Numeri razionali
Costruzione aritmetica e costruzione geometrica
(con un cenno alla costruzione geometrica dei numeri reali)

Esponiamo brevemente due costruzioni di Q^+, l'insieme dei numeri razionali positivi, la prima **aritmetica**, la seconda **geometrica**. Ciò significa che la costruzione si fonderà nel primo caso sulle proprietà del semigruppo (abeliano regolare ordinato archimedeo) *N*, che ha come supporto l'insieme dei numeri naturali (usiamo il medesimo simbolo per denotare la struttura e il suo sostegno), nel secondo quelle dell'*analogo* (nel senso che gode di tutte le proprietà dianzi elencate, e in più della divisibilità) semigruppo Σ_S, o più semplicemente Σ, che ha come supporto l'insieme dei *segmenti liberi* dello *spazio ordinario* **S** (se ne darà un cenno di descrizione nel paragrafo 5). Non è infondato ritenere che:

- *N* corrisponda all'intuizione del **discreto** (*tempo*, palesemente "futuro"; *Z*, l'insieme degli interi relativi, corrisponderebbe invece a *tutto* il tempo);

- Σ a quella del **continuo** (*spazio*; si badi bene però, "spazio geometrico", "spazio ideale", o "del pensiero", e *non* "spazio fisico" *reale*! - non entriamo in particolari sull'enorme pasticcio di denominazioni ormai "tradizionali" che però appaiono purtroppo del tutto *inadeguate*, numeri *reali*, numeri *irrazionali*, *numeri* complessi, *etc.*).

1.

L'idea che sovrintende alla costruzione aritmetica è la seguente. I numeri razionali sono collegati a una relazione di equivalenza ρ sull'insieme $N\times N$ delle coppie ordinate di numeri naturali. L'equivalenza tra due coppie ordinate (a,b) e (c,d) si enuncia anche in termini di *proporzionalità*:

$$(a,b)\ \rho\ (c,d) \Leftrightarrow a : b = c : d \text{ (che si legge: a sta a b come c sta a d).}$$

Q^+ non è altro che l'insieme quoziente $N\times N/\rho$, sicché, dal punto di vista della "natura" dei numeri razionali, concepiti come "grandezze" di origine aritmetica, sussiste la seguente relazione di inclusione insiemistica:

$$Q^+ \subset \mathrm{P}(N\times N).$$

La classe di equivalenza della coppia ordinata (a,b) si indica con il simbolo familiare $\frac{a}{b}$, sicché: $[(a,b)] = \frac{a}{b}$. Si ha a che fare quindi con **due** ben distinti

concetti, quello di coppia ordinata di numeri naturali e di numero razionale associato. Se si volesse, si potrebbe introdurre un terzo concetto, corrispondente secondo noi in maniera adeguata a quello intuitivo di *frazione*, relativo alle coppie ordinate costituite da un numero razionale q e da un suo rappresentante (a,b), ossia (q,(a,b)), con q = [(a,b)], ma su ciò non insistiamo.

La definizione di ρ trae origine dalle seguenti "necessarie" proprietà (che si può pensare, se si vuole, *definiscano* ρ in casi particolari). Le lettere latine minuscole designano, com'è da attendersi, numeri naturali qualsiansi.

(1) $\frac{a}{b} = \frac{c}{d} \Leftrightarrow \frac{b}{a} = \frac{d}{c}$

(2) $\frac{a}{b} = \frac{a}{x} \Leftrightarrow b = x$

(in virtù di (1), vale l'analoga: $\frac{a}{b} = \frac{x}{b} \Leftrightarrow a = x$)

(3) $\frac{a}{b} = \frac{ma}{mb}$ ("invarianza di scala").

Dalle proprietà precedenti discende la definizione generale di ρ. Infatti, se $\frac{a}{b} = \frac{c}{d}$, deve essere anche, per (2), $\frac{a}{b} = \frac{ca}{cb}$, $\frac{c}{d} = \frac{ac}{ad}$, $\frac{ca}{cb} = \frac{ac}{ad}$ e quindi: cb = ad (per (3)). Se si preferisce, $\frac{a}{b} = \frac{da}{db}$, $\frac{c}{d} = \frac{bc}{bd}$, $\frac{da}{db} = \frac{bc}{bd}$ e quindi la stessa identità: da = bc. Pervenuti alla condizione "necessaria":

(4) bc = ad,

è facile constatare che essa definisce effettivamente una relazione di equivalenza in $N \times N$, la quale soddisfa la (1), la (2) e la (3). Come dire pure che esiste una e una sola relazione di equivalenza del tipo in discorso soddisfacente alle condizioni predette. Si noti il ruolo essenziale che, in ciò che precede, riveste la commutatività del prodotto tra numeri naturali.

Costruito l'insieme Q^+, il passo successivo consiste nel "trasferimento" della struttura algebrica (di somma e prodotto) da N a Q^+, *idem* per la relazione d'ordine.

(5) $\frac{a}{b} + \frac{c}{d} = \frac{da}{db} + \frac{bc}{bd} = \frac{da + bc}{bd}$

(6) $\frac{a}{b} * \frac{c}{d} = \frac{ca}{cb} * \frac{bc}{bd} = \frac{ca}{bd}$

(7) $\frac{a}{b} \leq \frac{c}{d} \Leftrightarrow \frac{da}{db} \leq \frac{bc}{bd} \Leftrightarrow da \leq bc.$

Naturalmente bisogna "verificare" che le tre regole euristiche precedenti definiscono effettivamente strutture del tipo ricercato su Q^+, indipendentemente cioè dalla scelta dei rappresentanti di ciascuno dei numeri razionali coinvolti nelle operazioni algebriche o nella relazione d'ordine. Si potrà poi *verificare* la validità di alcune proprietà algebriche che estendono le analoghe già valide in *N*, per esempio la *distributività* della somma rispetto al prodotto, *etc.*.

Osservazioni importanti.
Secondo la costruzione accennata, *N non* è un sottoinsieme di Q^+, quindi scrivere $N \subset Q^+$ *non* è corretto. Però, esiste ovviamente un'immersione canonica di *N* in Q^+, sicché tra i due insiemi numerici in oggetto esiste una relazione del tipo che abbiamo altrove chiamato una *quasi-inclusione*:

$$N \rightarrowtail Q^+$$
$$a \mapsto \frac{a}{1} = \frac{am}{m}.$$

L'operazione di <u>divisione</u> in *N* è un'operazione binaria *esterna*:

$$N \times N \rightarrow Q^+$$
$$(a,b) \mapsto \frac{a}{b},$$

che corrisponde nient'altro che alla proiezione canonica del dominio sul suo insieme quoziente che figura quale codominio. Quando il risultato è un numero intero (naturale), si dice che b *divide* a, e tale circostanza si indica spesso in simboli con: $b \mid a$.

2.

Detto quindi che un numero razionale $q \in Q^+$ può essere concepito come una totalità di coppie ordinate di numeri naturali, e che quando si scrive $q = \frac{a}{b}$ si è scelto un rappresentante nella relativa classe di equivalenza (rispetto a ρ), dedichiamo questo paragrafo allo studio delle rappresentazioni in forma frazionaria di un fissato numero razionale q.

E' manifesto che nell'insieme q comparirà *una e una sola* coppia ordinata (m,n) tale che m sia il <u>minimo</u> di tutti i primi elementi (*numeratori*) delle coppie

ordinate appartenenti a q (poiché *N* è un insieme bene ordinato, e una ρ-classe di equivalenza non è vuota). E' facile persuadersi che, se m è il minimo numeratore di una frazione esprimente q, il corrispondente n sarà il minimo denominatore. Quando si scrive $q = \frac{m}{n}$ si dice che il numero razionale è stato espresso ai minimi termini.

Vogliamo dimostrare adesso il seguente fondamentale:

Teorema 1. Ferme restando le notazioni precedenti, $q = \frac{m}{n} = \frac{a}{b}$ implica che esiste un numero naturale k tale che a = km, b = kn (si dice anche che a e b sono *equimultipli* rispettivi di m e di n).

Facciamo precedere la dimostrazione del Teorema 1 da una serie di considerazioni di pura natura aritmetica.

Introduciamo prima di tutto la funzione aritmetica $\psi : N \to N$ che associa ad ogni numero naturale n il numero dei suoi divisori, sicché sarà:

$\psi(1) = 1, \psi(2) = 2, \psi(3) = 2, \psi(4) = 3, \psi(5) = 2, \psi(6) = 4,\ldots$.

Un numero naturale n si chiama primo se $\psi(n) = 2$, cioè, se n è maggiore di 1, e i suoi unici divisori sono 1 e n.

Teorema 2. Ogni numero naturale $n > 1$ o è primo, o è un prodotto di numeri primi.

Dim. 2 è un numero primo, 3 è un numero primo, 4 è uguale a 2 per 2, *etc.*. Preso in generale un numero naturale $n \geq 2$, si cominci a scorrere la successione 2, 3, 4,... , rispondendo alla domanda: 2 divide n? Se sì, si finisce, e si ricomincia dal numero "naturale" $\frac{n}{2}$, ponendo la domanda: 2 divide n? Se no, ci si chiede: 3 divide n? 4 divide n?, *etc.*, finché non si trova un numero naturale p che divide n, eventualmente p = n. E' ovvio che p è necessariamente un numero primo (se non lo fosse, avremmo dovuto rispondere sì a una precedente domanda relativa a un divisore proprio di n). Ciò osservato, si prende in considerazione il numero "naturale" $\frac{n}{p}$, e se questo non è uguale ad 1 si itera il procedimento, fino ad arrivare a dimostrare il teorema 2 (in modo assolutamente "costruttivo") nella seguente forma più precisa:

Teorema 3. Dato un qualsiasi numero naturale $n > 1$, è possibile determinare *univocamente* una "sequenza" finita $q_1 \leq q_2 \leq q_3 \leq \ldots$ di numeri primi, tale che risulti:

$$n = q_1 * q_2 * q_3 * \ldots .$$

Ovviamente, il numero n è primo se e soltanto se la precedente sequenza consiste di un solo elemento.

Alla decomposizione di n in un prodotto di numeri primi si arriva in maniera certamente *univoca*, in virtù dell'algoritmo sopra descritto, ma non è chiaro *a priori* che una siffatta decomposizione sia *unica*. Vale a dire, che non si possa descrivere un'altra procedura che arrivi a un'analoga sequenza finita $r_1 \leq r_2 \leq \ldots$ di numeri primi tale che $n = r_1 * r_2 * r_3 * \ldots$ e che sia *distinta* dalla precedente (nel senso che o le due sequenze abbiano *lunghezze* diverse, o numeri primi diversi appaiano nello stesso punto della sequenza). Ciò può essere per fortuna escluso, grazie al seguente:

Lemma di Euclide. Se un numero primo p divide un prodotto di numeri naturali ab, allora p divide certamente o a o b (ossia, divide b se non divide a, e divide a se non divide b).

Infatti, se $q_1 * q_2 * q_3 * \ldots = r_1 * r_2 * r_3 * \ldots$, ecco che per esempio r_1, dividendo il prodotto che figura nel LHS della precedente identità, deve dividere uno dei fattori che vi appaiono, ma, essendo questi primi, r_1 non potrà che coincidere con uno di questi, anzi con il minimo, sicché necessariamente $r_1 = q_1$, *etc.*, dal momento che si potrà allora scrivere: $q_2 * q_3 * \ldots = r_2 * r_3 * \ldots$, e così via.

Perverremo alla dimostrazione del precedente lemma (che costituisce la Prop. 30 del Libro VII degli *Elementi* di Euclide) soltanto dopo alcune utili considerazioni che esporremo nel paragrafo seguente. Limitiamoci per il momento a osservare che la decomposizione, o *fattorizzazione*, di un numero naturale in un prodotto di numeri primi di cui sopra è quindi *unica*, e che ci si può limitare alla considerazione di numeri primi distinti qualora si introduca per ciascuno di essi la relativa *molteplicità*, fino ad arrivare quindi a una fattorizzazione nella forma:

$$n = q_1^{h_1} * q_2^{h_2} * q_3^{h_3} * \ldots .$$

Se si introduce la successione $p_1 = 2 < p_2 = 3 < p_3 = 5 < \ldots$ di *tutti* i numeri primi, si può definire, per ogni numero primo p, la funzione *molteplicità* di p in n (per numeri naturali $n \geq 2$), in simboli $h_p(n)$: sarà questa uguale a 0 se p non divide n, e uguale altrimenti al massimo esponente h per cui p^h divide n. La successione delle molteplicità $h_1(n)$, $h_2(n)$,... (dove si è scritto per semplicità $h_1(n)$ in luogo di $h_{p_1}(n)$, *etc.*), sarà *definitivamente nulla*, tale cioè che $h_p(n) = 0$ per tutti i numeri primi da un certo numero in poi (da un certo indice in poi). Tale circostanza dà senso al seguente *prodotto infinito*, che è un modo di esprimere la decomposizione unica di n in un prodotto di numeri primi (*teorema*

fondamentale dell'aritmetica):

$$n = p_1^{h_1(n)} * p_2^{h_2(n)} * p_3^{h_3(n)} * \ldots = \prod_{p \text{ primo}} p^{h_p(n)} .$$

Il teorema fondamentale dell'aritmetica permette di calcolare esplicitamente la funzione $\psi(n)$:

Teorema 4. Sia n un numero naturale arbitrario maggiore di 1. Se n viene scritto canonicamente come $n = q_1^{h_1} * q_2^{h_2} * q_3^{h_3} * \ldots$, allora risulta:

$$\psi(n) = (h_1+1)*(h_2+1) *(h_3+1)*\ldots .$$

[La funzione $\psi(n)$ non va confusa con la *funzione di Eulero* $\varphi(n)$, che calcola il numero degli elementi k di σ_n *primi* con n, ossia tali che non abbiano alcun divisore a comune con n tranne 1. E' chiaro che $\varphi(1) = 1$, e che $\varphi(p) = p-1$ per ogni numero primo p. Inoltre $\varphi(p^h) = p^h-p^{h-1}$ per ogni esponente naturale h. Il calcolo completo della funzione φ si effettua per il tramite della decomposizione di un numero naturale in fattori primi, e del seguente importante lemma, che enunciamo senza dimostrazione: se a e b sono due numeri naturali primi tra loro, allora $\varphi(ab) = \varphi(a)\varphi(b)$. φ risulta cioè, ma solo per tali coppie di numeri, una *funzione moltiplicativa*.]

