Appunti del corso

Elementi di Geometria da un Punto di Vista Superiore

tenuto dal Prof. Salvatore Coen

Università di Bologna - Anno Accademico 2013/2014

Michele Santa Maria

Indice

Introduzione

Questo testo è ricavato dagli appunti da me presi durante il corso *Elementi di Geometria da un Punto di Vista Superiore*, tenuto dal professor Salvatore Coen nell'anno accademico 2013/14 all'Università di Bologna.

Nel corso degli appunti ho lasciato come esercizi quelle verifiche che in classe sono state lasciate da fare autonomamente a casa e che risultano prove non troppo complesse o comunque di tipo meccanico. Quegli esercizi che sono stati lasciati e che hanno invece richiesto uno sforzo maggiore li ho riportati come osservazioni dimostrate o esempi.

Prego chiunque legga questo testo di contattarmi nel caso trovasse alcuni errori nel testo (o anche solo per osservazioni/domande/chiarimenti) all'indirizzo email: msm139@gmail.com

Nota: Leggendo questi appunti potrebbe sorgere la domanda: perché questo corso contiene la parola "*Geometria*" nel titolo, anche se non vi è alcun contenuto geometrico? La realtà è che non è chiaro nemmeno a me. Nell'ultima settimana del corso abbiamo analizzato alcune parti degli *Elementi di Euclide*, in riferimento ad alcune proposizioni geometriche, che non ho però riportato negli appunti perché sono state poche ore totalmente staccate dal resto del corso (*too little too late*).

Capitolo 1

Nozioni Preliminari di Teoria degli Insiemi

In questo capitolo iniziale introdurremo molte definizioni e alcuni risultati basilari della teoria degli insiemi che vengono poi usati in diversi momenti durante il corso.

Definizione 1.0.1 Un *ordinamento* (indicato con il simbolo $\leq$) su un insieme $\mathcal{X}$ è un sottoinsieme del prodotto cartesiano $\mathcal{X} \times \mathcal{X}$ che verifica le seguenti proprietà:

- $\forall\, x \in \mathcal{X} \quad x \leq x$ (proprietà riflessiva)
- $\forall\, x, y \in \mathcal{X} \quad x \leq y, y \leq x \Longrightarrow x = y$ (proprietà antisimmetrica)
- $\forall\, x, y, z \in \mathcal{X} \quad x \leq y, y \leq z \Longrightarrow x \leq z$ (proprietà transitiva)

Un ordinamento si dice *totale* se $\forall\, x, y \in \mathcal{X}$ vale $x \leq y$ oppure $y \leq x$.

Notazione 1: nel caso in cui si abbiano $x, y \in \mathcal{X}$ tali che $x \leq y$ e $x \neq y$ scriveremo semplicemente $x < y$.

Notazione 2: per ogni insieme ordinato $\mathcal{X}$ indicheremo $\mathcal{X}^+ := \{x \in \mathcal{X} \mid x > 0\}$.

Definizione 1.0.2 Dato un ordinamento "$\leq$" su un insieme $\mathcal{X}$ chiameremo "ordinamento *opposto* a $\leq$" un altro ordinamento "$\preceq$" su $\mathcal{X}$ per cui vale che $x \preceq y \Leftrightarrow y \leq x$.

Esercizio 1.0.1 Dimostrare che l'ordinamento opposto è anch'esso un ordinamento.

Definizione 1.0.3 Un'applicazione $f : \mathcal{X} \longrightarrow \mathcal{Y}$ tra insiemi $(\mathcal{X}, \leq)$, $(\mathcal{Y}, \preceq)$ ordinati si dice *crescente* (o che *mantiene l'ordine*) se $\forall\, a, b \in \mathcal{X}$ con $a \leq b$ vale $f(a) \preceq f(b)$.

Si dice che f è *strettamente crescente* se $a < b \Rightarrow f(a) \prec f(b)$.

Osservazione Se f è una funzione strettamente crescente tra insiemi totalmente ordinati allora è anche iniettiva.

Definizione 1.0.4 Sia dato un insieme con ordinamento $(\mathcal{X}, \leq)$ e un suo sottoinsieme $\mathcal{A} \subseteq \mathcal{X}$. Se $\exists\, M \in \mathcal{A}$ tale che $a \leq M \quad \forall\, a \in \mathcal{A}$ allora chiamiamo M il *massimo* di $\mathcal{A}$ in $\mathcal{X}$, e lo indico con $M = \max_{\mathcal{X}} \mathcal{A}$.

Rispettivamente, se $\exists\, m \in \mathcal{A}$ tale che $m \leq a \quad \forall\, a \in \mathcal{A}$ allora chiamiamo m il *minimo* di $\mathcal{A}$ in $\mathcal{X}$, e lo indico con $m = \min_{\mathcal{X}} \mathcal{A}$.

Se non sarà necessario potremo fare a meno di indicare lo spazio $\mathcal{X}$ in cui $\mathcal{A}$ è immerso semplificando le notazioni in $M = \max \mathcal{A}$ e $m = \min \mathcal{A}$.

Osservazione Il massimo (o minimo) di un insieme, se esiste, è unico.

Dimostrazione: Per ipotesi sappiamo che esiste $M = \max \mathcal{A}$.

Supponiamo per assurdo che esista un altro massimo di $\mathcal{X}$, e lo indichiamo con M'.

Allora vale che $M \leq M'$ perché $M \in \mathcal{A}$ e M' è massimo.

Ma anche che $M' \leq M$ perché $M' \in \mathcal{A}$ e M è massimo.

Dunque, per la proprietà antisimmetrica abbiamo $M \leq M'$, $M' \leq M \Longrightarrow M = M'$.

□

Definizione 1.0.5 Preso nuovamente un insieme con ordinamento $(\mathcal{X}, \leq)$ e un suo sottoinsieme $\mathcal{A} \subseteq \mathcal{X}$ chiamiamo *maggioranti* (rispettivamente *minoranti*) tutti gli $y \in \mathcal{X}$ tali che $a \leq y\ \forall a \in \mathcal{A}$ (rispettivamente $y \leq a$).

chiamiamo inoltre *estremo superiore* di $\mathcal{A}$ il minimo dei suoi maggioranti, ovvero l'elemento $x \in \mathcal{X}$ per cui vale $x = \min\{y \in \mathcal{X} \,|\, a \leq y\ \forall a \in \mathcal{A}\}$, e lo indico con $\sup_{\mathcal{X}} \mathcal{A}$.

chiamiamo poi *estremo inferiore* il massimo dei suoi minoranti, e lo indico con $\inf_{\mathcal{X}} \mathcal{A}$.

Anche stavolta per semplicità di notazione ometteremo l'insieme di appartenenza $\mathcal{X}$ ogni volta che non sarà strettamente necessario specificarlo.

Osservazione L'estremo superiore (o inferiore) di un insieme, se esiste, è unico.

La dimostrazione si basa semplicemente sul fatto che l'estremo superiore è definito come un massimo, che abbiamo già dimostrato essere unico.

Osservazione Se M è massimo di un insieme $\mathcal{A}$ allora è anche un suo estremo superiore.

Dimostrazione: M è sicuramente un maggiorante per definizione di massimo; ma è anche il minimo dei maggioranti perché se esistesse M' maggiorante tale che $M' \leq M$ avremmo immediatamente anche che $M \leq M'$ perché il massimo di un insieme è contenuto nell'insieme stesso.

□

Proposizione 1.0.1 *Sia $(\mathcal{X}, \leq)$ un insieme totalmente ordinato; consideriamo $\mathcal{A} \subseteq \mathcal{X}$, $\mathcal{A} \neq \emptyset$ e $M, m \in \mathcal{X}$. Allora valgono le seguenti:*

1. *$M = \sup_{\mathcal{X}} \mathcal{A}$ se e soltanto se valgono le due proprietà:*

   (α) $a \leq M \ \forall a \in \mathcal{A}$

   (β) $\forall x \in \mathcal{X}$ *tali che* $x < M \ \exists\, a \in \mathcal{A}$ *tale che* $x < a \leq M$

2. *$m = \inf_{\mathcal{X}} \mathcal{A}$ se e soltanto se valgono le due proprietà:*

   (α') $m \leq a \ \forall a \in \mathcal{A}$

   (β') $\forall x \in \mathcal{X}$ *tali che* $m < x \ \exists\, a \in \mathcal{A}$ *tale che* $m \leq a < x$

Dimostrazione: Dimostriamo il punto (1):

$\boxed{\Longrightarrow}$ sappiamo che $M = \sup_{\mathcal{X}} \mathcal{A}$.

Ma allora la proprietà (α) vale perché M è maggiorante di $\mathcal{A}$.

Per dimostrare la proprietà (β) abbiamo che, poiché $M = \min\{\text{maggioranti di } \mathcal{A}\}$, se prendiamo $x < M$ esso non è un maggiorante. Ma se non è un maggiorante significa che esiste un $a \in \mathcal{A}$ tale che $a \not\leq x$. Visto che $\mathcal{X}$ è totalmente ordinato $a \not\leq x \Rightarrow x < a$, e sicuramente $a \leq M$ poiché M è un maggiorante di $\mathcal{A}$.

$\boxed{\Longleftarrow}$ Sappiamo che valgono (α) e (β).

Da (α) abbiamo che M è sicuramente un maggiorante di $\mathcal{A}$, dunque quello che voglio mostrare è che sia il più piccolo possibile. Supponiamo quindi per assurdo che esista un certo $x \in \mathcal{X}$ maggiorante anch'esso, ma tale che $x < M$.

La proprietà (β) mi assicura che $\exists a \in \mathcal{A}$ tale che $x < a \leq M$, quindi x in realtà non può essere un maggiorante.

Il punto (2) si dimostra in modo analogo.

□

Definizione 1.0.6 Dato $(\mathcal{X}, \leq)$ insieme ordinato, sia $\mathcal{A} \subseteq \mathcal{X}$ con $\mathcal{A} \neq \emptyset$. si dice che $\mathcal{A}$ è *superiormente limitato* (o *inferiormente limitato*) se ammette dei maggioranti (o minoranti).

Lo spazio $(\mathcal{X}, \leq)$ si dice inoltre *completo* (rispetto a $\leq$) quando $\forall \mathcal{A} \subseteq \mathcal{X}$ con $\mathcal{A} \neq \emptyset$ vale che: se $\mathcal{A}$ è superiormente limitato allora $\exists \sup_{\mathcal{X}} \mathcal{A}$.

Proposizione 1.0.2 *$(\mathcal{X}, \leq)$ è completo $\Longleftrightarrow$ $\forall \mathcal{A} \subseteq \mathcal{X}$ con $\mathcal{A} \neq \emptyset$ vale che: se $\mathcal{A}$ è inferiormente limitato allora $\exists \inf_{\mathcal{X}} \mathcal{A}$.*

Dimostrazione: $\boxed{\Longleftarrow}$ Prendiamo $\mathcal{A} \subseteq \mathcal{X}$ con $\mathcal{A} \neq \emptyset$ e $\mathcal{A}$ superiormente limitato e vogliamo dimostrare che $\exists \max_{\mathcal{X}} \mathcal{A}$.

