1 Ottobre 2018

I Reali: un approccio quasi assiomatico.

Indice

1 Primi passi.

Dovendo introdurre i reali è d'obbligo un riferimento al mondo greco, al loro gusto per la riflessione teorica, ed al fatto che la scoperta della non commensurabilità del lato e della diagonale del quadrato abbia messo in crisi i fondameni di una concezione del mondo, che vedeva tutto come proveniente da un armonico assembramento di particelle elementari.

Ciò si applicava in particolare anche alle grandezze geometriche, intuitivamente recepite come omogenee: questa scoperta metteva in crisi il fatto che due grandezze avessero sempre un comune sottomultiplo e quindi che tutti i rapporti fra grandezze

potessero esser valutati in termini di rapporti di numeri interi, arrivando in un certo senso a valutare quanti elementi corpuscolari simili le costituissero.

Ad esempio si pensi al processo pitagorico che poteva portare alla determinazione di una possibile grandezza in comune tra due grandezze pensate come lunghezze di due segmenti. Si prende il segmento più corto e si ricopre quello più lungo con tante copie di quello più corto: se si arriva a ricoprirlo si finisce altrimenti si prende il segmento rimanente e si cerca di ricoprire il più corto con tante copie di quest'ultimo. Anche qui se ci si riesce si termina altrimenti si ricomincia. Per i pitagorici questo procedimento avrebbe dovuto sempre terminare e questo è praticamente equivalente alla commensurabilità: una sorta di algoritmo di Euclide geometrico. La scoperta di grandezze incommensurabili dava una scossa proprio a questa concezione.

A tutto ciò si aggiunse l'azione critica di altri pensatori come Zenone che non riuscivano a conciliare questa visione con il fatto che una grandezza finita potesse risultare dalla somma di un numero infinito di grandezze finite (Achille e la tartaruga).

Anche se queste idee saranno presenti in sottofondo lungo tutto il testo, ripercorrerle in dettaglio è però fuori dagli scopi di queste brevi note e preferiamo rimandare per una trattazione più sistematica a testi di storia della matematica o della scienza.

Vogliamo qui solo introdurre in modo rapido l'insieme dei numeri reali seguendo un approccio astratto che si rifà a Dedekind, ancorché anche egli, almeno a suo dire, probabilmente altro non fece che evidenziare le idee già espresse nel mondo greco, rifacendosi al metodo per confrontare due grandezze detto di esaustione e al principio di Eratostene, che per comodità del lettore riportiamo qui di seguito utilizzando terminologie più moderne.

Pricipio di Eratostene. Diremo che due grandezze a e b sono nella stessa proporzione di altre due grandezze A e B se comunque fissati due numeri interi positivi m e n si ha

$$ma < nb \text{ se e solo se } mA < nB$$

$$ma > nb \text{ se e solo se } mA > nB$$

Fissiamo il contesto. Il nostro punto di partenza saranno gli insiemi numerici, nel senso che *daremo per noti* gli insiemi dei numeri naturali ($\mathbb{N}$), dei numeri interi ($\mathbb{Z}$) e, dopo qualche precisazione, dei numeri razionali ($\mathbb{Q}$) con le loro principali proprietà e la usuale rappresentazione decimale dei numeri razionali, anche se su quest'ultima cosa torneremo diffusamente alla fine della dispensa.

Cerchiamo un insieme X che estenda gli insiemi $\mathbb{N}$, $\mathbb{Z}$ e $\mathbb{Q}$ e in cui si possano fare delle operazioni e delle considerazioni che ad esempio in $\mathbb{Q}$ non si possono fare, come ad esempio la misurazione della diagonale del quadrato o provare che "Achille raggiunge la tartaruga".

Abbiamo pertanto bisogno di un insieme X e del fatto che su questo insieme si possano fare (siano cioè definite) due operazioni che chiameremo *somma* e *prodotto* e che indicheremo rispettivamente con $+$ e con $\cdot$. Una operazione (binaria) su X altro non è che una legge che associa ad una coppia di elementi di X un altro

elemento di X: si pensi all'usuale somma in $\mathbb{Z}$. Vorremo inoltre poter operare con un certo numero di regole di calcolo: chiederemo quindi che le operazioni soddisfino un numero minimo di "regole" da cui poter ricavare le altre, cioè che le operazioni verifichino un elenco, se pur minimo, di assiomi.

Abbiamo quindi bisogno di un insieme X, la natura dei cui elementi per ora lasciamo nel vago, e su X pensiamo definite due operazioni, cioè due applicazioni che chiameremo rispettivamente "somma" e "prodotto"

$$X \times X \to X, (x, y) \to x + y$$

$$X \times X \to X, (x, y) \to x \cdot y$$

che verificano i seguenti assiomi:

1. assiomi per l'operazione somma

   S1 (associatività) $\forall x, y, z \in X \quad (x + y) + z = x + (y + z)$

   S2 (commutatività) $\forall x, y \in X \quad x + y = y + x$

   S3 (esitenza elemento neutro) $\exists u \in X : \forall x \in X \quad x + u = x$

   S4 (esitenza inverso) $\forall x \in X \exists x' : x + x' = u$

2. assiomi per l'operazione prodotto

   P1 (associatività) $\forall x, y, z \in X \quad (x \cdot y) \cdot z = x \cdot (y \cdot z)$

   P2 (commutatività) $\forall x, y \in X \quad x \cdot y = y \cdot x$

   P3 (esitenza elemento neutro) $\exists e \in X : \forall x \in X \quad x \cdot e = x$

   P4 (esitenza inverso) $\forall x \neq u \ \exists x' : x \cdot x' = e$

3. e di un assioma che "leghi" il comportamento delle due operazioni, cioè che le operazioni definite non siano del tutto indipendenti tra di loro:

   Dis (distributività) $\forall x, y, z \in X \quad x \cdot (y + z) = x \cdot y + x \cdot z$

Per comodità di notazione indicheremo con 0 l'elemento neutro per l'operazione $+$ e con 1 quello per l'operazione $\cdot$ e indicheremo con $-x$ l'inverso dell'elemento x per l'operazione $+$ e con x^{-1} quello per l'operazione $\cdot$ ed abbrevieremo con $x - x$ la scrittura $x + (-x)$.

Dagli assiomi discende immediatamente che l'elemento neutro per la somma è unico; supponiamo infatti che ve ne siano due u e v: risulta immediatamente dagli assiomi S3 ed S2 che $u = u+v = v$. Allo stesso modo si ha che l'inverso per la somma è unico; siano infatti x' ed x" due inversi per x si ha $x' = 0+x' = (x"+x)+x' = x"+(x+x') = x" + 0 = x"$. Notare che l'assioma S2 permette di non fare distinzioni tra inverso

destro e sinistro. Avremo anche bisogno di richiedere che $1 \neq 0$. Proprietà analoghe si dimostrano per il prodotto.

Da questi assiomi discendono immediatamente, con dimostrazioni analoghe a quelle viste, quelle che potremmo chiamare *regole di calcolo in* X e che sono le usuali regole aritmetiche. Vediamone qualcuna.

