I NUMERI RAZIONALI

PREREQUISITI. Per la comprensione del testo sono richieste alcune nozioni elementari su insiemi, relazioni d'equivalenza e d'ordine, funzioni, operazioni, numeri naturali, strutture algebriche.

SCOPI. Ripasso di nozioni già note dal corso di Algebra I e dalla scuola secondaria. Conoscenze integrative.

Contenuti:

§ 1) Frazioni e numeri razionali assoluti: equivalenza, operazioni, ordinamento. Estensione al campo razionale.

§ 2) Numeri razionali come operatori su grandezze: operazioni, ordinamento, estensione al campo razionale.

§ 3) Anelli e campi, l'anello degli interi, il campo dei quozienti. La caratteristica ed il sottocampo minimo. I due gruppi additivo e moltiplicativo del campo razionale.

§ 4) Risolvere equazioni algebriche, dai numeri razionali ai reali ed ai complessi.

§ 1. 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.

Ricordiamo come:

- Le coppie (a, b) di elementi di $\mathbf{N}^+$ sono dette *frazioni* e sono scritte nella forma $\frac{a}{b}$.
- L'operazione tra le frazioni è: $\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}$.
- L'elemento neutro è la frazione $\frac{1}{1}$.
- La relazione $\frac{a}{b} \sim \frac{c}{d} \Leftrightarrow a \cdot d = b \cdot c$ è di equivalenza ed è compatibile con la moltiplicazione.
- L'inverso di $\left[\frac{a}{b}\right]$ è $\left[\frac{b}{a}\right]$.
- Il sottomonoide $\left\{\left[\frac{a}{1}\right] \,\middle|\, a \in \mathbf{N}^+\right\}$ è isomorfo ad $\mathbf{N}^+$.
- Identificando a con $\left[\frac{a}{1}\right]$, si ha $\left[\frac{a}{b}\right] = a \cdot b^{-1}$.

Il gruppo quoziente è denotato con $\mathbf{Q}^+$. 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 $\left(\overline{\mathbf{Q}},+,0\right)$. I numeri razionali relativi sono allora 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 $\mathbf{Q}^+ = \left\{ x \in \mathbf{Q} \;\middle|\; x = \left[a, 0\right], a \neq 0 \right\}$ e negativi i loro opposti. Questo sottoinsieme è chiuso rispetto all'addizione ed alla moltiplicazione e per ogni elemento $x \in \mathbf{Q}$ non nullo, uno ed uno solo tra x e –x è positivo. L'ordinamento in $\mathbf{Q}$ è definito allora ponendo: $x \leq y$ 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 $\leq$ in $\mathbf{Q}$ è definito da:

- $x \leq y$ se x è negativo ed y è positivo o nullo;
- $x \leq y$ se x ed y sono entrambi positivi e $x \leq y$ come razionali assoluti;
- $x \leq y$ se sono entrambi negativi e $-y \leq -x$ 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*.

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

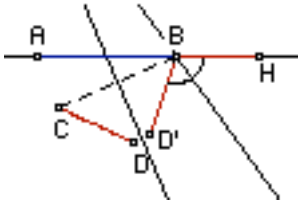
In tal modo, per ogni $a, b \in \mathbf{Q}$ le due equazioni $a + x = b$ e $a \cdot x = b$ (con $a \neq 0$) nell'incognita x hanno una ed una sola soluzione.

§ 2. I numeri 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.

Si consideri l'insieme Σ dei segmenti del piano, compresi quelli degeneri, ossia ridotti ad un punto. Su di esso opera il gruppo Γ delle *isometrie piane*, ossia delle trasformazioni biiettive del piano che lasciano invariate le distanze. Perciò si considerano "uguali" due segmenti *isometrici*, cioè per i quali esista una isometria che trasformi l'uno nell'altro. Questa "uguaglianza" è una relazione d'equivalenza, che produce un insieme quoziente che denotiamo con Σ/Γ.

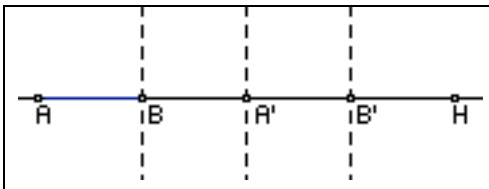
A meno di queste uguaglianze, ossia sull'insieme Σ/Γ quoziente di Σ rispetto all'azione di Γ, i segmenti si possono sommare: dati AB e CD, non degeneri, sulla retta AB si considera un segmento BH uguale a CD, in modo che B *stia fra* A ed H. Allora si pone AB + CD = AH, e la definizione è ben posta perché invariante per isometrie.



Il segmento CD è trasportato sulla retta AB mediante due simmetrie assiali, rispetto all'asse di CB e alla bisettrice di $D'\hat{B}H$.
La somma è il segmento AH.

