-1} (un decimo), ecc. I numeri b_0, b_1, ... si dicono *approssimazioni per eccesso* di x' a meno di 10^0 (una unità), 10^{-1} (un decimo), ecc.

Ripetiamo ora per y':

$c_0=1$	$c_1=1,7$	$c_2=1,71$	$c_3=1,714$	$c_4=1,7142$	$c_5=1,71428$ ...
$d_0=2$	$d_1=1,8$	$d_2=1,72$	$d_3=1,715$	$d_4=1,7143$	$d_5=1,71429$ ...

Ricordiamo ora la seguente proprietà dei numeri razionali:

$$\text{se } a \le x \le b \text{ e } c \le y \le d \text{ allora } a+c \le x+y \le b+d$$

Pertanto, per ogni $n \in \mathbf{N}$ si ha $a_n+c_n \le s \le b_n+d_n$.

Posto $u_n=a_n+c_n$, $v_n=b_n+d_n$, si ha:

$u_0=1$	$u_1=\mathbf{2},0$	$u_2=\mathbf{2,0}4$	$u_3=\mathbf{2,04}7$	$u_4=\mathbf{2,047}5$	$u_5=\mathbf{2,0476}1$ ...
$v_0=3$	$v_1=\mathbf{2},2$	$v_2=\mathbf{2,0}6$	$v_3=\mathbf{2,04}9$	$v_4=\mathbf{2,047}7$	$v_5=\mathbf{2,0476}3$ ...

(in grassetto le cifre esatte di s', il quale, ricordiamo, è 2,047619...). In generale u_n e v_n hanno n-1 cifre esatte di s', cioè è incerta solo l'ultima. Si osservi però che nel caso di u_6 e v_6, essendo un 9 la cifra successiva esatta di s', non si ha per il momento la certezza che la cifra 1 sia esatta.

Si ha però $u_7 = \mathbf{2,0476190}$ e $v_7 = \mathbf{2,0476192}$.

Passiamo ora alla moltiplicazione. Sia $p = xy = 4/7$. Il numero decimale corrispondente è p' = 0,571428571428.... Cerchiamo di ricavarlo a partire da x' ed y', osservando che per i numeri razionali positivi si ha:

$$\text{se } 0 \le a \le x \le b \text{ e } 0 \le c \le y \le d \text{ allora } a\,c \le x\,y \le b\,d$$

Pertanto per ogni $n \in \mathbf{N}$ si ha $a_n\,c_n \le p \le b_n\,d_n$. Posto $f_n = a_n c_n$, $g_n = b_n d_n$, si ha (in grassetto le cifre esatte di p'):

$f_0=0$	$f_1=\mathbf{0},51$	$f_2=\mathbf{0,5}643$	$f_3=\mathbf{0,57}07...$	$f_4=\mathbf{0,5713}4...$	$f_5=\mathbf{0,5714}2...$
$g_0=2$	$g_1=\mathbf{0},72$	$g_2=\mathbf{0,5}848$	$g_3=\mathbf{0,57}28...$	$g_4=\mathbf{0,5715}4...$	$g_5=\mathbf{0,5714}4...$

Di qui si deduce una regola, simile a quella per l'addizione, per ricavare le cifre esatte di p' a partire da quelle di x' ed y'. Anche qui occorre la consueta cautela quando si hanno le cifre 9 e 0.

Regole simili, un bel po' più complicate, si possono dedurre anche per la sottrazione e la divisione di numeri decimali periodici positivi.

A questo punto è possibile usare queste regole per definire le operazioni anche fra numeri decimali non periodici. Per esempio siano:

x' = 1,71771177711177771111....

y' = 3,012345678910111213141516171819202122232 4... .

Cerchiamo di ricavarne la somma s'. Le successioni sono:

$a_0=1$	$a_1=1,7$	$a_2=1,71$	$a_3=1,717$	$a_4=1,7177$	$a_5=1,71771$	...
$b_0=2$	$b_1=1,8$	$b_2=1,72$	$b_3=1,718$	$b_4=1,7178$	$b_5=1,71772$	...