1. $\forall x \in X \quad x \cdot 0 = 0 \cdot x = 0$

   Prova: $x \cdot 0 = x \cdot (0 + 0) = x \cdot 0 + x \cdot 0$ da cui $x \cdot 0 = 0$ □

2. $(-x)y = -(xy) = x(-y)$

   Prova: $0 = 0 \cdot y = (x + (-x))y = xy + (-x)y$ da cui $(-x)y = -(xy)$ ed analogamente a destra. □

3. $(-x)(-y) = xy$

   Prova: Da (2) si ha $(-x) \cdot y = -(x \cdot y)$. Sempre per (2) $(-x) \cdot (-y) = -(-x) \cdot (y) = x \cdot y$ per unicità dell'opposto. □

Analogamente a queste si ricavano tutte le altre usuali regole di calcolo: osserviamo in particolare che la regola di calcolo (1) fornisce una giustificazione del fatto che nell'assioma P4 viene posta la condizione di non essere l'elemento neutro per la somma.

Un insieme dotato di due operazioni verificanti questi 9 assiomi viene detto brevemente *corpo commutativo* o *campo*.

Avremo bisogno inoltre che sull' insieme X sia definita anche una relazione di ordine che indicheremo con $\leq$.

Gli assiomi (le richieste) per la relazione d'ordine sono i seguenti

O1 (dicotomia) $\forall x, y \in X$ è vera una delle seguenti due relazioni $x \leq y$ o $y \leq x$

O2 (riflessività) $\forall x \in X x \leq x$

O3 (antisimmetria) $x \leq y$ e $y \leq x \Rightarrow x = y$

O4 (transitività)$x \leq y$ e $y \leq z \Rightarrow x \leq z$

Con i seguenti due assiomi esprimiamo infine che tale relazione sia compatibile con le operazioni esistenti

14 $x \leq y \Rightarrow x + z \leq y + z \forall x, y, z \in X$

15 $x \geq 0$ e $y \geq 0 \Rightarrow x \cdot y \geq 0$

Un insieme verificante tutti questi 15 assiomi viene detto brevemente un *campo ordinato*. Un esempio di insieme siffatto, cioè di campo ordinato è l'insieme dei numeri razionali $\mathbb{Q}$.

Anche qui si può verificare rapidamente che da questi assiomi si possono dedurre le usuali regole di calcolo.

Un insieme X dotato di queste propietà è una *estensione* di $\mathbb{Q}$, nel senso che esiste una applicazione iniettiva $\Phi : \mathbb{Q} \to X$ che "rispetta" la struttura, cioè

$\forall a, b \in Q$

- $\Phi(a + b) = \Phi(a) + \Phi(b)$
- $\Phi(a \cdot b) = \Phi(a) \cdot \Phi(b)$
- $a \leq b \Rightarrow \Phi(a) \leq \Phi(b)$

Una tale Φ si ottiene in questo modo: facciamo corrispondere all'elemento $0 \in \mathbb{Q}$ l'elemento neutro per la somma ed al numero razionale 1 l'elemento neutro per il prodotto; definiamo $\Phi(n)$ la somma di n volte l'elemento neutro per il prodotto ed infine ponendo $\Phi(\frac{m}{n}) = \Phi(m) \cdot (\Phi(n))^{-1}$ si ha una estensione a tutto $\mathbb{Q}$. L' applicazione Φ così definita è iniettiva (perché?).

Quindi in un insieme dotato di queste proprietà sappiamo "ritrovare" i numeri naturali, gli interi ed i razionali. Continueremo ad indicare con la simbologia usuale gli interi e i razionali anche pensati dentro X se la cosa non dà adito a confusione.

Fatte queste premesse, dentro un campo ordinato possiamo rifare tutti gli abituali calcoli dell'aritmetica elementare, per esempio risolvere equazioni e disequazioni lineari. Per il momento con la parola "risolvere" intenderemo solo descrivere in modo a noi più intelligibile il sottoinsieme descritto dalla relazione.

Vediamo su un esempio che cosa significhi: trasformiamo la descrizione di alcuni insiemi applicando gli assiomi (si cerchi di comprendere ad ogni passaggio la sua liceità, nel senso quali assiomi ci garantiscono che i due insiemi sono uguali)

$\{x \in X | 3x + 1 > 4\} = \{x \in X | 3x + 1 - 1 > 4 - 1\} = \{x \in X | 3x > 3\} = \{x \in X | x > 1\}$

Ma ancora un insieme con queste proprietà non ci basta. Infatti $\mathbb{Q}$ è un esempio di campo ordinato e abbiamo già detto che in $\mathbb{Q}$ non è possibile trovare un numero il cui quadrato sia 2, cioè risolvere l'equazione $x^2 = 2$.

Mostriamolo, ripercorrendo più o meno la prova dei greci per l'incommensurabilità della diagonale del quadrato.

Proposizione 1.1. *Non esiste alcun elemento $r \in \mathbb{Q}$ tale che $r^2 = 2$*

Prova: Vogliamo provare che per nessun numero razionale $\frac{m}{n}$ si ha $(\frac{m}{n})^2 = 2$. Supponiamo che al contrario ciò sia vero: possiamo supporre che m, n siano primi tra di loro (perché?) e quindi di diversa parità. Da $m^2 = 2n^2$ deduciamo che m non puo' esser dispari (altrimenti il suo quadrato sarebbe ancora dispari) quindi m^2 è divisibile per 4, quindi anche n^2 è pari e quindi anche n lo è arrivando ad una contraddizione..

□

Dedekind ($\sim$ 1875) riprese il punto di vista dei greci e chiese un altro assioma, oggi conosciuto come assioma di continuità o completezza.

16 **Assioma di continuità.** Se A e B sono due sottoinsiemi non vuoti di X con $A \leq B$ nel senso che $\forall a \in A,\ b \in B\ a \leq b$ allora esiste in X un elemento c tale che

$$A \leq c \leq B$$

nel senso che $\forall a \in A, b \in B\ a \leq c \leq b$

Un insieme verificante tutti i 16 assiomi esposti verrà detto *campo ordinato completo.*

Assunzione: da questo momento supporremo che l'insieme X sia un campo ordinato completo.

Mostriamo a solo titolo esemplificativo come l'assioma di completezza garantisca l'esistenza in un campo ordinato completo della radice di 2.

Proposizione 1.2. *Sia X un campo ordinato completo. L'equazione $x^2 = 2$ ammette almeno una soluzione.*

Prova: Indichiamo con $A = \{x \in X | x > 0 \text{ e } x^2 < 2\}$ e $B = \{x \in X | x > 0 \text{ e } x^2 > 2\}$

Dagli assiomi risulta che $A < B$ nel senso che ogni elemento di A è minore di ogni elemento di B e pertanto per l'assioma 16 esiste un elemento separatore c in X. $A \leq c \leq B$.

Quello che vogliamo provare è che $c^2 = 2$.

Supponiamo per assurdo che $c^2 \neq 2$; allora $c^2 < 2$ oppure $c^2 > 2$. In entrambi i casi si perviene ad una contraddizione; svolgiamo l'argomentazione nel primo caso, l'altro è analogo.

Arriveremo ad un assurdo mostrando che esiste in X un $\delta > 0$ tale che $(c+\delta)^2 < 2$: questa è una contraddizione perché $(c + \delta)^2 < 2 \Rightarrow c + \delta \in A$ e $\delta > 0 \Rightarrow c + \delta > c$ contro il fatto che ogni elemento di A è minore di c.