La classe dei punti, ossia dei segmenti degeneri AA, è l'elemento neutro, che denoteremo con O; l'addizione è commutativa ed associativa, ed inoltre vale la legge di cancellazione: $AB + CD = AB + EF \Rightarrow CD = EF$.
Si tratta cioè di un *monoide commutativo regolare* $(\Sigma / \Gamma, +, O)$.

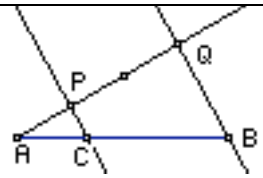
Su questo monoide i numeri naturali agiscono innanzi tutto come *multipli interi*: $\forall n \in \mathbf{N}$, $\forall AB \in \Sigma$, si pone: $nAB = \begin{cases} AA & \text{se } n = 0 \\ (n-1)AB + AB & \text{se } n > 0 \end{cases}$.



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

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

$$\forall n \in \mathbf{N}^+, \forall AB \in \Sigma,\ \frac{1}{n}AB = AC \Leftrightarrow nAC = AB$$

	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:

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

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: $(m \cdot q)AB = (n \cdot p)AB$, 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 $\frac{m}{n},\ \mathrm{MCD}\left(m, n\right) = 1$, 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 l'azione di Γ, 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, 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 $\frac{m}{n} \leq \frac{p}{q} \Leftrightarrow m \cdot q \leq n \cdot p$. In particolare, si ha $\frac{m}{n} \leq \frac{p}{n} \Leftrightarrow m \leq p$, 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, $(\Sigma / \Gamma, +, O)$ 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 e del gruppo delle sue trasformazioni isometriche.
- Si opera di fatto sul quoziente dell'insieme dei segmenti rispetto alla relazione d'isometria, 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 sono comunque date 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 sia la migliore. 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.

§ 3. Il campo razionale e le sue proprietà

Vediamo ora il percorso universitario, ossia la costruzione di **Q** a partire dall'anello degli interi. Vediamo anche più a fondo le sue proprietà additive, moltiplicative e d'ordine.

Ricordiamo che un *anello* $(A,+,\cdot,1_A)$ è una struttura algebrica nella quale $(A,+)$ è un gruppo abeliano; $(A,\cdot,1_A)$ è un monoide e valgono le due *proprietà distributive* (destra e sinistra) di $\cdot$ rispetto a $+$, ossia:

$$\forall a,b,c\in A,\begin{cases}a\cdot(b+c)=a\cdot b+a\cdot c\\(a+b)\cdot c=a\cdot c+b\cdot c\end{cases}.$$

L'elemento neutro 0_A dell'addizione $+$ è elemento assorbente della moltiplicazione.

Se l'operazione $\cdot$ è commutativa l'anello si dice *commutativo*, e si dice *dominio d'integrità* se inoltre vale la *legge di annullamento del prodotto*:

$$x\cdot y=0_A\Rightarrow x=0_A \text{ oppure } y=0_A.$$

In tal modo, il prodotto di due elementi non nulli è non nullo. L'insieme $A\setminus\{0_A\}$ costituisce quindi un sottomonoide regolare del monoide moltiplicativo.

Esempio 3.1. Nel gruppo ciclico $(\mathbf{Z},+)$ ottenuto dalla simmetrizzazione del monoide commutativo regolare $(\mathbf{N},+,0)$ si può definire una moltiplicazione nel modo seguente. Poiché ogni elemento non nullo è o un numero naturale (*positivo*) o l'opposto di un numero naturale (e lo diremo *negativo*), definiamo il prodotto $a\cdot b$ nel modo seguente:

- Se a e b sono entrambi positivi, si moltiplicano come in N e si ha un numero positivo.
- Se a è negativo, b positivo, allora $a\cdot b=-((-a)\cdot b)$, che è negativo perché opposto di un positivo.
- Se a è positivo, b negativo, allora $a\cdot b=-(a\cdot(-b))$, che è negativo.
- Se sono entrambi negativi, allora $a\cdot b=(-a)\cdot(-b)$, che è positivo.
- Se uno dei due è = 0, il prodotto è = 0.

Si ottiene allora un'operazione associativa, commutativa, con elemento neutro 1, elemento assorbente 0, distributiva rispetto al + e che sugli interi positivi o nulli è come su **N**. Pertanto abbiamo un anello commutativo $(\mathbf{Z}, +, \cdot, 1)$, detto anello degli interi relativi, ed è anche un dominio d'integrità.