Pertanto:

$c_0=3$	$c_1=3,0$	$c_2=3,01$	$c_3=3,012$	$c_4=3,0123$	$c_5=3,01234$	...
$d_0=4$	$d_1=3,1$	$d_2=3,02$	$d_3=3,013$	$d_4=3,0124$	$d_5=3,01235$	...

Si ha così, mettendo in grassetto le cifre via via "sicure":

$u_0=4$	$u_1=\mathbf{4},7$	$u_2=\mathbf{4,7}2$	$u_3=\mathbf{4,7}29$	$u_4=\mathbf{4,730}0$	$u_5=\mathbf{4,7300}5$	...
$v_0=6$	$v_1=\mathbf{4},9$	$v_2=\mathbf{4,7}4$	$v_3=\mathbf{4,7}31$	$v_4=\mathbf{4,730}2$	$v_5=\mathbf{4,7300}7$	...

Dunque il numero cercato s' = x'+y' è 4,7300...

Si osservi che le due successioni per difetto ed eccesso che approssimano i numeri dati o i risultati sono successioni di Cauchy, e che la loro differenza tende a zero, ossia stanno nello stesso laterale dell'ideale delle successioni convergenti a zero.

Se uno almeno dei due numeri è negativo, per il prodotto si moltiplicano i valori assoluti e si aggiusta il segno con la regola consueta. Per l'addizione si procede come per i numeri interi relativi: a seconda dei segni si sommano o si sottraggono i valori assoluti e si aggiusta poi il segno.

Chiamando con **R** l'insieme dei numeri decimali (positivi e negativi), con le operazioni di addizione e moltiplicazione sopra accennate si ottiene un **campo**, il quale contiene il campo dei numeri decimali periodici, isomorfo al campo **Q** dei numeri razionali. Chiameremo **R** *campo dei numeri reali*.

In **R** l'ordinamento lessicografico, completato al solito modo per i numeri negativi, dà luogo ad un **ordinamento totale** che risulta essere anche **completo**, ossia ogni sottoinsieme non vuoto A di **R**, che ammetta maggioranti, possiede anche l'estremo superiore.

Proviamo a spiegarlo: A ammette anche dei maggioranti interi: sia b_0 il minimo intero che sia un maggiorante di A. Sia poi $a_0 = b_0-1$:

- tra i numeri a_0 $a_0+0,1$ $a_0+0,2$ $a_0+0,3$ ... $a_0+0,9$ $a_0+1 = b_0$, indichiamo con b_1 il più piccolo che sia maggiorante di A e poniamo $a_1 = b_1-0,1$;
- tra i numeri a_1 $a_1+0,01$ $a_1+0,02$ $a_1+0,03$ ... $a_1+0,09$ $a_1+0,1 = b_1$, indichiamo con b_2 il più piccolo che sia maggiorante di A e poniamo $a_2 = b_2-0,01$;
- tra i numeri a_2 $a_2+0,001$ $a_2+0,002$ $a_2+0,003$ .... $a_2+0,009$ $a_2+0,01 = b_2$, indichiamo con b_3 il più piccolo che sia maggiorante di A e poniamo $a_3 = b_3-0,001$;
- …

Così seguitando, otteniamo una coppia di successioni

$$a_0 \le a_1 \le a_2 \le \dots \le a_n \le \dots , \quad b_0 \ge b_1 \ge \dots \ge b_n \ge \dots$$

di numeri decimali finiti tali che per ogni $n \in \mathbf{N}$ si ha $a_n \le b_n$ ed inoltre $b_n - a_n = 10^{-n}$. Tale coppia di successioni individua un numero reale x_0 che si prova essere l'estremo superiore di A cercato.