Supponiamo quindi che $c^2 < 2$: questo implica che esiste un altro elemento $\varepsilon \in X$ tale che $c^2 + \varepsilon < 2$. Ad esempio posso prendere $\varepsilon = \frac{2-c^2}{2}$, in quanto $c^2 < 2 \Rightarrow c^2 + 2 < 4$ e quindi $c^2 + \frac{2-c^2}{2} < 2$.

Risulta, applicando gli assiomi,

$(c+\delta)^2 = c^2 + 2c\delta + \delta^2 = c^2 + \delta(2c+\delta)$

Pertanto se $\delta < c$ si ha

$(c+\delta)^2 = c^2 + \delta(2c+\delta) < c^2 + 3c\delta$

e se $\delta < \frac{\varepsilon}{3c}$ risulta

$(c+\delta)^2 < c^2 + 3c\delta < c^2 + \varepsilon < 2$

Quindi prendendo $\delta = min\{c, \frac{\varepsilon}{3c}\}$ si ha $c + \delta \in A$ che, come abbiamo detto, è in contraddizione con $c \geq A$.

□

Osserviamo che se chiediamo a tale elemento di essere positivo allora non solo esiste ma è anche unico. Siano infatti x e y due elementi in X tali che $x^2 = y^2 = 2$

Da $x^2 = y^2$ otteniamo $(x-y)(x+y) = 0$ e dalla positività di x e y otteniamo $x = y$.

Questo ragionamento opportunamente esteso porta a provare anche che in X per ogni $a > 0$ e n intero positivo l'equazione $x^n = a$ ha soluzioni in X.

2 Alcune proprietà (importanti) di $\mathbb{R}$.

Talvolta indicheremo con $\mathbb{R}$ un campo ordinato completo X. Tale notazione sarà giustificata tra qualche paragrafo quando avremo accennato all'unicità di un siffatto X che quindi potremo chiamare il campo dei *reali*

Proposizione 2.1. $\mathbb{N}$ *non è limitato in* $\mathbb{R}$

Prova: Ragioniamo per assurdo. Sia

$$M = \{x \in \mathbb{R} | x \geq n \ \forall n \in \mathbb{N}\}$$

e supponiamo che M sia non vuoto.

Essendo ogni elemento di $\mathbb{N}$ minore di ogni elemento di M per l'assioma di continuità esiste un elemento c separatore.

$$\mathbb{N} \leq c \leq M \quad (*)$$

Esiste quindi un numero naturale m tale che

$$c - 1 < m \leq c$$

altrimenti $c - 1$ apparterrebbe a M.

Si avrebbe pertanto $c < m + 1$ in contrasto con (*) □

Da qui discende immediatamente

Proposizione 2.2 (**Proprietà di Archimede**). *Siano $x, y \in X$ con $x > 0$. Esiste un intero positivo n tale che $nx > y$*

Prova: La Proposizione 2.1 garantisce che esiste un $n > \frac{y}{x}$ da cui la proposizione. □

Proposizione 2.3. *Per ogni elemento $x \in X$ esiste (unico) un intero k tale che*

$$k \leq x < k + 1$$

Prova: Suppuniamo $x > 0$. L'insieme $S = \{n \in \mathbb{N} |\ n \leq x\}$ è non vuoto e per la Proposizione 2.1 finito. $k = \max S$ verifica le richieste. La prova per il caso in cui $x < 0$ è del tutto analoga. □

L'intero la cui esistenza è garantita da questa proposizione viene detto *la parte intera di x* e viene comunemente indicato con $[x]$; cioè si ha

$$[x] \leq x < [x] + 1.$$

Proposizione 2.4. *Dato un elemento $x \in X$ ed un altro elemento $\varepsilon \in X$ positivo, esiste un numero razionale $r \in \mathbb{Q} \subset X$ tale che*

$$r \leq x < r + \varepsilon$$

Prova: Per prima cosa scegliamo un naturale m, la cui esistenza è assicurata dalla Proposizione 2.1, tale che $m > \frac{1}{\varepsilon}$, cioè $\frac{1}{m} < \varepsilon$. Per Prop.2.2 esiste un intero n tale che

$$n \leq mx < n + 1$$

e quindi

$$\frac{n}{m} \leq x < \frac{n}{m} + \frac{1}{m} < \frac{n}{m} + \varepsilon$$

Quindi $\frac{n}{m}$ verifica le richieste. □

Proposizione 2.5 (**Densità di $\mathbb{Q}$ in X**). *Dati due elementi x e y di X con $x < y$ esiste un numero razionale tra x e y.*

Prova: Per la proposizione precedente esiste $\overline{r} \in \mathbb{Q}$ tale che $\overline{r} \leq y < \overline{r} + (y - x)$. Ne segue che $x = y - (y - x) < \overline{r}$ e quindi

$$x < \overline{r} \leq y$$

.

Volendo un razionale r tale che

$$x < r < y$$

è sufficiente osservare che esiste un intero $m > \frac{1}{\overline{r}-x}$, cioè $\overline{r} - x > \frac{1}{m}$ da cui $x < \overline{r} - \frac{1}{m}$, e poiché $\overline{r} - \frac{1}{m} < \overline{r} \leq y$ si ha che il razionale $r = \overline{r} - \frac{1}{m}$ verifica $x < r < y$. □

Proposizione 2.6 (**Non esistenza di infinitesimi**). *Se* $x \in X$ *e* $|x| \leq \frac{1}{n} \quad \forall n \in \mathbb{N} \setminus \{0\}$ *allora* $x = 0$.

Prova: Se fosse $x \neq 0$ si avrebbe che $\frac{1}{|x|}$ contraddirrebbe la proprietà di Archimede. □

3 Estremo superiore ed estremo inferiore.

Partiamo da una considerazione: ogni sottoinsieme $A \subset X$ non vuoto e finito ammette massimo e minimo. Lo si può facilmente provare per ricorrenza. Detto n il numero di elementi di A la proprietà è banalmente vera se $n = 1$. Supponendo vera la proprietà per ogni insieme costituito da $n-1$ elementi, si tolga ad A un qualsiasi elemento .....

Questa proprietà non susssiste più per gli insiemi infiniti, come ci si convince facilmente considerando $A = (0,1) = \{x \in \mathbb{R} | 0 < x < 1\}$. È chiaro che un qualsiasi numero maggiore di 1 non è il massimo di A perché non appartiene all'insieme ed è anche immediato che A non può contenere un elemento più grande di tutti: se ad esempio d fosse tale elemento dovrebbe essere $d < 1$ e quindi $d < \frac{1+d}{2} < 1$. Quindi A non ha massimo ed analogamente si vede che non ha minimo.

Però l'assioma di continuità ci assicura una cosa:

Proposizione 3.1 (**Estremo superiore**). *Sia* X *un corpo ordinato completo ed* $A \subset X$ *un sotoinsieme non vuoto limitato superiormente. L'insieme* M *dei maggioranti di* A *ammette minimo.*

Prova: Gli insiemi A e M sono entrambi non vuoti e $\forall a \in A, \forall m \in M \quad a \leq m$. L'assioma di continuità garantisce l'esistenza di un elemento separatore c.

$$A \leq c \leq M.$$

Dunque per ogni $a \in A$ si ha $a \leq c$ e questo prova che c è un maggiorante. D'altra parte per ogni $m \in M$ si ha $c \leq m$ e questo basta a concludere che c è il minimo dei maggioranti. □

L'elemento individuato nella proposizione precedente si chiama *estremo superiore di* A e viene indicato spesso come $\sup A$.