Sia $\mathcal{B} = \{\text{maggioranti di } \mathcal{A}\} = \{b \in \mathcal{X} \mid a \leq b \ \forall a \in \mathcal{A}\}$, che sappiamo essere non vuoto.

Visto che $\mathcal{A} \neq \emptyset$ abbiamo che $\mathcal{B}$ è inferiormente limitato, quindi per ipotesi sappiamo che $\exists \inf_{\mathcal{X}} \mathcal{B} = m$. Vediamo che m è proprio il minimo di B:

Se consideriamo $\mathcal{L} = \{\text{minoranti di } \mathcal{B}\}$ abbiamo che $m = max_{\mathcal{X}}\mathcal{B}$ per definizione di estremo inferiore. Ma $\forall a \in \mathcal{A}$ vale $a \leq b \; \forall b \in \mathcal{B} \Longrightarrow a \in \mathcal{L} \Longrightarrow a \leq m \Longrightarrow m \in \mathcal{B}$.

$\boxed{\Longrightarrow}$ stesso ragionamento scambiando maggioranti con minoranti.

□

Un esempio di insieme non completo è $\mathbb{Q}$, visto che $\sqrt{2}$ non gli appartiene. Ma c'è anche un altro modo di scoprire che $\mathbb{Q}$ non è razionale che è molto più generale ed istruttivo:

Esempio 1.0.1 Sia $p \in \mathbb{Q}$ un numero positivo che non sia quadrato di nessun altro razionale[1], e sia $\mathcal{S} = \{q \in \mathbb{Q} \,|\, q \leq 0\} \cup \{q \in \mathbb{Q} \,|\, q^2 < p\}$.

Allora $\mathcal{S}$ è superiormente limitato in $\mathbb{Q}$, ma non ammette estremo superiore.

Dimostrazione: Dimostriamo per prima cosa che $\mathcal{S}$ è superiormente limitato.

Sicuramente $p \neq 1$, quindi analizziamo i due casi:

$p > 1$) se prendiamo $q = \frac{1}{p} \Longrightarrow q^2 = \frac{1}{p^2} < 1 < p \Longrightarrow q \in \mathcal{S}$, quindi $\mathcal{S} \neq \emptyset$.

Inoltre p è maggiorante di $\mathcal{S}$ perché se esistesse $q \in \mathcal{S}$ tale che $p \leq q$ allora avremmo che $p < p^2 \leq q^2$, quindi q non potrebbe stare in $\mathcal{S}$.

$p < 1$) 1 è maggiorante.

Quindi adesso sappiamo che in ogni caso $\mathcal{S}$ è sicuramente limitato superiormente. Supponiamo per assurdo che $\exists \sup_{\mathbb{Q}} \mathcal{S} = E > 0$. e consideriamo la seguente funzione:

$$f : \mathbb{Q}^* \longrightarrow \mathbb{Q} \qquad f(x) = \frac{x(x^2 + 3p}{3x^2 + p}$$

e le seguenti due formule:

$$(1) f(x) - x = \frac{2x(p - x^2)}{3x^2 + p} \qquad (2) f^2(x) - p = \frac{(x^2 - p)^3}{3x^2 + p}$$

Se $E^2 < p$ abbiamo: dalla (1) $f(E) - E > 0 \Rightarrow f(E) > E$ e dalla (2) $f^2(E) - p < 0 \Rightarrow f(E) \in \mathcal{S}$, che uniti danno un assurdo perché E è un maggiorante.

Se $E^2 > p$ abbiamo: dalla (1) $f(E) < E$ e dalla (2) $f^2(E) > p$, che uniti danno un assurdo perché $f(E)$ sarebbe un maggiorante di $\mathcal{S}$ più piccolo di E che è definito come il minimo dei maggioranti.

□

[1] Un numero di questo tipo sappiamo già che esiste: $\sqrt{2}$.

Capitolo 2

I Numeri Naturali: $\mathbb{N}$

2.1 Definizione di $\mathbb{N}$

Definiamo come $\mathbb{N}$ un insieme che soddisfa la seguenti proprietà:

1. Esiste un elemento $0 \in \mathbb{N}$
2. Esiste una funzione S (*successore*) tale che $0 \notin S(\mathbb{N})$
3. S è iniettiva
4. Se $\exists\, M \subseteq \mathbb{N}$ tale che $(0 \in M) \wedge (m \in M \Rightarrow S(m) \in M) \Longrightarrow M = \mathbb{N}$[1]

Ma questo di per sé non ci dice che un tale insieme esista, ed è effettivamente impossibile da verificare a questo livello, quindi se ne postula l'esistenza:

Assioma di Peano: *esiste* $\mathbb{N}$ *come definito sopra.*

Una volta definito $\mathbb{N}$ in questo modo cercheremo nell'arco di questo capitolo di dimostrare vari risultati aritmetici usando solo le nozioni definite e dimostrate in precedenza.

Definizione 2.1.1 Un insieme che verifica la proprietà (4) sopra citata si dice *induttivo.*

Una delle prime cose che è utile osservare è che la funzione $S : \mathbb{N} \longrightarrow \mathbb{N}^*$ [2] sopra definita non solo è iniettiva, ma è anche surgettiva. Dunque è in realtà una bigezione!

Difatti preso $A = \{n \in \mathbb{N} \mid \exists\, m \in \mathbb{N} \text{ tale che } S(m) = n\} \cup \{0\} = S(\mathbb{N}) \cup \{0\}$ vale:

Se $n \in A \Longrightarrow n = S(m) \Longrightarrow S(n) = S(S(m)) \Longrightarrow S(n) \in A$.

Dunque abbiamo appena mostrato che A è induttivo, e quindi per la proprietà (4) abbiamo $A = \mathbb{N}$.

[1] Questa proprietà viene anche chiamata **Assioma d'Induzione**.

[2] Con il simbolo $\mathbb{N}^*$ indichiamo l'insieme $\mathbb{N}\backslash\{0\}$.

Visto che abbiamo dimostrato che la funzione S è una bigezione tra $\mathbb{N}$ ed $\mathbb{N}^*$ possiamo sempre trovare per ogni $n \neq 0$ un elemento m tale che $S(m) = n$. Tale elemento m sarà da ora in poi chiamato *predecessore* di n.

Esercizio 2.1.1 Le quattro proprietà che definiscono $\mathbb{N}$ sono tutte indipendenti? Prova a toglierne una e trovare un insieme che soddisfi le rimanenti!

2.2 Operazioni in $\mathbb{N}$

Sull'insieme dei Numeri Naturali riusciamo a definire delle operazioni in maniera *induttiva*.

$\oplus$ **Somma** Fissiamo un certo $m \in \mathbb{N}$ e definiamo la *somma* di m con un qualsiasi altro elemento $n \in \mathbb{N}$ (denotata $m + n$) come segue:

$$\begin{cases} m + 0 = m \\ m + S(n) = S(m + n) \end{cases}$$

L'operazione appena definita è ben posta poiché se indichiamo come $A = \{n \in \mathbb{N} \mid m+n$ è un naturale ben definito $\}$ abbiamo che $0 \in A$ e che se $n \in A$ allora anche $S(n) \in A$, dunque A è induttivo, quindi $A = \mathbb{N}$.

Osserviamo che con questa notazione possiamo anche scrivere il successivo in un altro modo:

$$S(n) = S(n + 0) = n + S(0) = n + 1$$

E grazie a questa osservazione abbiamo anche che

$$m + (n + 1) = m + S(n) = S(m + n) = (m + n) + 1$$

$\otimes$ **Prodotto** Fissato $m \in \mathbb{N}$ definiamo la *moltiplicazione* di m con un qualsiasi altro elemento $n \in \mathbb{N}$ (denotata $m \cdot n$) come segue:

$$\begin{cases} m \cdot 0 = 0 \\ m \cdot S(n) = m \cdot n + m \end{cases}$$

Anche stavolta possiamo ricavare subito una utile proprietà:

$$m \cdot 1 = m \cdot S(0) = m \cdot 0 + m = 0 + m = m$$

Esercizio 2.2.1 Dimostrare che anche la moltiplicazione è un'operazione ben definita[3].

[3]Non lo svolgo perché si dimostra in modo analogo a quanto fatto per la somma: preso l'insieme dei naturali per cui essa è ben definita cerchiamo di dimostrare che esso è induttivo.

⊛ **Potenza** Fissato $m \in \mathbb{N}$ definiamo *elevamento a potenza* di m con un qualsiasi altro elemento $n \in \mathbb{N}$ (denotata m^n) come segue:

$$\begin{cases} m^0 = 1 \\ m^{S(n)} = m^n \cdot m \end{cases}$$

Esercizio 2.2.2 Dimostrare che anche l'elevamento a potenza è ben definito.

Osservazione Avendo già osservato che è possibile scrivere $S(n)$ come $n+1$ si ricavano immediatamente le utili formule algebriche a cui siamo solitamente abituati:
$m \cdot (n+1) = m \cdot S(n) = m \cdot n + m$
$m^{n+1} = m^{S(n)} = m^n \cdot m$

2.3 Proprietà delle Operazioni

Avendo definito le operazioni nel nostro insieme $\mathbb{N}$ adesso dimostriamone le principali proprietà:

Teorema 2.3.1 *$\mathbb{N}$ con l'operazione "+" è un semigruppo additivo commutativo (cioè la somma è associativa e commutativa) con 0 come elemento neutro.*
Inoltre vale che $\forall a, b, c \in \mathbb{N}$ si ha $a + b = a + c \Leftrightarrow b = c$. [4]

Dimostrazione: Iniziamo col dimostrare che la somma è associativa:
vogliamo dimostrare che $\forall a, b, c \in \mathbb{N} \quad (a+b)+c = a+(b+c)$, e lo facciamo per induzione su c con a e b fissati:
$\boxed{c = 0}$ $(a+b)+0 = a+b = a+(b+0)$.
$\boxed{c \Rightarrow S(c)}$ sappiamo per ipotesi che $(a+b)+c = a+(b+c)$ e vogliamo dimostrare che $(a+b)+S(c) = a+(b+S(c))$.
Ma $(a+b)+S(c) = S((a+b)+c)$ per definizione della somma.
$S((a+b)+c) = S(a+(b+c))$ per ipotesi induttiva.
$S(a+(b+c)) = a+(S(b+c)) = a+(b+S(c))$ di nuovo per definizione di somma in entrambi i passaggi.
Dunque l'associatività della somma è dimostrata.

[4] Questa proprietà in particolare viene chiamata *Legge di Cancellazione* della somma.

Passiamo a dimostrare la commutatività:

Si fa in modo sostanzialmente analogo; vogliamo dimostrare che $a+b=b+a \forall a,b \in \mathbb{N}$, ma stavolta ci servirà ricorrere ad una induzione doppia. Diciamo di voler dimostrare la proprietà per induzione su a:

$\boxed{a=0}$ vogliamo dimostrare che $0+b=b+0$, allora lo facciamo per induzione su b:

- Se $b=0$ abbiamo:
$$0+0=0+0=0$$
- Se è vero che $0+b=b+0$, per il successivo di b abbiamo:
$$0+S(b)=S(0+b)=S(b+0)=S(b)=S(b)+0$$
in cui abbiamo usato la definizione di somma e l'ipotesi induttiva su b.

