Costruzione dei Reali Secondo Cauchy.

Dato un qualunque campo ordinato K mostreremo come si può costruire un'estensione, che sia un campo ordinato Ω in cui valga il *teorema di convergenza di Cauchy*. Se, in particolare, K è il campo dei numeri razionali $\mathbb{Q}$, allora Ω sarà il campo dei numeri reali.

Una successione infinita di elementi $a_1, ..., a_n = \{a_n\}$ in un campo ordinato K è detta *successione fondamentale* o *di Cauchy*, se, per ogni elemento positivo ϵ di K, esiste un intero $n = n(\epsilon)$ (n dipende da ϵ) tale che

(1) $|a_p - a_q| < \epsilon$ per $p > n, q > n$.

Osserviamo innanzitutto che una successione fondamentale è limitata superiormente e inferiormente. Infatti per $q = n+1$, da (1) si ha[1]

$$|a_p| \leq |a_q| + |a_p - a_q| \leq |a_{n+1}| + \epsilon = M \qquad \forall p > n.$$

Ora proviamo che somme e prodotti di successioni fondamentali sono ancora successioni fondamentali.

Siano $\{a_n\}$ e $\{b_n\}$ due successioni fondamentali; quindi $\forall \epsilon > 0$ esiste $n_1 = n_1(\epsilon) \in \mathbb{N}$ tale che

$$|a_p - a_q| < \frac{1}{2}\epsilon \qquad \forall p, q > n_1$$

ed in corrispondenza dello stesso ϵ esiste $n_2 = n_2(\epsilon) \in \mathbb{N}$ tale che

$$|b_p - b_q| < \frac{1}{2}\epsilon \qquad \forall p, q > n_2.$$

Scegliendo $n > \max\{n_1, n_2\}$ si ha

$$|(a_p + b_p) - (a_q + b_q)| = |(a_p - a_q) + (b_p - b_q)| \leq$$

[1] Abbiamo usato la disuguaglianza triangolare.

$$\leq |a_p - a_q| + |b_p - b_q| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon$$

quindi la successione $\{a_n + b_n\}$ è anch'essa una successione fondamentale.

Similmente $\exists M_1, M_2$ tali che

$$|a_p| < M_1 \qquad \forall p > n_1,$$

$$|b_p| < M_2 \qquad \forall p > n_2,$$

ed inoltre, $\forall \epsilon > 0$ esistono $n' \geq n_1, n'' \geq n_2$ tali che

(2) $|a_p - a_q| < \frac{\epsilon}{2M_2} \qquad \forall p > n', q > n'$;

(3) $|b_p - b_q| < \frac{\epsilon}{2M_1} \qquad \forall p > n'', q > n''$.

A questo punto, moltiplicando la relazione (2) per $|b_p|$ e la relazione (3) per $|a_q|$ si ottiene

$$|a_p b_p - a_q b_p| \leq |b_p||a_p - a_q| \leq M_2 \cdot \frac{\epsilon}{2M_2} = \frac{\epsilon}{2};$$

$$|a_q b_p - a_q b_q| \leq |a_q||b_p - b_q| \leq M_1 \cdot \frac{\epsilon}{2M_1} = \frac{\epsilon}{2}.$$

Quindi, se $n > \max\{n', n''\}$, si ha

$$|a_p b_p - a_q b_q| = |a_p b_p - a_q b_p + a_q b_p - a_q b_q| \leq$$

$$\leq |a_p b_p - a_q b_p| + |a_q b_p - a_q b_q| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon.$$

Abbiamo dimostrato che la successione $\{a_n \cdot b_n\}$, prodotto di due successioni fondamentali, è una successione fondamentale.

Le successioni fondamentali formano dunque un anello A (si possono facilmente verificare le opportune proprietà di somma e prodotto).