Proposizione 3.2 (**Caratterizzazione del sup).** Sia A un sottoinsieme non vuoto di un corpo ordinato completo X limitato superiormente. L'elemento $L = \sup A$ è caratterizzato dalle seguenti proprietà:

1. $\forall a \in A \; L \geq a$
2. $\forall \varepsilon > 0 \; \exists a \in A : a > L - \varepsilon$

Prova: La condizione 1 dice che L è un maggiorante mentre la 2 dice che ogni elemento inferiore ad L non lo è.

Se L è il $\sup A$ verifica banalmente le proprietà 1). Se non verificasse la proprietà 2) esisterebbe un $\varepsilon_0 > 0$ tale che $L - \varepsilon_0$ risulti maggiore o uguale ad ogni elemento di A in contraddizione col fatto che L è il minimo dei maggioranti.

Viceversa supponiamo che L verifichi le proprietà (1) e (2) della proposizione. Dobbiamo verificare che allora L è il minimo dei maggioranti di A.

Supponiamo che non lo sia cioè $L \neq \sup A$. Poiché $\sup A$ è il minimo dei maggioranti ed L è un maggiorante si ha $L - \sup A > 0$; la condizione (2) prendendo $\varepsilon = L - \sup A$ ci dice che esiste $a \in A$ con $a > L - \varepsilon = L - L + \sup A = \sup A$ contraddicendo il fatto che $\sup A$ è un maggiorante di A. □

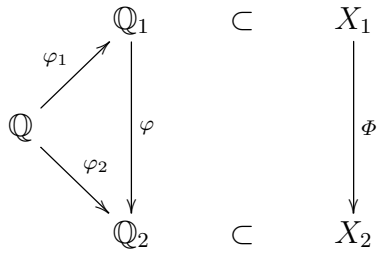
4 Un teorema di unicità.

Un teorema importante a questo punto è quello che ci assicura l'unicità di un tale X.

Proposizione 4.1. *Siano X_1 e X_2 due corpi ordinati completi. Allora esiste una applicazione biunivoca $\Phi : X_1 \to X_2$ che rispetta le operazioni, nel senso che*

1. $\Phi(x + y) = \Phi(x) + \Phi(y)$
2. $\Phi(x \cdot y) = \Phi(x) \cdot \Phi(y)$
3. $x \leq y \Rightarrow \Phi(x) \leq \Phi(y)$

L'idea della prova è di costruire questa Φ a partire dalle mappe φ_1 e φ_2 che "riconoscono" $\mathbb{Q}$ dentro rispettivamente X_1 e X_2.



Idea della prova. Siano $\mathbb{Q}_1$ e $\mathbb{Q}_2$ i razionali in X_1 e in X_2, cioè i sottoinsiemi $\varphi_i(\mathbb{Q})$. L'applicazione $\varphi = \varphi_2 \circ \varphi_1^{-1}$ da $\mathbb{Q}_1$ a $\mathbb{Q}_2$ è una applicazione biunivoca che conserva le operazioni e l'ordinamento. È possibile prolungare questa applicazione ponendo per ogni $x \in X_1$ $\Phi(x) = sup\{\varphi(y)\ y \in \mathbb{Q}_1\ y < x\}$. Resta da provare, e viene lasciato come esercizio, che tale estensione Φ è biunivoca e conserva la struttura.

Questo teorema ci garantisce che comunque noi troviamo un insieme che verifica gli assiomi enunciati questo sarà un modello di un tale X, insieme che d'ora in poi chiameremo insieme dei numeri reali e che indicheremo con $\mathbb{R}$

5 Rappresentazione decimale.

Cerchiamo di esprimere i numeri reali in una forma più agevole. Innanzitutto ricordiamo che dentro questo insieme $\mathbb{R}$ abbiamo una copia dei razionali che continuiamo a scrivere con l'abituale notazione $\frac{m}{n}$ con $m, n \in \mathbb{Z}$.

Per *numeri decimali* intenderemo i razionali della forma $\dfrac{a}{10^m}$ ove a è un intero ed m un naturale.

Osserviamo che i numeri decimali sono un sottoinsieme dei numeri razionali e che sommando o moltiplicando tra loro due numeri decimali si ottiene ancora un numero decimale. Cioè in questo insieme si possono fare tutte le operazioni che si possono fare sui razionali salvo il fatto che in generale l'inverso di un decimale non nullo non è detto che sia un decimale. Quindi questo insieme con le operazioni indotte da quelle dei razionali verifica tutti gli assiomi di corpo tranne l'assioma P4. (Sinteticamente: non formano un campo ma una struttura diversa che viene detta *anello* .)

Seguendo la prova della Proposizione 2.5 possiamo provare che anche i decimali sono densi in $\mathbb{R}$: ciò ci permetterà fissato un n e dato un elemento $x \in \mathbb{R}$ di scegliere un decimale che meglio approssimi per difetto x a meno di 10^{-n}, nel senso che si puó trovare un m tale che $\frac{m}{10^n} \leq x < \frac{m+1}{10^n}$.

Useremo iterativamente questa osservazione: ciò legittimerà in $\mathbb{R}$ un procedimento del tutto analogo al procedimento pitagorico per misurare due grandezze pensandole come lunghezze, procedendo al confronto e dividendo successivamente l'intervallo residuo in 10 parti uguali al fine di cercare un sottomultiplo comune. Punto essenziale di tutto il procedimento sarà il concetto di *parte intera,* cioè l'esistenza per ogni $x \in \mathbb{R}$ di un intero n tale che $n \leq x < n + 1$.

Dato $x \in \mathbb{R}$ iniziamo con l' individuare come fatto nella Prop 2.3 la sua parte intera, cioè il massimo intero a_0 minore o uguale a x: $a_0 = [x]$. Ponendo $r_0 = x - a_0$ avremo che $0 \leq r_0 < 1$. Quindi potremo pensare $x = a_0 + r_0$ e se $0 \neq r_0$ ripetiamo il ragionamento ed indichiamo con a_1 il massimo intero tale che $a_1 \leq 10r_0$, quindi si avrà $0 \leq a_1 \leq 9$. Quindi $r_0 = \frac{a_1}{10^1} + r_1$ con $0 \leq r_1 < \frac{1}{10}$. Cioè

$$x = a_0 + \frac{a_1}{10} + r_1$$

con $r_1 < \frac{1}{10}$. Ripetiamo il ragionamento con $100r_1$ e costruiamo a_2, r_2. Iterando avremo $x = a_0 + \frac{a_1}{10} + \frac{a_2}{10^2} + r_2$ con $r_2 < \frac{1}{10^2}$.

Proseguendo iterativamente si ha $r_{k-1} = a_k \frac{1}{10^k} + r_k$ con $0 \leq r_k < \frac{1}{10^k}$: pertanto si viene a creare una successione di interi $\{a_i\}$ per cui $a_0 + \frac{a_1}{10} + \frac{a_2}{10^2} + \ldots \frac{a_n}{10^n} \leq x < a_0 + \frac{a_1}{10} + \frac{a_2}{10^2} + \ldots \frac{a_n}{10^n} + \frac{1}{10^n}$.