$\boxed{a \Rightarrow S(a)}$ Sapendo che $a+b=b+a$ vogliamo dimostrare che $S(a)+b=b+S(a)$, e lo facciamo di nuovo per induzione su b:

- Se $b=0$ abbiamo:
$$S(a)+0=S(a+0)=S(0+a)=0+S(a)$$
in cui usiamo sia l'ipotesi induttiva su a che la definizione di somma.
- Se è vero che $S(a)+b=b+S(a)$, per il successivo di b abbiamo:
$$S(a)+S(b)=S(S(a)+b)=S(b+S(a))=S(S(b+a))=$$
$$=S(S(a+b))=S(a+S(b))=S(S(b)+a)=S(b)+S(a)$$
in cui usiamo la definizione di somma ed entrambe le ipotesi induttive su a e b.

Abbiamo quindi dimostrato associatività e commutatività della somma, quindi la prima parte del teorema è fatta.

Infine dimostriamo la Legge di Cancellazione:

Chiamiamo $A=\{a \in \mathbb{N} \mid a+b=a+c \implies b=c\}$ e cerchiamo di dimostrare che in realtà $A=\mathbb{N}$.

Sicuramente $0 \in A$ poiché $0+b=0+c \Leftrightarrow b=c$.

Se prendiamo un certo $a \in A$, per il suo successivo vale:

$$S(a)+b=S(a)+c \Leftrightarrow b+S(a)=c+S(a) \Leftrightarrow$$
$$\Leftrightarrow S(a+b)=S(a+c) \Leftrightarrow a+b=a+c \implies b=c$$

in cui abbiamo usato la definizione di somma, il fatto che S sia una funzione iniettiva e infine il fatto che $a \in A$.

Dunque A è insieme induttivo, quindi $A=\mathbb{N}$.

□

Proposizione 2.3.1 $\forall a, b \in \mathbb{N}$ *vale* $a + b = 0 \iff a = 0, b = 0$

Dimostrazione: $\boxed{\Longleftarrow}$ Ovvio[5].

$\boxed{\Longrightarrow}$ Se fosse $a \neq 0$ sapremmo che $\exists\, k \in \mathbb{N}$ tale che $a = S(k)$;

Ma allora avremmo $a + b = S(k) + b = S(k + b) \neq 0$ per definizione della funzione successore.

Si può poi ragionare analogamente per b.

□

Passiamo adesso alle proprietà della moltiplicazione:

Teorema 2.3.2 $\mathbb{N}$ *con l'operazione "$\cdot$" è un semigruppo moltiplicativo commutativo (cioè la moltiplicazione è associativa e commutativa) con 1 come elemento neutro.*

Inoltre vale che $\forall a, b, c \in \mathbb{N}$ *si ha* $a \cdot (b + c) = a \cdot b + a \cdot c$ *(cioè la vale la proprietà* distributiva *della somma rispetto al prodotto).*

Dimostrazione: Stavolta dimostriamo prima di tutto la proprietà distributiva per induzione su c (quindi con a e b fissati qualsiasi in $\mathbb{N}$), perché ci servirà poi per dimostrare gli altri punti.

$\boxed{c = 0}$ $a \cdot (b + 0) = a \cdot b = a \cdot b + 0 = a \cdot b + a \cdot 0$, in cui usiamo solo la definizione di moltiplicazione e le proprietà della somma dimostrate prima.

$\boxed{c \Rightarrow S(c)}$ Sappiamo che $a \cdot (b + c) = a \cdot b + a \cdot c$, quindi per il successivo di c abbiamo:

$$a \cdot (b + S(c)) = a \cdot S(b + c) = a \cdot (b + c) + a = a \cdot b + a \cdot c + a = a \cdot b + a \cdot S(c)$$

in cui usiamo sia la definizione di moltiplicazione che l'ipotesi induttiva.

Quindi la proprietà distributiva è dimostrata.

Possiamo adesso dimostrare che la moltiplicazione è associativa, e lo facciamo anche stavolta per induzione su c:

$\boxed{c = 0}$ $(a \cdot b) \cdot 0 = 0 = (b \cdot 0) = a \cdot (b \cdot 0)$, in cui abbiamo usato solo la definizione di moltiplicazione data prima.

$\boxed{c \Rightarrow S(c)}$ Sappiamo che $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, quindi per $S(c)$ abbiamo:

$$(a \cdot b) \cdot S(c) = (a \cdot b) \cdot c + (a \cdot b) = a \cdot (b \cdot c) + a \cdot b = a \cdot (b \cdot c + b) = a \cdot (b \cdot S(c))$$

Da notare che questa volta abbiamo usato anche la proprietà distributiva, ed è per questo che ci serviva dimostrarla prima.

[5] Attenzione! Ovvio solo perché abbiamo già fatto questo calcolo in precedenza, altrimenti partendo dalle sole definizioni di $\mathbb{N}$ e somma **non** è ovvio!

Passiamo ora a dimostrare la commutatività, ovvero che $\forall a, b \in \mathbb{N}$ vale $a \cdot b = b \cdot a$.

Proprio come abbiamo fatto per la somma anche stavolta dovremo usare una doppia induzione. Proviamo a dimostrare la proprietà per induzione su a:

$\boxed{a = 0}$ vogliamo dimostrare che $0 \cdot b = b \cdot 0$, e lo facciamo per induzione su b:

- Se $b = 0$ abbiamo che $0 \cdot 0 = 0 = 0 \cdot 0$;
- Se è vero che $0 \cdot b = b \cdot 0$, allora per il successore di b abbiamo che:

$$0 \cdot S(b) = 0 \cdot b + 0 = b \cdot 0 = 0 = S(b) \cdot 0$$

in cui abbiamo usato sia la definizione di moltiplicazione che l'ipotesi induttiva su b.

$\boxed{a \Rightarrow S(a)}$ sappiamo che $a \cdot b = b \cdot a$ e vogliamo dimostrare che funziona tutto anche con il successore di a. Anche stavolta lo dimostriamo per induzione su b:

- Se $b = 0$ abbiamo che $0 \cdot S(a) = 0 \cdot a + 0 = a \cdot 0 = 0 = S(a) \cdot 0$;
- Se è vero che $S(a) \cdot b = b \cdot S(a)$, per il successore di b vale:

$$S(a) \cdot S(b) = S(a) \cdot b + S(a) = b \cdot S(a) + (a + 1) = b \cdot a + b + a + 1 =$$

$$= a \cdot b + a + b + 1 = a \cdot S(b) + (b + 1) = S(b) \cdot a + S(b) = S(b) \cdot S(a)$$

in cui usiamo la definizione di moltiplicazione, le proprietà della somma dimostrate in precedenza ed entrambe le ipotesi induttive su a e su b.

E con questo anche la commutatività è dimostrata.

□

Osservazione Avendo dimostrato la commutatività della nostre operazioni e la distributività a sinistra, vale sicuramente anche la distributività a destra!

Proposizione 2.3.2 $\forall a, b \in \mathbb{N}$ *vale* $a \neq 0, b \neq 0 \Longrightarrow a \cdot b \neq 0$.

Dimostrazione: Se a e b sono entrambi non nulli esistono a' e b' tali che $a = S(a')$ e $b = S(b')$.

Da ciò abbiamo che $a \cdot b = S(a') \cdot S(b') = (a' + 1) \cdot S(b') = a' \cdot S(b') + S(b') = a' \cdot (b' + 1) + b' + 1 = S(a' \cdot (b' + 1) + b')$, e questo non può essere zero per definizione di funzione successore.

□

2.4 Ordinamento in $\mathbb{N}$

Sul nostro insieme $\mathbb{N}$ definito nei paragrafi precedenti possiamo definire un *ordinamento* nel modo in cui siamo abituati a pensarlo:

Definizione 2.4.1 Dati $m, n \in \mathbb{N}$ diciamo che $m \leq n \iff \exists\, a \in \mathbb{N}$ tale che $n = m + a$.
Questa relazione viene chiamata *ordinamento canonico* su $\mathbb{N}$.
indichiamo inoltre con $m < n$ il fatto che $\exists\, a \in \mathbb{N}$ tale che $a \neq 0$ e $n = m + a$.

Proposizione 2.4.1 *L'ordinamento appena definito è totale su* $\mathbb{N}$*, e con questo ordinamento* $\mathbb{N}$ *è illimitato superiormente.*

Dimostrazione: Si può verificare molto velocemente che $\mathbb{N}$ è illimitato superiormente, perché se così non fosse avremmo un naturale $\widehat{n}$ che è più grande di tutti gli altri. Ma di certo $\widehat{n} \leq S(\widehat{n})$, poiché $S(\widehat{n}) = \widehat{n} + 1$, il che è assurdo perché $S(\widehat{n}) \in \mathbb{N}$.

Verificare che l'ordinamento è totale è un po' meno immediato.
Fissiamo un certo $m \in \mathbb{N}$ e consideriamo l'insieme $A = \{n \in \mathbb{N} \mid m, n$ sono confrontabili[6]$\}$ e cerchiamo di dimostrare che $A = \mathbb{N}$.
Sicuramente $0 \in A$ poiché $m = 0 + m \Longrightarrow 0 \leq m$.
Inoltre se un certo $n \in A$ allora abbiamo che:

- Se $m = n$ vale che $S(n) = n + 1 = m + 1 \Longrightarrow m \leq S(n) \Longrightarrow S(n) \in A$;
- Se $m < n$ vuol dire che $\exists\, a \in \mathbb{N}$ tale che $n = m + a$. Ma allora $S(n) = S(m + a) = m + a + 1 = m + (a + 1) \Longrightarrow m \leq S(n) \Longrightarrow S(n) \in A$;
- Se $n < m$ vuol dire che $\exists\, a \in \mathbb{N}$ tale che $m = n + a$ e $a \neq 0$ (altrimenti si avrebbe $m = n$). Ma allora se $a \neq 0$ esiste il suo predecessore, ovvero un elemento a' tale che $S(a') = a$.

  Da ciò ricaviamo $S(n) + a' = n + 1 + a' = n + (a' + 1) = n + S(a') = n + a = m \Longrightarrow S(n) \leq m \Longrightarrow S(n) \in A$.

Quindi in definitiva abbiamo provato che A è un insieme induttivo da cui abbiamo subito che $A = \mathbb{N}$.

□

Proposizione 2.4.2 *Presi* $m, n \in \mathbb{N}$ *abbiamo che le seguenti sono equivalenti:*

1. $m < n$
2. $n = m + c, c > 0$

[6] Ricordiamo che due elementi m, n si dicono *confrontabili* se vale $m \leq n$ oppure $n \leq m$.

3. $m+1 \leq n$

Dimostrazione: $\boxed{1 \Rightarrow 2}$ Dalla definizione di ordinamento abbiamo subito che $\exists\, c$ tale che $n = m + c$. Se fosse $c = 0$ avremmo $n = m + 0 = m$, il che è assurdo perché per ipotesi abbiamo $m \leq n, m \neq n$.

$\boxed{2 \Rightarrow 3}$ Se abbiamo che $n = m+c, c > 0$ sappiamo che esiste il predecessore di c, ovvero un elemento $c' \in \mathbb{N}$ tale che $S(c') = c$. Da ciò ricaviamo che $(m+1) + c' = m + (c'+1) = m + c = n \Longrightarrow (m+1) \leq n$.