Una successione fondamentale $\{a_m\}$ che converge a *zero*, ovvero tale che $\forall \epsilon > 0$ esiste $n_1 \in \mathbb{N}$ tale che

$$|a_p| < \epsilon \qquad \forall p > n_1$$

è detta *successione nulla.*

Definizione 1. *Un sottoinsieme Y di un anello A è detto ideale se $a \in y$ implica $a \cdot r \in Y$ per ogni $r \in A$.*

Lemma 1. *Le successioni nulle formano un ideale Y.*

DIMOSTRAZIONE. Se $\{a_p\}$ e $\{b_p\}$ sono successioni nulle, allora $\forall \epsilon > 0 \, \exists n_1, n_2 \in \mathbb{N}$ t.c.

$$|a_p| < \frac{1}{2}\epsilon \, \forall p > n_1,$$

$$|b_p| < \frac{1}{2}\epsilon \, \forall p > n_2,$$

scegliendo $n > \max\{n_1 n_2\}$ si ottiene

$$|a_p - b_p| < |a_p| + |b_p| < \epsilon \, \forall p > n.$$

Quindi $\{a_p - b_p\}$ è una successione nulla. Se, inoltre, $\{a_p\}$ è una successione nulla e $\{c_p\}$ è una qualunque successione fondamentale, troviamo M ed n' tali che

$$|c_p| < M \quad \forall p > n'$$

e $\forall \epsilon$ troviamo $n = n(\epsilon) \geq n'$ tale che

$$|a_p| < \frac{\epsilon}{M} \quad \forall p > n.$$

Segue che

$$|a_p c_p| < |a_p||c_p| < \epsilon \, \forall p > n,$$

quindi $\{a_p c_p\}$ è una successione nulla, il che prova che Y è un ideale.

□

L'insieme quoziente $A/Y = \Omega$ è un campo.

Infatti basterà provare che ogni elemento $a \neq [0]$ ammette l'inverso, ovvero che l'equazione $(*) a \cdot x = \underline{1}$ ha sempre soluzione (se $a \neq [0]$). L'elemento neutro $\underline{1}$ corrisponde alla successione fondamentale $\{1, 1, ..., 1\}$. Sicuramente esistono $n \in \mathbb{N}$ e $\eta > 0$ tali che

$$|a_q| \geq \eta \text{ per } q > n,$$

infatti se, $\forall n \in \mathbb{N}$ e $\forall \eta > 0$ si avesse $|a_p| < \eta$ per qualche $q > n$, allora per un certo η potremmo scegliere n abbastanza piccolo in modo che, $\forall p > n, q > n$, si avrebbe

$$|a_p - a_q| < n \text{ quindi } |a_p| < 2\eta \, \forall p > n.$$

Quindi la successione $\{a_p\}$ sarebbe nulla, contrariamente all'ipotesi. La successione fondamentale $\{a_p\}$ rimane nella stessa classe di equivalenza (rispetto alla relazione introdotta) se rimpiazziamo i termini $a_1, ..., a_n$ con η. Allora si avrà $|a_p| \geq \eta \quad \forall p \in \mathbb{N}$ e in particolare $a_p \neq 0$.

La successione $\{a_p^{-1}\}$ è una successione fondamentale. Infatti $\forall \epsilon > 0 \, \exists n \in \mathbb{N}$ tale che

(4) $|a_p - a_p| < \epsilon \eta^2$ per $p > n, q > n$.

Ora, se si avesse $|a_p^{-1} - a_q^{-1}| \geq \epsilon$ per un certo $p \geq n$ e $q > n$, allora, moltiplicando per $|a_p| \geq n$ e $|a_q| \geq n$ seguirebbe che:

$$|a_q - a_p| = |a_p a_q (a_p^{-1} - a_q^{-1})| \geq \epsilon \eta^2$$

che contraddice (4). Per cui

$$|a_p^{-1} - a_q^{-1}| < \epsilon \text{ per } p > n, q > n.$$

Ovviamente la successione fondamentale $\{a_p^{-1}\}$ risolve l'equazione $(*)$.