Ora se x è per caso un numero decimale è chiaro che questo procedimento si arresta e si potrà allora scrivere

$$x = a_0 + \frac{a_1}{10} + \frac{a_2}{10^2} + \ldots \frac{a_n}{10^n}$$

scrittura che usualmente viene abbreviata con $a_0, a_1 a_2 \ldots a_n$

Altrimenti questo processo non si arresta e indicheremo $a_0 + \frac{a_1}{10} + \frac{a_2}{10^2} + \ldots + \frac{a_n}{10^n} + \ldots$ con la scrittura $a_0, a_1 a_2 \ldots$, scrittura che chiameremo espansione decimale (finita o infinita) di x. Chiaramente si ha che $0 \leq x - a_0, a_1 a_2 \ldots a_n \leq \frac{1}{10^n}$.

Se consideriamo i due insiemi A e B composti, A dalle espansioni decimali finite *approssimanti per difetto* e B da quelle *approssimanti per eccesso,* risulta chiaro da tutto ciò che precede e dalla prop 3.2 che x è *l'elemento separatore* tra questi due insiemi.

Osserviamo che *le cifre costruite con questa rappresentazione non possono essere tutte definitivamente uguali a 9.*

Infatti sia $a_0, a_1 a_2 \ldots a_k 9999 \ldots$ una espansione decimale con tutti 9 dalla $(k+1)$-esima cifra in poi. Arrestando lo sviluppo alla n-esima cifra decimale con n arbitrariamente grande (maggiore di k) abbiamo

$$a_0 + \frac{a_1}{10} + \frac{a_2}{10^2} + \ldots + \frac{a_k}{10^k} + \frac{9}{10^{k+1}} + \ldots + \frac{9}{10^n} = a_0 + \frac{a_1}{10} + \frac{a_2}{10^2} + \ldots + \frac{a_k}{10^k} + \frac{9}{10^{k+1}}(1 + \frac{1}{10} + \ldots \frac{1}{10^{n-k-1}}) = a_0 + \frac{a_1}{10} + \frac{a_2}{10^2} + \ldots + \frac{a_k}{10^k} + \frac{9}{10^{k+1}} \frac{1 - \frac{1}{10^{n-k}}}{1 - \frac{1}{10}} =$$

$$a_0 + \frac{a_1}{10} + \frac{a_2}{10^2} + \ldots + \frac{a_k}{10^k} + \frac{1}{10^k} - \frac{1}{10^n} = a_0 + \frac{a_1}{10} + \frac{a_2}{10^2} + \ldots + \frac{a_k + 1}{10^k} - \frac{1}{10^n}$$

cosa che dimostra che lo svipluppo decimale coincide (perché?) con $a_0, a_1 \ldots \{a_k + 1\}0000 \ldots$.

D'ora in poi useremo sempre la convenzione di identificare uno sviluppo decimale in cui le cifre da un certo punto in poi, diciamo dalla $k+1$-esima, siano tutte uguali a

9 con lo sviluppo decimale avente le stesse cifre fino alla $k-1$-esima, per k-esima la k-esima aumentata di 1 e le restanti 0. In simboli

$$a_0, a_1a_2 \dots a_k 9999999 \dots = a_0, a_1a_2 \dots (a_k + 1)000000 \dots$$

iterando il procedimento qualora anche $a_k + 1$ risultasse uguale a 9.

Chiameremo *allineamento decimale ridotto* un allineamento decimale $a_0, a_1a_2 \dots a_n \dots$ in cui tutte le cifre non sono definitivamente uguali a 9 ed indicheremo con D l'insieme degli allineamenti decimali ridotti.

Proposizione 5.1. *Il procedimento di approssimazione descritto induce una applicazione biunivoca di* $\mathbb{R}$ *su* D*.*

Prova: Indichiamo con d l'applicazione da $\mathbb{R}$ a D che risulta dal procedimento di approssimazione descritto. Dato un numero reale x e l'espansione decimale $d(x)$ abbiamo già osservato che x risulta essere l'estremo superiore degli allineamenti decimali. [1]

Indichiamo ora con s l'applicazione da D a $\mathbb{R}$ ora descritta che associa ad una espansione decimale il sup dell'insieme A delle espansioni decimali approssimanti per difetto

$$a_0, a_1a_2 \dots a_n \dots \to x = \sup_{n\in\mathbb{N}}\{a_0, a_1a_2 \dots a_n\}$$

Per quanto ora provato abbiamo che l'applicazione $\mathbb{R} \to D \to \mathbb{R}$ è l'identità di $\mathbb{R}$. Basta mostrare (esercizio) che anche l'altra composizione $D \to \mathbb{R} \to D$ è a sua volta l'identità di D.

Infatti ciò implica che le due applicazioni d e s risultano iniettive e suriettive. Ragioniamo sulla d.

- **iniettività** Se $d(a) = d(b)$ si ha $sd(a) = sd(b)$ ma essendo $sd = id$ ciò implica $a = b$.
- **surgettività** Sia $u \in D$. $s(u)$ è in $\mathbb{R}$ e $ds(u) = u$ quindi l'elemento $v = s(u)$ di $\mathbb{R}$ è tale che $d(v) = u$.

□

[1] Infatti $a_0, a_1 \dots \leq x$ e $\forall n\ x - \frac{1}{10^n} < a_0, a_1a_2 \dots a_n$ e notare che per ogni $x' < x$ si può prendere n in modo tale che $x - \frac{1}{10^n} > x'$ così

$$x' \leq x - \frac{1}{10^n} < a_0, a_1a_2 \dots a_n.$$

6 Rappresentazione decimale e numeri razionali: algoritmo della frazione generatrice.

Abbiamo identificato il corpo dei reali $\mathbb{R}$ con l'insieme dei decimali illimitati D. Ovviamente una espansione decimale finita rappresenta un razionale, ma ci si convince immediatamente che non ogni razionale è rappresentabile con una espansione decimale finita: si prenda ad esempio $\frac{1}{3}$ e si vede con l'usuale divisione che l'espansione decimale è $0,333333\ldots$, espansione che viene indicata convenzionalmente con la scrittura $0,\overline{3}$.

Ci chiediamo se abbiamo un modo di riconoscere le espansioni decimali che rappresentano un razionale e, in caso affermativo, un algoritmo per risalire a tale decimale.

Procedendo in maniera analoga a quanto fatto per dimostrare che le cifre nella rappresentazione decimale non possono essere tutte definitivamente uguali a 9 costruiamo l'algoritmo, ben noto sin dalla scuola media, della *frazione generatrice.* Più precisamente proviamo il seguente teorema.

Proposizione 6.1. *Sia α l'espansione decimale $a_0, a_1a_2\ldots$. Supponiamo che esista una sequenza di cifre $b_1\ldots b_p$ che a partire da un certo punto in poi si ripeta costantemente, cioè α sia della forma*

$$a_0, a_1\ldots a_h b_1\ldots b_p b_1\ldots b_p b_1\ldots b_p\ldots$$ [2]

Allora α è l'espansione decimale di un numero razionale.

Useremo per un tale α la notazione classica $\alpha = a_0, a_1\ldots a_h\overline{b_1\ldots b_p}$, chiamando $b_1\ldots b_p$ il periodo e $a_1\ldots a_h$ l'antiperiodo.

Dimostrazione. Una espansione decimale può essere sempre pensata come la somma di un intero più una espansione decimale con $a_0 = 0$. Pertanto dimostreremo la cosa per le espansioni del tipo $0, a_1\ldots a_h\overline{b_1\ldots b_p}$.

