Numeri

Pino Vigna Suria

25 3 2003

1 Numeri naturali

Definizione 1. *Un* sistema di numeri naturali *è una terna ordinata* $(\mathbb{N}, 0, \sigma)$, *dove* $\mathbb{N}$ *è un insieme,* $0 \in \mathbb{N}$, *e* σ *è una funzione iniettiva di* $\mathbb{N}$ *in sé che soddisfa i seguenti assiomi:*

N1 $0 \notin \sigma(\mathbb{N})$.

N2 Se U *è un sottoinsieme di* $\mathbb{N}$ *tale che* $0 \in U$ *e* $\sigma(U) \subseteq U$ *allora* $U = \mathbb{N}$.

Sia $(\mathbb{N}, 0, \sigma)$ un sistema di numeri naturali, chiameremo σ - *chiuso* un sottoinsieme U di $\mathbb{N}$ tale che $\sigma(U) \subseteq U$, gli elementi di $\mathbb{N}$ saranno detti *numeri naturali* e la funzione σ prende il nome di *funzione successore.* È facilissimo controllare che $\{0\} \bigcup \sigma(\mathbb{N})$ è σ-chiuso e quindi $\sigma(\mathbb{N}) = \mathbb{N} - \{0\}$.

Proposizione 1. *Esiste un sistema di numeri naturali se e solo se esiste un insieme infinito.*

Dimostrazione. Ricordiamo che un insieme X si dice *infinito* se esiste una funzione iniettiva ma non suriettiva da X in sé. Una delle due implicazioni è dunque evidente.

Supponiamo allora di avere un insieme X e una funzione f di X in sé che sia iniettiva ma non suriettiva. Sia $x \in X - f(X)$. Definiamo una famiglia $\mathcal{N}$ di sottoinsiemi di X nel modo seguente:

$$\mathcal{N} = \{Y \subseteq X \text{ tali che } x \in Y \text{ e } f(Y) \subseteq Y\}.$$

$\mathcal{N}$ non è vuoto perché X vi appartiene ed è facile controllare che $\mathbb{N} = \bigcap \mathcal{N}$ è a sua volta un elemento di $\mathcal{N}$. Indicando con σ la restrizione di f a $\mathbb{N}$ si verifica facilmente che la terna ordinata $(\mathbb{N}, x, \sigma)$ è effettivamente un sistema di numeri naturali. □

Lo strumento più importante nel maneggiare un sistema di numeri naturali è costituito dal seguente teorema, che viene chiamato *principio di definizione per ricorsività.*

Teorema 1. *Siano* $(\mathbb{N}, 0, \sigma)$ *un sistema di numeri naturali,* X *un insieme,* x *un suo elemento e* $f \in X^X$.

Esiste un'unica funzione $\phi : \mathbb{N} \longrightarrow X$ *tale che*

- $\phi(0) = x$.
- $\forall n \in \mathbb{N} \quad \phi(\sigma(n)) = f(\phi(n))$.

Dimostrazione. Siano $\phi, \psi \in X^{\mathbb{N}}$ funzioni che soddisfano quanto richiesto e sia $U = \{n \in \mathbb{N}$ tali che $\phi(n) = \psi(n)\}$. $0 \in U$ perché $\phi(0) = x = \psi(0)$, e U è σ-chiuso perché, se $n \in U$, allora

$$\phi(\sigma(n)) = f(\phi(n)) = f(\psi(n)) = \psi(\sigma(n)).$$

Quindi $U = \mathbb{N}$ e l'unicità è dimostrata.

Per quanto riguarda l'esistenza osserviamo che una funzione $\phi : \mathbb{N} \longrightarrow X$ è un sottoinsieme $\phi \subseteq \mathbb{N} \times X$ tale che $\forall n \in \mathbb{N} \quad \exists ! \, y \in X$ tale che $(n, y) \in \phi$. Definiamo una famiglia $\oplus$ di sottoinsiemi di $\mathbb{N} \times X$ ponendo

$$\Phi = \{W \subseteq \mathbb{N} \times X \text{ tali che } (0, x) \in W \text{ e } (n, y) \in W \Rightarrow (\sigma(n), f(y)) \in W\}.$$

Tale famiglia non è vuota perché $\mathbb{N} \times X \in \Phi$ ed evidente che $\phi = \bigcap \Phi \in \Phi$, per cui si tratta solo di verificare che ϕ è una funzione.

Sia $U = \{n \in \mathbb{N}$ tali che $\exists ! \, y \in X$ tale che $(n, y) \in \phi\}$.

Verifichiamo che $0 \in U$; certamente $(0, x) \in \phi$ e sia, per assurdo, $x \neq y \in X$ tale che $(0, y) \in \phi$. Poniamo $W = \phi - \{(0, y)\}$; si tratta di un sottoinsieme proprio di ϕ e l'assurdo verrà manifestato controllando che $W \in \Phi$. Evidentemente $(0, x) \in W$ e , se $(n, z) \in W$ allora $(\sigma(n), f(z)) \in W$ visto che sta certamente in ϕ ed è una coppia ordinata diversa da $(0, y)$ in quanto $\sigma(n) \neq 0$.

Se riusciamo a provare che U è σ-chiuso deduciamo che $U = \mathbb{N}$ e dunque ϕ è una funzione. Supponiamo dunque che $n \in U$ e che, per assurdo, $\sigma(n) \notin U$, chiamiamo y l'unico elemento di X tale che $(n, y) \in \phi$; certamente $(\sigma(n), f(y)) \in \phi$ e dunque l'ipotesi assurda che stiamo esaminando ci dice che esiste $f(y) \neq z \in X$ tali che $(\sigma(n), z) \in \phi$. Definiamo $W = \phi - \{(\sigma(n), z)\}$ e troveremo l'assurdo provando che $W \in \Phi$. Certamente $(0, x) \in W$ in quanto

tale coppia ordinata sta in ϕ ed è diversa da $(\sigma(n), z)$; sia poi $(m, t) \in W$ e verifichiamo che anche $(\sigma(m), f(t)) \in W$. Negare questa inclusione significa che $(\sigma(m), f(t)) = (\sigma(n), z)$ e, dal fatto che σ è iniettiva, possiamo dedurne che $m = n$ e che $f(t) = z$, quindi $(n, t) = (m, t) \in W \subseteq \phi$. Dal fatto che $n \in U$ si evince che $t = y$ e quindi $z = f(t) = f(y)$, assurdo. □

Scegliamo un qualunque elemento $m \in \mathbb{N}$ e applichiamo il principio di definizione per ricorsività scegliendo $X = \mathbb{N}$, $x = m$, $f = \sigma$. Troveremo un'unica funzione $\sigma_m : \mathbb{N} \longrightarrow \mathbb{N}$ caratterizzata da

$$\sigma_m(0) = m \text{ e, } \forall n \in \mathbb{N}, \quad \sigma_m(\sigma(n)) = \sigma(\sigma_m(n)).$$

Questo ci permette di definire un'operazione binaria interna, detta *somma*,

$$+ : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$$

ponendo $m + n = \sigma_m(n)$.

Tale operazione è dunque caratterizzata da $\forall m \in \mathbb{N} \quad m + 0 = m$ e da $\forall m, n \in \mathbb{N} \quad m + \sigma(n) = \sigma(m + n)$; queste due proprietà saranno sufficienti per provare le rilevanti proprietà della somma elencate nel seguente

Teorema 2. $\forall n, m, p \in \mathbb{N}$ *valgono le seguenti* proprietà della somma

1. $0 + m = m$.
2. $\sigma(m) + n = \sigma(m + n)$.
3. $(m + n) + p = m + (n + p)$, proprietà associativa della somma.
4. $m + n = n + m$, proprietà commutativa della somma.
5. $m + n = 0 \Leftrightarrow m = n = 0$.
6. $m + n = m + p \Leftrightarrow n = p$, proprietà di cancellazione.

Dimostrazione. Si tratta di verifiche semplici fino alla noia, a condizione che si rispetti l'ordine proposto.

1. Sia $U = \{m \in \mathbb{N} \text{ tali che } 0 + m = m\}$. Ovviamente $0 \in U$; inoltre, se $m \in U$, allora
$$0 + \sigma(m) = \sigma(0 + m) = \sigma(m).$$
Cioè U è σ-chiuso e quindi $U = \mathbb{N}$.

2. Sia $m \in \mathbb{N}$ e poniamo $U = \{n \in \mathbb{N} \text{ tali che } \sigma(m) + n = \sigma(m+n)\}$. Certamente $0 \in U$ e, se $n \in U$, allora

$$\sigma(m) + \sigma(n) = \sigma(\sigma(m) + n) = \sigma(\sigma(m+n)) = \sigma(m + \sigma(n)).$$

Dunque $U = \mathbb{N}$.

3. Siano $m, n \in \mathbb{N}$ e poniamo

$$U = \{p \in \mathbb{N} \text{ tali che } (m+n) + p = m + (n+p)\}.$$

Se $p \in U$ allora

$$(m+n) + \sigma(p) = \sigma((m+n) + p) = \sigma(m + (n+p))$$

$$= m + \sigma(n+p) = m + (n + \sigma(p)).$$

Dunque U è σ-chiuso; dato che, ovviamente, $0 \in U$ si conclude.

4. Siano $m \in \mathbb{N}$ e $U = \{n \in \mathbb{N} \text{ tali che } m + n = n + m\}$. $0 \in U$ in quanto $m + 0 = m = 0 + m$ e, se $n \in U$ allora

$$m + \sigma(n) = \sigma(m+n) = \sigma(n+m) = \sigma(n) + m.$$

E si vince.

5. Supponiamo che sia $n \neq 0$. Siccome $\{0\} \cup \sigma(\mathbb{N}) = \mathbb{N}$ esiste $p \in \mathbb{N}$ tale che $n = \sigma(p)$. Ma allora $m + n = m + \sigma(p) = \sigma(m+p) \in \sigma(\mathbb{N})$ e quindi $m + n \neq 0$.

6. Sia $U = \{m \in \mathbb{N} \text{ tali che } \forall n, p \in \mathbb{N} \quad m + n = m + p \Rightarrow n = p\}$. Evidentemente $0 \in U$, inoltre, se $m \in U$, allora $\sigma(m+n) = \sigma(m) + n = \sigma(m) + p = \sigma(m+p)$ implica, per l'iniettività di σ, che $m + n = m + p$ e quindi $n = p$, cioè U è σ-chiuso.

□

La 3 rende inutili le parentesi e ne approfitteremo spudoratamente. Posto $1 = \sigma(0)$ avremo che $\forall n \in \mathbb{N} \quad \sigma(n) = n + \sigma(0) = \sigma(n+0) = \sigma(n)$ per cui, d'ora in avanti, se sarà opportuno, non useremo più la funzione σ, rimpiazzandola con la nuova notazione. Definiamo una relazione in $\mathbb{N}$ ponendo

$$n \leq m \Leftrightarrow \exists p \in \mathbb{N} \text{ tale che } m = n + p.$$

Dalle proprietà della somma si deduce immediatamente che questa relazione è riflessiva e transitiva; ma è anche antisimmetrica

Proposizione 2. $\leq$ *è una relazione d'ordine totale su* $\mathbb{N}$.

Dimostrazione. Siano $m, n \in \mathbb{N}$ tali che $m \leq n$ e $n \leq m$, cioè esistono $p, r \in \mathbb{N}$ tali che $m = n + p$, $n = m + r$, allora

$$m + 0 = m = n + p = (m + r) + p = m + (r + p).$$

Dalla proprietà di cancellazione segue che $r + p = 0$ e dunque $r = p = 0$. Perciò $m = n$.

Come al solito si dirà che $m < n$ se $m \leq n$ e $m \neq n$, cioè se esiste $p \neq 0$ tale che $n = m+p$, o, in altre parole, esiste $r \in \mathbb{N}$ tale che $n = m+r+1$.

Per provare che $\leq$ è un ordine totale su $\mathbb{N}$, sia $m \in \mathbb{N}$ e $U = \{n \in \mathbb{N}$ tali che $n \leq m$ o $m \leq n\}$. $0 \in U$ in quanto $0 \leq m$. Supponiamo poi che $n \in U$ e proviamo che $n + 1 \in U$. Distinguiamo le due eventualità

- $n < m$, cioè

  $$\exists r \in \mathbb{N} \text{ tale che } m = n + r + 1 = n + r + 1 = n + 1 + r$$

  e quindi $n + 1 \leq m$ e $n + 1 \in U$.

- $m \leq n$ e quindi esiste $p \in \mathbb{N}$ tale che $n = m + p$. Ma allora $n + 1 = m + p + 1 = m + p + 1$ e di nuovo $n + 1 \in U$. La conclusione è la solita.

□

La relazione d'ordine totale appena introdotta gode delle seguenti proprietà:

Proposizione 3. $\forall m, n, p \in \mathbb{N}$

1. $m \leq n \Rightarrow m + 1 \leq n + 1$ *e* $m < n \Rightarrow m + 1 < n + 1$.
2. $m < n \Rightarrow m + 1 \leq n$.
3. $m \leq n \Rightarrow m + p \leq n + p$ *e* $m < n \Rightarrow m + p < n + p$. *(*compatibilità dell'ordine con la somma).

Dimostrazione. 1. $n = m + p \Rightarrow n + 1 = m + p + 1 = m + 1 + p$.

2. Esiste $r \in \mathbb{N}$ tale che $n = m + r + 1 = m + r + 1 = m + 1 + r$.

3. $n = m+r \Rightarrow n+p = (m+r)+p = m+(r+p) = m+(p+r) = (m+p)+r$.

□

Se $n \leq m \in \mathbb{N}$ chiameremo *differenza* di m e n l'unico numero naturale $m - n \in \mathbb{N}$ tale che $n + (m - n) = m$.

Proposizione 4. $\leq$ *è un buon ordinamento su* $\mathbb{N}$.