Il campo Ω contiene, in particolare, le classi di equivalenza che sono rappresentate da successioni del tipo $\{a, a, a, a, a, ..., a\}$. Queste ultime formano un sottoanello K' di Ω isomorfo a K; infatti ad ogni $a \in K$ corrisponde una classe di equivalenza di questo tipo, ad elementi a diversi corrispondono diverse classi di equivalenza, e alla somma e al prodotto corrispondono la somma e il prodotto di classi, rispettivamente. Se adesso identifichiamo gli elementi di K' con quelli di K, Ω diventa un campo che è estensione di K nel senso seguente.

Definizione 2. *Se A è e un sottocampo (sottoinsieme che è a sua volta un campo) di un campo Ω, Ω è detto campo estensione di A.*

Definizione 3. *Una successione fondamentale $\{a_p\}$ si dice positiva se esiste $\epsilon > 0$ in K e $n \in \mathbb{N}$ tale che $a_p > \epsilon \, \forall p > n$.*

Chiaramente la somma e il prodotto di due successioni fondamentali positive sono positive. Similmente, la somma di una successione $\{a_p\}$ positiva e di una $\{b_p\}$ nulla è sempre positiva; questo si può provare scegliendo n abbastanza grande da avere

$$a_p > \epsilon \quad \forall p > n$$

$$|b_p| < \frac{1}{2}\epsilon \quad \forall p > n$$

allora $a_p + b_p > \frac{1}{2}\epsilon \, \forall p > n$. Quindi tutte le successioni di una classe sono positive se una di esse è positiva. In questo caso la classe stessa è detta positiva. Una classe K è detta negativa se $(-K)$ è positiva.

Se né $\{a_p\}$ né $\{-a_p\}$ sono positive, allora, $\forall \epsilon > 0$ e $\forall n \in \mathbb{N}$, esistono $r > n$ e $s > n$ tali che

$$a_r \leq \epsilon \text{ e } -a_r \leq \epsilon.$$

Scegliendo n abbastanza grande da avere per $p > n, q > n$ $|a_p - a_q| < \epsilon$, allora scegliendo prima $q = r$ e $p > n$ arbitrario, si conclude che

$$a_p = (a_p - a_q) + a_r < \epsilon + \epsilon = 2\epsilon,$$

e poi per $q = s$ e $p > n$ arbitrario

$$-a_p = (a_q - a_p) - a_s < 2\epsilon.$$

Di conseguenza

$$|a_p| < 2\epsilon \quad \forall p > n$$

e $\{a_p\}$ è una successione nulla. Per cui le uniche tre possibilità sono che una successione $\{a_p\}$ sia positiva, negativa o nulla e così per le classi di equivalenza. Poichè la somma e il prodotto di classi di equivalenza positive sono classi di equivalenza positive, possiamo affermare che Ω è un campo ordinato.

Si vede subito che l'ordinamento di K si conserva in Ω.

Se una successione $\{a_p\}$ definisce un elemento α, e una successione $\{b_p\}$ un elemento β di Ω, segue da

(5) $a_p \geq b_p$ per $p > n$.

che $\alpha \geq \beta$. Infatti se fosse $\alpha < \beta$, quindi $\beta - \alpha > 0$, allora esisterebbero $\epsilon > 0$ e $m \in \mathbb{N}$ tali che la successione $\{b_p - a_p\}$ verifica

(6) $b_p - a_p > \epsilon > 0$ per $p > m$.

Scegliendo $p = m + n$ in (6) la (5) viene contraddetta. È utile ricordare che $a_p > b_p$ non implica che $\alpha > \beta$ ma solo che $\alpha \geq \beta$.

Il fatto che ogni successione fondamentale sia limitata dell'alto, implica che, per ogni $\omega \in \Omega$, esiste un elemento s di K che supera ω. Se l'ordinamento di K è <u>Archimedeo</u> esiste un intero $n > s$; quindi per ogni ω esiste $n > \omega$, ovvero, l'ordinamento di Ω è <u>Archimedeo</u>.