$\boxed{3 \Rightarrow 1}$ $m + 1 \leq n \Longrightarrow \exists\, a \in \mathbb{N}$ tale che $n = (m+1) + a$. Ma allora $n = m + (a+1)$ e $a + 1$ è sicuramente diverso da 0, quindi abbiamo proprio la definizione di $m < n$.

□

Definizione 2.4.2 Sia $m \leq n$. chiamiamo *differenza tra* n *e* m il numero naturale $(n-m)$ tale che $n = m + (n - m)$.

Proposizione 2.4.3 *Le operazioni di somma e prodotto mantengono la relazione d'ordine canonica su* $\mathbb{N}$*, ovvero* $\forall a, b, c \in \mathbb{N}$ *valgono le seguenti:*

1. $a < b \Longrightarrow a + c < b + c$

2. $a < b \Longrightarrow a \cdot c < b \cdot c$ *se* $c > 0$

3. $m, n \in \mathbb{N}$, $m < n \Longrightarrow a^m < a^n$ *se* $a > 1$

4. $m \in \mathbb{N}$, $a < b \Longrightarrow a^m < b^m$ *se* $m > 0$

Inoltre le proprietà elencate sopra valgono anche se si sostituisce "<" con "≤" ovunque.

Dimostrazione: $\boxed{1}$ $a < b \Longrightarrow \exists\, k > 0$ tale che $b = a + k$. Ma quindi $b + c = (a + k) + c = (a + c) + k \Longrightarrow a + c < b + c$.

$\boxed{2}$ $a < b \Longrightarrow \exists\, k > 0$ tale che $b = a + k$. Quindi $b \cdot c = a \cdot c + k \cdot c$ e per un'osservazione fatta in precedenza abbiamo che $k > 0, c > 0 \Rightarrow k \cdot c > 0$, da cui abbiamo direttamente che $a \cdot c < b \cdot c$.

$\boxed{3}$ Lo dimostriamo per induzione su n:

- $n = 0$ è impossibile perché $m < n$.
- Se $n = 1$ abbiamo che $m < n \Rightarrow m = 0$ e sappiamo già per ipotesi che $a^0 = 1 < a = a^1$.
- Se vale $a^m < a^n$, per il successore di n avremo che:

  $$1 < a \Longrightarrow a^n = 1 \cdot a^n < a \cdot a^n = a^n \cdot a = a^{S(n)}$$

  in cui usiamo anche le proprietà appena dimostate.

  Da ciò abbiamo subito che $a^m < a^n < a^{S(n)} \Longrightarrow a^m < a^{S(n)}$ per transitività.

4 Stavolta lo dimostriamo per induzione su m:

- Se $m = 1$ $a^1 = a < b = b^1$ per ipotesi.
- Se vale $a^m < b^m$, per il successore di m avremo

$$a^{S(m)} = a^m \cdot a < a^m \cdot b = b \cdot a^m < b \cdot b^m = b^{S(m)} \Longrightarrow a^{S(m)} < b^{S(m)}$$

in cui abbiamo usato la definizione di elevamento a potenza, l'ipotesi induttiva e la transitività dell'ordinamento.

□

In realtà sotto opportune ipotesi le proprietà dimostrate adesso possono essere anche invertite!

Proposizione 2.4.4 *$\forall a, b, c \in \mathbb{N}$ valgono le seguenti:*

1. $a + c < b + c \Longrightarrow a < b$; *inoltre* $a + c = b + c \Longrightarrow a = b$
2. $a \cdot c < b \cdot c$, $c > 0 \Longrightarrow a < b$; *inoltre* $a \cdot c = b \cdot c$, $c > 0 \Longrightarrow a = b$ [7]
3. $a^m < a^n$, $a > 1 \Longrightarrow m < n$; *inoltre* $a^m = a^n$, $a > 1 \Longrightarrow m = n$
4. $a^m < b^m$, $m > 0 \Longrightarrow a < b$; *inoltre* $a^m = b^m$, $m > 0 \Longrightarrow a = b$

Dimostrazione: Dimostriamo solo il punto (1), poiché gli altri si dimostrano esattamente allo stesso modo:

Sappiamo che $a + c < b + c$.
Se avessimo $a = b$ avremmo sicuramente che $a + c = b + c$, che è falso per ipotesi.
Se avessimo $b < a$ dal punto (1) della proposizione precedente ricaverei che $b+c < a+c$, il che è nuovamente falso per ipotesi.
L'unica alternativa valida è a questo punto che $a < b$.

Inoltre se abbiamo che $a + c = b + c$ ripetiamo un ragionamento simile:
Se avessimo $a < b$ di nuovo avremmo che $a + c < b + c$, e allo stesso modo se avessimo $b < a$ avremmo che $b + c < a + c$.
Quindi l'unica alternativa valida è che $a = b$.

□

[7] Questa è chiamata *legge di cancellazione* del prodotto.

2.5 Proprietà di $\mathbb{N}$

Dopo aver definito in $\mathbb{N}$ le operazioni e l'ordinamento opportuni possiamo mostrare varie proprietà del nostro insieme.

Nota: prima di proseguire poniamo che se non ci sarà ambiguità di notazione indicheremo il prodotto di due interi senza il simbolo "$\cdot$" tra di loro, ovvero: $ab = a \cdot b$.

Proposizione 2.5.1 *Preso un insieme $Y \subseteq \mathbb{N}$, $Y \neq \emptyset$, sono vere le seguenti:*

1. *Y ammette minimo in $\mathbb{N}$*
2. *Se $M = \sup_{\mathbb{N}} Y \Longrightarrow M = \max_{\mathbb{N}} Y$*
3. *Y superiormente limitato $\Longrightarrow$ Y ammette massimo*

Dimostrazione: 1 Supponiamo per assurdo che Y non ammetta minimo.

Allora sicuramente $0 \notin Y$ perché altrimenti sarebbe necessariamente il minimo.

definiamo adesso $X = \{n \in \mathbb{N} \mid n < y \, \forall y \in Y\}$ l'insieme dei minoranti di Y.

Da ciò che abbiamo detto prima $0 \in X$, da cui X è non vuoto.

Ma abbiamo di più: se $n \in X$ dobbiamo avere che anche $(n+1) \in X$ altrimenti avremmo che $n < y \, \forall y$, ma $\exists \, \widehat{y}$ tale che $n + 1 \geq \widehat{y}$, da cui ricaviamo:

$$n < \widehat{y} \leq n + 1 \Longrightarrow n + 1 \leq \widehat{y} \leq n + 1 \Longrightarrow \widehat{y} = n + 1$$

il che ci dice che $\widehat{y}$ è proprio il minimo di Y, che per ipotesi non esiste.

Quindi $0 \in X$, $(n \in X \Rightarrow (n + 1) \in X) \Longrightarrow X$ è induttivo $\Longrightarrow X = \mathbb{N} \Longrightarrow Y = \emptyset$, il che è assurdo.

2 Per definizione di estremo superiore abbiamo che $M = \min\{n \in \mathbb{N} \mid y \leq n \, \forall y \in Y\}$.

Se M non fosse il massimo di Y (ovvero $M \notin Y$) avremmo che $y < M \, \forall y \in Y$, da cui $y \leq M - 1 \, \forall y \in Y$, quindi anche $M - 1$ è un maggiorante di Y ed è più piccolo di M, il che è assurdo perché M è per definizione il minimo dei maggioranti.

3 Se Y è superiormente limitato esiste l'insieme X dei suoi maggioranti.

Ma allora per il punto (1) questo insieme ha un minimo m, che diviene per definizione l'estremo superiore di Y.

Ma allora per il punto (2) m è in realtà il massimo di Y.

□

Proposizione 2.5.2 *Sia $m \in \mathbb{N}$, e indichiamo con $\mathbb{N}_m = \{n \in \mathbb{N} \mid m \leq n\}$; Preso $A \subseteq \mathbb{N}_m$ se abbiamo che $m \in A$ e vale $(n \in A \Longrightarrow S(n) \in A)$ allora $A = \mathbb{N}_m$.*

Dimostrazione: Basta considerare l'insieme $B = \{n \in \mathbb{N} \mid n + m \in A\} \subseteq \mathbb{N}$ e dimostrare che è induttivo.

□

Proposizione 2.5.3 *Presi $a, b \in \mathbb{N}$, $a > 0$ valgono le seguenti:*

1. *$\exists\, n$ tale che $na > b$* [8]
2. *$b > 1 \Longrightarrow bn \leq b^n \; \forall n$*
3. *$b > 1 \Longrightarrow \exists\, n$ tale che $b^n \leq a < b^{n+1}$*

Dimostrazione: 1 Se prendiamo $n = b + 1$ abbiamo che

$$a > 0 \Rightarrow a \geq 1 \Rightarrow ab \geq b$$

da cui ricaviamo

$$na = (b+1)a = ab + a \geq b + a \geq b + 1 > b$$

2 Lo dimostriamo per induzione su n:

- Se $n = 0$ abbiamo $b0 = 0 \leq 1 = b^0$
- Se vale $bn \leq b^n$, allora dalle ipotesi di partenza abbiamo che

$$1 < b \Rightarrow 2 \leq b \qquad\qquad 1 \leq n \Rightarrow b \leq bn$$

da cui ricaviamo per il successivo di n

$$b(S(n)) = b(n+1) = bn + b \leq bn + bn = 2bn \leq 2b^n \leq bb^n = b^{n+1} = b^{S(n)}$$

3 Consideriamo l'insieme $X = \{n \in \mathbb{N} \mid a < b^n\}$.

Certo questo insieme è non vuoto perché $1 < b \Rightarrow a < ab \leq b^a$ per il punto precedente.

Ma allora esiste $x = \min X$ per cui vale $a < b^x$ e $a \geq b^{x-1}$ perchè è minimo.

Dunque se chiamiamo $n = x - 1$ abbiamo che

$$b^n \leq a < b^{n+1}$$

□

[8] Questa proprietà ci dice che $\mathbb{N}$ è *archimedeo*.

Teorema 2.5.1 (Divisione Euclidea) *Presi $a, b \in \mathbb{N}$ con $b > 0$, esistono unici $q, r \in \mathbb{N}$ t.c.*

$$a = bq + r, \quad r < b$$

Dimostrazione: Dimostriamo innanzitutto l'esistenza per induzione su a:

$\boxed{a = 0}$ Basta prendere $q = r = 0$.

$\boxed{a \Rightarrow S(a)}$ sappiamo che la divisione euclidea vale per a e vogliamo due naturali q', r' per cui la divisione euclidea valga anche per $a + 1$. Ma se consideriamo $a + 1$ abbiamo che $a + 1 = bq + r + 1$. Dobbiamo ora distinguere due casi:

Se $r = b - 1$ allora $a + 1 = b(q + 1) + 0$ è una divisione euclidea.

Se $r < b - 1$ allora $a + 1 = bq + (r + 1)$ lo è di nuovo.

Passiamo ora a dimostrare l'unicità: supponiamo che valga $a = bq + r = bq' + r'$.

Se fosse $q = q'$ avremmo che $bq = bq' \Longrightarrow r = r'$ e quindi avremmo la nostra tesi.