Iniziamo la prova, per semplicità, con un α avente $h = 0$ e $p = 1$, cioè della forma $0,\overline{b_1}$. Dalle considerazioni fatte all'inizio del capitolo, abbiamo per l'allineamento decimale arrestato all'ennesima cifra, che indicheremo con $[0,\overline{b}_1]_n$,

$$[0,\overline{b_1}]_n = \frac{b_1}{10}+\frac{b_1}{10^2}+\ldots+\frac{b_1}{10^n} = \frac{b_1}{10}\left(1+\frac{1}{10}+\frac{1}{10^2}+\ldots+\frac{1}{10^{n-1}}\right) = \frac{b_1}{10}\left(\frac{1-\frac{1}{10^n}}{1-\frac{1}{10}}\right)$$

$$= \frac{b_1}{9}(1-\frac{1}{10^n})$$

[2] in altri termini

$$a_{h+1} = b_1, a_{h+2} = b_2, \ldots, a_{h+p} = b_p, a_{h+p+1} = b_1, a_{h+p+2} = b_2, \ldots, a_{h+2p} = b_p, a_{h+2p+1} = b_1\ldots$$

e quindi, essendo $0 < b_1 \leq 9$, per ogni n si ha che $[0,\overline{b_1}]_n \leq \frac{b_1}{9} < [0,\overline{b_1}]_n + \frac{1}{10^n}$ e quindi che $0,\overline{b}_1$ è l'allineamento decimale di $\frac{b_1}{9}$.

Se $\alpha = 0,\overline{b_1 b_2}$ abbiamo analogamente

$$\begin{aligned}
[0,\overline{b_1 b_2}]_{2n} &= \frac{b_1}{10} + \frac{b_2}{10^2} + \frac{b_1}{10^3} + \frac{b_2}{10^4} + \ldots + \frac{b_1}{10^{2n-1}} + \frac{b_2}{10^{2n}} = \\
&= \frac{b_1}{10}(1 + \frac{1}{10^2} + \ldots + \frac{1}{10^{2(n-1)}}) + \frac{b_2}{10^2}(1 + \frac{1}{10^2} + \ldots + \frac{1}{10^{2(n-1)}}) = \\
&= \left(\frac{b_1}{10} + \frac{b_2}{10^2}\right)\left(\frac{1 - \frac{1}{10^{2n}}}{1 - \frac{1}{10^2}}\right) = \frac{10b_1 + b_2}{99}\left(1 - \frac{1}{10^{2n}}\right) = \frac{b_1 b_2}{99}\left(1 - \frac{1}{10^{2n}}\right)
\end{aligned}$$

e questo mostra, ricordando che $d(x)$ è il $\sup D$, che $0,\overline{b_1 b_2}$ è l'allineamento decimale del razionale $\frac{b_1 b_2}{99}$. A questo punto dovrebbe esser chiaro come dimostrare il caso generale di una espansione decimale periodica senza antiperiodo.

Per il caso in cui ci sia un antiperiodo, iniziamo dal caso $\alpha = 0, a_1\overline{b_1}$.

$$\begin{aligned}
0, a_1\overline{b_1} &= 0, a_1 + 0, 0\overline{b_1} = \frac{a_1}{10} + \frac{1}{10} \cdot 0,\overline{b_1} = \frac{1}{10}(a_1 + \frac{b_1}{9}) = \frac{1}{10}(\frac{a_1 \cdot 9 + b_1}{9}) = \\
&= \frac{1}{10}(\frac{a_1 \cdot (10-1) + b_1}{9}) = \frac{1}{10} \cdot \frac{a_1 b_1 - a_1}{9} = \frac{a_1 b_1 - a_1}{90}
\end{aligned}$$

Da queste considerazioni non dovrebbe esser difficile, e lo lasciamo al lettore, ricavare il noto algoritmo:

La frazione generatrice di un decimale periodico α è il numero razionale con al numeratore il numero ottenuto dalle cifre di α sottraendo l'antiperiodo e al denominatore tanti 9 quante sono le cifre del periodo seguiti da tanti zeri quante sono le cifre dell'antiperiodo. □

Esercizio 6.2.

1. *Caratterizzare i razionali che si rappresentano con una espansione decimale finita.*
2. *Calcolare il numero delle cifre del periodo dell'espansione decimale di $\frac{1}{7}$ e di $\frac{1}{9}$*
3. *Provare come conseguenza dell'algoritmo di divisione che l'espansione decimale che rappresenta un numero razionale è finita o periodica.*

7 Approssimazione.

La Proposizione 2.3 ci garantisce che i numeri razionali della forma $\frac{a}{10^k}$ sono densi in $\mathbb{R}$, cioè per ogni $x \in \mathbb{R}$ ed $\varepsilon \in \mathbb{R}$ esistono $b \in \mathbb{Z}, m \in \mathbb{N}$ tali che

$$\frac{b}{10^m} \leq x < \frac{b}{10^m} + \varepsilon$$

.

La rappresentazione tramite allineamenti decimali finiti ci fornisce una serie di coppie di valori del tipo $a_0, a_1a_2 \dots a_k$ che differiscono da x per al più 10^{-k}. Per esempio per trovare una rappresentazione decimale di $\sqrt{2}$ non è difficile con una calcolatrice verificare che $\sqrt{2}$ è compreso tra $1,4$ e $1,5$ poiché $1,4^2 < 2 < 1,5^2$, Analogamente quadrando e confrontando otteniamo

$$1,41 < \sqrt{2} < 1,42$$

$$1,414 < \sqrt{2} < 1,415$$

$$1,4142 < \sqrt{2} < 1,4143$$

$$1,41421 < \sqrt{2} < 1,41422$$

$$1,414213 < \sqrt{2} < 1,414214$$

$$1,4142135 < \sqrt{2} < 1,4142136$$

$$1,41421356 < \sqrt{2} < 1,41421357$$

$$1,414213562 < \sqrt{2} < 1,414213563$$

Attenzione. Occorre fare attenzione nell'uso di valori approssimati perché l'approssimazione può facilmente peggiorare.

Si prenda ad esempio per $\sqrt{6}$ l'espansione decimale $2,44$ che approssimaper difetto a meno di $\frac{1}{100}$. Ricordando che $\sqrt{6} = \sqrt{2}\sqrt{3}$ utilizzando per $\sqrt{2}$ e $\sqrt{3}$ le rispettive espansioni decimali per difetto approssimate a meno di $\frac{1}{100}$, cioè $1,41$ e $1,73$, moltiplicandole tra di loro otteniamo per $\sqrt{6}$ l'approssimazione per difetto $2,43$ (più precisamente $2,4393$) che è una approssimazione peggiore di $2,44$: $2,44^2 = 5,9536$ e $2,43^2 = 5,9049$.

8 Radici e potenze.

Abbiamo visto che nel corpo ordinato completo $\mathbb{R}$ l'equazione $x^2 = 2$ ha soluzioni. Vediamo ora, con dimostrazione analoga, che dato un elemento $a > 0$ di $\mathbb{R}$ esiste un solo elemento positivo in $\mathbb{R}$ tale che

Proposizione 8.1. *Ogni numero reale positivo a ha un'unica radice n-esima positiva.*

Prova: Procediamo in modo analogo a quanto già fatto per $\sqrt{2}$.