Dimostrazione. Sia $\emptyset \neq A \subseteq \mathbb{N}$. Se $0 \in A$, ne è evidentemente il minimo. Supponiamo dunque che $0 \notin A$ e poniamo

$$U = \{n \in \mathbb{N} \text{ tali che } \forall a \in A \quad n < a\}.$$

Visto che A non è vuoto $U \neq \mathbb{N}$, e, dato che $0 \in U$, possiamo concludere che U non è σ-chiuso, cioè esiste $n \in U$ tale che $n+1 \notin U$. Se $a \in A$ avremo che $n < a$ e dunque $n+1 \leq a$; d'altra parte il fatto che $n+1 \notin U$ ci assicura che $n+1$ è il minimo cercato. □

Fissato $m \in \mathbb{N}$ applichiamo il principio di definizione per ricorsività scegliendo, per X, x, f, rispettivamente $\mathbb{N}, 0, \sigma_m$; esso ci garantisce l'esistenza e l'unicità di una funzione $\sigma_m^* : \mathbb{N} \longrightarrow \mathbb{N}$ caratterizzata da

$$\sigma_m^*(0) = 0 \text{ e } \sigma_m^*(n+1) = \sigma_m(\sigma_m^*(n)) \quad \forall n \in \mathbb{N}.$$

Definiamo un'operazione binaria interna, detta *prodotto* su $\mathbb{N}$ ponendo $mn = \sigma_m^*(n)$. Essa è dunque caratterizzata da

$$m0 = 0 \text{ e } m(n+1) = m + mn$$

e gode delle proprietà elencate nel seguente

Teorema 3. $\forall n, m, p \in \mathbb{N}$ *valgono le seguenti* proprietà del prodotto

1. $0m = 0$.
2. $1m = m1 = m$.
3. $m(n+p) = mn + np$ *e* $(m+n)p = mp + np$, proprietà distributiva.
4. $mn = nm$, proprietà commutativa del prodotto.
5. $mn = 0 \Leftrightarrow m = 0$ *o* $n = 0$.

6. $mn = mp$ *e* $m \neq 0 \Leftrightarrow n = p$.

7. $(mn)p = m(np)$, proprietà associativa del prodotto.

8. $m < n$ *e* $p \neq 0 \Rightarrow mp < np$.

Dimostrazione. 1. Sia $U = \{m \in \mathbb{N} \text{ tali che } 0m = 0\}$. Certamente $0 \in U$, inoltre, se $m \in U$, allora $0(m+1) = 0 + 0m = 0 + 0 = 0$. Dunque $U = \mathbb{N}$.

2. $m1 = m(0+1) = m+m0 = m$. Sia poi $U = \{m \in \mathbb{N} \text{ tali che } 1m = m\}$. Se $m \in U$ allora $1(m+1) = 1+1m = 1+m = m+1$; cioè U è σ-chiuso. Siccome $0 \in U$ abbiamo che $U = \mathbb{N}$.

3. Fissati $m, n \in \mathbb{N}$ sia $U = \{p \in \mathbb{N} \text{ tali che } m(n+p) = mn+mp\}$. Per le proprietà della somma $0 \in \mathbb{N}$. Se $p \in U$ allora $m(n+(p+1)) = m(n+p+1) = m+m(n+p) = m+(mn+mp) = mn+(m+mp) = mn+m(p+1)$. Dunque $U = \mathbb{N}$ e la prima eguaglianza è provata.

   Sia $U = \{p \in \mathbb{N} \text{ tali che } (m+n)p = mn+mp\}$. Certamente $0 \in U$, e, se $p \in U$, allora $(m+n)(p+1) = (m+n)+(m+n)p = (m+n)+(mp+np) = (m+mp)+(n+np) = m(p+1)+n(p+1)$.

4. Fissato $m \in \mathbb{N}$ sia $U = \{n \text{ tali che } mn = nm\}$. Se $n \in U$ allora $m(n+1) = mn+m = nm+m = (n+1)m = (n+1)m$.

5. Supponiamo che $m \neq 0$, $n \neq 0$, cioè $m = r+1$, $n = t+1$. Allora $mn = (r+1)(t+1) = (r+1)+(r+1)t = (r+(r+1)t)+1 \neq 0$.

6. Fissato $0 \neq m \in \mathbb{N}$ sia $U = \{n \in \mathbb{N} \text{ tali che } \forall p \in \mathbb{N}\, mn = mp \Rightarrow n = p\}$. La proprietà appena dimostrata implica che $0 \in U$. Sia $n \in U$ e sia $p \in \mathbb{N}$ tale che $m(n+1) = mp$, siccome $m(n+1) \neq 0$ avremo che $p \neq 0$ e dunque esiste $r \in \mathbb{N}$ tale che $p = r+1$. Ma allora $m+mn = m(n+1) = mp = m(r+1) = m+mr$ e la proprietà di cancellaione della somma implica che $mn = mr$, dato che $n \in U$ avremo che $n = r$, da cui segue subito che $n+1 = r+1 = p$. Dunque U è σ-chiuso e si vince al solito modo.

7. Fissati $m, n \in \mathbb{N}$, sia $U = \{p \in \mathbb{N} \text{ tali che } (mn)p = m(np)\}$. Certamente $0 \in U$, e, se $p \in U$, allora $(mn)(p+1) = mn+(mn)p = mn+m(np) = m(n+np) = m(n(p+1))$ e si vince.

8. Se $n = m + r + 1$ allora $np = (m + r + 1)p = mp + (r + 1)p$. Visto che $(r + 1)p \neq 0$, si ha la tesi.

□

In un sistema di numeri naturali vale il seguente *algoritmo di divisione*:

Proposizione 5. *Siano $m \in \mathbb{N}$ e $0 \neq n \in \mathbb{N}$; esistono e sono unici $p, r \in \mathbb{N}$ tali che $m = np + r$ e $r < n$.*

Dimostrazione. Cominciamo con il provare l'unicità: supponiamo che $p, q, r, t \in \mathbb{N}$ soddisfino le condizioni $r < n$, $t < n$, $m = np + r = nq + t$. Supponiamo, per assurdo che sia $p < q$ ossia esiste $s \in \mathbb{N}$ tale che $p = q + s + 1$. Avremo allora

$$nq + t = n(q + s + 1) + r = nq + (n(s + 1) + r)$$

e, dalla proprietà di cancellazione della somma deduciamo che $t = n(s+1)+r$; ma $n(s + 1) = n + ns \geq n$, da cui si evince che $t = n(s + 1) + r \geq n + r \geq n + 0 = n$, contraddicendo il fatto che $t < n$.

Per quanto riguarda l'esistenza, consideriamo l'insieme

$$W = \{s \in \mathbb{N} \text{ tali che } m < ns\}.$$

Dato che $n(m + 1) \geq 1(m + 1) = m + 1 > m$ tale insieme non è vuoto, e, chiaramente $0 \notin W$; pertanto esiste $p \in \mathbb{N}$ tale che $np \leq m$ ma $n(p+1) > m$. Dunque esiste $r \in \mathbb{N}$ tale che $m = np + r$. Ci basta allora controllare che $r < n$; Se, per assurdo, $r \geq n$ allora $m = np + r \geq np + n = n(p + 1)$ contraddicendo la scelta di p. □

Poniamo $p = m \div n$ e $r = m \mod n$. Posto $2 = 1 + 1$ diciamo che un numero naturale m é *pari* se $m \mod 2 = 0$ ed è *dispari* se $m \mod 2 = 1$. È facile vedere che il prodotto di due numeri dispari è ancora dispari.

2 Numeri interi

Gli anelli considerati in questa dissertazione sono commutativi, unitari e $1 \neq 0$.

Definizione 2. *Un* semigruppo *è una coppia ordinata $(S, +)$, dove S è un insieme e $+$ è un'operazione interna su S che gode delle seguenti proprietà:*

SG1 $\forall a, b, c \in S \quad (a + b) + c = a + (b + c)$.

SG2 $\exists 0 \in S$ *tale che* $a + 0 = 0 + a = a \, \forall a \in S$.

SG4 $\forall a, b \in S \quad a + b = b + a$.

Un semigruppo si dice cancellativo *se*

SGC $\forall a, b, c \in S \quad a + c = b + c \Rightarrow a = b$.

Ogni gruppo abeliano è un semigruppo cancellativo.

Definizione 3. *Un* semianello *è una terna ordinata* $(S, +, \cdot)$, *dove* $(S, +)$ *è un semigruppo e* $\cdot$ *è un'operazione interna su* S *che gode delle seguenti proprietà:*

SA1 $\forall a, b, c \in S \quad (ab)c = a(bc)$.

SA2 $\forall a, b, c \in S \quad (a + b)c = ac + bc$.

SA3 $\exists 0 \neq 1 \in S$ *tale che* $a1 = 1a = a \, \forall a \in S$.

SA4 $\forall a, b \in S \quad ab = ba$.

Un semianello $(S, +,)$ *si dice* cancellativo *se il semigruppo* $(S, +)$ *lo è.*

Ogni anello è un semianello cancellativo.

Nella sezione precedente abbiamo visto che, se $(\mathbb{N}, 0, \sigma)$ è un sistema di numeri naturali, allora $(\mathbb{N}, +)$ è un semigruppo cancellativo e $(\mathbb{N}, +, \cdot)$ è un semianello cancellativo.

Definizione 4.

- *Siano* $(S, +)$, $(T, *)$ *semigruppi e* $f : S \longrightarrow T$ *una funzione. Si dice che* f *è un* omomorfismo di semigruppi *se* $\forall a, b \in S \quad f(a + b) = f(a) * f(b)$. *Se* f *è biettiva si dice che un* isomorfismo di semigruppi. *Si dice che* S *e* T *sono* isomorfi *se esiste un isomorfismo di semigruppi tra di loro.*

- *Siano* $(S, +,)$, $(T, *,)$ *semianelli e* $f : S \longrightarrow T$ *una funzione. Si dice che* f *è un* omomorfismo di semianelli *se* f *è un omomorfismo di semigruppi,* $\forall a, b \in S \quad f(ab) = f(a)f(b)$ *e* $f(1) = 1$.

Definizione 5. *Sia* S *un semigruppo. Un* completamento a gruppo *di* S *è una coppia ordinata* (T, j), *dove* T *è un gruppo abeliano e* $j : S \longrightarrow T$ *è un omomorfismo iniettivo di semigruppi che gode delle seguente* proprietà universale del completamento*: per ogni gruppo* A *e ogni omomorfismo di semigruppi* $\alpha : S \longrightarrow A$ *esiste un unico morfismo di gruppi* $\beta : T \longrightarrow A$ *tale che il diagramma*

$$\begin{array}{ccc} S & \xrightarrow{\alpha} & T \\ j \searrow & & \swarrow \beta \\ & T & \end{array}$$

è commutativo.

È facile vedere che, se (T, j) e (R, i) sono completamenti di S allora esiste un unico isomorfismo di gruppi $\gamma : T \longrightarrow R$ tale che il diagramma

$$\begin{array}{ccc} S & \xrightarrow{i} & R \\ j \searrow & & \swarrow \gamma \\ & T & \end{array}$$

è commutativo. Infatti se $\gamma : T \longrightarrow R$ e $\delta : R \longrightarrow S$ sono gli unici omomorfismi di gruppi tali che $\gamma \circ j = i$ e $\delta \circ i = j$ allora $\gamma \circ \delta \circ i = i$ e $\delta \circ \gamma \circ j = j$. Dall'unicità si evince che $\delta \circ \gamma = id_T$ e $\gamma \circ \delta = id_R$.

In modo analogo, con le ovvie modifiche si può definire il completamento ad anello di un semianello e dedurre le proprietà essenziali.

Supponiamo che (T, j) sia un completamento del semigruppo (rispettivamente semianello) S; è molto facile controllare che l'insieme $T' = \{j(a) - j(b)$ tali che $a, b \in S\}$ è un sottogruppo (sottoanello) di T e anche che (T', j) è ancora un completamento di S. Quindi esiste un unico omomorfismo di gruppi (di anelli) $\phi : T' \longrightarrow T$ tale che $\phi \circ j = j$; ma l'inclusione $i : T' \longrightarrow T$ soddisfa entrambe queste richieste e quindi $\phi = i$; ma abbiamo appena visto che ϕ è un isomorfismo e quindi i è suriettivo e dunque $T' = T$.

Teorema 4. *Un semigruppo $(S, +)$ ha un completamento se e solo se è cancellativo.*

Dimostrazione. Supponiamo che (T, j) sia un completamento di S e che $a, b, c \in S$ soddisfino la relazione $a+c = b+c$. Allora avremo che $j(a)+j(c) = j(b)+j(c)$. Sommando ad entrambi i termini di questa eguaglianza l'opposto di $j(c)$ si ottiene che $j(a) = j(b)$ e subito dopo $a = b$, visto che j è iniettiva.

Se, viceversa, S è cancellativo definiamo sul prodotto cartesiano $S \times S$ una relazione ρ ponendo

$$(a, b)\rho(c, d) \Leftrightarrow a + d = b + c.$$

È facile vedere che questa relazione è riflessiva e simmetrica: è anche transitiva, infatti se $a+d=b+c$ e $c+f=d+e$ avremo che $(a+f)+(c+d)=(b+e)+(c+d)$; visto che S è cancellativo segue che $a+f=b+e$. ρ è dunque una relazione d'equivalenza: indichiamo con T l'insieme quoziente così ottenuto e con $[a,b]$ la classe d'equivalenza di $(a,b)\in S\times S$. Definiamo un'operazione interna su T ponendo

$$[a,b]+[c,d]=[a+c,b+d]$$

Questa operazione è ben definita perché, se $a,a',b,b',c,c',d,d'\in S$ soddisfano $a+b'=b+a'$ e $c+d'=d+c'$ allora

$$(a+c)+(b'+d')=(a+b')+(c+d')=(b+a')+(d+c')=(b+d)+(a'+c').$$

È facile verificare che $(T,+)$ è un gruppo abeliano, in cui l'elemento neutro è dato dalla classe $[a,a]$ qualunque sia $a\in S$, e l'opposto di $[a,b]$ è $[b,a]$.

Definendo poi $j:S\longrightarrow T$ mediante $j(a)=[a,0]$ si ottiene un omomorfismo di semigruppi.

Resta da verificare che (T,j) soddisfa la proprietà universale. Sia dunque A un gruppo e $\alpha:S\longrightarrow A$ un omomorfismo di semigruppi. Definiamo $\beta:T\longrightarrow A$ ponendo $\beta([a,b])=\alpha(a)-\alpha(b)$. β è ben definita perché se $a+b'=b+a'$ allora $\alpha(a)+\alpha(b')=\alpha(b)+\alpha(a')$, da cui segue che $\beta([a,b)]=\alpha(a)-\alpha(b)=\alpha(a')-\alpha(b')=\beta[a',b']$.