Terminiamo questo paragrafo osservando che dal lemma di Euclide si ottiene facilmente la dimostrazione in sospeso (del teorema 1).

Dim. (del teorema 1). Sia dunque $\frac{m}{n} = \frac{a}{b}$. In forza dell'ipotesi che $\frac{m}{n}$ costituisce *la* (l'uso dell'articolo determinativo è legittimo) rappresentazione nei minimi termini del numero razionale in parola, si sa che m ed n sono primi tra loro, ovvero non hanno un divisore comune tranne 1 (altrimenti questo eventuale divisore comune maggiore di 1 si potrebbe cancellare a numeratore e denominatore nella rappresentazione della frazione, pervenendo così a termini ancora più minimi, un assurdo). Dalla $mb = na$ si deduce quindi che m divide a, ed n divide b (se m ed n non sono uguali ad 1, si utilizzi la loro fattorizzazione unica in un prodotto di numeri primi, ciascuno dei quali, con la relativa molteplicità, non potrà "stare" in n, e dovrà allora stare in a; abbiamo fatto riferimento al caso di m), ovvero che: esistono numeri naturali $u, v \in N$ tali che $a = um$, $b = vn$. Ma $mb = na = mvn = num \Rightarrow u = v$, sicché ecco dimostrato il teorema per $k = u = v$.

[Abbiamo provato il teorema 1 a partire dal lemma di Euclide, seguendo un procedimento inverso a quello del grande geometra alessandrino. Egli infatti dimostrò il lemma in questione a partire dal teorema 1, e la circostanza si presenta così semplice che non vi insistiamo - e intendiamo ciò non nel senso

che è semplice dimostrare il teorema 1, bensì che è semplice dimostrare che esso implica il lemma di Euclide!]

3.

Prima di offrire la dimostrazione lasciata in sospeso (del lemma di Euclide), dedichiamo qualche attenzione alle (conosciute sin dalle scuole medie) costruzioni del massimo comune divisore e minimo comune multiplo di due numeri a, b arbitrariamente fissati in *N*. In simboli, rispettivamente:
D = MCD(a,b), m = mcm(a,b).

E' chiaro infatti *a priori* che, dati due numeri naturali a, b, gli insieme dei rispettivi divisori sono finiti e non disgiunti (contengono entrambi il numero 1), sicchè la loro intersezione è non vuota e limitata, d'onde l'esistenza di un *massimo* comune divisore. Analogamente, esistono di certo dei multipli comuni (per esempio: ab, e quindi infiniti, almeno: 2ab, 3ab,...), sicché l'insieme dei multipli comuni è non vuoto e si può introdurre il *minimo* comune multiplo (per il *buon ordinamento* di *N*).

Algoritmo euclideo delle divisioni successive e calcolo del MCD.

Una volta che si abbia a disposizione la fattorizzazione unica di un numero naturale in un prodotto di numeri primi, è facile dimostrare che il MCD coincide con il prodotto di tutti i primi comuni ai due numeri in oggetto, presi con la *minima* delle molteplicità con cui essi appaiono nelle fattorizzazioni in parola, mentre il mcm coincide con il prodotto di tutti i primi comuni e non comuni ai due numeri in oggetto, presi con la *massima* delle molteplicità con cui essi appaiono nelle fattorizzazioni in parola.

In questa sezione illustriamo un procedimento per il calcolo esplicito del MCD e del mcm che *non* fa ricorso alla fattorizzazione in numeri primi, la cui determinazione è senz'altro più laboriosa.

Supponendo per esempio $a \geq b$, potremo senz'altro scrivere (enfatizziamo quando opportuno la presenza di un prodotto, e la distinzione tra i "ruoli" dei fattori, con il simbolo $*$):

(8) $a = q_1 * b + r_1$,

grazie al noto elementare algoritmo della *divisione con resto* (*per difetto*). I due coefficienti q_1 e r_1, il primo dei quali è un elemento di *N*, il secondo un elemento di N_0, risultano univocamente determinati dalla precedente identità qualora il *resto* venga scelto positivo o nullo, e minore del *divisore* b (rammentiamo che a si dice il *dividendo* della divisione e q_1 il relativo *quoziente*). Osserviamo che l'algoritmo delle divisioni successive si può far partire anche dal caso $a < b$,

convenendo di scrivere banalmente $a = 0*b + a$.

[La possibilità di effettuare tale "operazione" riposa sul cosiddetto *postulato di Archimede*: $a \geq b \Rightarrow a = 1*b + (a-b)$, ma non è detto che sia $a-b < b$, cioè $a < 2b$. Se $a \geq 2b$, si scrive $a = 2*b + (a-2b)$, e si ripete il ragionamento: non è detto che sia $(a-2b) < b$, ovvero $a < 3b$, e se $a \geq 3b$ si va avanti. Il procedimento deve avere comunque termine, con il *primo* numero naturale q tale che $qb > a$ (nelle attuali ipotesi $q \geq 2$), e la divisione con resto sarà espressa allora dall'identità:
$a = (q-1)*b + (a-(q-1)b)$, dove il resto $a-(q-1)b$ è maggiore o uguale di zero e strettamente minore di b (vedi anche quanto se ne dirà nel paragrafo 7.]

Se $r_1 = 0$ non c'è molto da dire: b divide a, e $\frac{a}{b} = q_1$. Se invece $r_1 > 0$, la disuguaglianza $r_1 < b$ permette di *iterare* l'algoritmo della divisione con resto al caso dei due numeri naturali b ed r_1 (rispettivamente dividendo e divisore), pervenendo così a una nuova identità del tipo:

(9) $b = q_2*r_1 + r_2$,

con un nuovo quoziente q_2 e un nuovo resto $r_2 < r_1$. Se per esempio r_2 non è zero, possiamo riscrivere:

(10) $r_1 = q_3*r_2 + r_3$, *etc.*.

Supponiamo per semplicità che sia proprio $r_3 = 0$. In effetti, in questo che si chiama l'*algoritmo euclideo delle divisioni successive*, la sequenza dei resti $r_1, r_2, r_3,...$ è *monotòna strettamente decrescente*: $r_1 > r_2 > r_3 >...$, sicché il procedimento deve necessariamente arrestarsi a un certo passo in cui il resto diventa zero (noi abbiamo appena supposto, per esaminare un caso particolare, che sia il terzo). Riproponiamo allora le tre identità ottenute, in vista di una loro elaborazione che permetta di dedurre delle interessanti informazioni, mettendo in risalto la circostanza che deve risultare necessariamente, nelle attuali condizioni, $q_3 \geq 2$, perché altrimenti sarebbe $r_1 = r_2$, contro l'ipotesi $r_2 < r_1$.

(11) $a = q_1*b + r_1$
(12) $b = q_2*r_1 + r_2$
(13) $r_1 = q_3*r_2$.

Bene, si comprende subito che:

Teorema 5. r_2, l'*ultimo resto non nullo* nella catena di divisioni successive, coincide con il massimo comune divisore dei numeri a e b.

Dim. Infatti, ogni numero naturale d che divida a e b deve dividere

necessariamente $r_1 = a - q_1*b$, e quindi anche $r_2 = b - q_2*r_1$. Riassumendo, si procede *dall'alto verso il basso*: $d \mid a, b \Rightarrow d \mid a, b, r_1 \Rightarrow d \mid a, b, r_1, r_2$. Viceversa, è chiaro che r_2 è un divisore di a e di b, dal momento che esso risulta un divisore di r_1 (dalla (13)), e quindi un divisore di b (in forza della (12)), e infine un divisore di a, in forza della (11): r_2 divide b ed r_1, e quindi divide pure $a = q_1*b + r_1$. Riassumendo, si procede adesso *dal basso verso l'alto*:
$r_2 \mid r_1 \Rightarrow r_2 \mid r_1, b \Rightarrow r_2 \mid r_1, b, a$.

Dalle identità sopra riportate si deduce anche l'*identità di Bézout*, [Così denominata (come talora accade in questi casi, la consuetudine appare però infondata) da Etienne Bézout (1730-1783), autore di 6 volumi di un *Cours de mathématique* (1764-1769), dal quale fu estratto il primo manuale americano di geometria analitica (pubblicato nel 1826), e di una *Théorie générale des equations algébriques* (1779).] che esprime il MCD di due numeri naturali a e b come combinazione lineare a coefficienti interi, ovviamente *con segno*, degli stessi a e b. Ossia:

Teorema 6. Esistono elementi $\lambda, \mu \in Z$, tali che valga la relazione:

$$D = MCD(a,b) = \lambda a + \mu b.$$

Dim. Continuando a rimanere nel caso particolare preso in considerazione, una possibile coppia di valori λ, μ che realizzano l'identità in oggetto si trova subito nel seguente modo. Dalla (12) si trae $r_2 = b - q_2*r_1$, e sostituendo qui il valore di r_1 che si trova dalla (11), vale a dire: $r_1 = a - q_1*b$, ecco che si ottiene infine:
$r_2 = b - q_2r_1 = b - q_2(a-q_1b) = (1+q_1q_2)a - q_2b$ (si procede *dal basso verso l'alto*, a partire dalla penultima identità), cvd.

Può essere interessante notare che, conformemente alla costruzione illustrata, i segni positivo o negativo compaiono alternativamente davanti all'uno o all'altro dei coefficienti λ, μ, a seconda della *lunghezza* della catena di divisioni successive, e che comunque esistono *infiniti valori* di λ, μ (positivi o negativi; potrebbe anche essere per esempio $\lambda = 0$, $\mu = 1$, se b divide a) per i quali sussiste un'identità del tipo di Bézout. Risulta infatti: $(b)a + (-a)b = 0$ (come dire che a e b sono sempre *linearmente dipendenti* su *Z*), sicché risulta pure, sommando:
$D = (\lambda+b)a + (\mu-a)b$, o anche, sottraendo:
$D = (\lambda-b)a + (\mu+a)b$, e inoltre, evidentemente:
$D = (\lambda+2b)a + (\mu-2a)b$, *etc.*.
Il procedimento fa comprendere che si può sempre scegliere per esempio il coefficiente λ positivo, o negativo, ad arbitrio, e che lo stesso vale per μ. Anzi, che se abbiamo un'identità del tipo $D = \lambda a + \mu b$, con λ positivo e maggiore di b, si può ridurre il coefficiente di a fino a farlo diventare minore di b (al limite uguale a zero, se D = b, ossia b divide a). Ci si persuade facilmente che, escluso il caso banale D = b, esistono anzi una e una sola identità di Bézout del tipo:
$D = \lambda'a + \mu'b$, con λ' positivo e minore di b (corrispondentemente, μ' sarà

negativo, e il suo opposto minore di a), e un'unica altra del tipo:
$D = \lambda"a + \mu"b$, con $\mu"$ (che risulta uguale a $\mu'+a$) positivo e minore di a, e $\lambda"$ (che risulta uguale a $\lambda'-b$) negativo con opposto minore di b (potremmo chiamare *canoniche* queste due particolari e distinte identità di Bézout).

Complemento. A proposito di identità di Bézout canoniche, ci si persuade approfondendo un po' il discorso che quella ottenibile mediante l'algoritmo sopra indicato, a partire dalla catena di divisioni successive:
$a = q_1*b + r_1$, $b = q_2*r_1 + r_2$, $r_1 = q_3*r_2. + r_3$,..., $r_{n-2} = q_n*r_{n-1}. + r_n$, $r_{n-1} = q_{n+1}*r_n$.
è certamente una delle due tali (si supponga al solito a > b, e si escluda ancora il caso banale D = b; come abbiamo già accennato, risulterà λ positivo e μ negativo, o viceversa, a seconda della *parità* della lunghezza della catena, ossia, come pure presto si dirà, a seconda della parità della *profondità* del numero razionale $\frac{a}{b}$). Cominciamo con il notare che alla medesima identità di Bézout desumibile dalla catena di divisioni successive si può arrivare procedendo dall'alto verso il basso, anziché dal basso verso l'alto, per il che converrà di introdurre dal secondo passo della costruzione in poi **tre** diverse identità. Val forse la pena di mettere in evidenza esplicitamente prima che:
$D = MCD(a,b) = MCD(b,r_1) = MCD(r_1,r_2) = ... = MCD(r_{n-1},r_n) = r_n$,
e quindi che il procedimento descritto consiste sostanzialmente nel pervenire a D costruendo via via coppie di numeri che ammettono sempre D come MCD, ma diventano progressivamente più "piccole" (in un ovvio "ordinamento" stabilito componente per componente: si paragona il primo elemento di una coppia con il primo elemento di un'altra, e lo stesso si fa per i due secondi), fino al caso finale di una coppia (r_{n-1},r_n) tale che r_n divida r_{n-1}, e quindi risulti $D = r_n$.
<u>Primo passo</u>, $a = q_1*b + r_1$:
$a = q_1*b + r_1$ /// $r_1 = 1*a - q_1*b$
<u>Secondo passo</u>, $b = q_2*r_1 + r_2$:
$a = q_1*b + r_1 = q_1*(q_2*r_1 + r_2) + r_1 = (1+q_1q_2)*r_1 + q_1*r_2$ /// $b = q_2*r_1 + r_2$ ///
$r_2 = b - q_2*r_1 = b - q_2*(a-q_1b) = -q_2*a + (1+q_1q_2)*b$
[Data la catena strettamente discendente $\mathbf{a > b > r_1 > r_2 > ... > r_n}$ (n = lunghezza della catena meno 1 = profondità di $\frac{a}{b}$ è supposto essere un numero naturale), nella prima delle tre identità indicate si esprime a come combinazione lineare della coppia di numeri immediatamente successivi; la medesima cosa vale per quanto riguarda b; i resti r_1 *etc.* si esprimono invece sempre come combinazione lineare (ovviamente a coefficienti interi relativi, mentre nelle prime due identità i coefficienti sono numeri naturali) di a e di b.]
<u>Terzo passo</u>, $r_1 = q_3*r_2 + r_3$:
$a = (1+q_1q_2)*r_1 + q_1*r_2 = (1+q_1q_2)*(q_3r_2 + r_3) + q_1*r_2 =$
$= [q_3(1+q_1q_2)+q_1]*r_2 + (1+q_1q_2)*r_3$ /// $b = q_2*r_1 + r_2 = q_2*(q_3r_2 + r_3) + r_2 =$
$= (1+q_2q_3)*r_2 + q_2*r_3$ /// $r_3 = r_1 - q_3*r_2 = (1*a - q_1*b) - q_3*[-q_2*a + (1+q_1q_2)*b] = = (1+q_2q_3)*a - [q_1+q_3(1+q_1q_2)]*b$, <u>*etc.*</u>.
Si comprende insomma come si possano descrivere le tre identità ottenute
all'i-mo passo $r_{i-2} = q_i*r_{i-1} + r_i$ ($i \geq 3$) nel seguente modo:
$a = A_i*r_{i-1} + B_i*r_i$ /// $b = C_i*r_{i-1} + D_i*r_i$ /// $r_i = E_i*a + F_i*b$,
e tutto sta a comprendere cosa accade al passo successivo, cioè l'(i+1)-mo. Le identità in esame vanno modificate tenendo conto della nuova divisione:
$r_{i-1} = q_{i+1}*r_i + r_{i+1}$, con l'effetto che appunto:
$a = A_i*r_{i-1} + B_i*r_i = A_i*(q_{i+1}*r_i + r_{i+1}) + B_i*r_i = (q_{i+1}A_i+B_i)*r_i + A_i*r_{i+1}$.
Analogamente per b risulta:

$b = C_i*r_{i-1} + D_i*r_i = C_i*(q_{i+1}*r_i + r_{i+1}) + D_i* r_i = (q_{i+1}C_i+D_i)*r_i + C_i*r_{i+1}$,
mentre per il resto r_{i+1} si ottiene:
$r_{i+1} = r_{i-1} - q_{i+1}*r_i = (E_{i-1}*a + F_{i-1}*b) - q_{i+1}*(E_i*a + F_i*b) =$
$= (E_{i-1}-q_{i+1}E_i)*a + (F_{i-1}-q_{i+1}F_i))*b.$
Insomma, la sequenza dei coefficienti A_i, B_i è definibile *ricorsivamente* attraverso la regola: $A_{i+1} = q_{i+1}A_i + B_i$; $B_{i+1} = A_i$, la quale ha validità per ogni valore dell'indice $i \geq 1$ (in particolare, se $i > 1$, l'identità $A_{i+1} = q_{i+1}A_i + B_i$ si può riscrivere come $A_{i+1} = q_{i+1}A_i + A_{i-1}$). e permette di calcolarli tutti facilmente a partire da $A_1 = q_1$, $B_1 = 1$. Lo stesso sussiste per la sequenza dei coefficienti C_i, D_i, che è definibile *ricorsivamente* attraverso la regola:
$C_{i+1} = q_{i+1}C_i + D_i$; $D_{i+1} = C_i$, la quale ha validità adesso per ogni valore dell'indice $i \geq 2$ (in particolare, se $i > 2$, l'identità $C_{i+1} = q_{i+1}C_i + D_i$ si può riscrivere come $C_{i+1} = q_{i+1}C_i + C_{i-1}$). Notiamo che la definizione ricorsiva rimane invariata, ma si parte dai valori: $C_2 = q_2$, $D_2 = 1$.
Guardiamo infine a quella che più ci interessa delle tre identità ottenute ad ogni passo, ossia la $r_i = E_i*a + F_i*b$ (in cui possiamo semplicemente supporre $i \geq 1$; si tratta di quella che potremmo dire una sequenza di "identità di Bézout", l'ultima delle quali risulta l'identità desiderata). La definizione ricorsiva che controlla la sequenza dei coefficienti E_i, F_i è, per ogni $i > 1$: $E_{i+1} = E_{i-1} - q_{i+1}E_i$, e lo stesso vale per le F: $F_{i+1} = F_{i-1} - q_{i+1}F_i$. Si parte naturalmente adesso da: $E_1 = 1$, $E_2 = -q_2$, a cui si accompagnano le analoghe:
$F_1 = -q_1$, $F_2 = 1+q_1q_2$. Ciò permette di stabilire le identità che collegano i coefficienti E, F ai coefficienti A, C: $E_i = (-1)^{i-1}C_i$; $F_i = (-1)^iA_i$. (per ogni $i > 1$).
La dimostrazione è abbastanza agevole. Si verifica direttamente la validità delle identità in parola nel caso $i = 2$ ($E_2 = -C_2 = -q_2$; $F_2 = A_2 = 1+q_1q_2$), e poi si procede per induzione (si supponga quindi $i > 2$), utilizzando la definizione ricorsiva dianzi illustrata.
$E_{i+1} = E_{i-1} - q_{i+1}E_i = (-1)^{i-2}C_{i-1} - q_{i+1}(-1)^{i-1}C_i = (-1)^i(C_{i-1}+q_{i+1}C_i) = (-1)^iC_{i+1}$
(si rammenti che attualmente $C_{i+1} = q_{i+1}C_i + C_{i-1}$);
$F_{i+1} = F_{i-1} - q_{i+1}F_i = (-1)^{i-1}A_{i-1} - q_{i+1}(-1)^iA_i = (-1)^{i+1}(A_{i-1}+q_{i+1}A_i) = (-1)^{i+1}A_{i+1}$
(si rammenti che attualmente $A_{i+1} = q_{i+1}A_i + A_{i-1}$).
Ciò premesso, è chiaro che, pervenuti all'n-mo passo (quello in cui appare l'ultimo resto r_n diverso da zero) si ottiene l'identità di Bézout che andavamo cercando:
$r_n = D = E_n*a + F_n*b = \lambda a + \mu b$, ossia che: $\lambda = E_n = (-1)^{n-1}C_n$; $\mu = F_n = (-1)^nA_n$.
Tanta cura nei dettagli serve ad assicurare che, a parte il segno, λ è minore di b, allo stesso modo che μ è minore di a. Infatti:
$b = C_n*r_{n-1} + D_n*r_n \Rightarrow C_n < b$; $a = .A_n*r_{n-1} + B_n*r_n \Rightarrow A_n < a$.
(Informiamo che ritroveremo le medesime definizioni ricorsive di cui sopra in:
http://www.cartesio-episteme.net/mat/fraz-cont.doc,
dove ci occuperemo di *frazioni continue* e dei loro *convergenti*. Dato anche quanto se ne vedrà qui nel prossimo paragrafo, possiamo presentare subito la seguente identità:

$$\frac{a}{b} = \frac{A_n r_{n-1} + A_{n-1} r_n}{C_n r_{n-1} + C_{n-1} r_n} = \frac{A_n q_{n+1} r_n + A_{n-1} r_n}{C_n q_{n+1} r_n + C_{n-1} r_n} = \frac{A_n q_{n+1} + A_{n-1}}{C_n q_{n+1} + C_{n-1}} = \frac{A_{n+1}}{C_{n+1}},$$

la quale dimostra che il rapporto tra A_{n+1} e C_{n+1} esprime proprio la frazione $\frac{a}{b}$, ridotta però ai "minimi termini".) Concludiamo questo lungo complemento informando che nel prosieguo del corso si descriverà la situazione in esame attraverso gli *ideali* dell'*anello* dei numeri interi (relativi) *Z*. L'ideale *generato* da due numeri naturali a, b è appunto l'insieme delle loro combinazioni lineari a coefficienti interi relativi, ed è facile dimostrare che un siffatto ideale è necessariamente *principale*, ovvero è generato da un solo elemento (l'ideale è costituito insomma dalla totalità dei multipli di questo elemento). In effetti *tutti* gli ideali di *Z* sono principali, sicché si parlerà di un *anello a ideali principali* (sottolineiamo che converrà comunque occuparsi di anelli *commutativi* e *unitari* - ed eventualmente privi di *divisori dello zero*, nel qual caso si parla di *domini*, o *domini d'integrità* - sia per non dover distinguere tra multipli destri e multipli sinistri di un elemento, o tra ideali destri e ideali sinistri, sia per poter

sempre annoverare un elemento tra i multipli di se stesso). Di siffatti generatori ne esistono precisamente due, uno dei quali positivo, l'altro negativo, e si prova senza difficoltà che il generatore positivo (l'uso dell'articolo determinativo è adesso legittimo) coincide proprio con il MCD dei due numeri a, b. Gli algoritmi sopra descritti andranno allora intesi come "programmi" capaci di individuare tale generatore mediante semplici operazioni aritmetiche a partire dai due numeri assegnati, ma è chiaro che quanto abbiamo imparato *precede* in un ordine "naturale" la teoria degli anelli astratti, anzi, che fornisce una motivazione per lo studio di essa. Per esempio, si introduce la classe dei cosiddetti *domini bézoutiani*, ossia di quei domini tali che ogni loro ideale finitamente generato sia principale (un dominio bézoutiano tale che ogni suo ideale sia finitamente generato - a tale circostanza si fa riferimento dicendo che il dominio è *noetheriano* [In onore di Emily (Emmy) Noether (1882-1935), figura di una certa rilevanza nella storia dell'algebra del XX secolo.] - è quindi nient'altro che un dominio a ideali principali, ma l'interesse della definizione consiste precisamente nel fatto che esistono domini bézoutiani non noetheriani). L'anello Z e quello dei polinomi in una indeterminata sopra un *campo* K qualsiasi costituiscono due notevoli esempi di domini bézoutiani che sono anche noetheriani (addirittura di *domini euclidei*, con terminologia che prende le mosse proprio da quanto abbiamo in precedenza discusso), mentre un anello di polinomi in più indeterminate, nonostante i suoi coefficienti siano presi sempre in un campo, e sebbene presenti diverse "buone proprietà" che lo rendono simile a Z (per esempio, vi si può ancora parlare di *fattorizzazione unica* in polinomi "primi", e di MCD di due polinomi), cessa di essere bézoutiano, ancorché ogni suo ideale continui a risultare finitamente generato (tale ultimo risultato, relativo cioè alla noetherianità di un tale dominio, è conseguenza di un famoso *teorema di Hilbert*, il cosiddetto *teorema della base*).

Grazie all'identità di Bézout possiamo dimostrare finalmente il lemma di Euclide (e quindi il teorema fondamentale dell'aritmetica che da esso dipende, come abbiamo visto).

Dim. (del lemma di Euclide). Supponiamo infatti, ferme restando le notazioni, che $p \mid ab$, e che p non divida a. I numeri p e a risultano allora primi tra loro, ossia: $MCD(p,a) = 1$, e quindi potremo scrivere $\lambda p + \mu a = 1$ per certi numeri interi relativi λ, μ. Da questa identità si trae, moltiplicando entrambi i membri per b, e supponendo per esempio $ab = pk$ ($k \in N$):

$$b = \lambda pb + \mu ab = \lambda pb + \mu pk = p(\lambda b + \mu k),$$

ciò che esprime appunto b come un multiplo di p (è appena il caso di notare che il termine $\lambda b + \mu k$, a priori un numero intero relativo, è certamente un numero naturale), cvd.

(Si osservi volendo che la dimostrazione illustrata dimostra immediatamente, senza passare cioè attraverso il teorema fondamentale dell'aritmetica, il seguente enunciato "più generale": se a, b, p sono tre numeri naturali qualsiasi tali che $p \mid ab$, allora dall'ipotesi che a e p siano primi tra loro si deduce che p divide necessariamente b).

Essendo ormai ovvio che i divisori comuni di a e b sono tutti e soli i divisori di D (e quindi in numero finito, pari a $\psi(D)$), occupiamoci invece dei multipli

comuni ad a e b. Sussiste il seguente:

Teorema 7. m = mcm(a,b) = $\frac{ab}{D}$, e i multipli comuni ad a e b sono tutti e soli i multipli di m.

Dim. E' intanto evidente che la quantità $\frac{ab}{D} = a\frac{b}{D} = b\frac{a}{D}$ è un numero naturale, e che si tratta di un multiplo comune ad a e b. Proveremo adesso che, se viceversa n è un multiplo comune ad a e b, ossia n = ha = kb, per certi numeri naturali h, k, allora n è un multiplo di m, ossia, esiste un numero naturale t tale che n = tm. Bene, dato che D è il massimo comune divisore di a e b, risulterà a = Da', b = Db', con a', b' primi tra loro, sicché n = ha = kb $\Rightarrow \frac{h}{k} = \frac{b}{a} = \frac{b'}{a'}$. L'ultima frazione è espressa ai minimi termini, sicché, in virtù del teorema 1, h e k saranno equimultipli rispettivamente di b' e a': h = rb', k = ra', per qualche numero naturale r. Insomma, n = ha = rb'a = $ra\frac{b}{D}$ = kb = ra'b = $rb\frac{a}{D}$ = $r\frac{ab}{D}$ = rm, cvd.

4.

La rappresentazione di un numero razionale come "frazione continua limitata".