Se $0 < x_1 < x_2$ si ha $0 < x_1^n < x_2^n$ quindi ogni numero reale non può avere più di una radice positiva.

Sia ora $a > 0$ e

$$A = \{x \in \mathbb{R} | x > 0 \; x^n \leq a\}.$$

A è non vuoto ed è superiormente limitato. Infatti

$$c = \min\{1, a\} \in A$$

$$d = \max\{1, a\} \in M$$

.

Esiste pertanto l'estremo superiore, poniamo $x = \sup A$ e proviamo che $x^n = a$.

Poiché $0 < c \leq x$, si scelga un ε tale che $0 < \varepsilon < x$. Allora, essendo $0 < x - \varepsilon < x < x + \varepsilon$ si ha

$$(x - \varepsilon)^n < x^n < (x + \varepsilon)^n.$$

Per le proprietà caratterizzanti l'estremo superiore, fra $x - \varepsilon$ e x vi è certamente un elemento di A mentre $x + \varepsilon \in A$. Pertanto

$$(x - \varepsilon)^n < a < (x + \varepsilon)^n.$$

Da ciò segue

$$|x^n - a| < (x + \varepsilon)^n - (x - \varepsilon)^n < 2^{n+1} x^{n-1} \varepsilon.$$ [3]

Quindi $|x^n - a|$ è minore di ogni prefissato numero positivo e quindi (Prop 2.6) $|x^n - a| = 0$ cioè $x^n = a$. □

A questo punto diventa facile definire che cosa si possa intendere per potenza a esponente reale. In $\mathbb{R}$ possiamo definire $x^n = x \cdot x \cdot \ldots \cdot x$ cioè il prodotto di n copie di x e indicando con $x^{\frac{1}{m}} = \sqrt[m]{x}$, che sappiamo esistere in bse alla proposizione precedente, abbiamo che ha senso la scrittura $x^{\frac{n}{m}} = (x^n)^{\frac{1}{m}}$ e se $x \neq 0$ definiamo $x^{-n} = \frac{1}{x^n}$ se x^n esiste ed infine $x^0 = 1$.

Dalle definizioni date si deducono le usuali regole di calcolo per le potenze

$$x^r \cdot x^s = x^{r+s}$$

$$(x^r)^s = x^{r \cdot s}$$

$$(x \cdot y)^r = x^r \cdot x^s$$

Per definire la potenza x^y nel caso di un esponente y reale qualunque ed una base x positiva si procede così : supponiamo $y > 0$ e $x > 1$: consideriamo l'insieme

$$E = \{x^r | r \in \mathbb{Q}\ r \leq y\};$$

[3] $(x + \varepsilon)^n - (x - \varepsilon)^n = ((x + \varepsilon) - (x - \varepsilon))(\sum_{k=0}^{k=n-1} (x + \varepsilon)^{n-1-k}(x - \varepsilon)^k < 2\varepsilon \cdot ((2x)^{n-1})$

dalle considerazioni fatte risulta che tale insieme è ben definito e che è limitato superiormente in quanto se r è un razionale maggiore di y ogni elemento di E è minore di x^r. Indichiamo con x^y l'estremo superiore dell'insieme E

$$x^y = \sup E.$$

È facile verificare che nel caso y sia razionale la definizione porta allo stesso valore definito in precedenza.

Poniamo per definizione

$$x^y = \begin{cases} \frac{1}{(\frac{1}{x})^y} & \text{se } y > 0 \text{ e } 0 < x < 1 \\ 1 & \text{se } x = 1 \text{ e } y \text{ qualunque} \\ \frac{1}{x^{-y}} & \text{se } y < 0 \text{ e } x \text{ qualunque positivo} \end{cases}$$

e si verificano le usuali proprietà dell'elavzione a potenza.

A questo punto è chiaro come fondare la seguente definizione

Definizione 8.2. *Se a è un numero reale positivo si definisce logarimo di b in base a il numero reale l definito da*

$$a^l = b.$$

Dalle regole di calcolo appena esposte risulta che

$$\log_a(b_1 \cdot b_2) = \log_a(b_1) + \log_a(b_2)$$

proprietà alla base del cosiddetto *regolo calcolatore*e che spiega l'utilizzazione delle scale logaritmiche.

9 Appendici.

A Divisibilità in $\mathbb{Z}$.

Richiamiamo qui brevemente alcuni concetti che dovrebbero esser noti dalla scuola media e che ci serviranno per dare un maggior fondamento ad alcuni concetti espressi anche in altre dispense.

Considereremo come primitivi gli insiemi $\mathbb{N}$ dei numeri naturali e $\mathbb{Z}$ degli interi con le loro operazioni: una trattazione che non consideri questi insiemi come primitivi esula dai limiti di queste dispense.

Per prima cosa ricordiamo la nozione di divisibilità in $\mathbb{Z}$: dati $a, b \in \mathbb{Z}$diciamo che a è *divisibile* per b o che b *divide* a (in simboli $a|b$) se esiste $c \in \mathbb{Z}$ tale che $a = bc$.

Diremo che un elemento $d \in \mathbb{Z}$ è il Massimo Comun Divisore di a e b se

1. d divide a e b
2. se $d'|a$ e $d'|b$ allora $d'|d$.

Teorema A.1. *$\forall a, b \in \mathbb{Z}$ esiste il MCD.*

Proveremo questo teorema utilizzando la *divisione euclidea*

Teorema A.2 (**Divisione euclidea**)**.** *Per ogni $a, b \in \mathbb{Z}$ con $b \neq 0$ esistono unici $q, r \in \mathbb{Z}$ tali che*

1. $a = bq + r$
2. $0 \leq r < |b|$

Prova: Consideriamo l'insieme

$$R = \{a - nb \geq 0\}$$

Tale insieme è non vuoto perché lameno uno dei due numeri che si ottengono ponendo $n = a$ oppure $n = -a$, appartiene a R. Infatti se $a + ab = a(1 + b) < 0$ ciò significa che a e $1 + b$ sono di segno discorde e quindi risulta $a - ab > 0$ perché se $a > 0$ allora deve essere $1 + b < 0$ cioè $b < -1$ e quindi $a(1 - b) > 0$mentre se $a < 0$ allora $1 + b > 0$ e quindi ancora $a(1 - b) > 0$.

Per il principio del buon ordinamento abbiamo che R ha un minimo elemento: indichiamo con r tale minimo e con q il rispettivo n.

Risulta $0 \leq r < |b|$: infatti se cosí non fosse si avrebbe $r' = r - |b| > 0$ e $r' = r - |b| = a - qb - |b| = a - \left(q + \frac{|b|}{b}\right) b = a - q'b$ e quindi avremmo che anche $r' \in R$ e iò in contraddizione che r è il minimo.

Deriviamo da questa condizione l'unicità del queoziente e del resto.

Se q' e r' sono due altri interi che verificano il teorema, da

1. $a = bq + r$ con $0 \leq r < |b|$
2. $a = bq' + r'$ con $0 \leq r' < |b|$

sottraendo la (2) dalla (1) otteniamo $-b(q - q') = r - r'$. La condizione sui resti implica che $r - r' \leq r < |b|$ e $r' - r \leq r' < |b|$, cioè in definitiva che $|r - r'| < |b|$. mentre $-b(q - q') = r - r'$ implica che $|b||q - q'| = |r - r'|$, cioè che $|q - q'| < 1$ il che implica $q = q'$ e di conseguenza $r = r'$.