Se così non fosse possiamo supporre senza perdita di generalità che $q' < q$. Ma allora abbiamo che

$$bq' + r' = bq + r = b(q - q') + bq' + r \Longrightarrow r' = b(q - q') + r$$

$$q' < q \Longrightarrow q - q' \geq 1 \Longrightarrow b(q - q') \geq b \Longrightarrow r' = b(q - q') + r \geq b + r \geq b$$

il che è un assurdo perché $r' < b$ per ipotesi.

□

Nelle notazioni del teorema precedente abbiamo che a viene chiamato *dividendo*, b *divisore* e q ed r sono rispettivamente il *quoziente* e il *resto* della divisione.

Esercizio 2.5.1 Il teorema della divisione euclidea è valido nell'insieme dei numeri razionali?

Teorema 2.5.2 (Unicità di $\mathbb{N}$) *Siano $(\mathbb{N}, 0, S)$, $(\mathbb{N}', 0', S')$ tue terne che verificano gli Assiomi di Peano. Allora l'applicazione*

$$f : \mathbb{N} \longrightarrow \mathbb{N}'$$

tale che $f(0) = 0'$ e $f(S(n)) = S'(f(n))$ è ben definita ed è un isomorfismo che mantiene gli ordini.

Dimostrazione: La buona definizione si vede direttamente da come è stata definita f, quindi non la verifichiamo.

Vediamo che f è iniettiva: definiamo $A = \{n \in \mathbb{N} \mid \text{ se } m < n \text{ allora } f(m) < f(n)\}$ e verifichiamo che questo insieme è tutto $\mathbb{N}$.

$0 \in A$ poiché $m < 0$ è impossibile.

Se $n \in A$ significa che $m < n \Longrightarrow f(m) < f(n)$. Ma allora se valesse che $m < n + 1$ avremmo due casi:

- Se $m = n$ allora $f(m) = f(n) < S'(f(n)) = f(S(n))$, quindi $S(n) \in A$.
- Se $m < n$ allora $f(m) < f(n) < S'(f(n)) = f(S(n))$, quindi $S(n) \in A$.

da cui A è induttivo, e quindi tutto $\mathbb{N}$.

Verifichiamo ora la surgettività: definiamo $B = \{n \in \mathbb{N}' \mid \exists\, m \in \mathbb{N} \text{ tale che } f(m) = n\}$ e verifichiamo anche stavolta che questo insieme è tutto $\mathbb{N}'$.

$f(0) = 0' \Longrightarrow 0 \in B$.

Se $n \in B$ allora $\exists\, m \in \mathbb{N}$ tale che $f(m) = n$, dunque se consideriamo $S(m)$ abbiamo che

$$f(S(m)) = S'(f(m)) = S'(n)$$

e ciò ci dice che anche $S'(n) \in B$, quindi B è induttivo, e quindi è tutto $\mathbb{N}'$.

□

Esercizio 2.5.2 Verificare che vale anche il viceversa del teorema appena annunciato, ovvero: siano $(\mathbb{N}, 0, S)$, $(\mathbb{N}', 0', S')$ come sopra. Se $g : \mathbb{N} \longrightarrow \mathbb{N}'$ è un isomorfismo che mantiene gli ordini allora deve verificare $g(0) = 0'$ e $g(S(n)) = S'(g(n))$.

2.6 Buon Ordinamento

In questo paragrafo daremo delle definizioni proseguendo le nozioni descritte nel capitolo 1 e vedremo come queste si adattino all'insieme dei numeri naturali definito in questo capitolo.

Definizione 2.6.1 Un insieme ordinato $(X, \leq)$ si dice *ben ordinato* se

$$Y \subseteq X,\ Y \neq \emptyset \implies \exists \min_X Y$$

Osservazione Se X è ben ordinato allora è anche totalmente ordinato.

Definizione 2.6.2 Un insieme ordinato $(X, \leq)$ si dice *naturalmente ordinato* se è ben ordinato e

$$Y \subseteq X,\ Y \neq \emptyset,\ Y \text{ superiormente limitato} \implies \exists \max_X Y$$

Osservazione Se X è ben ordinato allora è anche completo.

Un esempio di insieme naturalmente ordinato sono chiaramente i numeri naturali di cui abbiamo parlato fino ad ora, ma un esempio di insieme non naturalmente ordinato come lo possiamo trovare? Possiamo provare a costruirlo:

Siano $(\mathbb{N}, 0, S)$ e $(\mathbb{N}', 0', S')$ due terne soddisfacenti gli assiomi di Peano in cui sono definiti due ordinamenti che indichiamo con $\leq$ e $\leq'$ rispettivamente.

Allora definiamo un ordinamento $\preceq$ sull'insieme $\mathbb{N} \cup \mathbb{N}'$ come $\preceq\big|_{\mathbb{N}} = \leq$, $\preceq\big|_{\mathbb{N}'} = \leq'$, e se prendiamo $a \in \mathbb{N}$ e $b \in \mathbb{N}'$ diciamo che vale sempre $a \prec b$.

L'insieme $(\mathbb{N} \cup \mathbb{N}', \preceq)$ è ben ordinato? Bé si, poiché se prendiamo un sottoinsieme di $\mathbb{N} \cup \mathbb{N}'$ esso può essere tutto contenuto in $\mathbb{N}$ (quindi ammette minimo perché $\mathbb{N}$ è ben ordinato), può essere tutto contenuto in $\mathbb{N}'$ (quindi ammette minimo perché $\mathbb{N}'$ è ben ordinato), oppure può contenere elementi di entrambi gli insiemi di partenza $\mathbb{N}$ e $\mathbb{N}'$, nel qual caso avremo comunque un minimo perché tutti gli elementi di $\mathbb{N}$ sono minori di quelli di $\mathbb{N}'$ per l'ordinamento definito sopra.

Ma quest'insieme è naturalmente ordinato? Stavolta no, poiché ad esempio l'insieme $\mathbb{N}$ è un sottoinsieme di $\mathbb{N} \cup \mathbb{N}'$ che non ha massimo pur essendo superiormente limitato, visto che $0'$ è un suo maggiorante.

Ora che abbiamo definito una nozione di ordinamento molto forte come quella di insieme naturalmente ordinato possiamo definire nuove nozioni a partire da essa e trovare risultati analoghi a quelli trovati in $\mathbb{N}$, ma più generali.

Definizione 2.6.3 Sia $(X, \leq)$ un insieme naturalmente ordinato. Per ogni $x \in X$ possiamo definire due elementi
$S(x) := \min\{y \in X \mid x < y\}$ che chiamiamo *successivo* di x
$P(x) := \max\{y \in X \mid y < x\}$ che chiamiamo *precedente* si x

Proposizione 2.6.1 *Sia X naturalmente ordinato, e $x \in X$. Allora valgono le seguenti:*

1. $x \neq \min X \Longrightarrow \exists\, P(x)$
2. $x \neq \max X \Longrightarrow \exists\, S(x)$
3. $\exists\, S(x) \Longrightarrow P(S(x)) = x$
4. $\exists\, P(x) \Longrightarrow S(P(x)) = x$

Dimostrazione: Le prime due proprietà vengono direttamente dalla definizione di $S(x)$ e $P(x)$ in un insieme naturalmente ordinato.

$\boxed{3}$ $S(x)$ non è minimo perché $x < S(x)$, quindi sappiamo che $\exists\, P(S(x)) = \max\{y \in X \mid y < S(x)\}$, e visto che $x < S(x)$ abbiamo che $x \leq P(S(x))$.

Supponiamo per assurdo che si abbia $x < P(S(x))$.

Allora $P(S(x)) \in \{y \in X \mid x < y\}$, quindi $P(S(x)) \geq S(x) = \min\{y \in X \mid x < y\}$, da cui ricaviamo $P(S(x)) < S(x) \leq P(S(x))$, il che è assurdo.

La proprietà (4) si dimostra in modo totalmente analogo.

□

Abbiamo quindi generalizzato le nozioni di *successivo* e *precedente* senza fare uso di funzioni o operazioni come facevamo prima in $\mathbb{N}$. Vediamo ora di generalizzare la proprietà fondamentale dei numeri naturali: l'*induzione*.

Proposizione 2.6.2 *Sia* $(X, \leq)$ *un insieme naturalmente ordinato con* $m = \min X$*. Se* $A \subseteq X$ *è tale che* $m \in A$ *e* $(a \in A \Rightarrow S(a) \in A)$ *allora* $A = X$*.*

Dimostrazione: Poniamo per assurdo che l'insieme $X \setminus A$ è non vuoto.

Se è non vuoto ammette un minimo k che sarà per forza diverso da m poiché quest'ultimo sta in A. Dal momento che $k \neq m = \min X$ sappiamo che $\exists\, P(k)$.

Essendo k il minimo di $X \setminus A$ abbiamo che $P(k) \notin X \setminus A \Longrightarrow P(k) \in A$.

Ma allora per ipotesi $k = S(P(k)) \in A$, il che è assurdo.

□

Teorema 2.6.1 *Sia* $(X, \leq)$ *un insieme naturalmente ordinato non superiormente limitato. Se chiamiamo* $0 = \min X$ *e la funzione "successore"*

$$\begin{array}{rcl} S : X & \longrightarrow & X \\ x & \longmapsto & \min\{y \in X \mid x < y\} \end{array}$$

abbiamo che l'insieme X *con* 0 *e* S *appena definite soddisfa gli Assiomi di Peano.*

Dimostrazione: dobbiamo verificare che valgono i quattro assiomi di Peano per X, ma la realtà è che abbiamo dimostrato quasi tutto tramite il procedimento che abbiamo seguito fino ad ora. Difatti la condizione di X di essere non limitato superiormente ci da che la funzione S è ben definita, inoltre l'elemento 0 esiste perché X è naturalmente ordinato.

Dato che $0 = \min X$ abbiamo dimostrato precedentemente che esso non ha precedenti, e quindi non appartiene all'immagine di S, il che verifica il secondo assioma.

Per mostrare che la funzione S è iniettiva osserviamo che se prendiamo due elementi $m, n \in X$ con $m < n$ abbiamo che $S(m) = \min\{y \in X \mid m < y\}$, quindi $S(m) \leq n < S(n) \Rightarrow S(m) < S(n)$.

Infine il quarto assioma ci è dato direttamente dal teorema precedente.

□

I risultati fin qui esposti ci permettono di fornire una caratterizzazione abbastanza importante di questi insiemi tramite l'enunciato che possiamo riassumere come segue:

Ogni insieme che soddisfa gli Assiomi di Peano è naturalmente ordinato con l'ordinamento canonico e non superiormente limitato. Viceversa se prendiamo un insieme naturalmente ordinato non superiormente limitato possiamo definire una funzione S *ed un suo elemento* 0 *in modo che esso soddisfi gli Assiomi di Peano.*

Esercizio 2.6.1 Dimostrare che l'ordinamento canonico di $\mathbb{N}$ è l'unico ordinamento che mantiene la somma.

Capitolo 3

Insiemi Finiti e Infiniti

3.1 Definizione di Finito e Infinito

Non è semplice dare una definizione di cosa può essere un insieme finito o un insieme infinito, difatti si sono cimentati in questo diversi matematici.