Circa il gruppo delle unità di un anello $(A, +, \cdot, 1_A)$, nel caso di **Z** gli elementi unitari sono 1 e -1. In altri casi gli elementi unitari sono tutti gli elementi non nulli. Quando ciò accade in un anello commutativo, l'anello prende il nome di *campo*. La costruzione seguente immerge un dominio d'integrità in un campo. Se applicata all'anello **Z** degli interi, produce il campo razionale **Q**.

TEOREMA 3.2. 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 $\Phi\left(a\right) = \left[\frac{a}{1_A}\right]$, è un monomorfismo di anelli. Inoltre, per ogni $\left[\frac{a}{b}\right] \in Q\left(A\right)$ 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 $\mathrm{MCD}(a, b) = 1_A$.

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 3.3. 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 $b \in K$ si dice *maggiorante* di A se per ogni $a \in A$ 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 $(\mathbf{Q}, +, \cdot, \le)$ 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:

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

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

NOTA. In ogni campo ordinato K c'è un sottocampo K_0 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 $\frac{m}{n} \le \frac{p}{q}$ in **Q** allora $\frac{m1_A}{n1_A} \le \frac{p1_A}{q1_A}$ in K, e viceversa.

Esaminiamo ora separatamente i due gruppi additivo e moltiplicativo di **Q**.

3.4. 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 $k \in \mathbf{Z}$, non può essere $k \cdot \frac{m}{n} = \frac{1}{p}$, quindi il sottogruppo ciclico generato da $\frac{m}{n}$ 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 $n = mcm(k,s)$. 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, $H = \left\langle \left\{ \frac{h}{k}, \frac{r}{s} \right\} \right\rangle \le \left\langle \frac{1}{n} \right\rangle$, 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 $x \in \mathbf{Q}$, tale che $k \cdot x = \frac{m}{n}$. Ovviamente, è $x = \frac{m}{k \cdot n}$. Non è una proprietà comune:

infatti, oltre a $(\mathbf{Q}, +)$ 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 $\mathbf{C}$ denota il campo complesso e p un primo qualsiasi, e dai prodotti diretti di copie di $\mathbf{Q}$ per copie di questi gruppi. In particolare, lo stesso gruppo additivo reale $(\mathbf{R}, +)$, che è a sua volta divisibile, è prodotto diretto di *c* copie di $\mathbf{Q}$, dove c denota la potenza del continuo. (Lo stesso accade per il gruppo additivo complesso $(\mathbf{C}, +)$, che dunque è isomorfo ad $(\mathbf{R}, +)$, anche se non sembra!)

6) Il gruppo $(\mathbf{Q}, +)$ possiede sottogruppi notevoli. Uno di essi è naturalmente $(\mathbf{Z}, +)$. 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 $\mathbf{Z}$. Nel gruppo quoziente $\mathbf{Q}/\mathbf{Z}$, i quozienti $\mathbf{Q}_p/\mathbf{Z}$ 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 $\frac{m}{p^n} + \mathbf{Z}$, $0 \le m < p^n$, 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 $(\mathbf{Q}, +)$ 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 $x \in \mathbf{Q}$. Se x è intero, non c'è nulla da provare. Sia $x = \frac{m}{p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}}$, $r \ge 1$, ridotta ai minimi termini. Se $r = 1$, non c'è nulla da provare. Per induzione, sia $r > 1$, allora cerchiamo $u, v \in \mathbf{Z}$, 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, $(\overline{u}, v_r)$, per l'ipotesi induttiva esistono $v_1, \ldots, v_{r-1}$ tali che

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

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 $\mathbf{Q}/\mathbf{Z}$ la scomposizione è unica, ossia $\mathbf{Q}/\mathbf{Z}$ è *somma diretta* dei suoi sottogruppi $\mathbf{Q}_p/\mathbf{Z}$.

8) Come in ogni campo, per ogni $a \in \mathbf{Q}$, 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 $a \neq 0$, 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, $\mathrm{Aut}(\mathbf{Q}, +) \cong (\mathbf{Q}^*, \cdot)$.

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

1) Il gruppo moltiplicativo $\left(\mathbf{Q}^*,\cdot\right)$ 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:

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

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

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

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

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 $2^m\cdot3^n$, con $m,n\in\mathbf{Z}$, 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 $\mathbf{Z}$ 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: $\langle p \rangle = \left\{p^\alpha \mid \alpha \in \mathbf{Z}\right\}$. Ciò posto, sia $x = \dfrac{p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}}{q_1^{\beta_1} \cdot q_2^{\beta_2} \cdots q_s^{\beta_s}}$, 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 $x \in \langle p_1 \rangle \cdots \langle p_r \rangle \langle q_1 \rangle \cdots \langle q_s \rangle$, 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:

p	2	3	5	7	11	...
x^k	x^0	x^1	x^2	x^3	x^4	...