β è un omomorfismo di gruppi, infatti

$$\beta([a,b]+[c,d])=\beta([a+c,b+d])=\alpha(a)+\alpha(c)-\alpha(b)-\alpha(d)=$$

$$(\alpha(a)-\alpha(b))+(\alpha(c)-\alpha(d))=\beta([a,b])+\beta([c,d]).$$

Si vede facilmente che $\beta\circ j=\alpha$. Per quanto riguarda l'unicità di β sia $\gamma:T\longrightarrow A$ un omomorfismo di gruppi tale che $\gamma\circ j=\alpha$, allora, per ogni $[a,b]\in T$ avremo

$$\gamma([a,b])=\gamma([a,0]+[0,b])=\gamma([a,0]-[b,0])=$$

$$\gamma(j(a))-\gamma(j(b))=\alpha(a)-\alpha(b)=\beta([a,b]).$$

□

Supponiamo ora che $(S,+,\cdot)$ sia un semianello cancellativo e sia (T,j) il completamento del semigruppo $(S,+)$ descritto nella dimostrazione precedente. Definiamo un prodotto su T così:

$$[a,b][c,d]=[ac+bd,ad+bc].$$

Dobbiamo innanzitutto verificare che questa operazione è ben definita: siano dunque $a, b, c, d, a', b', c', d' \in S$ tali che $a+b' = b+a'$ e $c+d' = d+c'$. Avremo allora

$$ac+bd+a'd'+b'd'+cb'+da'+a'c+db' = c(a+b')+d(b+a')+a'(c+d')+b'(d+c') =$$

$$c(b+a')+d(a+b')+a'(c'+d)+b'(c+d') = a'c'+b'd'+ad+bc+ca'+db'+da'+cb'$$

Posto dunque $t = cb' + da' + a'c + db'$ avremo che

$$ac + bd + a'd' + b'd' + t = a'c' + b'd' + ad + bc + t$$

e dunque, per la proprietà di cancellazione,

$$ac + bd + a'd' + b'd' = a'c' + b'd' + ad + bc$$

che è quanto si doveva verificare. Controllare che $(T, +, \cdot)$ sia un anello è noioso ma molto facile. Si potrebbe anche osservare che (T, j) è un completamento del semianello S.

Se $(G, +)$ è un gruppo e $A \subseteq G$ poniamo $-A = \{x \in G \text{ tali che } -x \in A\}$.

Definizione 6. *Sia (T, j) un completamento ad anello di un semianello S. Si dice che S è* essenziale *se $j(S) \cap -j(S) = \{0\}$. Si dice che S è* raddoppiabile *se $j(S) \cup -j(S) = T$.*

Evidentemente queste due proprietà dipendono solo da S e non dalla scelta del completamento ma possono essere verificate direttamente nel semianello.

Proposizione 6. *Sia S un semianello cancellativo.*

S è essenziale se e solo se, per ogni $a, b \in S$, $a + b = 0 \Rightarrow a = b = 0$.

S è raddoppiabile se e solo se, per ogni $a, b \in S$, esiste $c \in S$ tale che $a + c = b$ oppure $b + c = a$.

Dimostrazione. Sia (T, j) un completamento di S.

Supponiamo che S sia essenziale e che $a, b \in S$ soddisfino $a+b = 0$; allora $0 = j(a+b) = j(a)+j(b)$ e quindi $j(a) = -j(b) \in j(S) \cap -j(S) = \{0\}$. Visto che j è iniettiva segue che $a = b = 0$.

Viceversa se esiste $0 \neq r \in j(S) \cap -j(S)$ allora esistono $0 \neq a \in S$ tali che $j(a) = r$ e $0 \neq b \in S$ tali che $j(b) = -r$. Ma allora $j(a + b) = j(a) + j(b) = 0$ e $a + b = 0$ perché j è iniettiva.

Supponiamo ora che S sia raddoppiabile e siano $a, b \in S$. Allora $j(a) - j(b) \in T = j(S) \cup -j(S)$; se $j(a) - j(b) \in j(S)$ allora esiste $c \in S$ tali che $j(a) - j(b) = j(c)$ da cui segue che $a = b + c$; se invece $j(a) - j(b) \in -j(S)$ allora esiste $c \in S$ tali che $j(a) - j(b) = -j(c)$ e $a + c = b$.

Viceversa supponiamo che valga la condizione citata nell'enunciato e sia $x \in T$; siano $a, b \in S$ tali che $x = j(a) - j(b)$; se esiste $c \in S$ tale che $a = b + c$ allora $x = j(b+c) - j(b) = j(c) \in j(S)$. Se invece esiste $c \in S$ tale che $b = a + c$ allora $x = j(a) - j(a + c) = -j(c) \in -j(S)$. □

Corollario 1. $\mathbb{N}$ *è un semianello essenziale e raddoppiabile.*

Definizione 7. *Un* anello ordinato *è una coppia ordinata* (A, A^+) *dove* A *è un anello e* A^+ *è un sottoinsieme di* A *chiuso rispetto alla somma e al prodotto e che soddisfa inoltre i due assiomi*

AO1 $A^+ \bigcap -A^+ = \{0\}$.

AO2 $A^+ \bigcup -A^+ = A$.

Osserviamo che $1 \in A^+$, infatti, se fosse per assurdo $1 \in -A^+$ allora $-1 \in A^+$ e dunque $1 = (-1)(-1) \in A^+$, che è assurdo. Inoltre vale la *regola dei segni*:

1. se $a, b \in A^+$ allora $ab \in A^+$.
2. se $a \in A^+, b \in -A^+$ allora $ab \in -A^+$.
3. se $a, b \in -A^+$ allora $ab \in A^+$.

Se (A, A^+) è un anello ordinato definiamo una relazione $\leq$ su A ponendo $x \leq y \Leftrightarrow y - x \in A^+$. È facile vedere che questa relazione è riflessiva e transitiva. Ci si rende conto facilmente che l'antisimmetria di $\leq$ ammonta al fatto che $A^+ \bigcap -A^+ = \{0\}$ e $\leq$ è un ordine totale su A precisamente perché $A^+ \bigcup -A^+ = A$; inoltre vale la seguente

Proposizione 7. *Sia* (A, A^+) *un anello ordinato. Per ogni* $a, b, c \in A$:
Se $a < b$ *allora* $a + c < b + c$.
Se $c > 0$ *e* $a < b$ *allora* $ac < bc$.
Se $c < 0$ *e* $a < b$ *allora* $ac > bc$.
Per ogni $0 \neq a \in A \quad a^2 > 0$.

Dimostrazione. Facile. □

L'esempio più rilevante di anello ordinato è ottenuto come segue: sia S un semianello cancellativo, essenziale e raddoppiabile e sia (T, j) un completamento ad anello di S. Allora $(T, j(S))$ è un anello ordinato.

Viceversa, se (A, A^+) è un anello ordinato, allora A^+ è un semianello cancellativo, essenziale e raddoppiabile e (A, i), dove $i : A^+ \longrightarrow A$ è l'inclusione, è un completamento di A^+.

Ogni completamento del semianello dei numeri naturali viene chiamato *anello degli interi relativi* e indicato con $(\mathbb{Z}, +, \cdot)$. L'abuso di linguaggio è pienamente sotto controllo in quanto due completamenti di due semianelli isomorfi sono ancora isomorfi.

La relazione d'ordine che abbiamo appena introdotto su $\mathbb{Z}$ è detta *ordine naturale su* $\mathbb{Z}$. Non prenderemo in considerazione altre relazioni d'ordine su tale anello. Inoltre identificheremo sistematicamente $\mathbb{N}$ con il sottosemianello $j(\mathbb{N})$ di $\mathbb{Z}$.

Proposizione 8. *$\mathbb{Z}$ è un dominio d'integrità.*

Dimostrazione. È una facile conseguenza del fatto che $\mathbb{N}$ è raddoppiabile: se $a, b \in \mathbb{Z}$ esistono $n, m \in \mathbb{N}$ tali che $a = \pm j(m),\ b = \pm j(n)$ e, se $0 = ab = \pm j(m)j(n)$ dall'iniettività di j segue che $mn = 0$ e quindi $m = 0$ o $n = 0$. □

Se S è un semianello e $s \in A$ possiamo prendere la funzione $\phi : S \longrightarrow S$ data da $\phi(x) = xs$. Applicando il principio di definizione per ricorsività alla terna ordinata $(S, 1, \phi)$ troviamo una funzione $\psi : \mathbb{N} \longrightarrow S$ caratterizzata da $\psi(0) = 1$ e $\psi(n + 1) = \psi(n)s$. Porremo $\psi(n) = s^n$. Abbiamo dunque definito una funzione

$$\begin{array}{ccccc} \mathbb{N} & \times & S & \longrightarrow & S \\ (n & , & s) & \longrightarrow & s^n \end{array}$$

ed è facile vedere che gode delle seguenti proprietà: $\forall n, m \in \mathbb{N},\ \forall s \in S \quad s^{m+n} = s^m s^n$ e $\forall n \in \mathbb{N},\ \forall s, t \in S \quad (st)^n = s^n t^n$. In particolare la funzione $\mathbb{N} \longrightarrow (S, \cdot)$ che manda n in s^n è un omomorfismo di semigruppi. Se S è un semicampo, e quindi $(S, \cdot)$ è un gruppo, la proprietà universale del completamento ci garantisce che tale funzione può essere estesa unicamente a un omomorfismo di gruppi $\mathbb{Z} \longrightarrow (S, \cdot)$ che denoteremo con lo stesso simbolo.

3 Numeri razionali

Definizione 8. *Sia A un anello. Un* completamento a campo *(o* campo dei quozienti*) di A è una coppia ordinata (Q, j) dove Q è un campo e $j : A \longrightarrow Q$ è un omomorfismo iniettivo di anelli che gode della seguente* proprietà universale*: per ogni campo K e ogni omomorfismo iniettivo di anelli $\alpha : A \longrightarrow K$ esiste un unico omomorfismo di anelli $\beta : Q \longrightarrow K$ tale che il diagramma*

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & K \\ j \searrow & & \swarrow \beta \\ & Q & \end{array}$$

è commutativo.

È facile vedere che un completamento a campo, se esiste, è essenzialmente unico e che, se (Q, j) è un completamento a campo di A allora $Q = \{j(a)(j(b)^{-1}$ tali che $a \in A$, $0 \neq b \in A\}$.

Proposizione 9. *Un anello A ha un completamento a campo se e solo se è un dominio d'integrità.*

Dimostrazione. Sia $j : A \longrightarrow Q$ un completamento di A e siano $a, b \in A$ tali che $a \neq 0$, $ab = 0$. Allora $0 = j(ab) = j(a)j(b)$ e $j(a) \neq 0$ dato che j è iniettiva. Ma allora $0 = j(a)^{-1}0 = j(a)^{-1}(j(a)j(b)) = j(b)$; visto che j è iniettiva segue che $b = 0$.

Viceversa, supponiamo che A sia un dominio d'integrità e poniamo $A^* = A - \{0\}$. Sull'insieme $A \times A^*$ definiamo la relazione $\sim$ ponendo $(a, b) \sim (c, d)$ se e solo se $ad = bc$. Questa relazione è ovviamente riflessiva e simmetrica, è anche transitiva perché, se $(a, b) \sim (c, d) \sim (e, f)$, allora $afd = bcf = bde$ da cui segue che $(af - be)d = 0$; dato che $d \neq 0$ abbiamo che $(a, b) \sim (e, f)$. Indichiamo con $\frac{a}{b}$ la classe di (a, b) in $Q = A \times A^*/\sim$. In Q definiamo una somma e un prodotto ponendo

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

$$\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}.$$

È facile verificare che queste due operazioni sono ben definite e che Q è un anello. L'elemento neutro della somma è $\frac{0}{b}$, qualunque sia $b \in A^*$. In realtà $(Q, +, \cdot)$ è un campo e l'inverso di $\frac{a}{b} \neq 0$ è $\frac{b}{a}$.

La funzione $j : A \longrightarrow Q$ definita da $j(a) = \frac{a}{1}$ è un omomorfismo iniettivo di anelli e soddisfa la proprietà universale: dato infatti un omomorfismo iniettivo di anelli $\alpha : A \longrightarrow K$ possiamo e dobbiamo definire $\beta : Q \longrightarrow K$ mediante $\beta(\frac{a}{b}) = \alpha(a)\alpha(b)^{-1}$. □

Se $(\mathbb{Q}, j)$ è un completamento a campo del dominio d'integrità $\mathbb{Z}$ si dice che $\mathbb{Q}$ è un *campo dei razionali*.

Se (Q, j) è un completamento a campo del dominio d'integrità A, prima ancora della costruzione di Q abbiamo visto che, per ogni $x \in Q$ esistono $a \in A$ e $0 \neq b \in A$ tali che $xj(b) = j(a)$. Se ora (A, A^+) è un anello ordinato tale che A è un dominio d'integrità e (Q, j) è un completamento di A poniamo

$$Q^+ = \{x \in Q \text{ tali che } \exists a \in A^+, \exists b \in A^* \cap A^+ \text{ tali che } xj(b) = j(a)\}.$$

È facile vedere che Q^+ è un sottosemianello di Q e che $Q^+ \cap -Q^+ = \{0\}$. Inoltre, se $xj(b) = j(a)$ e $ab \in A^+$ allora $xj(b^2) = j(ab)$ e quindi $x \in Q^+$; se, invece $ab \in -A^+$ allora $-xj(b^2) = j(-ab)$ e quindi $x \in -Q^+$. Abbiamo provato che (Q, Q^+) è un anello ordinato, o meglio, un *campo ordinato*.

La funzione $j : A \longrightarrow Q$ rispetta l'ordine.

4 Omomorfismi canonici

Una semplice applicazione del principio di definizione per ricorsività consente di concludere che esiste, sostanzialmente, un solo sistema di numeri naturali, dove il significato della parola è spiegato nell'enunciato del seguente

Teorema 5. *Siano* $(\mathbb{N}, 0, \sigma)$ *e* $(\mathbb{N}', 0', \sigma')$ *sistemi di numeri naturali. Esiste un'unica biezione* $\phi : \mathbb{N} \longrightarrow \mathbb{N}'$ *tale che* $\phi(0) = 0'$ *e il diagramma*

$$\begin{array}{ccc} \mathbb{N} & \xrightarrow{\phi} & \mathbb{N}' \\ \sigma \downarrow & & \downarrow \sigma' \\ \mathbb{N} & \xrightarrow{\phi} & \mathbb{N}' \end{array}$$

è commutativo.