In questo paragrafo partiremo da quella che può essere una definizione abbastanza semplice di insieme finito o infinito per poi legarla ad altre definizioni più complesse date da matematici illustri quali **Dedekind** o **Cantor**.

Definizione 3.1.1 Diciamo che X è *finito in senso ordinario* (*O-finito*) se esiste $k \in \mathbb{N}$ tale che la funzione $f : X \longrightarrow I_k := \{n \in \mathbb{N} \mid 1 \leq n \leq k\}$ è bigettiva.

X si dice poi *infinito in senso ordinario* (*O-infinito*) se non è finito in senso ordinario.

Proposizione 3.1.1 *X è O-infinito se presi $a_1, \ldots, a_n \in X$ con $a_i \neq a_j \ \forall i \neq j$ vale che $X \backslash \{a_1, \ldots, a_n\}$ è ancora O-infinito.*

Dimostrazione: Supponiamo che non lo sia, ovvero che $X \backslash \{a_1, \ldots, a_n\}$ sia O-finito.

Allora esiste un k per cui la funzione $f : X \backslash \{a_1, \ldots, a_n\} \longrightarrow I_k$ è bigettiva.

definiamo allora una funzione $g : X \longrightarrow I_{k+n}$ come segue:

$$g(x) = \begin{cases} f(x) & \text{se } x \in X \backslash \{a_1, \ldots, a_n\} \\ i + k & \text{se } x = a_i \end{cases}$$

Questa funzione è iniettiva perché la f è iniettiva e vale $a_i \neq a_j \ \forall i \neq j$.

Inoltre è surgettiva perché preso un qualsiasi $h \in I_{k+n}$ abbiamo che se $h \leq k$ esiste un certo $x_h \in X \backslash \{a_1, \ldots, a_n\}$ tale che $g(x_h) = f(x_h) = h$ perché f è surgettiva; mentre se $h > k$ allora $g(a_{h-k}) = h$ per come abbiamo definito la funzione g.

Questo dimostra che anche X è O-finito, il che è assurdo per ipotesi.

□

Purtroppo però la definizione appena data ha un punto debole: si basa sull'esistenza dei numeri naturali. Ora vorremmo invece dare una definizione di insieme finito e infinito che sia indipendente dai numeri naturali.

Definizione 3.1.2 Diciamo che $X(\neq \emptyset)$ è *infinito secondo Dedekind* (*D-infinito*) se esiste una funzione $f : X \longrightarrow X$ iniettiva tale che $f(X) \subsetneq X$.[1]

X si dice poi *finito secondo Dedekind* (*D-finito*) se non è infinito secondo Dedekind.

Ma chi ci dice che un insieme di questo tipo esiste?

Sicuramente conosciamo i numeri naturali essi sono un esempio di insieme D-infinito: basta prendere come funzione f la funzione S di successore.

Ma questa definizione è forte proprio perché è indipendente dai numeri naturali, quindi in effetti nessuno ci assicura che un tale insieme esista, quindi dovremo porlo come assioma.

Assioma di Dedekind: *Esiste un insieme infinito secondo Dedekind.*

Osservazione Se X e Y sono insiemi in bigezione tra di loro allora vale che

X è O-finito (oppure D-finito) $\iff$ Y è O-finito (oppure D-finito).

Proposizione 3.1.2 *Gli insiemi del tipo I_n definiti sopra sono D-finiti $\forall n \geq 1$.*

Dimostrazione: Dobbiamo dimostrare che non esiste una funzione iniettiva $f : I_n \longrightarrow I_n$ tale che $f(I_n) \subsetneq I_n$. Lo facciamo dunque per induzione su n:

$\boxed{n = 1}$ Sicuramente non esistono funzioni iniettive da I_1 a $\emptyset = I_0$.

$\boxed{n \Rightarrow n+1}$ Sappiamo che I_n è D-finito.

Supponiamo per assurdo che I_{n+1} non lo sia, ovvero che esista una funzione iniettiva $\varphi : I_{n+1} \longrightarrow I_{n+1}$ tale che $\varphi(I_{n+1}) \subsetneq I_{n+1}$. Possono quindi verificarsi due situazioni:

- $\varphi(n+1) = n+1$: in questo caso abbiamo che $\varphi\big|_{I_n}$ è iniettiva e $\varphi(I_n) \subsetneq I_n$ poiché questo valeva nell'insieme I_{n+1} e la φ lascia fisso $n+1$, ma questo è assurdo per ipotesi induttiva.

- $\varphi(n+1) \neq n+1$: stavolta non abbiamo un punto fisso già per ipotesi, ma cerchiamo di ricondurci al caso precedente tramite l'utilizzo di una funzione ausiliaria.

  Definiamo quindi una funzione $\sigma : I_{n+1} \longrightarrow I_{n+1}$ in modo che

$$\sigma(k) = \begin{cases} k & \text{se } k \notin \{n+1, \varphi(n+1)\} \\ n+1 & \text{se } k = \varphi(n+1) \\ \varphi(n+1) & \text{se } k = n+1 \end{cases}$$

[1] Che equivale a dire che f deve essere iniettiva ma non surgettiva.

questa funzione non è altro che una permutazione degli elementi di I_{n+1} che scambia $n+1$ con $\varphi(n+1)$ e lascia fisso tutto il resto, ed è quindi evidentemente bigettiva.

Visto che per ipotesi $\varphi(I_{n+1}) \subsetneq I_{n+1}$ prendiamo[2] un qualsiasi $m \in I_{n+1} \setminus \varphi(I_{n+1})$ consideriamo la funzione $\sigma \circ \varphi : I_{n+1} \longrightarrow I_{n+1}$.

Essa è sicuramente iniettiva perché composizione di funzioni iniettive, ed inoltre vale $\sigma \circ \varphi(I_{n+1}) \subsetneq I_{n+1}$ poiché $\sigma(m) \notin \sigma \circ \varphi(I_{n+1})$.

Non solo, vale anche che $\sigma \circ \varphi(n+1) = n+1$, e quindi siamo nelle ipotesi del caso precedente, che abbiamo già dimostrato.

□

Corollario *X è O-finito $\Longrightarrow$ X è D-finito.*
o equivalentemente
X è D-infinito $\Longrightarrow$ X è O-infinito.

Abbiamo già osservato che se ammettiamo l'esistenza dell'insieme dei numeri naturali allora sicuramente esiste anche un insieme D-infinito. Ma vale il viceversa? Proviamo a vedere un po'.

Teorema 3.1.1 *Esiste $\mathcal{D}$ D-infinito $\Longleftrightarrow$ Esistono $X(\neq\emptyset)$, $\theta \in X$, $f : X \to X$ t.c.*

1. *f è iniettiva*
2. *$f(X) = X\backslash\{\theta\}$*
3. *$\forall A \subseteq X$ se vale che $\theta \in A$ e $f(A) \subseteq A$ allora $A = X$*
4. *f non ha punti fissi*

Dimostrazione: $\boxed{\Leftarrow}$ Sicuramente se X soddisfa le proprietà richieste è D-infinito.
$\boxed{\Rightarrow}$ Siano $\mathcal{D}$ un insieme D-infinito, e $\varphi : \mathcal{D} \longrightarrow \mathcal{D}$ iniettiva tale che $\varphi(\mathcal{D}) \subsetneq \mathcal{D}$.
Vogliamo dunque costruire X,θ,f che soddisfino le richieste.

Prendiamo un qualsiasi $\theta \in \mathcal{D}\backslash\varphi(\mathcal{D})$ e definiamo la famiglia di sottoinsiemi

$$\mathcal{A} := \{A \subseteq \mathcal{D} \mid \theta \in A,\ \varphi(A) \subseteq A\}$$

essa è non vuota poiché $\mathcal{D} \in \mathcal{A}$.

Poniamo allora

$$X = \bigcap_{A \in \mathcal{A}} A \qquad\qquad f = \varphi\big|_X$$

[2] **Attenzione!** Stiamo implicitamente usando l'**Assioma della Scelta**!

in cui f è befinita poiché preso $x \in X$ abbiamo che $f(x) \in f(A)\ \forall A \Rightarrow f(x) \in X$.

Cerchiamo adesso di dimostrare che X,f,θ così presi soddisfano le proprietà elencate sopra.

1. Certo f è iniettiva perché lo era φ.

2. Sapevamo già che se $x \in \mathcal{D}$ allora $\varphi(x) \neq \theta$ proprio per come abbiamo scelto θ, dunque a maggior ragione se $x \in X$ allora $f(x) \neq \theta$, il che ci dimostra la seguente inclusione: $f(X) \subseteq X\backslash\{\theta\}$.

   Per dimostrare l'altra inclusione prendiamo un certo $y \in X\backslash\{\theta\}$ e cerchiamo un $x \in X$ tale che $f(x) = y$.

   Sicuramente $\theta \in X\backslash\{y\}$, ma non è possibile che $f(X\backslash\{y\}) \subseteq X\backslash\{y\}$, altrimenti avremmo che $X\backslash\{y\} \in \mathcal{A}$ da cui $X \subseteq X\backslash\{y\}$.

   Allora se $f(X\backslash\{y\})$ non è tutto contenuto in $X\backslash\{y\}$ ma $f(X) \subseteq X\backslash\{\theta\}$ (che sappiamo già) allora deve esistere un certo $x \in X\backslash\{y\} \subseteq X$ tale che $f(x) = y$.

   Quindi $X\backslash\{\theta\} \subseteq f(X)$.

3. Se prendiamo $A \subseteq X$ tale che $\theta \in A$ e $f(A) \subseteq A$ allora $A \in \mathcal{A}$ proprio per come è definita la famiglia di sottoinsiemi (ricordando che f è semplicemente φ ristretta ad X).

   Ma X è l'intersezione degli A della famiglia $\mathcal{A}$, dunque

   $$X \subseteq A \subseteq X \qquad \Longrightarrow \qquad A = X$$

4. Definiamo l'insieme dei punti non fissi della funzione f

   $$B := \{x \in X \mid f(x) \neq x\}$$

   Sicuramente $\theta \in B$ proprio per definizione di θ;

   Inoltre preso $b \in B$ abbiamo che $b \neq f(b)$, ovvero $f(b) \neq f(f(b))$ per iniettività di f, ovvero $f(b) \in B$.

   Ma allora B verifica la proprietà (3), e quindi $B = X$.

□

Abbiamo dunque un'equivalenza tra l'esistenza di un insieme D-infinito ed un insieme che soddisfa quelle "strane" proprietà (anche se guardandole meglio non sono poi così strane, no?), ma possiamo fare di più!

Teorema 3.1.2 *Esiste un insieme D-infinito $\Longleftrightarrow$ Esiste un insieme naturalmente ordinato non superiormente limitato.*

Dimostrazione: Sappiamo dal teorema precedente che esiste un insieme D-infinito se e solo se esistono $X(\neq\emptyset)$, $\theta \in X$, $f : X \to X$ che soddisfano le 4 proprietà sopra elencate.

Ma se un insieme di questo tipo esiste esso soddisfa gli assiomi di Peano, e vale anche il viceversa, ovvero un insieme che soddisfa gli assiomi di Peano ha esattamente quelle caratteristiche con $\theta = 0$, $f = S$.