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 $\left(\mathbf{Q}^+, \cdot\right)$, quindi $\mathrm{Aut}\left(\mathbf{Q}^+, \cdot\right)$ 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.

§4. 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 4.1. 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 $4+x^2 > 0$ 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 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 4.2 .

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). 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:

TEOREMA 4.3 (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 $na > b$.

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:

TEOREMA 4.4. 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 coppia (A, B) di sottoinsiemi non vuoti e separati di **Q** tali che A∪B = **Q**. Le operazioni sono un poco artificiose, ma non troppo. 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.

Una costruzione molto elegante, ma assai poco comprensibile, è quella di **Cantor**. 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 $x = x_0,x_1x_2.....x_r\ \overline{a_1a_2...a_p}$. In tal caso, il numero naturale $a_1a_2...a_p$ si chiama *periodo* p(x) di x. Il numero naturale $x_0\cdot 10^r+x_1x_2.....x_r$ 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 che i numeri razionali corrispondono ai decimali periodici. Ma come definire le operazioni?

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

$$x' = 0,333333333333....\ ,\ y' = 1,714285714285714285.....$$

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 $n\in\mathbf{N}$ 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'):

$f_0=0$	$f_1=\mathbf{0},51$	$f_2=\mathbf{0,5}643$	$f_3=\mathbf{0,57}07...$	$f_4=\mathbf{0,571}34...$	$f_5=\mathbf{0,5714}2...$
$g_0=2$	$g_1=\mathbf{0},72$	$g_2=\mathbf{0,5}848$	$g_3=\mathbf{0,57}28...$	$g_4=\mathbf{0,571}54...$	$g_5=\mathbf{0,5714}4...$

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 poco 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":

$u_0=4$	$u_1=\mathbf{4},7$	$u_2=\mathbf{4,7}2$	$u_3=\mathbf{4,7}29$	$u_4=\mathbf{4,730}0$	$u_5=\mathbf{4,73005}$ ...
$v_0=6$	$v_1=\mathbf{4},9$	$v_2=\mathbf{4,7}4$	$v_3=\mathbf{4,7}31$	$v_4=\mathbf{4,730}2$	$v_5=\mathbf{4,73007}$ ...

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

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. Infatti: A ammette anche dei maggioranti interi, e sia b_0 il minimo intero che sia 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

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

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 facilmente 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:

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

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 (che approssima per eccesso il minore e per difetto il maggiore).

Ma l'equazione $x^2 + 1 = 0$ non ha soluzione neppure in **R**, quindi apparentemente non abbiamo risolto nulla.

Se però, partendo da **R**, "inventiamo" il simbolo i per denotare una soluzione di questa equazione, e attraverso questo i ampliamo **R**, l'ampliamento che si ottiene è sufficiente per risolvere **tutte** le equazioni algebriche di grado maggiore di 1.

Il procedimento è tecnicamente il seguente, detto *ampliamento quadratico*:
Nell'insieme $\mathbf{R}\times\mathbf{R}$ definiamo addizione e moltiplicazione nel modo seguente:

$$(a, b)+(c, d) = (a+c, b+d), \quad (a, b)\cdot(c, d) = (ac-bd, ad+bc) \qquad (**)$$

Possiamo facilmente verificare che $(\mathbf{R}\times\mathbf{R}, +, \cdot)$ è un campo. In particolare, gli elementi neutri additivo e moltiplicativo sono (0, 0) e (1, 0), e se $(a, b) \neq (0, 0)$ si ha $a^2+b^2 \neq 0$ e $(a,b)^{-1} = \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right)$.

Questo campo contiene un sottocampo $\mathbf{R}_1$ costituito dalle coppie (a, 0) ed isomorfo ad **R.** Identifichiamo (a, 0) con a e quindi $\mathbf{R}_1$ con **R.** Poniamo i = (0, 1). Allora:

$$(a, b) = (a, 0) + (b, 0)(0, 1) = a+bi.$$

Inoltre, $(0, 1)^2 = (-1, 0)$, ossia $i^2 = -1$. Ne segue che, in questo nuovo campo, i è soluzione dell'equazione $x^2+1 = 0$.

Denotiamo con **C** questo campo, che chiameremo *campo complesso*. L'elemento i si chiama *unità immaginaria*.

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 ha 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 4.5. Sia $k = \sqrt{5-\sqrt[3]{2}}+4$: è algebrico o trascendente?

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 $(x^2 - 8x + 11)^3 + 2 = 0$ e dunque è algebrico.

Ma, il numero $\pi = 3{,}14159...$ è algebrico o trascendente? Si può dimostrare che è trascendente, e come lui, anche $e = 2{,}71...$ (il numero di Nepero), le sue potenze con esponente razionale, i logaritmi naturali di numeri razionali, seno e coseno di numeri razionali ecc.