Dimostrazione. Usando come sistema di numeri naturali $(\mathbb{N}, 0, \sigma)$ e come (X, x, f) l'altro sistema troviamo un'unica $\phi : \mathbb{N} \longrightarrow \mathbb{N}'$ tale che $\phi(0) = 0'$ e il diagramma menzionato nell'enunciato commuta. Invertendo i ruoli dei sistemi di numeri naturali si trova una $\psi : \mathbb{N}' \longrightarrow \mathbb{N}$ tale che $\psi(0') = 0$

$$\begin{array}{ccc} \mathbb{N}' & \stackrel{\psi}{\longrightarrow} & \mathbb{N} \\ \sigma' \downarrow & & \downarrow \sigma \\ \mathbb{N}' & \stackrel{\psi}{\longrightarrow} & \mathbb{N} \end{array}$$

è commutativo. Affiancando i due diagrammi si ha che $\psi \circ \phi(0) = 0$ e il diagramma

$$\begin{array}{ccc} \mathbb{N} & \stackrel{\psi\circ\phi}{\longrightarrow} & \mathbb{N} \\ \sigma \downarrow & & \downarrow \sigma \\ \mathbb{N} & \stackrel{\psi\circ\phi}{\longrightarrow} & \mathbb{N} \end{array}$$

commuta. Siccome anche $id_{\mathbb{N}}$ ha queste proprietà, dall'unicità si evince che $\psi \circ \phi = id_{\mathbb{N}}$ e, analogamente, si vede che $\phi \circ \psi = id_{\mathbb{N}'}$ □

La funzione ϕ appena descritta si chiama *isomorfismo canonico* Alla luce di questo risultato chiameremo un qualunque sistema di numeri naturali *il* sistema dei numeri naturali; si tratta di un piccolo abuso di linguaggio di cui abbiamo piena coscienza e controllo.

Gli omomorfismi di semianelli sono piuttosto rari:

Proposizione 10. *Sia A un semianello cancellativo. Esiste un unico omomorfismo di semianelli, detto* omomorfismo canonico $\phi : \mathbb{N} \longrightarrow A$.

Dimostrazione. Cominciamo con l'unicità: siano $\psi, \phi : \mathbb{N} \longrightarrow A$ omomorfismi di semianelli e sia $U = \{n \in \mathbb{N} \text{ tali che } \psi(n) = \phi(n)\}$. $0 \in U$ perché $0+\phi(0) = \phi(0+0) = \phi(0)+\phi(0)$ e, dalla proprietà di cancellazione, si deduce che $\phi(0) = 0$, analogamente per ψ. Se $n \in U$ allora $\psi(\sigma(n)) = \psi(n+1) = \psi(n) + \psi(1) = \psi(n) + 1 = \phi(n) + 1 = \phi(n) + \phi(1) = \phi(n+1) = \phi(\sigma(n))$. Quindi $U = \mathbb{N}$.

Per quanto riguarda l'esistenza, applichiamo il principio di definizione per ricorsività alla terna $(A, 0, f)$, dove $f \in A^A$ è definita da $f(x) = x + 1$; esiste allora una funzione $\phi : \mathbb{N} \longrightarrow A$ caratterizzata da $\phi(0) = 0$ e $\phi(n + 1) = \phi(n) + 1$, $\forall n \in \mathbb{N}$.

Per controllare che ϕ è un omomorfismo di semigruppi, per ogni $m \in \mathbb{N}$ poniamo $U = \{n \in \mathbb{N}$ tali che $\phi(m + n) = \phi(m) + \phi(n)\}$. Certo $0 \in U$ e, se $n \in U$ allora

$$\phi(m+(n+1)) = \phi((m+n)+1) = \phi(m+n)+1 = (\phi(m)+\phi(n))+1 = \phi(m)+\phi(n+1).$$

Dunque U è σ-chiuso e $U = \mathbb{N}$.

Che $\phi(1) = 1$ è ovvio.

Infine, per ogni $m \in \mathbb{N}$ poniamo $U = \{n \in \mathbb{N}$ tali che $\phi(mn) = \phi(m)\phi(n)\}$. Certo $0 \in U$ e, se $n \in U$ allora

$$\phi(m(n + 1)) = \phi(mn + m) = \phi(mn) + \phi(m) = \phi(m)\phi(n) + \phi(m) =$$

$$\phi(m)(\phi(n) + 1) = \phi(m)\phi(n + 1).$$

E si conclude come al solito. □

Nei casi, per noi frequenti, in cui ϕ è iniettivo identificheremo sistematicamente $\mathbb{N}$ con un sottosemianello di A mediante l'omomorfismo canonico.

Ecco una situazione in cui questo avviene: se (A, A^+) è un anello ordinato allora l'omomorfismo canonico $\phi : \mathbb{N} \longrightarrow A$ è iniettivo e conserva l'ordine infatti è facile controllare per induzione che $\phi(\mathbb{N}) \subseteq A^+$ e, se esiste $n \in \mathbb{N}$ tale che $\phi(n + 1) = 0$, allora $\phi(n) = -\phi(1) = -1 \in -A^+ - \{0\}$; assurdo.

Se A è un anello si vede facilmente, usando la proprietà universale del completamento di un semianello e quanto detto in questa sezione, che esiste un solo omomorfismo di anelli $\phi : \mathbb{Z} \longrightarrow A$. Chiameremo anche questo *omomorfismo canonico*. È inettivo se $\phi : \mathbb{N} \longrightarrow A$ lo è.

Infine, se K è un campo , usando la proprietà universale del campo dei quozienti e quanto detto in questa sezione, si dimostra che esiste un solo *omomorfismo canonico* di anelli $\phi : \mathbb{Q} \longrightarrow K$. È inettivo se $\phi : \mathbb{N} \longrightarrow K$ lo è, cioè quando K è di caratteristica 0, e, in particolare, se K è un campo ordinato.

In particolare ci concederemo il perdonabile abuso di interpretare $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ come sottosemianello, sottoanello, sottocampo, di un qualunque campo ordinato.

5 Campi ordinati

Proposizione 11. *Ogni campo ordinato (K, K^+) gode delle seguenti proprietà:*

1. *Se $0 \neq x \in K^+$ allora $x^{-1} \in K^+$.*
2. *Per ogni $x \in K$ esiste $y \in K^+$ tale che $y > x$.*
3. *$0 < x < y \Rightarrow y^{-1} < x^{-1}$.*
4. *Per ogni $x < y \in K \quad \exists z \in K$ tale che $x < z < y$.*

Dimostrazione. 1. Per la regola dei segni.

2. Se $x \in K^+$ basta scegliere $y = x + 1$, altrimenti va bene $-x$.
3. Se, per assurdo, $x^{-1} \leq y^{-1}$ si ottiene
$$1 = xx^{-1} < yx^{-1} \leq yy^{-1} = 1.$$
4. Scegliamo $z = (x + y)2^{-1}$.

□

Si vede facilmente che, se (K, K^+) è un campo ordinato e F è un sottocampo di K allora $(F, F \cap K^+)$ è ancora un campo ordinato; inoltre se $f : K \longrightarrow E$ è un isomorfismo di anelli, allora $(E, f(K^+))$ è un campo ordinato.

Proposizione 12. *Se $(\mathbb{Q}, K^+)$ è un campo ordinato allora $K^+ = \mathbb{Q}^+$. In particolare se (K, K^+) è un campo ordinato allora $K^+ \cap \mathbb{Q} = \mathbb{Q}^+$.*

Dimostrazione. Abbiamo già visto che $\mathbb{N} \subseteq K^+$ e gli inversi degli elementi di K^+ continuano ad appartenervi. Quindi, per ogni $m, n \in \mathbb{N}$ tali che $n \neq 0$ $mn^{-1} \in K^+$, cioé $\mathbb{Q}^+ \subseteq K^+$. D'altra parte, se $x \notin \mathbb{Q}^+$ allora $-x \in \mathbb{Q}^+ \subseteq -K^+$ e quindi $x \notin K^+$. □

Sia (K, K^+) un campo ordinato ed introduciamo su K la relazione d'ordine descritta nella sezione precedente. Se $a, b \in K$ poniamo $]a, b[= \{x \in K$ tali che $a < x < b\}$. È facile vedere che $]a, b[\cap]c, d[=]\max(a, c), \min(b, d)[$ e quindi tutti gli *intervalli aperti* $]a, b[$ tali che $a, b \in K$ costituiscono una base per una topologia $\mathcal{T}$ su K che verrà chiamata *topologia standard* del

campo ordinato (K, K^+). Lo spazio topologico $(K, \mathcal{T})$ è di Hausdorff perché, se $a < b \in K$ allora $a \in]a-1, (a+b)2^{-1}[$, $b \in](a+b)2^{-1}, b+1[$ e questi due intervalli aperti sono disgiunti.

Teorema 6. *Un campo ordinato (K, K^+) è un* anello topologico*, cioè le due funzioni*

$$+ : K \times K \longrightarrow K$$

$$\cdot : K \times K \longrightarrow K$$

sono continue.

Dimostrazione. Naturalmente si intende che $K \times K$ ha la topologia prodotto di $\mathcal{T}$.

Proviamo che la somma è continua: siano $a < b \in K$ e

$$x_0, y_0 \in K \text{ tali che } a < x_0 + y_0 < b$$

e poniamo $\epsilon = \min((x_0 + y_0) - a, b - (x_0 + y_0))$ e $\delta = \epsilon 2^{-1}$. Si controlla facilmente che se $(x, y) \in]x_0 - \delta, x_0 + \delta[\times]y_0 - \delta, y_0 + \delta[$ allora $x + y \in]a, b[$.

Per quanto riguarda il prodotto: siano $a < b \in K$ e

$$x_0, y_0 \in K \text{ tali che } a < x_0 y_0 < b$$

e poniamo $\epsilon = \min((x_0 y_0) - a, b - (x_0 y_0))$. Poniamo

$$\delta_1 = \begin{cases} 1 & \text{se } y_0 = 0 \\ \epsilon(3y_0)^{-1} & \text{se } 0 \neq y_0 \in K^+ \\ \epsilon(-3y_0)^{-1} & \text{se } 0 \neq y_0 \in -K^+ \end{cases} \qquad \delta_2 = \begin{cases} 1 & \text{se } x_0 = 0 \\ \epsilon(3x_0)^{-1} & \text{se } 0 \neq x_0 \in K^+ \\ \epsilon(-3x_0)^{-1} & \text{se } 0 \neq x_0 \in -K^+ \end{cases}$$

Sia poi $\delta = \min(1, \epsilon 3^{-1}, \delta_1, \delta_2)$.

Si controlla facilmente che se $(x, y) \in]x_0 - \delta, x_0 + \delta[\times]y_0 - \delta, y_0 + \delta[$ allora $xy \in]a, b[$. □

Definizione 9. *Si dice che un campo ordinato (K, K^+) è* completo *se ogni suo sottoinsieme non vuoto e superiormente limitato ha un estremo superiore.*

Si dice che (K, K^+) è archimedeo *se per ogni $x \in K$ esiste $n \in \mathbb{N}$ tale che $n > x$.*

Un campo ordinato non archimedeo può essere descritto come segue: sia $\mathbb{Z}[X]$ l'anello dei polinomi in un'indeterminata a coefficienti in $\mathbb{Z}$; è un dominio d'integrità. Poniamo $\mathbb{Z}[X]^+ = \{\sum_{p=0}^{m} a_p X^p \text{ tali che } a_m \in \mathbb{N}\}$. È facile vedere che $(\mathbb{Z}[X], \mathbb{Z}[X]^+)$ è un anello ordinato ed il rispettivo campo dei quozienti $\mathbb{Z}(X)$ è ordinato come mostrato precedentemente ma non archimedeo perché $X > n, \quad \forall n \in \mathbb{N}$. Eppure

Proposizione 13. *Ogni campo ordinato completo è archimedeo.*

Dimostrazione. Un eventuale $x \in K$ che non goda della proprietà richiesta sarebbe un maggiorante per $\mathbb{N}$, che dunque avrebbe un estremo superiore λ e ci sarebbe $n \in \mathbb{N}$ tale che $n > \lambda - 1$. Ma allora $n+1 > \lambda$, contraddizione. □

Proposizione 14. *Se (K, K^+) è un campo ordinato archimedeo allora*

1. *Per ogni $0 \neq x \in K^+$ e per ogni $y \in K$ esiste $n \in \mathbb{N}$ tali che $nx > y$.*
2. *Per ogni $x \in K$ esiste un unico $n \in \mathbb{Z}$ tale che $n \leq x < n + 1$.*
3. *Per ogni $x > 1$ e per ogni $y \in K$ esiste $n \in \mathbb{N}$ tale che $x^n > y$.*
4. *$\mathbb{Q}$ è denso in K.*

Dimostrazione.

1. Basta applicare la proprietà archimedea a yx^{-1}.
2. Supponiamo dapprima $x \in K^+$. L'insieme $U = \{n \in \mathbb{N} \text{ tali che } n \leq x\}$ contiene 0 ma non è $\sigma-$ chiuso per la proprietà archimedea.

   Sia invece $-x \in K^+$ allora esiste un unico $n \in \mathbb{N}$ tali che $n \leq -x < n + 1$ da cui si deduce che $-n - 1 < x \leq -n$; se $x = -n$ l'affermazione è vera, altrimenti basta porre $p = -n - 1$ per avere $p < x < p + 1$.
3. Poniamo $0 \neq z = 1 - x \in K^+$ e proviamo per induzione che $\forall n \in \mathbb{N} \quad x^n = (1 + z)^n \geq 1 + nz$, dopo di che si usa 1. Ci basta ovviamente verificare che $U = \{n \in \mathbb{N} \text{ tali che } x^n = (1 + z)^n \geq 1 + nz\}$ è σ-chiuso. Se $n \in U$ allora

   $$(1+z)^{n+1} = (1+z)^n(1+z) \geq (1+nz)(1+z) = 1+(n+1)z+nz^2 \geq 1+(n+1)z.$$
4. Dobbiamo provare che, dati $x < y \in K$ esiste $q \in \mathbb{Q}$ tale che $x < q < y$. Per la proprietà archimedea esiste $n \in \mathbb{N}$ tale che $n > (y -$

$x)^{-1}$ cioè $1 < ny - nx$. Per 2 esiste $m \in \mathbb{N}$ tale che $m \leq nx$ ma $m+1 > nx$. Ma allora

$$nx < m + 1 < m + ny - nx \leq ny.$$

Perciò $q = (m+1)n^{-1}$ soddisfa quanto richiesto.