Ricordiamo adesso che abbiamo dimostrato nei paragrafi precedenti che esiste un insieme che soddisfa gli assiomi di Peano se e solo se esiste un insieme naturalmente ordinato non superiormente limitato (Teorema 2.6.1), che completa la nostra dimostrazione.

□

Nota: Esiste una dimostrazione di quest'ultimo teorema che non ricorre all'uso di $\mathbb{N}$ e delle teorie che abbiamo sviluppato nello scorso capitolo, ed è quest'altra dimostrazione che è stata fatta durante il corso. abbiamo però deciso di scrivere questa perché una volta sviluppata tutta la teoria del capitolo precedente mi sembra giusto poterne fare uso. Se si è interessati a leggere la dimostrazione alternativa si può far ricorso alle dispense messe in rete dal professor Coen o direttamente dal libro *L'Essenza e il Significato dei Numeri*, che è il libro in cui Dedekind scrive i risultati trovati da lui in quest'ambito, tradotto poi in italiano da Zarinski.

Corollario *Sia $\mathcal{D}$ un insieme D-infinito. Esiste allora un suo sottoinsieme $X(\neq\emptyset)$ per cui è possibile trovare un suo elemento θ e una funzione $f : X \to X$ in modo che vengano soddisfatte le 4 proprietà descritte nel teorema soprastante.*

Inoltre in tale sottoinsieme è possibile definire un ordinamento $\leq$ per cui $(X, \leq)$ risulti naturalmente ordinato e superiormente illimitato.

Esiste poi una bigezione tra X e $\mathbb{N}$ che mantiene l'ordine appena definito.

Corollario *X è D-infinito $\Longleftrightarrow \exists\, Y \subseteq X$ in corrispondenza biunivoca con $\mathbb{N}$*

Dimostrazione: $\boxed{\Rightarrow}$ Segue direttamente dalla dimostrazione del teorema 3.1.1.

$\boxed{\Leftarrow}$ Se Y è in corrispondenza biunivoca con $\mathbb{N}$ possiamo rinominare i suoi elementi in modo da scriverlo come $Y = \{y_n\}_{n\in\mathbb{N}}$.

Definiamo allora un'applicazione $f : X \to X$ come

$$f(x) = \begin{cases} x & \text{se } x \neq y_n \,\forall n \\ y_{n+1} & \text{se } x = y_n \end{cases}$$

in questo modo la f risulta essere ben definita ed iniettiva da X a $X\setminus\{y_0\}$, e quindi X è D-infinito.

□

Il corollario appena riportato ci da anche un'informazione celata che è di enorme importanza e va quindi esplicitata: il fatto che preso un insieme D-infinito sono sicuro che in esso sia contenuto un insieme in bigezione con $\mathbb{N}$ ci dice che $\mathbb{N}$ è "il più piccolo insieme infinito possibile"!

Vedremo più avanti che ci sono ordini di grandezza diversi anche tra gli insiemi infiniti, e sapere che $\mathbb{N}$ è comunque il più piccolo possibile potrebbe esserci molto utile.

C'è però rimasto un argomento in sospeso che è bene chiarire.

Abbiamo quindi definito due tipi di infinito: infinito in senso ordinario e infinito secondo Dedekind, e abbiamo provato che se un insieme è D-infinito allora sicuramente è O-infinito. Ma a noi piacerebbe dimostrare anche il viceversa, così da poter accordare le due definizioni e scrivere una volta per tutte *infinito*, senza "O" e senza "D".

Allora per fare questo dobbiamo però ammettere il famoso *Assioma della Scelta*, che era già entrato in gioco in uno dei teoremi precedenti, anche se in maniera un po' subdola e nascosta. Esplicitiamolo e usiamolo:

Assioma della Scelta: *Preso $X \neq \emptyset$ dico che $\exists\, f : \mathcal{P}(X)\backslash\{\emptyset\} \longrightarrow X$ tale che $\forall Y \in \mathcal{P}(X)\backslash\{\emptyset\}$ si ha $f(Y) \in Y$, in cui indichiamo con $\mathcal{P}(X)$ l'insieme delle parti di X.*

f è chiamata funzione di scelta.

Teorema 3.1.3 *X è O-infinito $\Longrightarrow$ X è D-infinito.*

Dimostrazione: Visto che abbiamo l'assioma della scelta sappiamo che esiste la funzione di scelta $f : \mathcal{P}(X)\backslash\{\emptyset\} \longrightarrow X$.

Definiamo allora una funzione $\sigma : \mathbb{N} \longrightarrow \mathcal{P}(X)\backslash\{\emptyset\}$ in maniera induttiva:

$$\begin{cases} \sigma(0) = X \\ \sigma(1) = X\backslash\{f(X)\} = \sigma(0)\backslash\{f(\sigma(0))\} \\ \sigma(2) = \sigma(1)\backslash\{f(\sigma(1))\} = X\backslash\{f(\sigma(1)), f(\sigma(0))\} \\ \vdots \\ \sigma(n) = \sigma(n-1)\backslash\{f(\sigma(n-1))\} = X\backslash\{f(\sigma(n-1)), \ldots, f(\sigma(0))\} \end{cases}$$

σ così definita è ben definita (ovvero $\sigma(n) \neq \emptyset\ \forall n$) perché si parte $\sigma(0) = X$ che è un insieme O-infinito e ad ogni passo togliamo un solo elemento, e è già stato dimostrato che se X è O-infinito allora rimane O-infinito anche se togliamo un numero finito di punti.

Quindi la funzione $f \circ \sigma : \mathbb{N} \to X$ risulta iniettiva poiché presi due interi $m < n$ vale

$$\begin{cases} f(\sigma(m)) \notin \sigma(n) \text{ per definizione di } \sigma(n) \\ f(\sigma(n)) \in \sigma(n) \text{ per definizione di funzione di scelta} \end{cases} \quad \Longrightarrow \quad f(\sigma(m)) \neq f(\sigma(n))$$

e quindi il nostro insieme X risulta D-infinito per il secondo corollario al teorema di prima, visto che $f \circ \sigma(\mathbb{N})$ è un sottoinsieme di X in bigezione con $\mathbb{N}$.

□

Per dimostrare quest'ultimo teorema abbiamo in effetti dovuto usare l'assioma della scelta perché abbiamo dovuto operare una serie di scelte potenzialmente infinite, il che non è detto che sia sempre possibile.

Adesso che abbiamo dimostrato quest'ultimo teorema abbiamo finalmente una corrispondenza tra la definizione di *infinito secondo Dedekind* e *infinito in senso ordinario*, dunque da adesso in poi smetteremo di fare questa distinzione e chiameremo un insieme che soddisfa una o l'altra proprietà semplicemente *infinito*.

3.2 Il Lemma di Zorn

L'Assioma della Scelta di cui abbiamo parlato poco prima è così importante che ne sono state trovate moltissime forme equivalenti, alcune abbastanza semplici (almeno a prima occhiata) e altre anche molto complesse. Una delle più famose è sicuramente il **Lemma di Zorn**, che enunceremo a breve, dopo aver dato un paio di definizioni supplementari di teoria degli insiemi:

Definizione 3.2.1 Sia $(X, \leq)$ un insieme ordinato. Un sottoinsieme C di X si dice *catena* se con l'ordinamento indotto risulta totalmente ordinato.
Si dice che X è *induttivo* quando ogni sua catena è superiormente limitata.
Un elemento $x \in X$ è detto *massimale* quando non vi sono $y \in X$ con $x < y$.

Lemma di Zorn: *Se $(X, \leq)$ è un insieme ordinato induttivo allora possiede elementi massimali.*

Questo "lemma" ha moltissime applicazioni, soprattutto in teorie algebriche, come ad esempio il seguente teorema:

Teorema 3.2.1 *Sia A un anello commutativo con identità, e sia I ideale proprio di A. Allora $\exists\, M$ ideale proprio di A tale che $I \subseteq M$ e M non è contenuto in nessun altro ideale proprio di A.*

Dimostrazione: Presa la famiglia $\mathcal{D}$ degli ideali propri di A contenenti I fissiamo in essa l'ordinamento per inclusione.

Di sicuro $\mathcal{D} \neq \emptyset$ poiché $I \in \mathcal{D}$.

Sia $\mathcal{C}$ una catena di $\mathcal{D}$, e sia

$$U = \bigcup \{F \in \mathcal{C}\}$$

Sicuramente U è un ideale proprio, perché se così non fosse avremmo che l'unità dovrebbe stare in uno degli ideali che lo compongono, che non sarebbe più proprio.

Ma d'altra parte $I \subseteq U$, e se un ideale contiene I di sicuro non può contenere U, quindi U è l'estremo superiore di questa catena: $U = \sup \mathcal{C}$. Quindi la catena $\mathcal{C}$ è superiormente limitata e $\mathcal{D}$ è induttivo.

Da ciò possiamo applicare Zorn e concludere che esiste un elemento massimale M che quindi soddisfa la relazione richiesta.

□

Capitolo 4

I Numeri Interi: $\mathbb{Z}$

4.1 Definizione di $\mathbb{Z}$

In questo capitolo vorremmo definire un nuovo insieme numerico che sia una sorta di estensione dell'insieme dei numeri naturali definito nei capitoli precedenti.

Partiamo dunque dall'insieme $\mathbb{N} \times \mathbb{N}$ su cui definiamo la seguente relazione di equivalenza:

$$(a, b) \sim (a', b') \quad \Leftrightarrow \quad a + b' = a' + b$$

e indichiamo con $[a, b]$ la classe di equivalenza di (a, b).

Definiamo quindi l'insieme dei **Numeri Interi**

$$\mathbb{Z} := (\mathbb{N} \times \mathbb{N})/_{\sim}$$

4.2 Operazioni e Ordinamento su $\mathbb{Z}$

Vorremmo anche definire su questo nuovo insieme delle operazioni e un ordinamento che siano "compatibili" con ciò che avevamo definito sui numeri naturali.

Per fare ciò il modo più semplice è definire questi aspetti in maniera costruttiva partendo da ciò che già abbiamo per $\mathbb{N}$, visto che gli elementi del nostro nuovo insieme non sono altro che coppie di numeri naturali.

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

Prodotto $[a, b] \cdot [c, d] := [ac + bd, ad + bc]$

Ordinamento $[a, b] \leq [c, d] \iff a + d \leq b + c$

Le operazioni e l'ordinamento così definiti risultano ben definiti semplicemente per le proprietà viste e dimostrate nel capitolo sui numeri naturali.

Esercizio 4.2.1 Verificare che con queste operazioni $\mathbb{Z}$ risulta un anello con identità moltiplicativa $[1,0]$, identità additiva $[0,0]$, e opposto $[a,b]^{-1} = [b,a]$. Inoltre risulta $[c,d] \geq (0,0)$ (ovvero "positivo") se e solo se $c \geq d$.

Esiste tra l'insieme dei numeri naturali $\mathbb{N}$ e questo nuovo insieme $\mathbb{Z}$ la particolare applicazione

$$\begin{array}{rcl} i : \mathbb{N} & \longrightarrow & \mathbb{Z} \\ n & \longmapsto & [n,0] \end{array}$$

che è iniettiva e rispetta le operazioni e l'ordinamento definiti nei due insiemi, ed è quindi un isomorfismo tra $\mathbb{N}$ e l'immagine $i(\mathbb{N}) = \{(n,0) \in \mathbb{Z}\}$.