Dall'algoritmo euclideo delle divisioni successive abbiamo tratto finora **due** conseguenze interessanti: il calcolo del MCD, e l'identità di Bézout. Facciamo vedere che da esso si può dedurre un'altra identità istruttiva, alla quale premettiamo qualche considerazione generale. Ogni numero razionale positivo x (il discorso varrà tal quale per i numeri reali positivi) si potrà sempre scrivere in modo unico nella forma x = [x] + x', dove [x] $\in N_0$ è un numero intero positivo o nullo che si dice la *parte intera* di x, e viene scritto qualche volta come Int(x), mentre x' è un numero razionale compreso tra 0 (incluso) e 1 (escluso), che si dice la *parte decimale* di x, o anche la *mantissa* di x: x' = Mt(x) = x-Int(x). Risulta ovviamente Int(x) = 0 ses $0 < x < 1$, e Mt(x) = 0 ses x è un numero naturale.

[Si osservi che la restrizione ai soli numeri positivi o nulli dipende tra l'altro dalla circostanza che siamo abituati a scrivere per esempio -3,14, che significa -(3+0,14), e quindi -3-0,14 , anziché -4 + 0,86, sicché dovremmo "decidere" se porre Int(-3,14) = -3 oppure Int(-3,14) = -4, nel primo caso introducendo un'approssimazione *per eccesso* anziché *per difetto*, come invece più consueto.]

Ciò premesso, ripartiamo dalle identità (11), (12), (13), e riscriviamo l'ultima di

esse nella forma $r_2 = \frac{1}{q_3} r_1$ (procediamo quindi pure stavolta *dal basso verso l'alto*, a partire però dall'ultima identità). Sostituendo questa espressione nella (12) si ottiene:

$$b = q_2 * r_1 + \frac{1}{q_3} r_1 = (q_2 + \frac{1}{q_3}) r_1,$$

e da questa:

$$r_1 = \frac{1}{q_2 + \frac{1}{q_3}} b.$$

Possiamo adesso sostituire tale valore nella (11), fino a trovare:

$$a = q_1 * b + r_1 = = q_1 * b + \frac{1}{q_2 + \frac{1}{q_3}} b = (q_1 + \frac{1}{q_2 + \frac{1}{q_3}}) b,$$

ergo, l'identità alla quale miravamo:

$$(14) \quad \frac{a}{b} = (q_1 + \frac{1}{q_2 + \frac{1}{q_3}}).$$

Senza nessuna perdita di generalità, abbiamo dimostrato quindi metà del seguente:

Teorema 8. Ogni numero razionale $x = \frac{a}{b}$ ($a, b \in N$) tale che $x \geq 1$, ossia $a \geq b$, individua una n-pla ordinata ($n \in N$) di numeri naturali $(q_1,q_2,...,q_n)$, con $q_n \geq 2$ se $n \geq 2$, tale che risulti:

$$x = q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \frac{1}{... + \frac{1}{q_n}}}}.$$

Viceversa, ogni siffatta n-pla ordinata $(q_1,q_2,...,q_n)$, con $q_n \geq 2$ se $n \geq 2$, rimane associata nel modo indicato a uno ed un solo numero razionale $x > 1$, che denoteremo con il simbolo $x = [q_1;q_2,...q_n]$ (capiremo presto il significato di quel punto e virgola; se $n = 1$, scriveremo semplicemente $x = [q_1]$ - senza nessun problema in ordine ad utilizzo delle parentesi quadrate per definire la parte intera di un numero razionale o reale).

Il numero (n-1) $\in N_0$ si può chiamare la *profondità* di x. E' ovvio che la profondità di x è uguale a zero se e soltanto se x è un numero naturale.

Dim. Sostanzialmente manca soltanto di persuadersi che la rappresentazione dianzi determinata per il numero razionale x è da esso unicamente determinata, cioè che da un'identità del tipo (procediamo ancora in un caso particolare):

$$x = q_1 + \frac{1}{q_2 + \frac{1}{q_3}} = k_1 + \frac{1}{k_2 + \frac{1}{k_3 + \frac{1}{... + \frac{1}{k_n}}}}$$ si deduce n = 3, $q_1 = k_1$, $q_2 = k_2$, *etc.*.

(qui i coefficienti k_i rappresentano manifestamente dei numeri naturali, ma k_1 potrebbe essere a priori anche uguale a zero). Diviene naturalmente adesso fondamentale l'ipotesi che l'ultimo termine della "parte frazionaria" di una siffatta rappresentazione, quando presente, sia maggiore o uguale di 2, perché altrimenti dall'identità $\frac{1}{4} = \frac{1}{3 + \frac{1}{1}}$ non è possibile dedurre il risultato desiderato.

Bene, tutto si riduce a osservare che vale il seguente "**piccolo lemma**", che enunciamo in corso d'opera: un numero razionale del tipo $y = \frac{1}{m_1 + \frac{1}{m_2 + \frac{1}{... + \frac{1}{m_k}}}}$,

per certi numeri naturali m_i (i = 1,...,k, k un qualsiasi numero naturale), oltre che sempre diverso da zero, è minore o uguale ad 1, ed è uguale ad 1 ses k = 1 e $m_1 = 1$. La dimostrazione dell'asserto è pressoché immediata. Cominciamo con il fatto che y è diverso da zero, una circostanza abbastanza ovvia, ma che proviamo comunque per induzione su n. Se k = 1, il numero razionale $\frac{1}{m_1}$ non è zero. Se k > 1, il numero $z = \frac{1}{m_2 + \frac{1}{... + \frac{1}{m_k}}}$ non è zero per l'ipotesi induttiva, e quindi non è tale neppure il nostro $y = \frac{1}{m_1 + z}$. Ciò premesso, se k = 1, il numero razionale $\frac{1}{m_1}$ non è superiore a 1, e coincide con 1 ses $m_1 = 1$. Se $k \geq 2$, possiamo introdurre l'inverso di y (che sappiamo essere diverso da zero),

$y^{-1} = m_1 + \dfrac{1}{m_2 + \dfrac{1}{\ldots + \dfrac{1}{m_k}}}$. E' chiaro che $y^{-1} > m_1 \geq 1$ (perché il secondo addendo nel RHS della precedente identità, un termine che appare effettivamente in virtù dell'ipotesi ammessa $k \geq 2$, è diverso da zero), sicché abbiamo $y^{-1} > 1 \Rightarrow y < 1$, cvd. Torniamo adesso alla dimostrazione momentaneamente interrotta. L'identità $q_1 = k_1$ risulta stabilita poiché questi due numeri interi rappresentano la parte intera dei numeri razionali in discorso, sicché abbiamo necessariamente: $\dfrac{1}{q_2 + \dfrac{1}{q_3}} = \dfrac{1}{k_2 + \dfrac{1}{k_3 + \dfrac{1}{\ldots + \dfrac{1}{k_n}}}}$. Passando agli inversi dei due termini di tale identità, si ottiene $q_2 + \dfrac{1}{q_3} = k_2 + \dfrac{1}{\ldots + \dfrac{1}{k_n}}$, e si capisce che $n = 2$ non potrà essere, perché sappiamo che il LHS dell'identità non è un intero ($\dfrac{1}{q_3}$ è un numero razionale diverso da 0 e minore di 1 per ipotesi). Il termine $\dfrac{1}{k_3 + \dfrac{1}{\ldots + \dfrac{1}{k_n}}}$ compare quindi effettivamente, ed è un numero razionale minore di 1, in forza dell'ipotesi $k_n \geq 2$, e del "piccolo lemma". Quindi dall'identità in esame si deduce che q_2 e k_2 sono le rispettive parti intere dei numeri razionali in considerazione, sicché certamente $q_2 = k_2$, e $\dfrac{1}{q_3} = \dfrac{1}{k_3 + \dfrac{1}{\ldots + \dfrac{1}{k_n}}}$. Questa diventa, di nuovo uguagliando di nuovo gli inversi di ambo i membri, $q_3 = k_3 + \dfrac{1}{\ldots + \dfrac{1}{k_n}}$, e possiamo ripetere il ragionamento pervenendo finalmente alla conclusione. $n > 3$ non potrà essere, perché altrimenti il RHS dell'identità non sarebbe un numero intero, che compare al LHS. Quindi, $n = 3$ e $q_3 = k_3$, cvd.

Quanto precede ammette un'ovvia analoga enunciazione nel caso di numeri razionali positivi minori di 1, ossia dal caso $a < b$, bastando partire nel teorema 8 dal caso $q_1 = 0$. (Tra questi numeri non ce n'è nessuno che sia intero. Corrispondono biunivocamente ai numeri razionali maggiori di 1 tramite la corrispondenza $x \mapsto x^{-1}$. Il numero $x = 1$ riveste un ruolo particolare, poiché è l'unico numero razionale positivo tale che $x = x^{-1}$, e comunque volendo si potrà scrivere, con riferimento al simbolismo precedente introdotto, $x = [1]$.)

Enunciamo lo stesso l'ormai scontato relativo asserto.

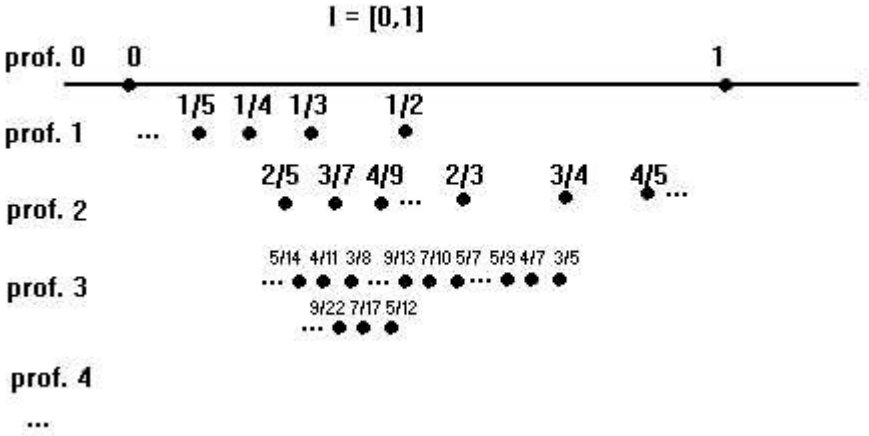
Teorema 9. Ad ogni numero razionale positivo $x = \frac{a}{b}$ ($a, b \in N$) tale che $x < 1$, ossia $a < b$, sono univocamente associabili un numero naturale n (che si dice la *profondità* di x) e un'unica n-pla ordinata di numeri naturali $(q_1,q_2,...,q_n)$, con $q_n \geq 2$, tali che risulti:

$$x = \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{... + \cfrac{1}{q_n}}}}.$$

Viceversa, ogni siffatta n-pla ordinata $(q_1,q_2,...,q_n)$, con $q_n \geq 2$, rimane associata nel modo indicato a uno ed un solo numero razionale x, $0 < x < 1$, che denoteremo come $x = [0;q_1,q_2,...q_n]$.

[Insomma, il teorema 9 rappresenta le mantisse non nulle dei numeri razionali, mentre nel teorema 8 si trova aggiunta a tali mantisse la parte intera.]

E' istruttivo osservare che il primo coefficiente q_1 nell'espansione di cui al teorema 1 fornisce il numero razionale $\frac{1}{q_1}$ di profondità 1 (cioè, un inverso di un numero naturale maggiore di 1) più vicino a x tra quelli maggiori o uguale di x. Analogamente, $\cfrac{1}{q_1 + \cfrac{1}{q_2}}$ rappresenta invece il numero razionale di profondità 2 più vicino a x tra quelli però minori o uguale di x, *etc.*. La seguente figura cerca di rappresentare, sebbene non perfettamente dal punto di vista dell'ordine tra i numeri indicati, la *stratificazione* dei numeri razionali x, $0 \leq x \leq 1$, in base alla loro profondità (si considera anche lo 0 di profondità 0, come tutti gli interi).



- **Profondità 0**: 0 e 1, mentre naturalmente, al di fuori dell'intervallo chiuso I, ci sono 2, 3,... .
- **Profondità 1**: gli inversi di 2, 3,..., ossia 1/2 > 1/3 > 1/4 > 1/5 >...

e naturalmente, al di fuori di I:
1+1/2 =3/2 > 1+1/3 = 4/3 > 1+1/4 = 5/4 > 1+1/5 = 6/5 >...
2+1/2 = 5/2 > 2+1/3 = 7/3 > 2+1/4 = 9/4 > 2+1/5 = 11/5 >...
3+1/2 > 3+1/3 > 3+1/4 > 3+1/5 >... *etc.*.
- **Profondità 2** Gli inversi dei numeri riportati nelle righe precedenti al di fuori di I: 2/3 < 3/4 < 4/5 < 5/6 <..., 2/5 < 3/7 < 4/9 < 5/11 <..., *etc.*
e naturalmente, al di fuori di I:
1+2/3 = 5/3 < 1+3/4 = 7/4 < 1+4/5 = 9/5 < 1+5/6 = 11/6 <...
1+2/5 = 7/5 < 1+3/7 = 10/7 < 1+4/9 = 13/9 < 1+5/11 = 16/11 <...
...
2+2/3 = 8/3 < 2+3/4 = 11/4 < 2+4/5 = 14/5 < 2+5/6 = 17/6 <...
2+2/5 = 12/5 < 2+3/7 = 17/7 < 2+4/9 = 22/9 < 2+5/11 = 27/11 <...
e così via...

[Vale la pena di informare da ultimo che era abitudine per esempio degli egiziani di cercare di rappresentare la mantissa di un numero razionale (positivo non intero) come somma di numeri razionali minori di 1 e di profondità 1, ossia di inversi di numeri interi maggiori di 1. E' ovvio per esempio che:
$\frac{3}{7} = \frac{1}{7}+\frac{1}{7}+\frac{1}{7}$, ma il "gioco" delle cosiddette *frazioni egiziane* consiste nel trovare decomposizioni con denominatori distinti, e quindi per esempio:
$\frac{3}{7} = \frac{1}{7} + \frac{2}{7} = \frac{1}{7} + \frac{1}{4} + \frac{1}{28}$ (usando per $\frac{2}{7}$ la decomposizione che viene offerta nel *papiro di Ahmes*, circa 1650 AC - detto anche *papiro di Rhind*, dal nome dell'antiquario scozzese che lo acquistò in Egitto nel 1858), e poi più "corte" possibile, o eventualmente con denominatori più piccoli possibile, *etc.*, un argomento interessante e forse ancora non del tutto esplorato.]