Nel campo Ω possiamo definire di nuovo i concetti di valore assoluto, successione fondamentale, successione nulla. Le successioni nulle di nuovo formano un ideale. Se una successione $\{a_p\}$ è equivalente ad una successione costante mediante la relazione di equivalenza indotta dalle successione nulle, ovvero, $\{a_p - \alpha\}$ è una successione nulla, diremo che la successione $\{a_p\}$ converge al limite α. In simboli

$$\lim_{p\to\infty} a_p = \alpha.$$

Le successioni fondamentali $\{a_p\}$ di K che sono state usate per definire gli elementi di Ω possono ovviamente venire considerate successioni fondamentali in Ω, poichè $K \subseteq \Omega$.

Proposizione 2. *Se la successione $\{a_p\}$ definisce l'elemento $\alpha \in \Omega$, allora $\lim_{p\to\infty} a_p = \alpha$.*

DIMOSTRAZIONE. Osserviamo che per ogni $\epsilon > 0$ in Ω esiste un $\epsilon' > 0$ in K, $\epsilon' < \epsilon$, per il quale esiste n tale che, per $p > n, q > n$, si ha

$$|a_p - a_q| < \epsilon'.$$

Cioè sia $a_p - a_q$ che $a_q - a_p$ sono minori di ϵ'. Se ora fissiamo p e facciamo tendere q a $+\infty$ segue che $a_p - \alpha$ e $\alpha - a_p$ sono entrambe minori di ϵ', quindi

$$|a_p - \alpha| \leq \epsilon' < \epsilon.$$

Quindi $\{a_p - \alpha\}$ è una successione nulla ($\Leftrightarrow \lim_{p\to\infty} a_p = \alpha$).

□

Ora vogliamo provare che il campo Ω non può essere esteso ulteriormente attraverso le successioni fondamentali, poichè ogni successione fondamentale $\{\alpha_p\}$ ha già un limite in Ω (Teorema di convergenza di Cauchy!!).

DIMOSTRAZIONE. Possiamo supporre che nella successione $\{a_p\}$ due elementi successivi qualunque, α_p e α_{p+1}, sono sempre diversi; se non fosse così basterebbe scegliere una sottosuccessione formata dagli α_p tali che $\alpha_p \neq \alpha_{p+1}$; oppure, se la successione α_p fosse costante da un certo p in poi, $\alpha_p = \alpha$ per $p > n$, sarebbe ovvio che

$$\lim_{p\to\infty} \alpha_p = \alpha.$$

Poniamo ora $|\alpha_p - \alpha_{p-1}| = \epsilon_p > 0$.

Poichè $\{\alpha_p\}$ è una successione fondamentale, $\{\epsilon_p\}$ è una successione nulla. Per ogni α_p scegliamo un a_p che lo approssimi, ovvero

$$|a_p - \alpha_p| < \epsilon_p.$$

Questo è sempre possibile, poichè α_p stessa è stata definita attraverso una successione fondamentale $\{a_{p_1}, ..., a_{p_n}$ con limite α_p. Inoltre $\forall \epsilon > 0$ esiste n' tale che

$$|\alpha_p - \alpha_q| < \frac{1}{3}\epsilon\, \forall p > n', q > n'$$

e n'' tale che

$$\epsilon_p < \frac{1}{3}\epsilon \quad \forall p > n''.$$

Se $n > \max\{n', n''\}$, allora, per $p > n, q > n$, si ha

$$|a_p - \alpha_p| < \frac{1}{3}\epsilon;\, |\alpha_p - \alpha_q| < \frac{1}{3}\epsilon;\, |\alpha_q - a_q| < \frac{1}{3}\epsilon$$

da cui

$$|a_p - a_q| \leq |a_p - \alpha_q| + |\alpha_p - \alpha_q| + |\alpha_q - a_q| < \epsilon.$$

Quindi le $\{a_p\}$ sono una successione fondamentale in K che definisce un elemento ω di Ω. La successione $\{\alpha_p\}$ differisce da questa successione fondamentale solo per una successione nulla $\{a_p - \alpha_p\}$; e quindi ha lo stesso limite ω.