Per esempio, sia $A = \{x \in \mathbf{R} \mid x > 0 \text{ e } x^2 < 2\}$. Si ha:

$a_0=1$ $a_1=1,4$ $a_2=1,41$ $a_3=1,414$ $a_4=1,4142$ $a_5=1,41421$ ...

$b_0=2$ $b_1=1,5$ $b_2=1,42$ $b_3=1,415$ $b_4=1,4143$ $b_5=1,41422$ ...

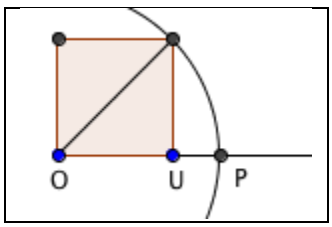
Infatti:

$a_0^2 = 1$	$a_1^2 = 1,96$	$a_2^2 = 1,9981$	$a_3^2 = 1,9993\dots$	$a_4^2 = 1,99996\dots$
$b_0^2 = 4$	$b_1^2 = 2,25$	$b_2^2 = 2,0164$	$b_3^2 = 2,0022\dots$	$b_4^2 = 2,00024\dots$

cosicché il numero x_0 è 1,4142...

Riassumendo, i numeri decimali sono un modello del campo reale. I numeri reali razionali, ossia i decimali periodici, formano a loro volta un campo ordinato isomorfo al campo razionale. Inoltre, **Q** è *denso* in **R**, nel senso che tra due numeri reali qualsiasi distinti c'è sempre un numero razionale, anzi, c'è un decimale finito.

L'approccio geometrico.(*) Partiamo dalla semiretta sulla quale, fissata l'unità di misura $\overline{OU}$, abbiamo "spalmato" prima i numeri naturali e poi i razionali "assoluti", identificando ogni numero razionale $r \ge 0$ col punto P tale che $\overline{OP} = r\overline{OU}$.



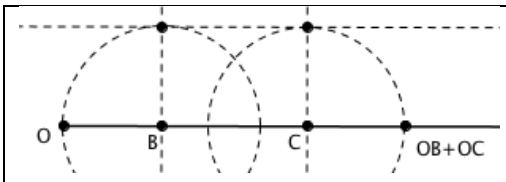
Sappiamo che non tutti i punti della semiretta sono associati ai numeri razionali: il segmento OP corrispondente alla diagonale del quadrato di lato OU non è commensurabile con OU. Però, P è l'estremo superiore dei segmenti OM < OP commensurabili con OU.

(*) Ci si può chiedere però se questo approccio geometrico sia ancora attuale e proponibile in una scuola superiore.

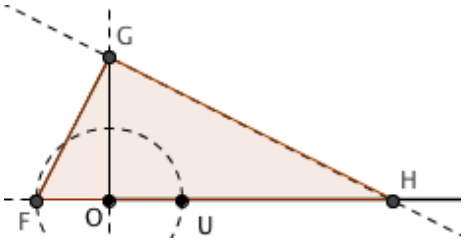
Allora, come visto nel modulo di Geometria, possiamo associare a P l'estremo superiore x dei numeri razionali r tali che rOU < OP.

Allora abbiamo il modo di "spalmare" i numeri reali ≥ 0 sulla semiretta, e si raggiungono tutti i punti.

C'è allora un modo di costruire la somma, il prodotto e l'inverso di un numero reale usando proprietà geometriche. Nel modulo di Geometria abbiamo visto come trasformare un rettangolo in un quadrato mediante il primo teorema di Euclide. Se ora fissiamo un segmento OU come unità di misura, col secondo teorema di Euclide possiamo trasformare il quadrato in un rettangolo di altezza unitaria.