5.

La costruzione di Q^+ per via geometrica parte dalla considerazione del semigruppo Σ dei *segmenti liberi* dello spazio ordinario **S**, o se si preferisce della *retta ordinaria* **R** (si badi bene alla distinzione tipografica tra **R** e *R*). In questo secondo caso si tratta semplicemente di classi di equivalenza di segmenti di **R**, dove l'equivalenza è quella indotta dal *gruppo delle traslazioni* di **R**. Diciamone brevemente qualcosa in più. Si prendono le mosse dall'insieme dei segmenti di **R**, indichiamolo brevemente con Seg(**R**), i sottoinsiemi individuati da un'arbitraria coppia (non ordinata) di punti distinti, che si chiamano *estremi* del segmento. I segmenti sono sottoinsiemi della retta che, in quanto alla loro "natura", sono concepiti "rigidi", ma il termine non deve indurre in equivoco: non c'è nessun riferimento alla "realtà materiale", quella di cui si sta parlando è una "realtà ideale". Essi, come i punti, non sono manifestamente dei "numeri", sebbene si possano sempre "confrontare" tra loro, e *in qualche caso* (segmenti *contigui*, cioè con un solo vertice comune) "sommare". La possibilità della citata operazione di confronto si esplicita attraverso la constatazione che l'intuizione

dello spazio riconosce in Seg(**R**) l'esistenza di una relazione ρ di *preordine totale* naturale (non vale cioè la proprietà antisimmetrica, abbiamo solamente riflessività e transitività), collegata alla relazione d'*ordine non totale* di *inclusione* (inclusione insiemistica, di origine perciò puramente "logica") e al concetto di *traslazione*. Un segmento $\overline{ab}$ sarà minore o uguale di un segmento $\overline{cd}$ se esiste una traslazione τ di **R** tale che $\tau(\overline{ab})$ è incluso in $\overline{cd}$, mentre naturalmente una traslazione di **R** rimane definita come una particolare corrispondenza biunivoca τ di **R** in sé (o, se si preferisce, un automorfismo di **R** nella categoria degli spazi totalmente ordinati - si fissi adesso arbitrariamente un *verso* di **R**), che induce un morfismo d'ordine (automorfismo) anche in Seg(**R**): $\overline{ab} \leq \overline{cd} \Rightarrow \tau(\overline{ab}) \leq \tau(\overline{cd})$, per ogni coppia di segmenti di **R**. Cioè preordine totale naturale su Seg(**R**) e traslazioni sono concetti strettamente interconnessi, uno definisce l'altro, senza possibilità, ci sembra, di poter decidere quale dei due "venga prima". Dovendo scegliere, ci piace pensare che la nostra mente "veda" nel gruppo delle traslazioni di **R** un particolare sottogruppo (strettamente 1-transitivo) di tutte le corrispondenze biunivoche di **R** in sé grazie a cui effettua il riconoscimento di chi tra due segmenti sia "più piccolo" di un altro, *sed de hoc satis*. La relazione di preordine appena descritta non è manifestamente una relazione d'ordine, e induce conseguentemente su Seg(**R**) una relazione d'equivalenza non banale (per la quale nel linguaggio comune, e della geometria classica, si usa il termine *uguaglianza*, che rischia l'introduzione di un ulteriore fraintendimento, data l'affinità semantica tra uguaglianza e identità, meglio quindi *congruenza*), che permette di costruire il relativo insieme quoziente Σ, i cui elementi diremo *segmenti liberi* (o *astratti*) di **R**.

[Si noti che non appare difficile trasportare le considerazioni sopra esposte al caso dell'intero spazio tridimensionale **S**, mediante l'introduzione di una più ricca fenomenologia di "movimenti rigidi" dell'ambiente - traslazioni, *rotazioni*, e loro prodotti - con l'effetto di avere anche in questo caso un insieme Seg(**S**), e un insieme quoziente che sarà palesemente "naturalmente isomorfo" a Σ. Vale a dire $\Sigma_{\mathbf{S}} \cong \Sigma_{\mathbf{R}}$, con simbolismo che ci pare *autoesplicativo*.]

L'insieme Σ così introdotto possiede una relazione d'ordine naturale (*ereditata* dal preordine naturale in Seg(**R**)), ma il bello è che esso ammette anche una *struttura algebrica* naturale, che rimane invece assente da enti geometrici quali **R**, **P**, **S** (che sono soltanto sostegni di strutture d'ordine o topologiche; **P** designa ovviamente il *piano ordinario*). Si può definire infatti la somma di due segmenti liberi semplicemente *giustapponendo* due loro rappresentanti, prendendone l'unione insiemistica, e infine la relativa classe di equivalenza. Un'operazione mentale che corrisponde evidentemente alla "somma" di due "cammini" (di tipo analogo è la somma di vettori, nella retta o nello spazio).

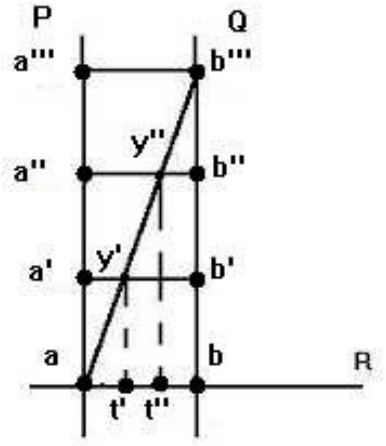
Σ è quindi il sostegno di un semigruppo abeliano (additivamente scritto) alquanto particolare, che riassume in sé tutte le proprietà geometriche delle quali

si ha bisogno al fine di descrivere precisamente il procedimento di *misura* di un segmento rispetto a un altro, come vedremo nel paragrafo successivo. Tale semigruppo risulta assai "simile" ad *N*, poiché è privo di elemento neutro, regolare, ordinato, archimedeo, *etc.*, ma ha in più una proprietà che risulterà fondamentale sia per la teoria che abbiamo in mente: la divisibilità. Vale a dire, per ogni numero naturale n e ogni elemento $\alpha \in \Sigma$, l'equazione (nella ξ):

$$n\xi = \alpha$$

ammette qualche soluzione in Σ. Essa è manifestamente unica, perché $n\xi = n\eta = \alpha$ implica necessariamente $\xi = \eta$. Se fosse infatti $\xi > \eta$, avremmo per esempio $n\xi > n\eta$, data la *compatibilità* tra struttura d'ordine e struttura algebrica: $\forall\ \alpha, \beta, \gamma, \delta \in \Sigma, (\alpha \leq \beta) \wedge (\gamma \leq \delta) \Rightarrow \alpha + \gamma \leq \beta + \delta$.

La divisibilità, pur esprimendosi in modo puramente algebrico, ha naturalmente un'origine geometrica (che fa ricorso ad altre proprietà della retta, ma in special modo alla sua possibilità di *immersione* nel piano ordinario **P**; quindi, alle caratteristiche della retta derivanti da proprietà della geometria piana). Illustriamo in quel che segue il procedimento che individua la soluzione dell'equazione precedente nel caso n = 3, ossia l'operazione di *tricotomia* di un segmento arbitrario (non libero) $\overline{ab}$ di **R**.



Si considera un qualsiasi segmento $\overline{ab}$ della retta ordinaria **R**, pensata però *immersa* nel piano ordinario **P** tramite una retta arbitraria R di **P**). Dal punto a si traccia la perpendicolare P alla retta R, e su P si considera il segmento $\overline{aa'}$ uguale ad $\overline{ab}$. Quindi lo si riporta tre volte di seguito, costruendo i segmenti $\overline{aa'}$, $\overline{a'a''}$, $\overline{a''a'''}$. Sulla retta Q, perpendicolare ad R nel punto b, si considerano i punti b', b'', b''', corrispondenti rispettivamente di a', a'', a''' per proiezione perpendicolare. Si prende infine in esame la diagonale $\overline{ab'''}$ del rettangolo abb'''a'''. Essa interseca il segmento $\overline{a'b'}$ nel punto y', il segmento $\overline{a''b''}$ nel punto y'', e le proiezioni perpendicolari di y', y'' sulla retta R, che abbiamo detto rispettivamente t' e t'',

forniscono la desiderata "tricotomia" del segmento $\overline{ab}$, ossia: $\overline{ax'} \equiv \overline{x'x''} \equiv \overline{x''b}$ (il simbolo ≡ si riferisce alla relazione d'equivalenza indotta dal gruppo delle traslazioni, che, come abbiamo già detto, si dice con termine geometrico proprio congruenza), e $\overline{ax'} \cup \overline{x'x''} \cup \overline{x''b} = \overline{ab}$. In altre parole, se sull'*asse* perpendicolare si rappresenta il numero intero n, su quello di partenza appare il suo "inverso" 1/n.

In virtù dell'unicità della soluzione in discorso, per ogni $n \in N$ e ogni $\alpha \in \Sigma$, sarà lecito introdurre il segmento libero $\frac{1}{n}\alpha$, che si può dire l'*n-ma parte* di α (un *sottomultiplo* di α tramite il numero naturale n, allo stesso modo che $n\alpha$ è un *multiplo* di α, sempre tramite il numero n).

E' facile persuadersi che siamo di fronte a due *azioni* (unitarie) del semigruppo moltiplicativo $(N,*)$ su Σ:

$$N\times\Sigma \to \Sigma \quad \text{(multiplo)}$$
$$(n,\alpha) \mapsto n\alpha$$

$$N\times\Sigma \to \Sigma \quad \text{(sottomultiplo)}$$
$$(n,\alpha) \mapsto \frac{1}{n}\alpha$$

tali che, "banalmente":

$$m(\frac{1}{n}\alpha) = \frac{1}{n}(m\alpha) = \frac{m}{n}\alpha$$

(l'ultima identità va intesa come una *definizione* del "simbolo" $\frac{m}{n}\alpha$).

In particolare: $n(\frac{1}{n}\alpha) = \frac{1}{n}(n\alpha) = \frac{n}{n}\alpha = 1\alpha = \alpha$, $n(\frac{m}{n}\alpha) = m\alpha$, *etc.*.

Sarebbe facile a questo punto constatare che un'eventuale identità del tipo:

$$\frac{m}{n}\alpha = \frac{m'}{n'}\alpha$$

è *indipendente* dal segmento α, e che essa sussiste se, e soltanto se, vale l'identità $\frac{m}{n} = \frac{m'}{n'}$ tra i "corrispondenti" numeri razionali (corrispondenti cioè alle coppie ordinate di numeri naturali che appaiono nel contesto), ossia se, e soltanto se, si verifica: $mn' = m'n$. Insomma, partendo adesso da un'azione insiemistica (in effetti, un'azione unitaria del semigruppo moltiplicativo *prodotto*

diretto $(N,*)\times(N,*)$), ma di chiara interpretazione geometrica:

$$(N\times N)\times\Sigma \to \Sigma$$
$$((m,n),\alpha) \mapsto \frac{m}{n}\alpha,$$

e andando a indagare quando due coppie ordinate di numeri naturali (m,n) e (m',n') *agiscono allo stesso modo* su Σ (cioè, appunto, $\frac{m}{n}\alpha = \frac{m'}{n'}\alpha$ per ogni segmento libero α in Σ - o per uno soltanto, è la stessa cosa!), si ritrova la stessa relazione di equivalenza ρ descritta nel paragrafo 1). Proponiamo una serie di *verifiche* istruttive (per un fissato $\alpha \in \Sigma$):

(15) $\frac{m}{n}\alpha = \frac{m'}{n'}\alpha \Leftrightarrow \frac{n}{m}\alpha = \frac{n'}{m'}\alpha$

(16) $\frac{m}{n}\alpha = \frac{m'}{n}\alpha \Leftrightarrow m = m'$

(17) $\frac{m}{n}\alpha = \frac{km}{kn}\alpha$ (per ogni numero naturale k),

la cui analogia con le (1), (2), (3) non sfuggirà di certo allo studente.

Fornita dunque per questa via un'interpretazione geometrica della relazione di equivalenza ρ - ma non ancora una costruzione geometrica di Q^+, poiché siamo sempre rimasti alla $Q^+ \subset P(N\times N)$ - conviene ormai procedere con lo studio della *teoria generale della misura* sul semigruppo Σ, introducendo cioè:

- una relazione d'equivalenza (diciamola ancora ρ, con leggero abuso di notazione, in quanto è legata a una *proporzionalità*, sebbene tra coppie ordinate di segmenti liberi, e non di numeri naturali) in $\Sigma\times\Sigma$;

- l'insieme quoziente $\Sigma\times\Sigma/\rho$, che verrà ad essere l'insieme dei *numeri reali positivi* R^+; quindi, dal punto di vista della "natura" di detti numeri, sussiste l'inclusione insiemistica: $R^+ \subset P(\Sigma\times\Sigma)$.

Saremo *costretti* allora a riconoscere che tra i numeri reali ve ne sono alcuni che possono dirsi *reali razionali* (corrispondenti al caso di coppie ordinate di segmenti tra loro *commensurabili*, tali cioè che uno sia un multiplo di un sottomultiplo dell'altro), il cui insieme sarà allora un *vero* sottoinsieme di R^+, e sarà lecito indicare con Q^+, dal momento che risulterà canonicamente isomorfo all'insieme Q^+ precedentemente costruito per via aritmetica (l'isomorfismo in

oggetto sarà in generale un isomorfismo di *tutte* le strutture naturali di cui i numeri razionali sono il supporto, algebriche e d'ordine). Risulterà insomma:

$$Q^+ \subset R^+ + \subset \mathrm{P}(\Sigma\times\Sigma), \text{ e non più } Q^+ \subset \mathrm{P}(N\times N).$$

La costruzione geometrica dei numeri reali positivi (che comprende come caso particolare quella dei numeri razionali positivi!), e l'introduzione delle relative strutture naturali - compresa l'*azione* (di gruppo moltiplicativo) $R^+\times\Sigma \to \Sigma$ che è preludio alla nozione di *spazio vettoriale reale* - esula dal modesto ambito di questo corso introduttivo di Algebra, ma nel prossimo paragrafo se ne darà comunque rapido un cenno.