□

Proposizione 15. *Sia (K, K^+) un campo ordinato.*

1. *$q : K \longrightarrow K$ data da $q(x) = x^2$ è continua.*
2. *Se (K, K^+) è completo allora $q(K) = K^+$.*
3. *Se (K, K^+) è completo e (K, P) è un campo ordinato allora $K^+ = P$.*

Dimostrazione. 1. q è la composizione di $+ : K \times K \longrightarrow K$ con $d : K \longrightarrow K \times K$ data da $d(x) = (x, x)$ e queste funzioni sono continue.

2. Sappiamo già che $q(K) \subseteq K^+$ e che $0 = q(0) \in q(K)$. Sia $0 \neq x \in K^+$ e poniamo

$$A = \{y \in K^+ \text{ tali che } y^2 < x\}.$$

A non è vuoto perché $0 \in A$ ed è superiormente limitato perché, se $x < n \in \mathbb{N}$ allora, per ogni $y \in A$, $y^2 < x < n \leq n^2$ da cui segue che $y < n$. Sia allora $a = \sup A$. Non può essere $a^2 < x$ perché altrimenti basta scegliere $n \in \mathbb{N}$ tale che $n \geq (2a+1)(x-a^2)^{-1}$ per ottenere che

$$(a + n^{-1})^2 = a^2 + 2an^{-1} + (n^{-1})^2 \leq a^2 + (2a+1)n^{-1} \leq x,$$

cioè $a + n^{-1} \in A$.

Se invece $x < a^2$ allora $a^2 \in]x, 2a^2 - x[$ e quindi esistono $b < a < c \in K$ tali che $q(]b, c[) \subseteq]x, 2a^2 - x[$, cioé nessun elemento in $]b, a[$ appartiene ad A e quindi $\sup A \leq b$; assurdo.

Perciò $a^2 = x$.

3. $K^+ = q(K) \subseteq P$; d'altra parte se $x \notin K^+$ allora $0 \neq -x \in K^+$ da cui $x \notin P$.

□

Proposizione 16. *Il campo ordinato $(\mathbb{Q}, \mathbb{Q}^+)$ è archimedeo ma non completo.*

Dimostrazione. Se $x \leq 0$ basta scegliere $n = 1$. Altrimenti esistono $0 \neq b \in \mathbb{N}$ e $0 \neq a \in \mathbb{N}$ tali che $xb = a$ da cui segue subito che $a + 1 > x$.

Per provare che $\mathbb{Q}$ non è completo si usa di solito un argomento che fa leva il fatto che non esiste un numero razionale q tale che $q^2 = 2$; dimostriamolo per assurdo: per ogni $0 \neq n \in \mathbb{N}$ poniamo $U(n) = \{m \in \mathbb{N} \text{ tali che } 2m^2 = n^2\}$. L'ipotesi assurda dice che l'insieme $U = \{n \in \mathbb{N} \text{ tali che } U(n) \neq \emptyset\}$ non è vuoto e quindi ha un minimo n. Sia $m \in U(n)$ Siccome n^2 è pari esiste $0 \neq p \in \mathbb{N}$ tale che $n = 2p$ e quindi $2m^2 = 2 \cdot 2 \cdot p^2$ da cui, per la proprietà di cancellazione del prodotto, $2p^2 = m^2$. Cioè $U(m) \neq \emptyset$ e questo è assurdo perché $m < n$.

Adesso è facile concludere che $(\mathbb{Q}, \mathbb{Q}^+)$ non è completo perchè $2 \in \mathbb{Q}^+$ ma $2 \notin q(\mathbb{Q})$. □

Proposizione 17. *Siano (K, K^+) un campo ordinato completo,(F, F^+) un campo ordinato, $f : K \longrightarrow F$ un isomorfismo di anelli. Allora*

1. *$(F, f(K^+))$ è un campo ordinato completo.*
2. *(F, F^+) è completo.*
3. *f rispetta l'ordine ed è un omeomorfismo.*

Dimostrazione. 1. Ovvio.

2. $f(K^+) = F^+$.

3. Ovvio.

□

Teorema 7. *Se (K, K^+) e (F, F^+) sono campi ordinati completi allora esiste un unico isomorfismo di anelli $f : K \longrightarrow F$. Per la proposizione precedente esso rispetta l'ordine ed è un omeomorfismo.*

Dimostrazione. Indichiamo con $Q(K), Q(F)$ i sottocampi primi di K e di F. Abbiamo già visto che l'unico omomorfismo di anelli tra di essi è l'omomorfismo canonico $\phi : Q(K) \longrightarrow Q(F)$. Componendolo nei due modi possibili con l'omomorfismo canonico $\psi : Q(F) \longrightarrow Q(K)$ e sfruttando l'unicità si vede facilmente che si tratta di isomorfismi, che sono uno l'inverso dell'altro. Ne segue facilmente che ogni omomorfismo di anelli $f : K \longrightarrow F$ rende commutativo il diagramma

$$\begin{array}{ccc} K & \xrightarrow{f} & F \\ \uparrow & & \uparrow \\ Q(K) & \xrightarrow{\phi} & Q(F) \end{array}$$

dove le frecce verticali sono le inclusioni. Cominciamo la dimostrazione del teorema verificando che esiste un'unica funzione $f : K \longrightarrow F$ tale che

- rispetta l'ordine stretto
- la sua restrizione a $Q(K)$ coincide con ϕ.

Una tale funzione è certamente continua perché $Q(F)$ è denso in F e ϕ è biettiva.

L'unicità è facile: supponiamo che f, g rispettino entrambe le condizioni, e, per assurdo, che esista $x \in K$ tale che $f(x) < g(x)$. Siccome $Q(F)$ è denso in F e ϕ è biettiva esiste $y \in Q(K)$ tale che $f(x) < \phi(y) < g(x)$ da cui segue che

$$f(x) < f(y) = g(y) < g(x)$$

da cui $x < y$ e $y < x$, assurdo.

Questo già prova l'unicità menzionata nell'enunciato.

Per quanto riguarda l'esistenza possiamo procedere come segue: per ogni $x \in K$ poniamo $S(x) = \{y \in Q(K) \text{ tali che } y < x\}$. Si tratta evidentemente di un sottoinsieme non vuoto e superiormente limitato di $Q(K)$. Anche $\phi(S(x))$ è superiormente limitato perché ϕ rispetta l'ordine. Poniamo $f(x) = \sup \phi(S(x))$. Evidentemente questa funzione soddisfa quanto richiesto.

f è un omomorfismo di anelli. Consideriamo la funzione $h : K \times K \longrightarrow F$ definita da $h(x, y) = f(x+y)-f(x)-f(y)$. Si tratta di una funzione continua in quanto ottenuta come composizione delle funzioni continue

$$\begin{array}{ccccccccc} (x,y) & \to & (x+y,x,y) & & (\alpha,\beta,\gamma) & \to & (\alpha-\beta,\gamma) & & \\ \in & & \in & & \in & & \in & & \\ K\times K & \to & K\times K\times K & \to & F\times F\times F & \to & F\times F & \to & F \\ & & \in & & \in & & \in & & \in \\ & & (a,b,c) & \to & (f(a),f(b),f(c)) & & (\lambda,\mu) & \to & \lambda-\mu \end{array}$$

Ma la funzione h si annulla su tutti gli elementi di $Q(K) \times Q(K)$ che è denso in $K \times K$ e dunque h è la funzione nulla perché F è di Haussdorff.

Analogamente si verifica che $f(xy) = f(x)f(y)$. Invertendo i ruoli tra F e K si vede facilmente, usando le opportune unicità, che f è un isomorfismo. □

Abbiamo provato che non può esistere, essenzialmente, più di un campo ordinato completo. La prossima sezione ne costruisce materialmente uno.

6 Numeri reali

Definizione 10. *Un sottoinsieme $S \subseteq \mathbb{Q}^+$ è detto* sezione *se soddisfa le seguenti proprietà:*

S0 $S \neq \emptyset$.

S1 $\forall x \in S \, \forall y > x$, $y \in S$.

S2 $\forall x \in S \, \exists y < x$ *tale che* $y \in S$.

Osserviamo che 0 non appartiene a nessuna sezione, per $S2$; se S è una sezione e $0 \neq x \in \mathbb{Q}^+$ l'insieme $U = \{n \in \mathbb{N} \text{ tali che } nx \notin S\}$ non coincide con $\mathbb{N}$, in quanto, dato $s \in S$, per la proposizione 14.3 esiste $n \in \mathbb{N}$ tali che $nx > s$ e, per $S1$, $nx \in S$. Visto che $0 \in U$ abbiamo che U non è $\sigma-$ chiuso, dunque esiste $n \in \mathbb{N}$ tale che $y = nx \notin S$ ma $y + x \in S$.

Per ogni $\alpha \in \mathbb{Q}^+$ definiamo

$$S(\alpha) = \{x \in \mathbb{Q} \text{ tali che } x > \alpha\};$$

Per la proposizione 11.2, $S(\alpha) \neq \emptyset$; la proprietà $S1$ è ovvia e la $S2$ segue dal punto .4. della stessa. Evidentemente ogni sezione è contenuta in $S(0)$. Denotiamo con $\mathcal{S}$ l'insieme di tutte le sezioni e notiamo che la funzione $S : \mathbb{Q} \longrightarrow \mathcal{S}$ è iniettiva.

Definiamo due operazioni in $\mathcal{S}$ ponendo

$$S + T = \{s + t \text{ tali che } s \in S \text{ e } t \in T\}$$

$$ST = \{st \text{ tali che } s \in S \text{ e } t \in T\}.$$

È ovvio che $S + T$ e ST sono sottoinsiemi non vuoti di $\mathbb{Q}^+$ e che soddisfano la proprietà $S2$. Per quanto riguarda la $S1$ notiamo che se $s \in S$, $t \in T$e $y > s + t$ allora $s' = s + y - (t + s) \in S$ e $y = s' + t \in S + T$. Inoltre se $s \in S$, $t \in T$e $y > st$ allora $s' = s + (y - st)t^{-1} \in S$ e $y = s't \in ST$.

Teorema 8. *$(\mathcal{S}, +)$ è un semicampo totalmente ordinato per inclusione, cancellativo, essenziale e raddoppiabile. La funzione $S : \mathbb{Q}^+ \longrightarrow \mathcal{S}$ è un omomorfismo di semianelli.*

Dimostrazione. Le proprietà associative della somma e del prodotto e le proprietà distributive e commutative sono ovvie.

Sia $S \in \mathcal{S}$; è ovvio che $S + S(0) \subseteq S$; viceversa, se $s \in S$ esiste $y < s$ tale che $y \in S$, ma allora $s - y \in S(0)$ e $s = y + (s - y) \in S + S(0)$. Abbiamo provato che $S(0)$ è elemento neutro per la somma.

Sia $S \in \mathcal{S}$ e $t > 1$; allora $st > s1 = s$ e quindi, per $S1$, $st \in S$; cioè $SS(1) \subseteq S$. Viceversa, se $s \in S$ esiste $y < s$ tale che $y \in S$, ma allora $1 < sy^{-1}$ e quindi $s = y(sy^{-1}) \in SS(1)$ e $S(1)$ è elemento neutro del prodotto.

Sia $S(0) \neq S \in \mathcal{S}$. Poniamo

$$T = \{t \in \mathbb{Q}^+ \text{ tali che } \exists z \in \mathbb{Q}^+ \text{ tale che } z < t \text{ e } zs > 1 \, \forall s \in S\}$$

Siccome $S(0) \neq S$ esistono $x, y \in \mathbb{Q}^+$ tali che $0 < x < y \notin S$, se $s \in S$ allora $s > y$ e quindi $sy^{-1} > 1$. Questo prova che $x^{-1} \in T$. È evidente che T è una sezione. Proviamo che $ST = S(1)$. Vedere che $ST \subseteq S(1)$ è molto facile. Viceversa sia $x > 1$. Per ogni $0 \neq y \in \mathbb{Q}$ poniamo $yS = \{ys \text{ tali che } s \in S\}$. Non è difficile verificare che si tratta ancora di una sezione. Supponiamo, per assurdo, che $S \subseteq xS$ e sia $U = \{n \in \mathbb{N} \text{ tali che } S \subseteq x^n S\}$. Evidentemente $0 \in U$ e supponiamo che $n \in U$. Per ogni $s \in S$ esiste $s' \in S$ tale che $s = x^n s'$; d'altra parte esiste $s'' \in S$ tale che $s' = xs''$ e dunque U è $\sigma-$ chiuso, cioè, per ogni numero naturale n abbiamo che $S \subseteq x^n S$. Visto che $S \neq S(0)$ esistono $0 < z < s$ tali che $z \notin S$, $s \in S$. Usando la proposizione 14.3, possiamo trovare $n \in \mathbb{N}$ tale che $x^n > sz^{-1}$; ma esiste $s' \in S$ tale che $s'x^n = s$ e allora $z > s'$, contraddicendo il fatto che $z \notin S$.

Abbiamo dunque provato che $S \nsubseteq xS$, cioè esiste $s \in S$ tale che $y = sx^{-1} \notin S$. Prendiamo $u \in S$ tale che $u < s$ e poniamo $z = ux^{-1}$. Abbiamo dunque

$$0 < z < y \notin S \text{ tali che } xz \in S.$$

Ma $z^{-1} \in T$ perché $z^{-1} > y^{-1}$ e, per ogni $s' \in S$ $y^{-1}s' > y^{-1}y = 1$; allora $x = (xz)z^{-1} \in ST$, cioè $T = S^{-1}$.

$(\mathcal{S}, +)$ è totalmente ordinato per inclusione: siano $S, T \in \mathcal{S}$ tali che $S \nsubseteq T$ e sia $s \in S$, $s \notin T$; per ogni $t \in T$ avremo che $t > s$, per $S1$ e quindi $T \subseteq S$.

Supponiamo che R, S, T siano sezioni tali che $S \subsetneqq T$ e proviamo che $S + R \subsetneqq T + R$. Siano a, $b \in T$ tali che $a < b$ e $b \notin S$. Per l'osservazione

che segue la definizione di sezione esiste $x \notin R$ tale che $x + (b - a) \in R$; prendiamo $r \in R$ tale che $r < x + (b - a)$. Allora $a + r \in T + R$ e affermo che $a + r \notin S + R$. Infatti se $a + r = s + r'$ con $r' \in R$ e $s \in S$, abbiamo che $b + x > a + r > b + r'$, da cui segue che $x > r'$, assurdo. Quindi $\mathcal{S}$ è cancellativo.

Per vedere che $\mathcal{S}$ è essenziale ci basta controllare che, per ogni $S, T \in \mathcal{S}$, $S + T \subseteq S$, e questo è facile.