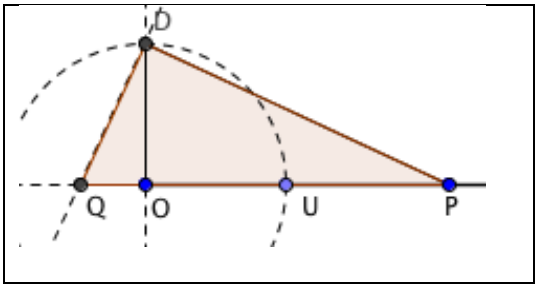
Somma di segmenti OB+OC con riga e compasso.



$OG^2 = OF \cdot OH =$
$= OU \cdot OH$

Dati quindi due segmenti OP ed OQ, si costruisce il lato OG del quadrato equivalente al rettangolo di lati OP ed OQ, e poi il segmento OH tale che $OH \cdot OU = OG^2 = OP \cdot OQ$ e quindi, passando alle misure rispetto ad OU, $\overline{OH} = \overline{OP} \cdot \overline{OQ}$.

Per il reciproco del numero reale positivo x, lunghezza del segmento OP rispetto ad OU,



basta prendere un segmento OD perpendicolare ad OP e tale che OD = OU, poi mandare da D la perpendicolare a PD e costruire il triangolo rettangolo PDQ. Allora, $OP \cdot OQ = OD^2 = OU^2$ $\Rightarrow \overline{OP} \cdot \overline{OQ} = 1$.

La simmetria rispetto al punto O trasferisce i punti P corrispondenti ai numeri reali positivi x nei punti P' dell'altra semiretta, cui attribuiamo valori *negativi* –x, come abbiamo visto per gli interi. La somma di numeri negativi o con segni opposti si costruisce geometricamente come simmetrica della somma o della differenza tra positivi. Per il prodotto, si usa la consueta regola dei segni.

Ma l'equazione $x^2 + 1 = 0$ non ha soluzione neppure in R, quindi non abbiamo ancora risolto tutti i problemi. Occorre quindi un passo ulteriore.

3.6. I NUMERI COMPLESSI

La formula risolutiva delle equazioni di terzo grado, trovata nel 1500 indipendentemente da Scipione Dal Ferro a Bologna e da Nicolò Fontana (Tartaglia) a Brescia, poi pubblicata da Gerolamo Cardano, nel caso di una equazione con tre soluzioni reali prevede l'estrazione della radice quadrata di un numero negativo. Ciò ha portato all'introduzione dei numeri complessi, studiati da Raffaele Bombelli e dapprima visti come un artificio di calcolo, poi resi "reali" dalla rappresentazione di Gauss e Argand come punti del piano o come vettori. Oggi i numeri complessi sono, nella matematica, l'ambiente naturale di lavoro della geometria algebrica, dell'analisi complessa, delle algebre di Lie, della rappresentazione dei gruppi finiti, ma anche, insospettabilmente, dei software di geometria dinamica, della grafica dei C.A.S. e, nell'ingegneria, dei controlli automatici dei processi di lavorazione e dell'elettrotecnica.

Costruzione formale. Un primo approccio è il seguente: aggiungiamo al campo reale una lettera, solitamente denotata con i, ma anche con j in certi indirizzi scolastici, e postuliamo che valgano le usuali proprietà delle operazioni del calcolo letterale, ma con l'aggiunta della condizione $i^2 = -1$. Allora avremo espressioni del tipo a+ib, con a e b reali. Poiché abbiamo postulato che valgano le usuali proprietà dell'addizione e della moltiplicazione, avremo:

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

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

$0 = 0+0i$

$1 = 1+0i$

$-(a+ib) = (-a)+i(-b)$

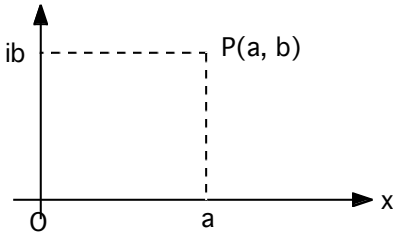
Inoltre, se a e b non sono entrambi nulli:

$$\frac{1}{a+ib} = \frac{a-ib}{(a+ib)(a-ib)} = \frac{a-ib}{a^2+b^2} = \frac{a}{a^2+b^2} + i\frac{-b}{a^2+b^2}$$

Pertanto, l'insieme di queste espressioni a+ib, con a, b reali, rispetto alle operazioni di addizione e moltiplicazione è un campo, che diremo "campo complesso" e denoteremo con **C**. Esso contiene il campo reale **R** come "sottocampo", costituito dai numeri complessi a+0i. I numeri del tipo 0+ib, con $b \neq 0$, sono detti numeri immaginari.