6.

Si è ormai compreso che una costruzione geometrica naturale dei numeri reali positivi (quelli con segno proverranno dalla considerazione di *vettori* anziché di segmenti, compreso il *vettore nullo*) deve prendere le mosse dal semigruppo Σ. La quinta definizione del libro V degli *Elementi* di Euclide riconduce precisamente la nozione di *misura* di un segmento libero α rispetto a un segmento libero β a una relazione di equivalenza ρ (*proporzionalità*) nell'insieme delle coppie ordinate $\Sigma\times\Sigma$, sicché tutta la costruzione assomiglia formalmente a quella già illustrata nel paragrafo 1. La misura di α rispetto a β è la stessa che la misura di γ rispetto a δ, in simboli:

$\alpha : \beta = \gamma : \delta$ (in parole: α sta a β come γ sta a δ)

se, e soltanto se, per ogni coppia ordinata (m,n) di numeri naturali, risulta:

(18) $\quad m\alpha < n\beta \Rightarrow m\gamma < n\delta,\ m\alpha > n\beta \Rightarrow m\gamma > n\delta,\ m\alpha = n\beta \Rightarrow m\gamma = n\delta.$

La procedura logica che guida la precedente definizione è abbastanza naturale. Si itera α un certo numero arbitrario m di volte (m un elemento di *N*), analogamente β un certo numero n di volte, fino a produrre $m\alpha = \alpha+\alpha+\ldots$ m volte, e $n\beta = \beta+\beta+\ldots$ n volte. Si fa altrettanto con γ e δ rispettivamente, in modo da produrre cioè pure $m\gamma$ e $n\delta$. Orbene, se risulta $m\alpha < n\beta$, deve essere anche $m\gamma < n\delta$; se risulta invece $m\alpha > n\beta$, deve essere anche $m\gamma < n\delta$; infine, se accade che sia $m\alpha = n\beta$, deve essere anche $m\gamma = n\delta$. Nell'ultimo caso α e β si dicono tra loro *commensurabili*, e la misura di α rispetto a β, si può rappresentare semplicemente con il numero reale razionale $\frac{n}{m}$. Se α e β sono tra loro *incommensurabili* (l'intuizione ordinaria dello spazio esige l'esistenza di tali coppie di segmenti, ossia di tali punti della retta; si pensi al celebre caso della diagonale e del lato di un quadrato), il relativo *numero reale* (esprimente cioè la misura di α rispetto a β) si dice *irrazionale* (vale a dire, *reale non razionale*).

[L'attenzione posta nei confronti di coppie di segmenti anche tra loro incommensurabili può essere considerata la *novità* all'origine dell'indagine greca sulla geometria ("razionalizzazione della geometria", o "geometria di precisione", da Pitagora ad Euclide attraverso Eudosso), del tutto lontana dalle "applicazioni pratiche" che caratterizzano le matematiche elaborate da altre culture, almeno per quanto finora conosciuto.]

Riportiamo per comodità dello studente (ma anche per apprezzare i vantaggi offerti dal moderno sintetico linguaggio simbolico) la famosa definizione nell'originale euclideo, secondo la traduzione che ne viene fornita in: *The thirteen books of Euclid's Elements*, Sir Thomas L. Heath, Dover Publications Inc., New York, 1956, vol. II, p. 114:

«Magnitudes are said to be in the same ratio, the first to the second and the third to the fourth, when, if any equimultiples whatever be taken of the first and third, and any equimultiples whatever of the second and fourth, the former equimultiples alike exceed, are alike equal to, or alike fall short of, the latter equimultiples respectively taken in corresponding order».

α

Essendo palese che ρ è effettivamente una relazione d'equivalenza, la *misura* $\mu(\alpha,\beta)$ viene ad essere definita come la ρ-classe di equivalenza $[(\alpha,\beta)]$, in simboli anche $\frac{\alpha}{\beta}$. Ossia, un numero reale (positivo) non è altro che una *frazione*, in cui numeratore e denominatore sono segmenti liberi dello spazio ordinario. E' ovvio che si potrà porre $1 = \frac{\alpha}{\alpha}$, $2 = \frac{\alpha+\alpha}{\alpha}$, *etc.*, qualunque sia α. Cioè, esiste un'*immersione naturale* di N in R^+, non tale però da costringerci a considerare i numeri naturali un caso particolare di numeri reali, anzi. Analogamente, si porrà $\frac{1}{2} = \frac{\alpha}{\alpha+\alpha}$, $\frac{3}{2} = \frac{\alpha+\alpha+\alpha}{\alpha+\alpha}$, *etc.*. La relazione $m\alpha < n\beta$ si interpreta con la disuguaglianza: $\frac{m}{n} < \frac{\beta}{\alpha}$ (ossia il numero razionale $\frac{m}{n}$ è un'*approssimazione inferiore* del numero reale $\frac{\beta}{\alpha}$), oppure con la disuguaglianza: $\frac{n}{m} > \frac{\alpha}{\beta}$ (ossia il numero razionale $\frac{m}{n}$ è un'*approssimazione superiore* del numero reale $\frac{\alpha}{\beta}$), *etc.*.

7.

Aggiungiamo al precedente paragrafo un'appendice storico-filosofica, ma non solo. Vale la pena infatti aggiungere che per la fondamentale relazione di equivalenza in esame abbiamo utilizzato la descrizione offerta da Euclide. Pur

non essendoci dubbi sulla correttezza contenutistica del procedimento che definisce in questa maniera l'insieme numerico dei reali (positivi), si potrebbe però volendo porre la questione se quella euclidea ne sia l'illustrazione più *adeguata*. Tale interrogativo venne formulato da Galileo Galilei, in un'opera pressoché ignorata. Verso i suoi ultimi anni, il famoso scienziato dedicò infatti un breve scritto al Libro V degli *Elementi* di Euclide [Principio di giornata aggiunta, Giornata quinta, ai *Discorsi e Dimostrazioni matematiche intorno a due nuove Scienze*, "Sopra le definizioni delle proporzioni d'Euclide". Volendo essere precisi, tale scritto non fu però incluso nella prima edizione dei *Discorsi...*, stampata nel 1638 a Leida, in Olanda, per i tipi del celebre editore Ludovico Elzeviro, essendo rimasto incompiuto. Galileo ne dettò quello che poté ad Evangelista Torricelli verso la fine del 1641, e quindi proprio nelle ultime settimane della sua vita. Fu pubblicato solo trent'anni più tardi, a cura di Vincenzo Viviani (1622-1703), un altro discepolo di Galileo: *Quinto libro degli Elementi di Euclide, ovvero Scienza universale delle proporzioni spiegate colla dottrina del Galileo, con nuov'ordine distesa e per la prima volta pubblicata da Vincenzo Viviani*, Firenze, 1674. Entrò poi a far parte stabile delle successive edizioni dei *Discorsi...*, a cominciare da quella fiorentina del 1718.], fornendo degli spunti di meditazione che possono essere considerati attuali anche ai nostri giorni (o meglio, specialmente ai nostri giorni!). Brevemente, per Galileo è in primo luogo evidente che il problema relativo al quando due coppie di grandezze debbano considerarsi tra loro proporzionali, pur appartenendo alla sfera di quei concetti che sono da ritenersi alla base di atti comuni a ogni umano intelletto («avendo il lettore concepito già nell'intelletto che cosa sia la proporzione fra due grandezze [...] mi sforzerò di secondare con la difinizione delle proporzioni il concetto universale degli uomini anche ineruditi nella geometria»), non possa essere riconosciuto come un dato primitivo ("immediato"), e sia invece necessario discuterlo con attenzione. Inoltre, l'autore ritiene che la definizione proposta da Euclide, ancorché logicamente ineccepibile, non risponda completamente alle esigenze di chiarezza inerenti all'importanza della questione. Tutti e tre i protagonisti del dialogo galileiano confessano tale insoddisfazione: Sagredo («Questa e' una certa ambiguità che io o' sempre avuta nella mente intorno alla quinta difinizione del quinto libro d'Euclide [...] non restai con quella chiarezza che avrei desiderato nella predetta proposizione»); Simplicio («Non ebbi mai il più duro ostacolo di questo in quella poca di geometria che io studiai già nelle scuole da giovanetto»); e infine lo stesso Salviati-Galileo («Io poi confesso che per qualche anno dopo aver istudiato il V libro d'Euclide, restai involto con la mente nella stessa caligine»). Il fisico pisano applica allora alla definizione euclidea di proporzione un criterio che dovrebbe essere tenuto sempre presente (non solo in matematica), relativo alla necessità di operare una distinzione tra asserzioni le quali, pur "logicamente equivalenti", si presentino in una sequenza temporale naturale in momenti diversi dell'indagine della ragione, tanto da potersi considerare l'una come una derivazione dell'altra, *ma non viceversa*.

«Per dare una difinizione delle suddette grandezze proporzionali la quale produca nell'animo del lettore qualche concetto aggiustato alla natura di esse grandezze proporzionali, dovremmo prendere una delle loro passioni, ma però la più facile di tutte e quella per appunto che si stimi la più intelligibile anco dal volgo non introdotto nelle matematiche [...] Così fece Euclide stesso in molt'altri luoghi. Sovvengavi che egli non disse, il cerchio essere una figura piana, dentro la quale segandosi due rette, il rettangolo sotto le parti dell'una sia sempre uguale al rettangolo sotto le parti dell'altra; ovvero, dentro la quale tutti i quadrilateri abbiano gli angoli opposti uguali a due retti. Quand'anche così avesse detto, sarebbero state buone difinizioni: ma mentre egli sapeva un'altra passione del cerchio, più intelligibile della precedente e più facile da formarsene concetto, chi non s'accorge che egli fece assai meglio a mettere avanti quella più chiara e più evidente come difinizione, per cavar poi da essa quell'altre più recondite e dimostrarle come conclusioni?».

Galileo si pone insomma, in relazione alla definizione V del Libro V degli *Elementi* di Euclide, sostanzialmente le stesse domande che più tardi formulerà in analoga circostanza il matematico inglese Augustus De Morgan (vedi il libro di Heath sopra citato, stesso volume, p. 122):

«What right had Euclid, or any one else, to expect that the preceding most prolix and unwieldy statement should be received by the beginner as the definition of a relation the perception of which is one of the most common acts of his mind, since it is performed on every occasion where similarity or dissimilarity of figure is looked for or presents itself? If the preceding question should be clearly answered, how can the definition of proportion ever be used; or how is it possible to compare every one of the infinite number of multiples of *A* with every one of the multiples of *B*?».

Ma mentre De Morgan cercò soprattutto di chiarire, e quindi di giustificare, l'approccio euclideo alla questione (il brano infatti così prosegue: «To the first question we reply that not only is the test proposed by Euclid tolerably simple, when more closely examined, but that it is, or might be made to appear, an easy and natural consequence of those fundamental perceptions with which it may at first seem difficult to compare it»), Galileo propose una propria definizione di uguali proporzioni da opporre a quella dell'antico maestro.

Accenniamo al procedimento (che rimanda chiaramente al concetto di "frazione continua illimitata", e alla relativa convergenza, quindi a una generalizzazione dei temi esposti nel paragrafo 4) con cui Galileo «ritenne di correggere dal punto di vista didattico-intuitivo la definizione V» (secondo Attilio Frajese, *Attraverso la storia della matematica*, Veschi, Roma, 1962, p. 158), rimandando per ulteriori commenti e approfondimenti ad altri luoghi presenti nel sito dello scrivente (in esso è riportato anche l'intero dialogo galileiano), e ribadendo che ciò che rimane comunque degno di nota è il fatto che Galileo fu spinto a operare

tale "correzione", e che il suo tentativo stimola noi a distanza di secoli a comprendere le motivazioni che lo ispirarono (e a imitare il suo *coraggio* nel discutere i "tabù" del proprio tempo, da Aristotele ad Euclide). Così, vengono alla mente altre possibili descrizioni geometriche della relazione d'equivalenza ρ, diverse sia da quella di Euclide sia da quella di Galileo, una delle quali presenteremo nel paragrafo successivo.

Ciò premesso, Galileo comincia con l'osservare che se $\alpha = \beta$, deve essere anche $\gamma = \delta$, e che se $\alpha > \beta$ deve essere anche $\gamma > \delta$, invitando allora a considerare sempre le *antecedenti* maggiori delle *conseguenti*. Il passo successivo invita al confronto tra le coppie $(\alpha\text{-}\beta,\beta)$ e $(\gamma\text{-}\delta,\delta)$, nella evidente constatazione che se $\alpha : \beta = \gamma : \delta$, e valgono le disuguaglianze supposte, allora deve essere anche:

$$\alpha\text{-}\beta : \beta = \gamma\text{-}\delta : \delta.$$

Secondo le parole di Galileo, l'*eccesso* di α su β rispetto a β deve essere *simile* all'eccesso di γ su δ rispetto a δ. Resta adesso soltanto da iterare il ragionamento, aggiungendo una nuova banale ma importante osservazione. Se risulta $\alpha\text{-}\beta = \beta$, dovrà risultare anche $\gamma\text{-}\delta = \delta$, mentre se $\alpha\text{-}\beta > \beta$, dovrà risultare $\gamma\text{-}\delta > \delta$ (se così non fosse, la relazione di proporzionalità tra i quattro segmenti α, β, γ, δ in discorso non potrebbe sussistere). Il caso $\alpha\text{-}\beta < \beta$ dovrà corrispondere allora al caso $\gamma\text{-}\delta < \delta$, e quando ciò si verifica basterà scambiare tra di loro le antecedenti e le conseguenti, andando a indagare quindi la proporzionalità tra β, $\alpha\text{-}\beta$, δ, $\gamma\text{-}\delta$, ovviamente nell'ordine indicato. Si invita allora a prendere in considerazione l'eccesso $(\alpha\text{-}\beta)\text{-}\beta = \alpha\text{-}2\beta$ rispetto a β, e a metterlo in relazione con il corrispondente eccesso $\gamma\text{-}2\delta$ rispetto a δ. Se $\alpha\text{-}2\beta = \beta$ *etc.*, è ormai palese come si dovrà andare avanti, allo stesso modo che è chiaro che Galileo esegue soltanto *alcuni* dei *test* proposti da Euclide per l'accertamento della validità di una relazione di proporzionalità. Il procedimento suggerito corrisponde a una serie di *divisioni euclidee successive*, però fra segmenti e non fra numeri naturali, e questa è un'altra delle *analogie* che abbiamo notato sussistere fra N e Σ, riconducibile peraltro manifestamente alla "archimedeicità" di entrambi i semigruppi in questione, e alla seguente fondamentale proprietà che collega ordine e struttura algebrica:

(19) $\forall\ \alpha, \beta \in \Sigma, \alpha > \beta \Leftrightarrow \exists\ (!)\ \xi \in \Sigma$ tale che $\alpha = \beta + \xi$
(l'asserto vale tal quale in N).