Verificare che $\mathcal{S}$ è raddoppiabile è relativamente raffinato: siano $T \subseteq S \in \mathcal{S}$ e definiamo

$$R = \{y \in \mathbb{Q}^+ \text{ tali che } \exists z \in \mathbb{Q}^+ \text{ tale che } z < y \text{ e } s + z \in T \ \forall s \in S\}.$$

$R \neq \emptyset$ perché $T \subseteq R$, soddisfa evidentemente $S1$ ed anche $S2$ in quanto, se $y \in R$, esiste $z \in \mathbb{Q}^+$ tali che $z < y$ e $s + z \in T \ \forall s \in S$. Evidentemente ogni r tale che $z < r < y$ appartiene ancora a R.

Ovviamente $S + R \subseteq T$. Inoltre, se $t \in T$ possiamo trovare $t', t'' \in T$ tali che $t'' < t' < t$: per l'osservazione che segue la definizione di sezione, esiste $y \notin S$ tali che $s = y + (t - t') \in S$. Se riusciamo a provare che $t - s \in R$ avremo che $t \in S + R$. Ma $t - s = t' - y > t'' - y \in \mathbb{Q}^+$ in quanto $y \notin S$ e $t'' \in T \subseteq S$; inoltre, per ogni $s' \in S$, $s' + (t'' - y) = t'' + (s' - y) > t'' \in T$.

Se $x, y \in \mathbb{Q}^+$ è ovvio che $S(x) + S(y) \subseteq S(x + y)$. Viceversa, se $r > x + y$ prendiamo $a \in \mathbb{Q}^+$ tali che $x + y < a < r$; allora $a - x \in S(y)$ e $r - a + x \in S(x)$ e quindi $r \in S(x) + S(y)$.

È anche ovvio che $S(x)S(y) \subseteq S(xy)$, viceversa, nel caso $x \neq 0$, se $r > xy$ prendiamo $a \in \mathbb{Q}^+$ tali che $xy < a < r$; allora $ax^{-1} \in S(y)$ e $rxa^{-1} \in S(x)$ e quindi $r \in S(x)S(y)$. Se $x = 0$ basta osservare che in un semianello cancellativo 0 è nullificatore del prodotto. □

Proposizione 18. *Se (A, A^+) è un anello ordinato e A^+ è un semicampo, allora (A, A^+) è un campo ordinato.*

Dimostrazione. Ci basta provare che, se $0 \neq x \in -A^+$, esiste $y \in A$ tale che $xy = 1$, ed è facile. Infatti se $z \in A$ soddisfa $(-x)z = 1$ allora $x(-z) = 1$. □

Sia $(\mathbb{R}, j)$ un completamento ad anello del semianello cancellativo $\mathcal{S}$, e poniamo $\mathbb{R}^+ = j(\mathcal{S})$; allora, visto che $\mathcal{S}$ è essenziale e raddoppiabile, $(\mathbb{R}, \mathbb{R}^+)$ è un campo ordinato.

Lemma 1. *Un campo ordinato (K, K^+) è completo se e solo se ogni sottoinsieme non vuoto e superiormente limitato di K^+ ha un estremo superiore.*

Dimostrazione. Sia A un sottoinsieme non vuoto e superiormente limitato di K. Se $A \cap K^+ \neq \emptyset$ l'estremo superiore di questo insieme (evidentemente ancora superiormente limitato) è anche estremo superiore di A. Se invece $A \cap K^+ = \emptyset$ poniamo $B = \{x \in -K^+ \text{ tali che } x > a \ \forall a \in A\}$ che non è vuoto perché $0 \in B$. Se $a \in A$ e $x \in B$ allora $a < x$ e quindi $-x < -a$; dunque $-B$ è un sottoinsieme non vuoto e superiormente limitato di K^+; sia $\mu = \sup -B$.

Affermo che $-\mu = \sup A$. Sia infatti $a \in A$ e supponiamo, per assurdo, che $-\mu < a$ e quindi $-a < \mu$ ed esiste $x \in B$ tale che $-x > -a$ e dunque $x < a$, contraddicendo la definizione di B. Supponiamo poi che $y < -\mu$, allora $\mu < -y$, sia $z \in K$ tale che $\mu < z < -y$. Ma allora $z \notin -B$, cioè esiste $a \in A$ tale che $a \geq -z > -y$. □

Teorema 9. $(\mathbb{R}, \mathbb{R}^+)$ *è un campo ordinato completo.*

Dimostrazione. Ci basta provare che un sottoinsieme non vuoto e superiormente limitato di $\mathcal{S}$ ha un estremo superiore, ed il nostro compito è particolarmente facilitato dal fatto che, se $S, T \in \mathcal{S}$ si ha che $S \leq T \Leftrightarrow T \subseteq S$. Sia dunque A un sottoinsieme non vuoto e superiormente limitato di $\mathcal{S}$. Esiste dunque una sezione T contenuta in tutti gli elementi di A; poniamo $S = \{s \in \mathbb{Q}^+ \text{ tali che } \exists x \in \bigcap A \text{ tali che } x < s\}$. Allora $T \subseteq S$ perché, se $t \in T$ esiste $t' \in T$ tale che $t' < t$; ma $t' \in \bigcap A$ e dunque $t \in S$. È facile verificare che S è una sezione; se $R \in A$ e $s \in S$ esiste $x \in \bigcap A \subseteq R$ tale che $x < s$, e allora $S \subseteq R$, cioè S è un maggiorante di A.

Supponiamo infine che $R < S \in \mathcal{S}$, cioè $S \subsetneqq R$ e sia $r \in R$, $r \notin S$. Sia $r' \in R$ tale che $r' < r$; certamente $r' \notin \bigcap A$ perché altrimenti $r \in S$ e dunque esiste $W \in A$ tale che $r' \notin W$. Questo prova che $R \subsetneqq W$ e quindi $W > R$.

In conclusione $S = \sup A$ ed il teorema è dimostrato. □

7 Rappresentazione dei numeri

Sia $(\mathbb{N}, 0, \sigma)$ un sistema di numeri naturali. Per ogni $n \in \mathbb{N}$ il *segmento di* n è l'insieme $n^- = \{m \in \mathbb{N} \text{ tali che } m < n\}$. Dalle proprietà dell'ordine naturale su $\mathbb{N}$ si deduce immediatamente che

- $0^- = \emptyset$.
- $m = n \Leftrightarrow m^- = n^-$.

- $m \leq n \Leftrightarrow m^- \subseteq n^-$.
- $(m+1)^- = m^- \cup \{m\}$.

Proposizione 19. *Per ogni numero naturale n ogni funzione $n^- \longrightarrow n^-$ che sia iniettiva è anche suriettiva.*

Dimostrazione. Sia

$U = \{n \in \mathbb{N}$ tali che ogni funzione iniettiva $n^- \longrightarrow n^-$ è anche suriettiva$\}$.

$0 \in U$ perché la funzione vuota è iniettiva e suriettiva.

Se $n \in U$ e $f : (n+1)^- \longrightarrow (n+1)^-$ è iniettiva poniamo $m = f(n)$ e sia g la biezione di $(n+1)^-$ che scambia tra loro m ed n e lascia invariati tutti gli altri elementi di $(n+1)^-$. Allora $g \circ f : (n+1)^- \longrightarrow (n+1)^-$ è una funzione iniettiva e manda n in se stesso; quindi la sua restrizione a n^- è una funzione iniettiva $n^- \longrightarrow n^-$, e dunque è anche suriettiva. Segue immediatamente che $g \circ f$ è suriettiva e dunque anche f lo è. Perciò $U = \mathbb{N}$. □

Proposizione 20. *Se $n, m \in \mathbb{N}$ ed esiste una funzione biettiva $f : n^- \longrightarrow m^-$ allora $n = m$.*

Dimostrazione. Sia $U = \{n \in \mathbb{N}$ tali che $\exists f : n^- \longrightarrow m^-$ biettiva $\Rightarrow n = m\}$. $0 \in U$ perché la funzione vuota, che è sempre iniettiva, è suriettiva se e solo se anche il suo codominio è vuoto. Siano $n \in U$ e $f : (n+1)^- \longrightarrow p^-$ una biezione. Evidentemente $p \neq 0$ perché non ci sono funzioni da un insieme non vuoto a quello vuoto, e quindi esiste $m \in \mathbb{N}$ tale che $p = m + 1$. Sia $g : (m+1)^- \longrightarrow (m+1)^-$ la biezione che scambia tra loro $f(n)$ e m e lascia fissi gli altri elementi. Allora la restrizione di $g \circ f$ a n^- è una biezione tra n^- e m^-, da cui segue che $m = n$ e quindi $n + 1 = m + 1 = p$. dunque U è anche σ- chiuso e il teorema è vero. □

Definizione 11. *Un insieme A si dice* finito *se esistono un numero naturale n e una biezione $f : n^- \longrightarrow A$.*

Se A è un insieme finito, m, n sono numeri naturali e $f : n^- \longrightarrow A$, $g : m^- \longrightarrow A$ allora $g^{-1} \circ f : n^- \longrightarrow m^-$ è una biezione, e dunque $m = n$. Tale numero è detto *il numero di elementi di A* e indicato con $\sharp A$.

Esercizio 1. *Provare le seguenti affermazioni*

1. *Se A è un insieme finito e $x \notin A$ allora anche $A \cup \{x\}$ è finito e* $\sharp(A \cup \{x\}) = \sharp A + 1$.

2. *Ogni sottoinsieme di un insieme finito è finito.*

3. *Se A, B sono insiemi finiti anche $A \cup B$ è finito e vale la* relazione di Grassmann
$$\sharp(A \cup B) + \sharp(A \cap B) = \sharp A + \sharp B.$$

4. *Se A, B sono insiemi finiti anche $A \times B$ lo è e*
$$\sharp(A \times B) = \sharp A \, \sharp B.$$

5. *Se A, B sono insiemi finiti anche B^A lo è e*
$$\sharp(B^A) = \sharp B^{\sharp A}.$$

6. *Se A è un insieme finito anche il suo insieme delle parti $\mathcal{P}(A)$ lo è e*
$$\sharp(\mathcal{P}(A)) = 2^{\sharp A}$$

7. *Un sottoinsieme di $\mathbb{N}$ è finito se e solo se è contenuto in un segmento.*

Aggiungiamo all'insieme di tutti i segmenti di $\mathbb{N}$ anche lui stesso, che chiameremo *segmento improprio.* È facile vedere che un sottoinsieme $A \subseteq \mathbb{N}$ è un segmento se e solo se $\forall m \in A$, $n \leq m \Rightarrow n \in A$, da cui segue facilmente che ogni unione o intersezione di segmenti è ancora un segmento.

Siamo pronti a provare che un insieme è infinito se e solo se non è finito: il lettore che a questo punto pensi "ci mancherebbe altro"è caldamente invitato a utilizzare meglio la versione cartacea di queste dispense e gli altri libri su cui ha studiato matematica fornendoli come cibo alla sua capra.

Teorema 10. *Sia X un insieme: le seguenti condizioni sono equivalenti.*

1. *X è infinito.*

2. *Se $\mathbb{N}$ è un sistema di numeri naturali esiste una funzione iniettiva $f : \mathbb{N} \longrightarrow X$.*

3. *X non è finito.*

Dimostrazione. Che $1 \Leftrightarrow 2$ è sostanzialmente il contenuto della dimostrazione del primo teorema di questa note. $1 \Rightarrow 3$ segue immediatamente dalle osservazioni di questa sezione.

$3 \Rightarrow 2$ è difficile. Poniamo

$$Y = \{(A, f) \text{ tali che } A \text{ è un segmento e } f : A \to X \text{ è iniettiva}\}.$$

Questo insieme non è vuoto perché $(0^-, \emptyset) \in Y$.

Introduciamo su Y una relazione, che si vede facilmente essere d'ordine, ponendo $(A, f) \leq (B, g) \Leftrightarrow A \subseteq B$ e $g_{|A} = f$.

Se $Z \subseteq Y$ è totalmente ordinato da $\leq$ poniamo $W = \bigcup_{(A,f)\in Z} A$ e definiamo $g : W \longrightarrow X$ come segue: se $n \in W$ esiste $(A, f) \in Z$ tale che $n \in A$; poniamo $g(n) = f(n)$; se $(B, h) \in Z$ e $n \in B$ allora: se $(B, h) \leq (A, f)$ allora $B \subseteq A$ e $f_{|B} = g$, per cui $f(n) = h(n)$, il che dimostra che g è ben definita; analogamente si procede se $(A, f) \leq (B, h)$. Inoltre f è iniettiva perché se $m \neq n \in W$ possiamo trovare $(A, f) \in Z$ tale che $n, m \in A$ e allora $g(m) = f(m) \neq f(n) = g(n)$. Evidentemente $(A, f) \leq (W, g) \quad \forall (A, f) \in Z$.

Abbiamo verificato che $(Y, \leq)$ è un insieme induttivo. Il lemma di Zorn ci garantisce l'esistenza di un elemento massimale $(A, f) \in Y$. Affermo che $A = \mathbb{N}$, il che prova il teorema. Supponiamo infatti che esista $n \in \mathbb{N}$ tali che $A = n^-$; allora $f : n^- \longrightarrow X$, essendo iniettiva non può essere suriettiva e quindi esiste $x \in X - f(n^-)$ definiamo $g : (n + 1)^- \longrightarrow X$ mediante

$$g(m) = \begin{cases} f(m) & \text{se} \quad m \in n^- \\ x & \text{se} \quad m = n. \end{cases}$$

Questa funzione è evidentemente iniettiva e quindi $(A, f) < ((n+1)^-, g) \in Y$, contro la sua massimalità. □

Da adesso fino alla fine della presente sezione denoteremo sistematicamente con c un numero naturale diverso da 0, con b il suo successore e con $\gamma : \mathbb{N} \longrightarrow \mathbb{N}$ la funzione data da $\gamma(n) = c \; \forall n \in \mathbb{N}$.

Il *supporto* di una funzione $f : \mathbb{N} \longrightarrow b^-$ è l'insieme $\text{supp}(f) = \{n \in \mathbb{N} \text{ tali che } f(n) \neq 0\}$. Esiste una sola funzione in $b^{-\mathbb{N}}$, detta la *funzione nulla* e indicata con il simbolo 0 tale che $\text{supp}(0) = \emptyset$.

Poniamo $b^{-(\mathbb{N})} = \{f \in b^{-\mathbb{N}} \text{ tali che } \text{supp}(f) \text{ è finito}\}$.