□

Ossrvazione A.3. *Osserviamo che il resto della divisione euclidea è positivo. Quindi abbiamo*

a	b	q	r
5	*2*	*2*	*1*
-5	*2*	*-3*	*1*
5	*-2*	*-2*	*1*
2	*5*	*0*	*2*

Teorema A.4. *Per ogni coppia di numeri interi a, b non nulli esiste il Massimo Comun Divisore.*

Prova: Otterremo questo teorema come conseguenza della divisione euclidea.

Siano infatti a, b due numeri interi ed eseguiamo la divisione euclidea di a per b:

$$a = bq + r$$

Se $r = 0$ è evidente che il Massimo Comun Divisore tra a e b è b.

Se $r \neq 0$ dividiamo b per r:

$$b = rq_1 + r_1$$

Se $r_1 = 0$ è evidente che r divide sia b che a e quindi è un divisore e viceversa che se d divide sia a che b divide r e quindi che r è il Massimo Comun Divisore tra a e b.

Se $r_1 \neq 0$ iteriamo l'operazione dividendo r per r_1.

$$r = r_1q_2 + r_2.$$

Ancora una volta se $r_2 = 0$ risulta che r_1 dividendo r e r_1 divide b e dividendo r e b divide a e quindi che r_1 è un divisore comune tra a e b. Viceversa se d divide sia a che b divide r e dividendo sia b che r divide r_1. Quindi r_1 è il Massimo comun divisore tra a e b.

Se $r_2 \neq 0$ iteriamo l'operazione fino a che non troviamo un resto $r_{n+1} = 0$, cosa assicurata dal fatto che ogni volta abbiamo per il resto r_i $r_i < r_{i-1}$.

Ragionando come prima, cioè risalendo e discendendo lungo le divisioni successive, si vede che r_n divide a e b e che se d divide a e b allora d divide r_n e quindi che r_n è il Massimo Comun Divisore tra a e b. □

B Qualche discorso sui razionali.

Consideriamo l'insieme delle coppie $(a, b) \in \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$ e su questo insieme la relazione

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

. È di immediata verifica che tale relazione è riflessiva simmetrica e transitiva, cioè è una relazione di equivalenza. Indichiamo con $[(a, b)]$ la classe di equivalenza della coppia (a, b) e con X l'insieme di tali classi.

Sull'insieme X possiamo definire due operazioni

$$[(a, b)] + [(c, d)] = [(ad + bc, bd)]$$

$$[(a, b)] \cdot [(c, d)] = [(ac, bd)]$$

Occorre verificare che la definizione data sia ben posta, cioè non dipenda dal rappresentante scelto per la classe.

Per la somma ciò significa che se (a', b') è un altro rappresentante della classe $[(a, b)]$, cioè $a'b = ab'$, e (c', d') un altro rappresentante della classe $[(c, d)]$, cioè $c'd = cd'$, si deve avere che $(ad+bc, bd) \sim (a'd'+b'c', b'd')$, cioè $(ad+bc)b'd' = (a'd'+b'c')bd$. Ma

$$(ad + bc)b'd' = ab'dd' + cd'bb' = a'bdd' + c'dbb' = (a'd' + b'c')bd$$

che è esattamente quello che si voleva. Per il prodotto la verifica è del tutto analoga. Indicheremo con $\frac{a}{b}$ la classe $[(a, b)]$. Pertanto $\frac{a}{b}$ e $\frac{a'}{b'}$ individuano la stessa classe se $(a, b) \sim (a', b')$. In particolare, poiché possiamo scegliere come rappresentante di una classe di equivalenza una coppia (a, b) ridotta ai minimi termini, cioè con a, b tali che $MCD(a, b) = 1$, in quanto $(a, b) \sim (ak, bk)$ per ogni $k \neq 0$, dovrebbe risultar chiaro che cosa si intenda con il fatto che un rappresentante può essere scelto "ridotto ai minimi termini" [4] e che la somma di due razionali $\frac{a}{b} + \frac{c}{d}$, entrambi ridotti ai minimi termini, si ottiene riducendo ai minimi termini $\frac{ad + bc}{bd}$.

[4] confronta in particolare l'affermazione in fondo alla pagina 9 della dispensa INSIEMI sulla rappresentazione di un numero razionale come frazione ridotta a minimi termini

Un'altra verifica immediata è che in questo insieme valgono le usuali proprietà delle operazioni nei razionali. E cioè, indicando con 0 la classe $(0, a)$ e con u la classe $[(a, a)]$ si ha

1. Entrambe le operazioni godono della proprietà associativa, cioè $\forall\ q, r, s \in X\ \ (q + r) + s = q + (r + s)$ e $\forall\ q, r, s \in X\ \ (q \cdot r) \cdot s = q \cdot (r \cdot s)$
2. Entrambe le operazioni godono della proprietà commutativa, cioè $\forall\ q, r \in X\ \ q + r = r + q$ e $\forall\ q, r \in X\ \ q \cdot r = r \cdot q$.
3. Esiste un elemento neutro per la somma, cioè $\exists$ 0tale che$\forall q \in X q+0 = 0+q = q$, ed un elemento neutro per il prodotto , cioè $\exists\ e$ tale che $\forall q \in X\ \ q \cdot e = e \cdot q = q$
4. Esiste un inverso per la somma per ogni elemento e un inverso per il prodotto per ogni elemento diverso da 0, cioè $\forall\ q \in X \exists\ q'$ tale che $q + q' = q' + q = 0$ e $\forall\ q \in X\ q \neq 0\ \exists\ q'$ tale che $q \cdot q' = q' \cdot q = e$.
5. Vale la proprietà associativa, cioè $\forall\ q, r, s \in X\ \ (q + r) \cdot s = q\dot{s} + r \cdot s$ e analogamente a sinistra.

Indicheremo rispettivamente con 0 l'elemento neutro per la somma e con 1 quello per il prodotto.

Si osservi che l'elemento neutro per la somma e per il prodotto sono unici, infatti se ce ne fossero due, 0 e $0'$ si avrebbe

$$0 = 0 + 0' = 0'$$

e analogamente per il prodotto.

Ciò implica che $\forall q \in X$ si ha $q \cdot 0 = 0$. Infatti $q \cdot 0 = q \cdot (0 + 0) = q \cdot 0 + q \cdot 0$ da cui per l'unicità dell'elemento neutro si ha $q \cdot 0 = 0$. Quindi, punto (4), non può esistere un elemento che moltiplicato per 0 dia 1.

Ragionando in modo analogo si verifica che in X come conseguenza delle proprietà appena dette valgono tutte le usuali regole di calcolo.

D'ora in poi indicheremo con $\mathbb{Q}$ l'insieme X con le operazioni definite.

In X sappiamo quindi risolvere le equazioni del tipo $ax = b$ con $a, b \in \mathbb{Z}$ però, come abbiam visto, non esiste nessun elemento q tale che $q^2 = 2$, cioè non sappiamo risolvere le equazioni del tipo $x^2 - 2 = 0$.

Con il passaggio al corpo (ordinato,completo) dei reali si estende $\mathbb{Q}$ ad un ambiente più ampio,dove in particolare una equazione come $x^2 - 2 = 0$ ha soluzione: questo ambiente fornirà anche l'ambiente ideale per trattare molte altre questioni.