Infatti, a partire da $\alpha > \beta$ si continuano a considerare multipli di β fino a che si incontra il primo di essi che supera α, insomma si scrive:

(i) $\alpha = q_1\beta + \rho_1$,

dove q_1 è un numero naturale univocamente determinato, coincidente con la parte intera di $\frac{\alpha}{\beta}$, e $\rho_1 < \beta$ (divisione *per difetto*) è un segmento libero pur esso univocamente determinato (conviene qui supporre che il *resto* possa anche essere uguale a *zero*, per trattare due casi come uno solo; adesso non c'è bisogno di $*$, poiché la differenza tra numeri e segmenti è anche tipograficamente evidente). Invero, giunti a questo punto, $\alpha - q_1\beta = \rho_1$ non è più maggiore di β, e bisogna scambiare tra loro le antecedenti con le conseguenti, andando a "dividere" β per ρ_1, *etc.*.

Prima di discutere a mo' di esempio gli (eventuali) due passi successivi, conviene formulare subito un'osservazione, atta a provare che il procedimento sarà, come è intuitivo attendersi, *convergente*. Il resto $\rho_1 < \beta$ soddisfa anche la disuguaglianza $\rho_1 < \frac{1}{2}\alpha$. Se $\beta \leq \frac{1}{2}\alpha$ l'asserto è ovvio (conseguenza immediata della $\rho_1 < \beta$), se $\beta > \frac{1}{2}\alpha$ è altrettanto ovvio, poiché $\rho_1 \leq \alpha - \beta \Rightarrow \rho_1 < \frac{1}{2}\alpha$.

Iteriamo adesso il procedimento ideato da Galileo, assumendo β come dividendo e ρ_1 come divisore. Risulterà:

(ii) $\beta = q_2\rho_1 + \rho_2$, con $\rho_2 < \rho_1$ e $\rho_2 < \frac{1}{2}\beta < \frac{1}{2}\alpha$.

Se ρ_2 è zero, $\rho_1 = \frac{1}{q_2}\beta$, $\alpha = q_1\beta + \frac{1}{q_2}\beta = (q_1 + \frac{1}{q_2})\beta \Rightarrow \frac{\alpha}{\beta}$ coincide con il numero razionale (di profondità 1) $q_1 + \frac{1}{q_2}$ (si noti che non può essere $q_2 = 1$, perché abbiamo supposto $\rho_1 < \beta$). Se ρ_2 non è zero, il numero razionale $q_1 + \frac{1}{q_2}$ è comunque un'*approssimazione* di $\frac{\alpha}{\beta}$. Si può scrivere infatti: $\frac{1}{q_2}\beta = \rho_1 + \frac{1}{q_2}\rho_2$, e sostituendo il valore che qui si ottiene per ρ_1 nella prima divisione euclidea, ecco che si deduce:

$\alpha = q_1\beta + \rho_1 = q_1\beta + \frac{1}{q_2}\beta - \frac{1}{q_2}\rho_2 = (q_1 + \frac{1}{q_2})\beta - \frac{1}{q_2}\rho_2$,

ossia: $\frac{\alpha}{\beta} = (q_1 + \frac{1}{q_2}) - \frac{1}{q_2}\frac{\rho_2}{\beta}$, ossia $(q_1 + \frac{1}{q_2})$ è un'approssimazione *per eccesso* di $\frac{\alpha}{\beta}$, e $\left|\frac{\alpha}{\beta} - (q_1 + \frac{1}{q_2})\right| = \frac{1}{q_2}\frac{\rho_2}{\beta} < \frac{1}{2q_2}\frac{\alpha}{\beta}$.

E' chiaro in che modo il ragionamento si sviluppa ulteriormente, *in modo finito*

se $\frac{\alpha}{\beta}$ è un numero razionale, *infinito* se è un numero irrazionale. La differenza fondamentale con il caso "aritmetico" illustrato nel paragrafo 3 è che la sequenza dei resti $\rho_1 > \rho_2 > \rho_3 > \ldots$ è sì ancora monotòna strettamente decrescente, ma non è detto che essa debba arrestarsi al caso di un resto nullo. Anzi, l'ipotesi di irrazionalità si traduce proprio nel fatto che tale circostanza *non* si verifica. In altre parole, descrivendo la "fenomenologia", si è costretti a riconoscere che, mentre *non* si può "pensare" una successione monotòna strettamente decrescente di numeri naturali, si può al contrario immaginare una successione monotòna strettamente decrescente di segmenti (liberi o no) di R, la più semplice delle quali si ottiene prendendo un segmento arbitrario, considerandone la metà, poi la metà della metà, *etc.*, appunto, *all'infinito*: il procedimento *non può* avere termine.

Ci sembra istruttivo far vedere come si articola almeno il passo immediatamente successivo a quello dianzi esaminato.

(iii) $\rho_1 = q_3 * \rho_2 + \rho_3$, con $\rho_3 < \rho_2$ e $\rho_3 < \frac{\rho_1}{2} < \frac{\alpha}{4}$, e quindi:

$$\frac{1}{q_3}\rho_1 = \rho_2 + \frac{1}{q_3}\rho_3,$$

$$\beta = q_2\rho_1 + \rho_2 = q_2\rho_1 + \frac{1}{q_3}\rho_1 - \frac{1}{q_3}\rho_3 = (q_2 + \frac{1}{q_3})\rho_1 - \frac{1}{q_3}\rho_3,$$

$$\frac{1}{q_2 + \frac{1}{q_3}}\beta = \rho_1 - \frac{1}{(q_2 + \frac{1}{q_3})q_3}\rho_3,$$

$$\alpha = q_1\beta + \rho_1 = q_1\beta + \frac{1}{q_2 + \frac{1}{q_3}}\beta + \frac{1}{(q_2q_3 + 1)}\rho_3 = (q_1 + \frac{1}{q_2 + \frac{1}{q_3}})\beta + \frac{1}{(q_2q_3 + 1)}\rho_3,$$

$$\frac{\alpha}{\beta} = (q_1 + \frac{1}{q_2 + \frac{1}{q_3}}) + \frac{1}{(q_2q_3 + 1)}\frac{\rho_3}{\beta},$$

ergo, se ρ_3 è zero, allora $q_3 \neq 1$, e $\frac{\alpha}{\beta} = q_1 + \frac{1}{q_2 + \frac{1}{q_3}}$, mentre se ρ_3 non è zero, allora $(q_1 + \frac{1}{q_2 + \frac{1}{q_3}})$ è un'approssimazione per difetto di $\frac{\alpha}{\beta}$, e:

$$\left|\frac{\alpha}{\beta} - \left(q_1 + \frac{1}{q_2 + \frac{1}{q_3}}\right)\right| = \frac{1}{q_2q_3 + 1}\frac{\rho_3}{\beta} < \frac{1}{4(q_2q_3 + 1)}\frac{\alpha}{\beta}.$$

Dovrebbe essere pertanto manifesto perché abbiamo calcolato esplicitamente questo terzo passo. Nell'ultima essenziale stima il coefficiente 2 che compariva al denominatore in precedenza è diventato un $4 = 2^2$ (per non dire dell'altro fattore che compare al denominatore della frazione: ha un'espressione complicata, ma si capisce che anch'esso comunque diverge - nel peggiore dei casi, che tutte le q_i siano uguali a 1, abbiamo in effetti un 8 in luogo di un 4). Questo 4 comparirà anche nella successiva approssimazione, che sarà però per difetto, mentre nella successiva ancora, che sarà per eccesso, interverrà il coefficiente $8 = 2^3$, una circostanza che da sola giustifica l'affermazione di convergenza che ci sta a cuore. Posto $x = \frac{\alpha}{\beta}$ (nel presente caso un numero reale maggiore di 1), la successione monotòna strettamente decrescente:
$x > \frac{x}{2} > \frac{x}{4} >...$ risulta certamente *infinitesima*, e quindi la differenza tra il numero x e quelle sue successive approssimazioni sarà "sempre più piccola".

Rimarrebbe da stabilire, come nel caso di un numero razionale, che la rappresentazione in *frazione continua* così determinata è unica, il che è come asserire che da un'identità del tipo:

$$x = \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{... + \cfrac{1}{q_n + ...}}}} = \cfrac{1}{k_1 + \cfrac{1}{k_2 + \cfrac{1}{... + \cfrac{1}{k_n + ...}}}}$$

(per un arbitrario numero irrazionale x minore di 1; q_i e k_i rappresentano attualmente dei numeri naturali), si può dedurre che $q_i = k_i$ per ogni valore dell'indice i. Inoltre, si potrebbe dimostrare che, per una scelta arbitraria dei coefficienti q_i, la frazione continua in parola è certamente convergente, ma lasciamo stare, riassumendo piuttosto il risultato al quale siamo pervenuti grazie a Galileo.

Una relazione di proporzionalità $\alpha : \beta = \gamma : \delta$ sussiste, *per definizione*, se e soltanto se, impostata la serie di divisioni euclidee successive:

$\alpha = q_1*\beta + \rho_1$,
$\beta = q_2*\rho_1 + \rho_2$,
$\rho_1 = q_3*\rho_2 + \rho_3$, *etc.*,

e la corrispondente serie a partire da γ, δ:

$\gamma = k_1*\delta + \chi_1$,
$\delta = k_2*\chi_1 + \chi_2$,

$\chi_1 = k_3*\chi_2 + \chi_3$, *etc.*,

risulta ordinatamente: $q_1 = k_1$, $q_2 = k_2$, $q_3 = k_3$, *etc.* (il primo quoziente q_1 potrebbe porsi anche uguale a zero, se si volesse trattare pure il caso $\alpha < \beta$).

Prima di abbandonare l'argomento, osserviamo che in effetti la definizione di Euclide è meno "oscura" di quanto possa apparire a prima vista (e viene affermato sia da Galileo sia da De Morgan), dal momento che, prescindendo dalla forma particolare con cui essa viene enunciata (pare che l'autore si faccia un proposito di non utilizzare i sottomultipli delle grandezze in gioco), equivale manifestamente alla seguente, la quale corrisponde precisamente all'"ordinario" procedimento di misura (che usa "passi", "piedi", "palmi", e loro sottomultipli):

(20) $\alpha : \beta = \gamma : \delta$ se e soltanto se, per ogni numero naturale n, la divisione con resto di α rispetto a $\frac{1}{n}\beta$ individua lo stesso quoziente q della divisione con resto di γ rispetto a $\frac{1}{n}\delta$.

Vale a dire, posto $\alpha = q(\frac{1}{n}\beta)+ \rho$, con $q \in N_0$ e $\rho \in \Sigma_0$ (è chiaro cosa sia detto insieme, un semigruppo con elemento neutro estensione di Σ, e la sua analogia con N_0!), $\rho < \frac{1}{n}\beta$ implica che $\gamma - q(\frac{1}{n}\delta)$ è un elemento di Σ_0 minore di $\frac{1}{n}\delta$.

L'equivalenza della (18) con la (20) è piuttosto semplice da dimostrare, e non vi insistiamo. Osserviamo soltanto che le (*a priori* infinite) verifiche che la (20) comporta possono ridursi a un qualsiasi sottoinsieme infinito:
$n_1 = 1 < n_2 < n_3 < ...$ di *N*, in corrispondenza del quale si determina la seguente successione di divisioni successive:

$$\alpha = q_1*\beta + \rho_1,\ \alpha = n_2q_1*\frac{1}{n_2}\beta + q_2*\frac{1}{n_2}\beta + \rho_2,\ ...$$

da cui si ottengono i seguenti "sviluppi infiniti":

$$\alpha = q_1*\beta + q_2*\frac{1}{n_2}\beta + q_3*\frac{1}{n_3}\beta + ...\ ,\ \frac{\alpha}{\beta} = q_1 + \frac{q_2}{n_2} + \frac{q_3}{n_3} + ...\ .$$

La più comune scelta della successione $n_1 = 1 < n_2 < n_3 < ...$ consiste oggi nelle posizioni: $n_1 = 1 = 10^0 < n_2 = 10 < n_3 = 10^2$, ... (rappresentazione di un numero reale in forma decimale), e che al posto del 10 si potrebbe porre altrettanto bene il 2 (rappresentazione binaria), o qualsiasi altro numero naturale k diverso da 1 (rappresentazione k-aria).