□

La costruzione di cui sopra quindi fornisce per ogni campo ordinato K un'estensione ordinata univocamente determinata da Ω, in cui il *Teorema di convergenza di Cauchy* è verificato. Se, in particolare K è il campo $\mathbb{Q}$ dei numeri razionali, allora Ω /'e il campo $\mathbb{R}$ dei numeri reali. Pertanto secondo questa teoria un numero reale è definito come una classe di equivalenza "modulo" l'ideale delle successioni fondamentali di numeri razionali.

Sia Σ un campo ordinato e $\mathcal{M}$ un insieme non vuoto di elementi di Σ. Se esiste un elemento $s \in K$ tale che $a \leq s$ per ogni $a \in \mathcal{M}$, allora s è detto maggiorante per $\mathcal{M}$ e si dice che $\mathcal{M}$ è limitato superiormente. Se esiste il minimo dei maggioranti, questo viene chiamato estremo superiore di $\mathcal{M}$.

Proposizione 3. *Consideriamo l'estensione Ω di K appena costruita: si può provare l'esistenza dell'estremo superiore se l'ordinamento di K, e quindi anche quello di Ω, è Archimedeo.*

DIMOSTRAZIONE. L'esistenza dell'estremo superiore non si può provare se l'ordinamento del campo in questione non è Archimedeo. Infatti, se consideriamo la successione di numeri naturali $1, 2, 3, ...$, allora esisterebbe un elemento s del campo maggiore di tutti i numeri naturali; la successione sarebbe quindi limitata. Se g fosse l'estremo superiore della successione, allora $2g$ sarebbe l'estremo superiore della successione $2, 4, 6....$ Poichè g è sicuramente positivo, $g < 2g$, ma g è un maggiorante per tutti i numeri della forma $2n$, e quindi $2g$ non può essere l'estremo superiore. Quindi l'estremo superiore può esistere solo in un campo Archimedeo.

□

Infine proviamo che

1) ogni campo ordinato Archimedeo è isomorfo (con un isomorfismo che conserva l'ordine) a un sottocampo K' del campo $\mathbb{R}$ dei numeri reali;
2) se il *Teorema dell'esistenza dell'estremo superiore* vale in K, allora $K' = \mathbb{R}$ e K è isomorfo (con un isomorfismo che conserva l'ordine) al campo $\mathbb{R}$ dei numeri reali.

DIMOSTRAZIONE 1). Ogni elemento a di K è estremo superiore di un insieme r di numeri razionali. Ad esempio si può scegliere come $r = \{x \in \mathbb{Q} : x < a\}$. Questo stesso insieme ha un estremo superiore a' in $\mathbb{R}$. La corrispondenza $a \to a'$ è un isomorfismo additivo, ovvero alla somma $a + b$ corrisponde $a' + b'$. Il nucleo (insieme degli elementi a che l'anamorfismo trasforma nello zero) dell'anamorfismo consiste solo nello zero e quindi questo anamorfismo è un isomorfismo additivo. Al prodotto $a \cdot b$ di due elementi corrisponde il prodotto $a' \cdot b'$. Quindi ai prodotti

$$(-a)b = -ab \text{ e } (-a)(-b) = ab$$

corrispondono in $\mathbb{R}$ i numeri

$$-a'b' = (-a')b' \text{ e } a'b' = (-a')(-b').$$

Pertanto, più in generale, prodotti corrispondono a prodotti. Elementi positivi di K' corrispondono a elementi positivi di K; quindi K è isomorfo (con un isomorfismo che conserva l'ordine) a K'.

□

DIMOSTRAZIONE 2). Se il teorema dell'esistenza dell'estremo superiore vale in K, allora, in particolare, ogni insieme di numeri razionali limitato dall'alto ha un estremo superiore a in K; lo stesso insieme ha anche un estremo superiore a' in K'. Da questo segue che ogni numero reale sta in K', dato che ogni numero reale è estremo superiore di un insieme di numeri razionali. Avremo dunque $K' = \mathbb{R}$.

□