Se $f, g \in b^{-(\mathbb{N})}$ allora l'insieme $D(f, g) = \{n \in \mathbb{N} \text{ tali che } f(n) \neq g(n)\} \subseteq \text{supp}(f) \cup \text{supp}(g)$ è finito e quindi $A(f, g) = \{n \in \mathbb{N} \text{ tali che } D(f, g) \subseteq n^-\} \neq \emptyset$ e quindi ha un minimo che, salvo il caso in cui $f = g$, non é 0;

se $f \neq g$ $\min(A(f,g))$ è dunque il successore di un numero naturale che indicheremo con il simbolo $\partial(f,g)$ In altri termini, posto $\partial(f,g) = n$ avremo che

$$f(n) \neq g(n) \text{ ma } f(m) = g(m) \quad \forall m > n.$$

Ovviamente $\partial(f,g) = \partial(g,f)$. Per ogni $0 \neq f \in b^{-(\mathbb{N})}$ il *grado* di f è il numero naturale $\partial(f) = \partial(f,0)$.

Se $f \neq g \in b^{-(\mathbb{N})}$ diciamo che $f \prec g$ se, posto $n = \partial(f,g)$ si ha che $f(n) < g(n)$ e definiamo una relazione su $b^{-(\mathbb{N})}$, che si vede facilmente essere un ordine totale, ponendo $f \preceq g \Leftrightarrow f = g$ oppure $f \prec g$.

Esercizio 2. *Mostrare che $\preceq$ è un buon ordinamento su $b^{-(\mathbb{N})}$.*

Non è facilissimo ma non verrà utilizzato nel seguito.

Sia ora S un semigruppo e $f : \mathbb{N} \longrightarrow S$. Fissato $n \in \mathbb{N}$, consideriamo la funzione $F : \mathbb{N} \times S \longrightarrow \mathbb{N} \times S$ definita da

$$F(m,s) = (m+1, s + f(n+m+1)).$$

il principio di definizione per ricorsività ci garantisce l'esistenza e unicità di una funzione $\phi : \mathbb{N} \longrightarrow \mathbb{N} \times S$ caratterizzata da

$$\phi(0) = (0, f(n)) \text{ e } \phi(m+1) = F(\phi(m)) \; \forall m \in \mathbb{N}.$$

Chiamiamo $\pi_1 : \mathbb{N} \times S \longrightarrow \mathbb{N}$ e $\pi_2 : \mathbb{N} \times S \longrightarrow S$ le proiezioni sui fattori, in modo che $z = (\pi_1(z), \pi_2(z)) \; \forall z \in \mathbb{N} \times S$ e poniamo

$$\phi_1 = \pi_1 \circ \phi : \mathbb{N} \longrightarrow \mathbb{N} \text{ e } \phi_2 = \pi_2 \circ \phi : \mathbb{N} \longrightarrow S.$$

Avremo dunque

$$(\phi_1(0), \phi_2(0)) = \phi(0) = (0, f(n)) \text{ e } (\phi_1(m+1), \phi_2(m+1)) = \phi(m+1) = F(\phi(m)) =$$

$$F(\phi_1(m), \phi_2(m)) = (\phi_1(m) + 1, \phi_2(m) + f(n + \phi_1(m) + 1)) \; \forall m \in \mathbb{N}$$

Da cui si deduce che $\phi_1 = id_{\mathbb{N}}$, che $\phi_2(0) = f(n)$ e che $\phi_2(m+1) = \phi_2(m) + f(n+m+1) \; \forall m \in \mathbb{N}$. Useremo la notazione

$$\sum_{p=n}^{n+m} f(p) = \phi_2(m).$$

Abbiamo dunque definito una funzione $\mathbb{N} \longrightarrow S$ caratterizzata dalle seguenti proprietà:

$$\sum_{p=n}^{n} f(p) = f(n) \text{ e } \sum_{p=n}^{n+m+1} f(p) = \sum_{p=n}^{n+m} f(p) + f(n+m+1).$$

Se $f : \mathbb{N} \longrightarrow S$ ha supporto finito poniamo

$$\sum_{p=n}^{\infty} f(p) = \begin{cases} 0 & \text{se } \ f = 0 \text{ oppure } \partial(f) < n \\ \sum_{p=n}^{\partial(f)} f(p) & \text{se } \ \partial(f) \geq n. \end{cases}$$

Alcune ovvie osservazioni ci saranno immediatamente utili:

Proposizione 21. *Siano $f, g, h \in S^{\mathbb{N}}, n, m, p, r \in \mathbb{N}$*

1. *se $f(n+p) + g(n+p) = h(n+p)\ \forall p \in (m+1)^-$ allora $\sum_{p=n}^{n+m} h(p) = \sum_{p=n}^{n+m} f(p) + \sum_{p=n}^{n+m} g(p)$.*
2. *se $f(n+p) + g(n+p) = h(n+p)\ \forall p \in (m+1)^-$ e f, g hanno supporto finito allora anche h ha supporto finito e $\sum_{p=n}^{\infty} h(p) = \sum_{p=n}^{\infty} f(p) + \sum_{p=n}^{\infty} g(p)$.*
3. *Se $r < m$ allora $\sum_{p=n}^{n+m} f(p) = \sum_{p=n}^{n+r} f(p) + \sum_{p=r+1}^{n+m} f(p)$.*
4. *Se f ha supporto finito allora $\sum_{p=n}^{\infty} f(p) = \sum_{p=n}^{n+m} f(p) + \sum_{p=n+m+1}^{\infty} f(p)$.*

Proposizione 22. *Per ogni $n \in \mathbb{N}$* $\quad \sum_{p=0}^{n} \gamma(p) b^p + 1 = b^{n+1}$.

Dimostrazione. Sia U l'insieme di tutti i numeri naturali su cui vale l'uguaglianza citata. Allora

$$\sum_{p=0}^{0} \gamma(p) b^p + 1 = \gamma(0) + 1 = c + 1 = b = b^1$$

e quindi $0 \in U$. Se $n \in U$ allora

$$\sum_{p=0}^{n+1} \gamma(p) b^p + 1 = (\sum_{p=0}^{n} \gamma(p) + c b^{n+1}) + 1 = (\sum_{p=0}^{n} \gamma(p)) + + c b^{n+1} =$$

$$b^{n+1} + c b^{n+1} = b b^{n+1} = b^{n+2}.$$

□

Teorema 11. *La funzione* $\psi : b^{-(\mathbb{N})} \longrightarrow \mathbb{N}$ *definita da*

$$\psi(f) = \sum_{p=0}^{\infty} f(p)b^p$$

è una biezione e conserva l'ordine.

Dimostrazione. Siano $f < g \in b^{-(\mathbb{N})}$, e consideriamo la funzione $h : \mathbb{N} \longrightarrow \mathbb{N}$ tale che $f(m) + h(m) = c = \gamma(m) \quad \forall m \in \mathbb{N}$.

Esiste $n \in \mathbb{N}$ tale che $f(n) < g(n)$ e $f(m) = g(m)\ \forall n > m$. Se $n = r + 1$ allora

$$\sum_{p=0}^{r+1} f(p)b^p + \sum_{p=0}^{r} h(p)b^p = f(n)b^n + \sum_{p=0}^{r} \gamma(p)b^p < (f(n) + 1)b^n$$

cioè $\sum_{p=0}^{n} f(p)b^p < (f(n) + 1)b^n$,e questa disuguaglianza è banalmente vera se $n = 0$; pertanto, in tutti i casi, possiamo calcolare:

$$\psi(f) = \sum_{p=0}^{n} f(p)b^p + \sum_{p=n+1}^{\infty} f(p)b^p < (f(n) + 1)b^n + \sum_{p=n+1}^{\infty} f(p)b^p \leq$$

$$g(n)b^n + \sum_{p=n+1}^{\infty} f(p)b^p \leq \sum_{p=0}^{n} g(p)b^p + \sum_{p=n+1}^{\infty} g(p)b^p = \psi(g).$$

ψ rispetta l'ordine stretto ed è quindi iniettiva.

Prima di affrontare la suriettività di ψ osserviamo che $0 \in \mathrm{Im}(\psi)$ e, ripetendo la dimostrazione della proposizione 14.3 si vede che $\forall n \in \mathbb{N}\ \exists m \in \mathbb{N}$ tali che $b^m > n$ quindi l'insieme $A = \{m \text{ tali che } b^m \leq n\}$ non è σ-chiuso e, per ogni $0 \neq n \in \mathbb{N}$ esiste un unico $\eta(n) \in \mathbb{N}$ tale che

$$b^{\eta(n)} \leq n < b^{\eta(n)+1}.$$

Supponiamo, per assurdo, che $\mathbb{N} - \mathrm{Im}(\psi) \neq \emptyset$ e sia n il suo minimo; poniamo $m = \eta(n)$. L'algoritmo di divisione ci procura $q \in \mathbb{N} \ni r < b^m$ tali che $n = b^m q + r$. Osserviamo che $q \geq 1$ mentre $q \geq b \Rightarrow n \geq b^m q \geq b^m b = b^{m+1}$ porterebbe immediatamente a una contraddizione con la scelta di m. Inoltre $n > r \Rightarrow r \in \mathrm{Im}(\psi)$. Perciò esiste $f \in b^{-(\mathbb{N})}$ tale che $\psi(f) = r$. Se $f \neq 0$ allora $r < b^m \Rightarrow \partial(f) < m$ ed, in particolare, $f(n) = 0\ \forall n \geq m$. La funzione

$g \in b^{-(\mathbb{N})}$ data da $g(n) = f(n)$ se $n < m,\ g(m) = q,\ g(n) = 0$ se $n > m$ soddisfa $\partial(g) = m$, inoltre

$$\psi(g) = \sum_{p=0}^{m} f(p)b^p = \psi(f) + qb^m = n.$$

Quindi $n \in \mathrm{Im}(\psi)$. □

Per ogni $n \in \mathbb{N}$ la successione $\psi^{-1}(n) \in b^{-(\mathbb{N})}$ è chiamata *rappresentazione* $b-$*aria* di n.

In quanto segue dovremo maneggiare pesantemente l'algoritmo di divisione, pertanto introduciamo una notazione che ne agevoli l'uso: poniamo pertanto, per ogni $n \in \mathbb{N},\ n' = n \div b,$ e $n'' = n \mod b$; questi due numeri sono pertanto caratterizzati da $n'' \in b^-$ e da $n = n'b + n'',\ \forall n \in \mathbb{N}$.

Siano $f, g \in b^{-(\mathbb{N})}$, vogliamo trovare $h \in b^{-(\mathbb{N})}$ tale che $\psi(f) + \psi(g) = \psi(h)$.

Usiamo il principio di definizione per ricorsività scegliendo $X = \mathbb{N} \times \mathbb{N} \times b^-$, $x = (0, (f(0) + g(0))', (f(0) + g(0))'')$, ρ, dove ρ è definita da

$$\rho(n, z, y) = (n + 1, (f(n + 1) + g(n + 1) + z)', (f(n + 1) + g(n + 1) + z)'').$$

Esiste dunque un'unica funzione $\phi : \mathbb{N} \longrightarrow \mathbb{N} \times \mathbb{N} \times b^-$ caratterizzata da

$$\phi(0) = (0, (f(0) + g(0))', (f(0) + g(0))'' \quad \text{e}$$

$$\phi(n + 1) = \rho(\phi(n))\ \forall n \in \mathbb{N}.$$

Chiamiamo π_1, π_2, π_3 le proiezioni $\mathbb{N}\times\mathbb{N}\times\mathbb{N} \longrightarrow \mathbb{N}$ e poniamo $\phi_1 = \pi_1 \circ \phi,\ r = \pi_2 \circ \phi,\ h = \pi_3 \circ \phi$. Un calcolo ormai prevedibile ci mostra che $\phi_1 = id_{\mathbb{N}}$, che

$$f(0) + g(0) = r(0)b + h(0) \text{ e che}$$

$$f(n + 1) + g(n + 1) + r(n) = r(n + 1)b + h(n + 1)\ \forall n \in \mathbb{N}.$$

Proposizione 23. *Nelle condizioni appena descritte:*

1. $\forall n \in \mathbb{N} \quad r(n) \in 2^-$.
2. $r \in 2^{-(\mathbb{N})}$ *e* $h \in b^{-(\mathbb{N})}$.
3. $\sum_{p=0}^{\infty} f(p)b^p + \sum_{p=0}^{\infty} g(p)b^p = \sum_{p=0}^{\infty} h(p)b^p$.

Dimostrazione. 1. Sia $U = \{n \in \mathbb{N} \text{ tali che } r(n) < 2\}$. $0 \in U$ perché

$$r(0)b \leq f(0) + g(0) \leq c + c < 2b.$$

Se $n \in U$ allora $r(n+1)b \leq f(n+1) + g(n+1) + r(n) < c + c + 2 = 2b$. quindi $U = \mathbb{N}$.

2. Sia $n \in \mathbb{N}$ tale che $f(m) = g(m) = 0 \ \forall m > n$, allora, per ogni $p \in \mathbb{N}$ avremo

$$r(n+1+p)b + h(n+1+p) =$$

$$f(n+1+p) + g(n+1+p) + r(n+p) = r(n+p) < b$$

da cui si deduce che $r(n+1+p) = 0$ e che $h(n+1+p) = r(n+p)$, quindi $\text{supp}(r) \subseteq (n+1)^-$ e $\text{supp}(h) \subseteq (n+2)^-$.

3.

$$\sum_{p=0}^{\infty} f(p)b^p + \sum_{p=0}^{\infty} g(p)b^p + \sum_{p=0}^{\infty} r(p)b^{p+1} =$$

$$f(0) + \sum_{p=0}^{\infty} f(\sigma(p))b^{p+1} + g(0)\sum_{p=0}^{\infty} g(\sigma(p))b^{p+1} + \sum_{p=0}^{\infty} r(p)b^{p+1} =$$

$$f(0) + g(0) + \sum_{p=0}^{\infty} (f(\sigma(p)) + g(\sigma(p)) + r(p))b^{p+1} =$$

$$r(0)b + (h)(0) + \sum_{p=0}^{\infty} (r(\sigma(p))b + (h)(\sigma(p)))b^{p+1} =$$

$$\sum_{p=0}^{\infty} (h)(p)b^p + \sum_{p=0}^{\infty} r(p)b^{p+1};$$

E dalla proprietà cancellativa segue la tesi.

□

Si dice che r è la *funzione riporto* e che h è ottenuta da f, g mediante l'*algoritmo della somma*.