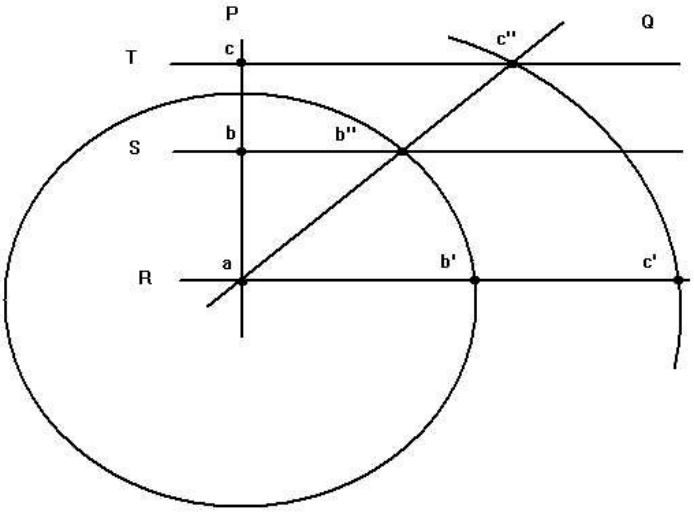
Val forse la pena di notare esplicitamente che il metodo proposto da Galileo permette di "canonizzare" in un certo modo il procedimento euclideo delle divisioni successive, con l'effetto che un numero reale è razionale se e soltanto se la sua corrispondente rappresentazione (in frazione continua) è finita (l'algoritmo ha termine), mentre un tale auspicabile risultato cessa di essere valido se si utilizzano altre forme di rappresentazione k-aria del numero. Come ben noto, tanto per fare un esempio: $\frac{1}{3}$ = 0,666... in forma decimale, *etc.* (sull'argomento si veda volendo la Nota 3 in:
http://www.dipmat.unipg.it/~bartocci/mat/fraz-cont.doc,
oltre a quanto se ne dice in:
http://www.dipmat.unipg.it/~bartocci/mat/eserciz.doc, e in:
http://www.dipmat.unipg.it/~bartocci/mat/antiper.doc). Non è difficile dimostrare che invece il risultato in questione continua a valere per la rappresentazione che potremmo dire *totale* di un numero razionale, ossia, che si può scrivere univocamente, ferme restando le notazioni precedenti, e per ogni coppia ordinata m, n di numeri naturali:

$$(21) \quad \frac{m}{n} = q_1 + \frac{q_2}{2} + \frac{q_3}{3} + \ldots \frac{q_r}{r}.$$

Sarebbe altrettanto agevole persuadersi che quella che compare nella formula precedente è una decomposizione della mantissa del numero razionale in oggetto in somma di frazioni egiziane (si rammenti l'inciso al termine del paragrafo 4), ma su ciò non insistiamo (se ne riparlerà in alcune pagine appositamente dedicate ad "Alcune curiosità su frazioni, somme e serie egiziane").

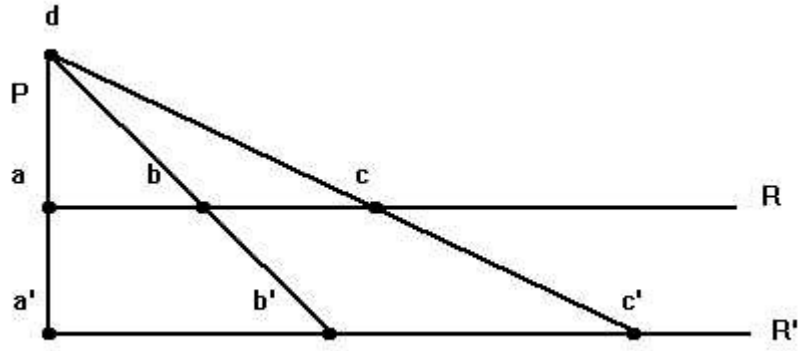
8.

Accenniamo infine, come promesso, alla possibilità di una *definizione puramente geometrica* di uguale proporzione, appoggiandoci alla geometria del piano (all'immersione cioè di **R** nel piano ordinario **P**) e al "teorema di Talete", che diverrebbe sotto questa prospettiva un *criterio di proporzionalità* e non un teorema.



La situazione dovrebbe essere "trascendentalmente chiara". Assegnate (in **P**) tre rette parallele R, S, T, e una comune perpendicolare P, si considerano i due segmenti $\overline{ab}$ e $\overline{ac}$ su P ($\overline{ab} < \overline{ac}$), e due segmenti arbitrari $\overline{ab'}$ e $\overline{ac'}$ su R (tali però che $\overline{ab'} < \overline{ac'}$, $\overline{ab'} > \overline{ab}$, $\overline{ac'} > \overline{ac}$). Ci si chiede quando sussiste la relazione di proporzionalità $\overline{ac} : \overline{ab} = \overline{ac'} : \overline{ab'}$. Basta riportare b' su S, ottenendo b" (b" è tale cioè che $\overline{ab''} \equiv \overline{ab'}$), tracciare la retta Q per a e b", prendere l'intersezione c" tra Q e T. La proporzione è soddisfatta, *per definizione*, se, e soltanto se, c" coincide con il punto che si ottiene riportando c' su T (ossia, $\overline{ac''} \equiv \overline{ac'}$). Non è difficile dimostrare che questo criterio "puramente geometrico" (e forse più vicino di tutti gli altri discussi a uno dei «most common acts» dell'intelletto umano) implica quello di Euclide, e ovviamente viceversa.

L'"intuizione" puramente geometrica della proporzionalità tra due coppie ordinate di segmenti ci sembra potersi descrivere agevolmente anche attraverso la seguente figura, che giustifica l'universale convinzione secondo la quale scegliere come unità di misura un certo segmento astratto α o un altro α' "è la stessa cosa" (tale affermazione si potrebbe precisare attraverso la descrizione di un isomorfismo canonico gruppale tra il gruppo Aut(Σ) e $R^+(*)$, il gruppo moltiplicativo di R^+; gli automorfismi in parola sono ovviamente inerenti alla categoria di competenza, che è quella dei semigruppi abeliani regolari ordinati, ma, del resto, un semplice automorfismo algebrico del semigruppo $\Sigma(+)$ risulta pure manifestamente un automorfismo d'ordine, in virtù della (19)).



La situazione dovrebbe essere ancora una volta trascendentalmente chiara. Si immaginino (in **P**) due copie della retta ordinaria **R** come le due rette parallele R e R' indicate in figura, e una comune perpendicolare P che individua su R ed R' rispettivamente i punti a, a', che si pensano come estremi di due unità di misura $\overline{ab}$ e $\overline{a'b'}$ scelte (in modo arbitrario) rispettivamente su R e su R' (supponiamo per esempio $\overline{ab} < \overline{a'b'}$). Scelti altrettanto arbitrariamente $\overline{ac} > \overline{ab}$, $\overline{a'c'} > \overline{a'b'}$ (ancora su R ed R' rispettivamente), ci si chiede quando sussiste la relazione di proporzionalità $\overline{ac} : \overline{ab} = \overline{a'c'} : \overline{a'b'}$. Considerato il punto $d \in P$ dal quale si ottiene il segmento $\overline{a'b'}$ per *proiezione* di $\overline{ab}$ da d su R', è necessario e sufficiente che c' coincida con quell'unico punto in R' che si ottiene per *proiezione* di c da d su R'. D'altronde, la relazione di proporzionalità in oggetto è manifestamente collegata ai ben noti criteri di similitudine tra triangoli:
$\overline{a'b'} : \overline{ab} = \overline{a'd} : \overline{ad}$, allo stesso modo che $\overline{a'c'} : \overline{ac} = \overline{a'd} : \overline{ad}$, da cui si inferisce che: $\overline{a'b'} : \overline{ab} = \overline{a'c'} : \overline{ac}$, e quindi $\overline{ac} : \overline{ab} = \overline{a'c'} : \overline{a'b'}$ per scambio degli "estremi" della proporzione, come appunto si voleva dimostrare.

Insomma, con un siffatto approccio "statico", contrapposto a quello che si potrebbe dire "dinamico" sia di Euclide che di Galileo (in entrambi i casi, meno apertamente nel primo che nel secondo, si ha a che fare con il concetto di *limite*), si esce dalla geometria della retta (che deve del resto essere concepita parte di un successivo momento di astrazione), per porre la questione dei "fondamenti" in relazione alle proprietà intuitive della geometria del piano (direttamente legate ai processi mentali attraverso il meccanismo della visione). Si ritrova per tale via (quale conseguenza abbastanza inaspettata, almeno per chi sia cresciuto nutrito dai "dogmi" del pensiero scientifico moderno), che la teoria delle parallele e il famoso V postulato di Euclide, più che l'aritmetica e la logica, giocano un ruolo importante anche nella genesi naturale del concetto di numero come misura.

9.

Terminiamo il nostro *excursus* con qualche commento generale. Nonostante verso la fine del XIX secolo il cosiddetto programma di "aritmetizzazione dell'analisi" abbia voluto «concepire i numeri reali come strutture concettuali,

invece che come grandezze intuitive ereditate dalla geometria euclidea» (Carl B. Boyer, *A History of Mathematics*, John Wiley & Sons, New York, 1968; trad. it. *Storia della matematica*, I.S.E.D.I., Torino, 1976; Oscar Mondadori, Milano 1980, 1990, p. 642), sicché un numero reale diventò o una particolare coppia ordinata di insiemi di numeri razionali (Dedekind), o una classe di equivalenza di particolari successioni di tali numeri (Cantor), *etc.*, (con l'effetto, tra l'altro, che ancora una volta non sarebbe possibile stabilire una "vera" relazione di inclusione $Q \subset R$, ma soltanto una quasi-inclusione), continuiamo a essere persuasi che la genesi autentica del concetto di numero reale sia di natura geometrica. Come già osservato, i numeri reali razionali "nascono" insieme ai numeri reali irrazionali, senza alcuna differenza di "specie" tra i due tipi di grandezze, e l'inclusione insiemistica $Q \subset R$ diviene in questo caso del tutto legittima e significativa.

Un punto non è un segmento, un segmento non è un segmento libero, un segmento libero non è un numero (reale positivo). Un numero reale positivo è una classe di equivalenza di coppie ordinate di segmenti liberi. Una volta introdotto il relativo insieme numerico, i passi successivi (non tutti ugualmente agevoli) sono (senza badare alla sequenza logica naturale, e senza pretese di completezza): la dimostrazione di un "lemma chiave", teso a provare che, nell'insieme delle frazioni geometriche che rappresentano un dato numero reale, ce n'è sempre una (e una soltanto) con numeratore o denominatore fissati in modo arbitrario (il lemma è *falso* nel caso di Q^+, quando si considerino numeratori e denominatori che siano numeri naturali, ma è vero quando si considerino numeratori e denominatori ... razionali!); l'introduzione di una struttura d'ordine totale in R^+; l'introduzione di una struttura algebrica interna di somma e di prodotto tra numeri reali, e di un prodotto esterno tra numeri reali e segmenti; l'illustrazione di un isomorfismo (canonico) tra i gruppi $\mathrm{Aut}(\Sigma(+))$ e $R^+(*)$, il gruppo moltiplicativo di R^+ (gli automorfismi in parola essendo inerenti alla categoria di competenza, che è quella dei semigruppi abeliani regolari ordinati); l'illustrazione di un isomorfismo (non canonico) tra i due semigruppi additivi $R^+(+)$ e $\Sigma(+)$; *etc.*, fino a descrivere: il passaggio dai segmenti ai segmenti ordinati (orientati), e quindi dai segmenti liberi ai vettori; la somma di vettori come somma di cammini orientati (niente incomprensibile regola della diagonale, per cui si ricorre a volte a motivazioni ... fisiche, con l'esempio della "somma di forze", *ignotum per ignotius*); i numeri reali con segno quali rapporti di vettori, con denominatore non nullo; la *regola dei segni* $-1*-1 = 1$ (di solito esposta in maniera astratta, o assurda, prendendo il caso del prodotto ... di due debiti, o persino "intimidatoria"; il poeta Wystan Hugh Auden, 1907-1973, rammenta una canzoncina che gli insegnavano a scuola: «Minus times minus is plus / The reasons for this we need not discuss»); e così via, pervenendo da ultimo: alla piena comprensione della struttura di *campo ordinato archimedeo completo* di R; all'introduzione degli spazi vettoriali reali $V(\mathbf{R})$, ma anche $V(\mathbf{P})$ e $V(\mathbf{S})$; all'interpretazione della dimensione geometrica mediante il concetto di

base lineare; alla dimostrazione dell'isomorfismo (canonico) tra il gruppo abeliano additivo V(**R**)(+) e il gruppo abeliano moltiplicativo delle traslazioni di **R**, *etc.*. Le "coordinatizzazioni cartesiane" stabiliranno un insieme di "isomorfismi" tra retta ordinaria (orientata) ed insieme dei numeri reali *R*, due insiemi che, pur risultando isomorfi, non saranno però canonicamente isomorfi: nessuna delle coordinatizzazioni di **R** potrà dirsi infatti in qualche modo "privilegiata" rispetto a un'altra. **R** non ha del resto singoli elementi privilegiati (tutti i punti sono "uguali" tra loro, un effetto secondo noi della transitività del gruppo delle traslazioni), mentre *R* ha elementi privilegiati, per esempio lo 0 e l'1 (anzi, un celebre *teorema di Staudt* assicura che *non* esistono automorfismi di campo di *R*, tranne l'identità). Allo stesso modo, Seg(**R**) e Σ non hanno singoli elementi privilegiati, essenzialmente perché il citato gruppo degli automorfismi di Σ agisce in maniera transitiva (strettamente 1-transitiva) su Σ. La confusione corrente tra *spazio ordinario* (geometrico) **S** e *spazio numerico* R^3 (da stabilire poi peraltro se *affine* o *vettoriale*), è a nostro parere un (ulteriore) sintomo dell'attuale decadenza della generale consapevolezza intorno ai "fondamenti della geometria", o più in generale della matematica.

(Dipartimento di Matematica e Informatica dell'Università degli Studi di Perugia
Corso di "Algebra 1 con Elementi di Logica 1" - Integrazione alle dispense
Umberto Bartocci, Perugia, ottobre 2005)