Ma, psicologicamente, esiste il campo complesso? Ha senso postulare l'esistenza di questa i tale che $i^2 = -1$ e che rispetta le consuete proprietà delle operazioni?

La costruzione geometrica. Consideriamo un sistema di assi cartesiani ortogonali. L'asse delle x, sul quale rappresenteremo i numeri reali, si chiama asse dei reali. L'asse delle ordinate lo chiameremo invece asse degli immaginari, perché su di esso rappresenteremo i numeri immaginari: ciascuno di questi ha come immagine il punto che ha per ordinata il coefficiente del numero immaginario.

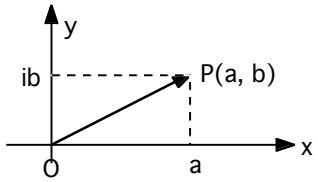


Si ha la biiezione tra **C** e il piano cartesiano:

$a+ib \leftrightarrow P(a, b)$

Il piano determinato da questi due particolari assi cartesiani si chiama piano di Gauss-Argand.

Se poi si considera ogni punto del piano di Gauss-Argand come estremo di un vettore avente come origine il punto origine O dei due assi cartesiani, si può parlare di corrispondenza biunivoca fra i vettori del piano e i numeri complessi.



Si ha la biiezione tra **C** e lo spazio vettoriale $\mathbf{R}^2$:

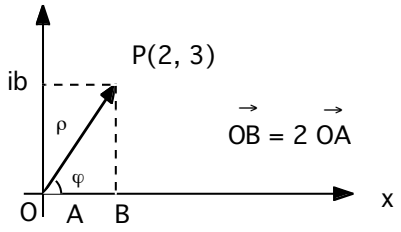
$a+ib \leftrightarrow P(a, b) \leftrightarrow \overrightarrow{OP}$

Si può ora rigirare il discorso: definire in $\mathbf{R}^2$ le operazioni nel modo seguente: $(a,b)+(c,d)=(a+c,b+d)$, $(a,b)\cdot(c,d)=(ac-bd,ad+bc)$. Si ottiene certamente un campo. Esso ha un sottocampo costituito dalle coppie (a, 0) e che possiamo identificare con **R**. Ossia, possiamo identificare a con (a, 0). Si ha poi $(0,1)^2=(-1,0)=-(1,0)=-1$. Posto allora i = (0, 1), si ha:

$$(a,b)=(a,0)+(0,b)=(a,0)+(0,1)\cdot(b,0)=a+ib$$

e quindi possiamo chiamare **C** questo campo, e ciò convince di più sulla sua esistenza.

Tuttavia, se l'addizione dei numeri complessi corrisponde alla somma dei vettori con la regola del parallelogramma, invece, il prodotto non ha un'interpretazione geometrica "naturale" e didatticamente appare artificiosa.



Sia $\vec{OA}$ il vettore unitario dell'asse dei reali. Consideriamo i numeri reali relativi come operatori che mutano il vettore unitario $\vec{OA}$ in un altro vettore avente la stessa direzione di $\vec{OA}$, lo stesso verso di $\vec{OA}$ o verso contrario a seconda che il numero considerato sia positivo o negativo, e la lunghezza uguale al prodotto della lunghezza di $\vec{OA}$ per il valore assoluto del numero.