Esercizio 3. *Siano $f < g \in b^{-(\mathbb{N})}$. Scimmiottando l'argomento appena esposto trovare $h \in b^{-(\mathbb{N})}$ tale che $\sum_{p=0}^{\infty} f(p)b^p + \sum_{p=0}^{\infty} h(p)b^p = \sum_{p=0}^{\infty} g(p)b^p$.*

Enunciare e dimostrare i criteri di divisibilità per c e per $b+1$; estenderli ai loro divisori.

Adesso esporremo, ma molto più allegramente, l'algoritmo della moltiplicazione: date $f, g \in b^{-(\mathbb{N})}$ vogliamo trovare

$$h \in b^{-(\mathbb{N})} \text{ tale che } \psi(f)\psi(g) = \psi(h)$$

Fissiamo $m \in \mathbb{N}$; usando opportunamente il principio di definizione per ricorsività possiamo trovare due funzioni $r(m, \quad) \in \mathbb{N}^{\mathbb{N}}, \quad s(m, \quad) \in b^{-\mathbb{N}}$ caratterizzate dalle seguenti proprietà:

$$g(m)f(0) = r(m,0)b + s(m,0),$$

$$\forall n \in \mathbb{N} \quad g(m)f(n+1) + r(m,n) = r(m,n+1)b + s(m,n+1).$$

Non è difficile controllare che $r(m, \quad), \ s(m, \quad)$ hanno supporto finito, sono la funzione nulla per m abbastanza grande e che

$$g(m)\psi(f) = \sum_{n=0}^{\infty} s(m,n)b^n.$$

D'altra parte

$$\psi(f)\psi(g) = \psi(f)\sum_{m=0}^{\infty} g(m)b^m =$$

$$\sum_{m=0}^{\infty} \psi(f)g(m)b^m = \sum_{m=0}^{\infty}(\sum_{n=0}^{\infty} s(m,n)b^n)b^m = \sum_{n=0}^{\infty}\sum_{m=0}^{\infty} s(m,n)b^{n+m}.$$

Il lettore è invitato a verificare l'ultima uguaglianza.

Utilizzando ancora una volta il principio di definizione per ricorsività si trovano due funzioni con supporto finito $h : \mathbb{N} \longrightarrow b^{-}, \quad \rho : \mathbb{N} \longrightarrow \mathbb{N}$ caratterizzate da

$$h(0) = s(0,0), \quad \rho(0) = 0$$

$$\forall p \in \mathbb{N} \quad \sum_{m=0}^{p+1} s(m, p+1-m) + \rho(p) = \rho(p+1)b + h(p+1).$$

La funzione h è quanto andavamo cercando, infatti

$$\psi(h) + b\sum_{p=0}^{\infty} \rho(p+1)b^{p+1} = \sum_{p=0}^{\infty} h(p)b^p + b\sum_{p=0}^{\infty} \rho(p+1)b^{p+1} =$$

$$h(0)+\sum_{p=0}^{\infty}h(p+1)b^{p+1}+\sum_{p=0}^{\infty}\rho(p+1)b^{p+2}=$$

$$s(0,0)+\sum_{p=0}^{\infty}(h(p+1)+\rho(p+1)b)b^{p+1}=$$

$$s(0,0)+\sum_{p=0}^{\infty}(\sum_{q=0}^{p+1}s(q,p+1-q)+\rho(p))b^{p+1}=$$

$$s(0,0)+\sum_{p=0}^{\infty}\sum_{q=0}^{p+1}s(q,p+1-q)b^{p+1}+\sum_{p=0}^{\infty}\rho(p)b^{p+1}=$$

$$\sum_{p=0}^{\infty}\sum_{q=0}^{p}s(q,p-q)b^{p}+\sum_{p=0}^{\infty}\rho(p)b^{p+1},$$

poniamo, nel primo addendo, $n=p-q,\ m=q$ cosicché possiamo continuare il conto con

$$\sum_{n=0}^{\infty}\sum_{m=0}^{m+n}s(m,n)b^{m+n}+\sum_{p=0}^{\infty}\rho(p)b^{p+1}=$$

$$\sum_{n=0}^{\infty}(\sum_{m=0}^{\infty}s(m,n)b^{m})b^{n}+\rho(0)+\sum_{p=0}^{\infty}\rho(p+1)b^{p+2},$$

che, usando la proprietà cancellativa ed il fatto che $\rho(0)=0$, fornisce quanto si cercava.

Il lettore che abbia l'ambizione di giustificare le acrobazie usate in alcuni dei calcoli precedenti ne trarrà adeguato beneficio a spese di un lavoro non difficile che richiede una certa accuratezza.

Desideriamo dare (almeno) una rappresentazione a tutti gli elementi di $\mathbb{R}^+$.

Poniamo $\mathbb{N}^+=\mathbb{N}-\{0\}$; è ovvio che nessun suo sottoinsieme proprio e σ-chiuso contiene 1. Se $f\in b^{-N^+}$ possiamo, per ogni $m\in\mathbb{N}$, considerare il numero reale $\sum_{p=1}^{m+1}f(p)b^{-p}\in\mathbb{R}^+$. Ma adesso verifichiamo che $\forall m\in\mathbb{N}\ \sum_{p=1}^{m+1}f(p)b^{-p}<1$. Si vede subito che

$$\forall m\in\mathbb{N},\ \sum_{p=1}^{m+1}f(p)b^{-p}\leq\sum_{p=1}^{m+1}\gamma(p)b^{-p}$$

per cui il risultato che desideriamo provare seguirà dal seguente

Lemma 2. *Per ogni* $m \in \mathbb{N}$, $\sum_{p=1}^{m+1} \gamma(p)b^{-p} + b^{-(m+1)} = 1$.

Dimostrazione. Sia U il sottoinsieme di $\mathbb{N}$ per cui vale l'enunciato. $0 \in U$ in quanto

$$\sum_{p=1}^{0+1} \gamma(p)b^{-p} + b^{-(0+1)} = cb^{-1} + b^{-1} = bb^{-1} = 1$$

Inoltre se $m \in U$ allora

$$\sum_{p=1}^{m+2} \gamma(p)b^{-p} + b^{-(m+2)} = \sum_{p=1}^{m+1} \gamma(p)b^{-p} + cb^{-(m+2)} + b^{-(m+2)} =$$

$$\sum_{p=1}^{m+1} \gamma(p)b^{-p} + bb^{-(m+2)} = \sum_{p=1}^{m+1} \gamma(p)b^{-p} + b^{-(m+1)} = 1.$$

Quindi $U = \mathbb{N}$. □

Poniamo $\sum_{p=1}^{\infty} f(p)b^{-p} = \sup_{m\in\mathbb{N}}\{\sum_{p=1}^{m+1} f(p)b^{-p}\}$, che ha perfettamente senso perché si tratta dell'estremo superiore di un insieme non vuoto e superiormente limitato di un campo ordinato completo.

Abbiamo così definito una funzione

$$\overline{\psi} : b^{-N^+} \longrightarrow [0,1] \subseteq \mathbb{R}^+.$$

Siccome $\mathbb{R}$ è archimedeo, per ogni $x \in \mathbb{R}$ esiste un unico $n \in \mathbb{Z}$ tale che $n \leq x < n+1$. Tale numero è chiamato *parte intera* di x e indicato con $[x]$. La sua proprietà più rilevante è la seguente: se $\mathbb{Z} \ni n \leq x$ allora $n \leq [x]$ e se $\mathbb{Z} \ni n > x$ allora $n > [x]$. Ovviamente se $x \in \mathbb{R}^+$ allora $[x] \in \mathbb{N}$.

Teorema 12. *La funzione* $\overline{\psi} : b^{-N^+} \longrightarrow [0,1]$ *è suriettiva.*

Dimostrazione. Cominciamo a provare che $1 = \overline{\psi}(\gamma)$. Dal lemma segue facilmente che 1 è un maggiorante per l'insieme $\{\sum_{p=1}^{m+1} \gamma(p)b^{-p}\}_{m\in\mathbb{N}}$. Inoltre, se $\lambda < 1$ possiamo trovare $m \in \mathbb{N}$ tale che $b^{m+1} > (1-\lambda)^{-1}$; ma allora, sempre usando il lemma, si vede che $\sum_{p=1}^{m+1} \gamma(p)b^{-p} = 1 - b^{-(m+1)} > \lambda$.

Sia allora $r \in [0,1[$. Per ogni $m \in \mathbb{N}^+$ usiamo l'algoritmo di divisione per trovare l'unico $\alpha(m) \in \mathbb{N}$ e l'unico $c(m) \in b^-$ tali che

$$[rb^m] = \alpha(m)b + c(m).$$

Affermo che

1. $\alpha(1) = 0, \quad \forall m \in \mathbb{N}^+ \quad \alpha(m+1) = \alpha(m)b + c(m)$.
2. $\forall m \in \mathbb{N} \quad \alpha(m+2) = \sum_{p=1}^{m+1} c(p)b^{m+1-p}$.
3. $\forall m \in \mathbb{N} \quad \sum_{p=1}^{m+1} c(p)b^{-p} \leq r < \sum_{p=1}^{m+1} c(p)b^{-p} + b^{-(m+1)}$.

Ovviamente il punto 3 conclude la dimostrazione.

1. $0 \leq r < 1 \Rightarrow 0 \leq rb < b$ e quindi $0 \leq [rb] < b$ cioè $\alpha(1) = 0$ e $c(1) = [rb]$. Per quanto riguarda la seconda affermazione abbiamo che, per ogni $m \in \mathbb{N}^+, \quad \alpha(m)b + c(m) \leq rb^m < \alpha(m)b + c(m) + 1$, da cui segue che $\alpha(m)b^2 + c(m)b \leq rb^{m+1} < \alpha(m)b^2 + c(m)b + b$ e quindi anche

   $$(\alpha(m)b + c(m))b \leq [rb^{m+1}] < (\alpha(m)b + c(m))b + b.$$

   Ne segue che $d = [rb^{m+1}] - (\alpha(m)b + c(m))b \in b^-$ e

   $$[rb^{m+1}] = (\alpha(m)b + c(m))b + d$$

   dall'unicità del divisore e del resto segue che $\alpha(m+1) = \alpha(m)b + c(m)$ (e anche che $d = c(m+1)$, ma di questo poco ci importa).

2. Sia U l'insieme dei numeri naturali per cui vale l'uguaglianza enunciata. $0 \in U$ perché $\alpha(2) = \alpha(1)b + c(1) = c(1) = \sum_{p=1}^{1} c(p)b^{1-p}$.

   Inoltre, se $m \in U$ allora

   $$\alpha(m+3) = \alpha(m+2)b + c(m+2) =$$

   $$\sum_{p=1}^{m+1} c(p)b^{m+2-p} + c(m+2)b^0 = \sum_{p=1}^{m+2} c(p)b^{m+2-p}.$$

   Quindi $U = \mathbb{N}$.

3. L'affermazione è banalmente vera per $m = 0$; sia dunque $m = n + 1$. dalle disuguaglianze

   $$\alpha(m+1)b + c(m+1) \leq rb^{m+1} < \alpha(m+1)b + c(m+1) + 1$$

   si deduce, moltiplicando per $b^{-(m+1)}$, che

   $$\alpha(m+1)b^{-m} + c(m+1)b^{-(m+1)} \leq r < \alpha(m+1)b^{-m} + c(m+1)b^{-(m+1)} + b^{-(m+1)}.$$

D'altra parte

$$\alpha(m+1)b^{-m} = \alpha(n+2)b^{-(n+1)} = (\sum_{p=1}^{n+1} c(p)b^{n+1-p})b^{-(n+1)} = \sum_{p=1}^{n+1} c(p)b^{-p},$$

da cui segue facilmente la tesi.

□

Chi legge avrà notato l'uso del risultato che segue, e che si prova facilmente per induzione:

Esercizio 4. *Sia A un anello, $a \in A$ e $f \in A^{\mathbb{N}}$,*

$$\forall n, m \in \mathbb{N}, \quad \sum_{p=n}^{n+m} af(p) = a \sum_{p=n}^{n+m} f(p).$$

Denotiamo con $b^{-\mathbb{Z})}$ l'insieme delle funzioni $f : \mathbb{Z} \longrightarrow b^-$ il cui supporto è superiormente limitato e consideriamo la funzione

$$\widetilde{\alpha}\colon b^{-(\mathbb{N})} \times b^{\mathbb{N}^+} \longrightarrow b^{-\mathbb{Z})}$$

definita da

$$\widetilde{\alpha}\ (f,g)(n) = \begin{cases} f(n) & \text{se} \quad n \geq 0 \\ g(-n) & \text{se} \quad n < 0 \end{cases}$$

Si tratta ovviamente di una biezione la cui inversa verrà denotata con α. Indichiamo poi con $\psi + \overline{\psi} : b^{-(\mathbb{N})} \times b^{\mathbb{N}^+} \longrightarrow \mathbb{R}^+$ la funzione definita da

$$(\psi + \overline{\psi})(f,g) = \psi(f) + \overline{\psi}(g) = \sum_{p=0}^{\infty} f(n)b^n + \sum_{p=1}^{\infty} g(n)b^{-n}$$

Abbiamo già controllato che si tratta di una funzione suriettiva, e pertanto sarà tale anche la funzione $\beta = (\psi + \overline{\psi}) \circ \alpha : b^{-\mathbb{Z})} \longrightarrow \mathbb{R}^+$. La notazione $\beta(h) = \sum_{p=-\infty}^{\infty} h(n)b^n$ è troppo accattivante per poter resistere dall'usarla.

Se $x \in \mathbb{R}^+$ chiameremo *rappresentazione $b-$aria* di x un qualunque elemento $h \in b^{-\mathbb{Z})}$ tale che $\beta(h) = x$.

Esercizio 5. *Assegnare convenientemente una relazione d'ordine totale su* $b^{-\mathbb{Z})}$ *in modo che* β *conservi l'ordine.*

Definire il concetto di successore immediato *in* $b^{-\mathbb{Z})}$ *e provare che, se* $f < g \in b^{-\mathbb{Z})}$ *allora* $\beta(f) = \beta(g) \Leftrightarrow g$ *è il successore immediato di* f.

Definire il concetto di elemento periodico *in* $b^{-\mathbb{Z})}$ *e provare che* $\beta(f) \in \mathbb{Q}^+ \Leftrightarrow f$ *è periodico.*

Enunciare e dimostrare l'algoritmo per trasformare $\beta(f) \in \mathbb{Q}^+$ *in un elemento della forma* $n\,m^{-1}$, $n \in \mathbb{N}$, $m \in \mathbb{N}^+$.

Indice