Consideriamo l'unità immaginaria i come l'operatore che fa ruotare di 90°, nel verso positivo e intorno alla sua origine, il vettore al quale esso è applicato.

Consideriamo il numero complesso a+ib come l'operatore che fa ruotare il vettore $\vec{OA}$ di un angolo $\varphi = \arctan\frac{b}{a}$ e ne modifica la lunghezza moltiplicando quella di $\vec{OA}$ per $\rho = \sqrt{a^2 + b^2}$.

Si può allora osservare come questo prodotto corrisponda alla composizione di funzioni, applicata agli "operatori" a+ib.

Poiché il triangolo OBP è rettangolo in B, possiamo scrivere: $\begin{cases} a = \rho \cdot \cos(\varphi) \\ b = \rho \cdot \mathrm{sen}(\varphi) \end{cases}$, per cui:

$$a + i\,b = \rho\,(\cos\varphi + i\,\mathrm{sen}\,\varphi).$$

Questa è la forma trigonometrica dei numeri complessi: ρ si chiama *modulo* e φ si chiama *argomento* del numero complesso a+ib.

Mediante le formule di addizione di seno e coseno si ottiene:

$$\rho_1\left(\cos\varphi_1 + i\cdot\mathrm{sen}\varphi_1\right)\cdot\rho_2\left(\cos\varphi_2 + i\cdot\mathrm{sen}\varphi_2\right) = \rho_1\rho_2\left(\cos\left(\varphi_1 + \varphi_2\right) + i\cdot\mathrm{sen}\left(\varphi_1 + \varphi_2\right)\right)$$

Pertanto, nel prodotto, i moduli si moltiplicano e gli argomenti si sommano. Ciò fa apparire un pò meno artificioso il prodotto di numeri complessi. Si ha poi la *formula di De Moivre* per le potenze:

$$\left(\rho\left(\cos\varphi + i\cdot\mathrm{sen}\varphi\right)\right)^n = \rho^n\left(\cos\left(n\varphi\right) + i\cdot\mathrm{sen}\left(n\varphi\right)\right)$$

La costruzione matriciale. Una costruzione del campo complesso mediante matrici quadrate d'ordine 2 è la seguente: sia $\overline{\mathbf{C}} = \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \,\middle|\, a, b \in \mathbf{R} \right\}$. Si verifica subito che questo insieme è chiuso rispetto all'addizione ed alla moltiplicazione di matrici:

$$\begin{bmatrix} a & -b \\ b & a \end{bmatrix} + \begin{bmatrix} c & -d \\ d & c \end{bmatrix} = \begin{bmatrix} a+c & -(b+d) \\ b+d & a+c \end{bmatrix}, \quad \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \cdot \begin{bmatrix} c & -d \\ d & c \end{bmatrix} = \begin{bmatrix} ac-bd & -(ad+bc) \\ ad+bc & ac-bd \end{bmatrix}$$

La corrispondenza $a + ib \to \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ tra $\mathbf{C}$ e $\overline{\mathbf{C}}$ è un "isomorfismo", ossia alla somma ed al prodotto di numeri complessi corrisponde la somma ed il prodotto delle corrispondenti matrici di $\overline{\mathbf{C}}$. In particolare, alla "norma" $a^2 + b^2$ di a+ib corrisponde il determinante di $\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$. Al numero complesso reale a+0i corrisponde la matrice "scalare" $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$; all'unità immaginaria i corrisponde la matrice $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, che al quadrato dà $\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = -\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \equiv -1$.

Quindi, possiamo identificare $\mathbf{C}$ e $\overline{\mathbf{C}}$. Le operazioni sono naturali, perché sono quelle solite fra matrici, ma difficilmente una matrice è percepita da uno studente generico come un numero, sia pure un po' più generale rispetto ai numeri reali.

La costruzione universitaria. L'anello $\mathbf{R}[x]$ dei polinomi nell'indeterminata x ed a coefficienti reali, comunque sia stato definito, è euclideo e quindi ha gli ideali principali, come noto dai corsi del triennio. Allora ogni ideale generato da un polinomio irriducibile è massimale ed il quoziente è un campo.

Si consideri l'ideale I generato dal polinomio irriducibile $x^2 + 1$. Poniamo $\mathbf{C} = \mathbf{R}[x]/I$. è un campo i cui elementi sono i laterali f+I, con $f \in \mathbf{R}[x]$.

L'applicazione $a \mapsto a + I$ da $\mathbf{R}$ a $\mathbf{C}$ è un monomorfismo, la cui immagine è un sottocampo isomorfo ad $\mathbf{R}$ e che identifichiamo con $\mathbf{R}$. Ossia $\forall a \in \mathbf{R}$ identifichiamo a+I con a.

Se dividiamo ora il polinomio f per $x^2 + 1$, otteniamo un quoziente q ed un resto r = a+bx, tali che $f = (x^2 + 1)q + r$. Allora f+I = r+I.

Posto i = x+I, ed identificata come detto la costante a con il laterale a+I, si ottiene:

$$a+bx+I = (a+I)+(b+I)(x+I) = a+bi.$$

Pertanto, ogni elemento del quoziente è rappresentabile mediante la scrittura a+ib.

Si osservi poi che:

$$i^2 = (x + I)^2 = x^2 + I = -1 + (x^2 + 1) + I = -1 + I = -1 .$$

Questa è a mio avviso la costruzione ottimale di **C**, ma naturalmente è solo universitaria.

Il campo complesso non è ordinato. Il campo reale è ordinato, nel senso che ha il sottoinsieme $\mathbf{R}^+$ dei numeri positivi chiuso rispetto a somma e prodotto ed inoltre, per ogni x non nullo, uno ed uno solo fra x e -x è positivo. Posto allora $x < y$ se y-x è positivo, si ha un campo ordinato.

Nell'insieme dei numeri complessi è naturalmente possibile definire ordini totali in tanti modi, ma in nessun caso si può ottenere un sottoinsieme $\mathbf{C}^+$ dei positivi con le stesse proprietà che ha $\mathbf{R}^+$. Infatti, abbiamo visto che, in un campo ordinato, 1 è positivo e quindi -1 è negativo. Inoltre, tutti i quadrati sono positivi.
Però, in C si ha $-1 = i^2$, ossia è un quadrato, quindi positivo, assurdo.
Dunque, il campo complesso non è un campo ordinato.

La chiusura algebrica. Nel campo complesso ogni equazione di II grado ha due soluzioni distinte oppure una doppia. Infatti, ogni elemento è un quadrato perfetto ed ha due radici quadrate.
Ma non solo: il *teorema fondamentale dell'algebra* afferma che ogni polinomio di grado $n \geq 1$ ha nel campo complesso almeno una radice e pertanto si scompone in n fattori di primo grado.
In particolare, ogni numero complesso ha esattamente n radici n – esime, per ogni $n \geq 2$.
Infatti, dalla formula $\left(\rho(\cos\varphi + i\cdot sen\varphi)\right)^n = \rho^n\left(\cos(n\varphi) + i\cdot sen(n\varphi)\right)$, si ricava che le radici n-esime di $\rho(\cos\varphi + i\cdot sen\varphi)$ sono date da $\sqrt[n]{\rho}\left(\cos\frac{\varphi+2\pi k}{n} + i\cdot sen\frac{\varphi+2\pi k}{n}\right),\ 0 \leq k < n$.

Nel caso del numero complesso 1, detta ε_k la radice n-esima corrispondente a k, si ha $\varepsilon_k = \varepsilon_1^k$, e si ottiene un sottogruppo ciclico generato da ε_1.

Il gruppo moltiplicativo: nel prodotto i moduli si moltiplicano e gli argomenti si sommano con la regola degli angoli; pertanto, si ha: $(\mathbf{C}^*,\cdot) \cong (\mathbf{R}^+,\cdot)\times\left(\frac{\mathbf{R}}{2\pi\mathbf{Z}},+\right) \cong (\mathbf{R},+)\times\left(\frac{\mathbf{R}}{2\pi\mathbf{Z}},+\right)$, ricordando che tramite i *logaritmi* si ha $(\mathbf{R}^+,\cdot) \cong (\mathbf{R},+)$.

NOTA. Il *teorema fondamentale dell'algebra*, enunciato dall'enciclopedista D'Alembert, ma dimostrato in modo completo da Gauss, afferma che in **C** ogni equazione algebrica f(x) = 0 di grado ≥ 1 ha almeno una soluzione. Si esprime questa proprietà dicendo che il campo complesso è *algebricamente chiuso*.

Allora entro **C** possiamo cercare le soluzioni di tutte le equazioni algebriche a coefficienti razionali. E qui si ha una sorpresa: queste soluzioni costituiscono un sottocampo proprio di **C**, il *campo dei numeri algebrici*: è numerabile come **Q**, mentre **C**, che contiene anche **R** non lo è. Pertanto, i numeri algebrici non solo non riempiono tutto **C**, ma sono un'esigua minoranza.
Si dimostra inoltre che anche questo sottocampo è algebricamente chiuso.

Si chiamano *numeri trascendenti* i numeri complessi non algebrici. Come detto, la quasi totalità dei numeri complessi è trascendente, ma un problema davvero difficile è vedere se un dato numero non razionale sia trascendente o algebrico.

Esempio. Sia $k = \sqrt{5-\sqrt[3]{2}} + 4$: è algebrico o trascendente su **Q**?

Con qualche passaggio si ha: $k - 4 = \sqrt{5-\sqrt[3]{2}}$, da cui :

$(k-4)^2 = 5-\sqrt[3]{2}$,

$[(k-4)^2-5]^3 = -2$,

$(k^2 - 8k + 11)^3 + 2 = 0$,

quindi k è soluzione dell'equazione $(x^2 - 8x + 11)^3 + 2 = 0$ a coefficienti interi e dunque è algebrico su **Q**.

Ma, il numero π = 3,14159... è algebrico o trascendente? Nella seconda metà dell'ottocento fu dimostrato che è trascendente, così come *e* = 2,71... (il numero di Nepero), le sue potenze con esponente razionale, i logaritmi naturali di numeri razionali, seno e coseno di numeri razionali, ecc.

Infine, una curiosità: ci sono campi contenenti propriamente **C**? Consideriamo l'anello di polinomi **C**[x]: è un dominio d'integrità, quindi ha il campo dei quozienti. Esso contiene ovviamente un sottocampo isomorfo a **C**. Tuttavia, quest'ultimo, visto come spazio vettoriale su **C**, ha dimensione infinita. Non esistono campi K con dimensione finita su **C** e diversi da **C**. Per ampliare **C** con dimensione finita occorre rinunciare a qualcosa: la proprietà commutativa del prodotto, per esempio, ed allora c'è il *corpo* **H** dei *quaternioni di Hamilton*, di dimensione 2 su **C**. Se si rinuncia anche alla proprietà associativa, ma non alla possibilità di risolvere le equazioni del tipo ax = b e bx = a, con a non nullo, allora ci sono anche gli *ottetti di Cayley*, di dimensione 4 su **C**.

La teoria delle equazioni sul campo complesso è rinviata al capitolo sulla Teoria di Galois.

Possiamo ricordare qui l'equazione $z^n = 1$, le cui soluzioni hanno modulo 1 e quindi appartengono al cerchio trigonometrico $x^2 + y^2 = 1$. Una radice è $z = 1$.

Gli argomenti differiscono tra loro di un angolo uguale a π/n, quindi nel piano di Argand-Gauss sono i vertici di un poligono regolare con n lati.