Facciamo adesso un'osservazione: preso un numero intero $[a,b]$ tale che si abbia $a \geq b$, allora esiste il numero naturale indicato con "$a - b$" che abbiamo definito nei capitoli precedenti. Ma da ciò possiamo ricavare che $(a,b) = (a-b,0)$, ovvero $[a,b] = [a-b,0]$.

Viceversa, se accade che $a \leq b$ ne risulterà per lo stesso ragionamento che $[a,b] = [0,b-a]$.

Così ogni elemento di $\mathbb{Z}$ si può scrivere come $[n,0]$ o $[0,n]$ (al di fuori di $[0,0]$, che possiamo decidere di scrivere 0).

Indicheremo quindi da ora in poi in maniera abbreviata i numeri interi come segue: $n := [n,0]$ o $-n := [0,n]$, ovvero come singoli invece che come coppie.

Una volta identificati gli interi in tale modo valgono ancora alcune delle proprietà che già avevamo dimostrato per i numeri naturali, ovvero:

Proposizione 4.2.1 *Siano $a, b \in \mathbb{Z}$. Valgono le seguenti*

1. $a < b \iff \exists\, c \in \mathbb{Z},\ c > 0$, *tale che* $b = a + c$
2. $a < b \iff a + c < b + c$
3. $a < b \iff ac < bc \quad \forall c > 0$

Capitolo 5

Gruppi, Anelli e Campi Ordinati

Nota: In questo capitolo considereremo acquisite e consolidate tutte le conoscenze dei corsi di Algebra di base, in cui si definiscono *Gruppi*, *Anelli* e *Campi* e se ne studiano le proprietà. Non verranno pertanto date definizioni in questo senso né dimostrate le proprietà basilari che si dimostrano in ogni corso che parli di strutture astratte di questo genere.

Partendo dalle conoscenze acquisite nei capitoli precedenti in questo capitolo ci occuperemo di osservare alcune proprietà a livello un po' più astratto di quanto fatto in precedenza, iniziando subito a collegare i due argomenti con la seguente proposizione:

Proposizione 5.0.2 *Sia A anello commutativo, e sia $h : \mathbb{N} \longrightarrow A$ una applicazione iniettiva che mantenga in A le operazioni di somma e prodotto di $\mathbb{N}$. Allora valgono i seguenti fatti:*

1. *h si estende ad un omomorfismo $g : \mathbb{Z} \longrightarrow A$;*
2. *Ogni sottoanello B di A che contiene $h(\mathbb{N})$ deve contenere anche $g(\mathbb{Z})$.;*
3. *La relazione d'ordine canonica su $\mathbb{Z}$ è l'unica relazione d'ordine che estende la relazione d'ordine di $\mathbb{N}$ e preserva la somma in $\mathbb{Z}$.*

Dimostrazione: $\boxed{1}$ Essendo A un anello commutativo ogni elemento a avrà il suo opposto (inverso additivo) che indichiamo con $\sim a$.

Avendo l'applicazione h definiamo g sugli elementi del tipo n e $-n$, che formano l'insieme $\mathbb{Z}$, nel modo seguente:

$$\begin{cases} g(n) = h(n) \\ g(-n) = \sim h(n) \end{cases}$$

L'applicazione $g : \mathbb{Z} \longrightarrow A$ così definita si può dimostrare che si comporta bene con le operazioni ed è quindi un morfismo; In particolare risulterà quindi un isomorfismo con la

sua immagine.

2 Se B è un sottoanello di A che contiene $h(\mathbb{N})$ per le sue proprietà deve contenere $h(n)$ e $\sim h(n)$ per ogni $n \in \mathbb{N}$. Ma allora di sicuro contiene tutti gli elementi di $g(\mathbb{Z})$ proprio per come abbiamo definito l'applicazione g.

3 Consideriamo ora un ordinamento $\preceq$ che mantenga la somma in $\mathbb{Z}$ ed estenda l'ordinamento canonico $\leq$ in $\mathbb{N}$. Prendiamo dunque due interi a, b con $a \prec b$ e cerchiamo di dimostrare che esiste un intero $c > 0$ per cui $b = a + c$, avendo così che $\prec = <$.

Per come abbiamo definito gli interi dovremo procedere per casi: se a e b sono del tipo $a = -n$, $b = -m$ abbiamo che $-n \prec -m$. Poiché l'ordine mantiene la somma $-n \prec -m \implies -n + (n + m) \prec -m + (n + m) \implies m \prec n$, e quindi $m < n$ perché $\prec$ estende l'ordinamento in $\mathbb{N}$. Ma allora in $\mathbb{N}$ sappiamo che esiste c tale che $n = m + c \implies n + (-m - n) = m + c + (-m - n) \implies b = a + c$, che è proprio ciò che volevamo.

Gli altri casi si fanno in maniera del tutto analoga.

□

5.1 Definizioni e Prime Proprietà

Definiamo ora cosa vogliamo dire con strutture astratte "ordinate".

Nota: durante tutto questo capitolo, dove non specificato diversamente, gli anelli saranno presi commutativi, non banali e con identità moltiplicativa indicata con "1" (o "1_A" se A è l'anello di appartenenza).

Definizione 5.1.1 Sia G un gruppo additivo commutativo con una relazione d'ordine $\leq$. Si dice che $(G, \leq)$ è un gruppo *ordinato* se la relazione è totale e se $\forall a, b \in G$ vale che

$$a < b \quad \implies \quad a + c < b + c \quad \forall c \in G$$

Si chiamano *positivi* gli $a \in G$ con $a > 0$ e *negativi* quelli tale che $a < 0$.

Definizione 5.1.2 Se A è un anello e $\leq$ è una relazione d'ordine su A, si dice che $(A, \leq)$ è un anello *ordinato* quando con tale relazione è un gruppo ordinato e $\forall a, b \in A$ vale che

$$a < b \quad \implies \quad ac < bc \quad \forall c \in A,\, c > 0$$

Definizione 5.1.3 Se C è un campo con $\leq$ relazione d'ord, allora $(C, \leq)$ è un campo *ordinato* se è anello ordinato.

Proposizione 5.1.1 *Sia A un anello ordinato e $a, b \in A$. Allora vale la* ***Regola dei Segni****, ovvero:*

- $a > 0, b > 0 \Longrightarrow ab > 0$
- $a > 0, b < 0 \Longrightarrow ab < 0$
- $a < 0, b > 0 \Longrightarrow ab < 0$
- $a < 0, b < 0 \Longrightarrow ab > 0$

In particolare $a^2 > 0 \ \forall a \in A$ e $1_A > 0$.

Inoltre A non possiede divisori di zero.

Dimostrazione: Iniziamo dalla regola dei segni, che dimostriamo usando la definizione della regola dei segni e le proprietà degli elementi di un anello che già conosciamo:
$a > 0, b > 0 \Longrightarrow ab > 0 \cdot b = 0$
$a > 0, b < 0 \Longrightarrow ab < a \cdot 0 = 0$
$a < 0, b > 0 \Longrightarrow ab < 0 \cdot b = 0$
$a < 0, b < 0 \Longrightarrow -a > 0, -b > 0 \Longrightarrow \quad ab = [-(-a)]b = (-a)(-b) > 0$

E quindi la regola dei segni è sistemata. Ma da questa derivano direttamente tutte le altre considerazioni, poiché:

$a^2 = a \cdot a > 0$ perché moltiplichiamo due elementi di segno concorde.

Per l'identità moltiplicativa vale lo stesso, poiché risulta un elemento quadrato: $1_A = 1_A \cdot 1_A = (1_A)^2 > 0$.

Infine se due elementi sono entrambi non nulli non faranno mai zero per la regola dei segni.

□

Grazie alla regola dei segni possiamo iniziare a descrivere un particolare sottoinsieme di un anello ordinato: l'insieme dei suoi elementi *positivi*, ovvero

$$\mathcal{P} = \{a \in A \mid a > 0\}$$

in cui A è un anello ordinato qualsiasi.

Questo sottoinsieme $\mathcal{P}$ di A ha alcune proprietà molto interessanti:

- $\mathcal{P}$ è chiuso per entrambe le operazioni definite su A.

  Infatti se $a, b \in \mathcal{P}$ allora abbiamo

  $$a > 0,\, b > 0 \Longrightarrow a + b > 0 + b > 0 \Longrightarrow a + b \in \mathcal{P}$$

  $$a > 0,\, b > 0 \Longrightarrow ab > 0 \text{ per la regola dei segni } \Longrightarrow ab \in \mathcal{P}$$

- $c \in \mathcal{P} \Longleftrightarrow -c \notin \mathcal{P}$.

  Vediamo le singole implicazioni:

  ($\Longrightarrow$) Sia $c \in \mathcal{P}$. Se fosse $-c \in \mathcal{P}$, cioè $-c > 0$ avremmo $c + (-c) > c \Rightarrow 0 > c > 0$, il che è assurdo.
  ($\Longleftarrow$) Sia $-c \notin \mathcal{P}$. Se fosse $c \notin \mathcal{P}$ avremmo che $c < 0$ perché l'ordinamento è totale. Ma $-c \notin \mathcal{P} \Longrightarrow -c < 0 \Longrightarrow c + (-c) < c \Longrightarrow 0 < c$, che porta nuovamente ad un assurdo.

Le proprietà che abbiamo osservato sono molto importanti poiché se in un anello A è presente un sottoinsieme con queste proprietà che non contenga l'elemento neutro per la somma, allora questo anello risulta *ordinabile* e tale sottoinsieme è in realtà necessariamente unico!

Proposizione 5.1.2 *Sia A un anello e sia $P \subseteq A$, $P \neq \emptyset$ con le seguenti proprietà:*

1. $\forall a, b \in P$ *vale* $a + b \in P$
2. $\forall a, b \in P$ *vale* $ab \in P$
3. $\forall c \in A, c \neq 0$ *vale* $c \in P \Leftrightarrow -c \notin P$
4. $0 \notin P$

Allora esiste un unico ordinamento $\leq$ su A per cui $P = \{a \in A \mid a > 0\}$, definito come

$$a \leq b \Longleftrightarrow a = b \text{ oppure } b - a \in P$$

Inoltre se $P \subseteq R \subseteq A$ e per R valgono tutte e quattro le proprietà di sopra allora $R = P$.

Dimostrazione: Se esiste un ordinamento per cui $(A, \leq)$ è anello ordinato e $P = \{a \in A \mid a > 0\}$, allora deve essere che

$$a \leq b \Longleftrightarrow a = b \text{ oppure } b - a \in P$$

quindi l'unicità è certa.

Verifichiamo allora che $(A, \leq)$, in cui $\leq$ è definita sopra, è davvero un anello ordinato.

In realtà le quattro proprietà che descrivono l'insieme P sono prese appositamente perché si verifichino immediatamente le proprietà riflessiva, antisimmetrica e transitiva dell'ordinamento definito sopra, e che esso sia compatibile con le operazioni definite in A, e lasciamo quindi le verifiche al lettore.

Ora, se esistesse un R tale che $P \subseteq R \subseteq A$ e che verifica i 4 punti, allora per R potremmo ripetere il ragionamento di prima e definire un ordinamento di A per cui R si scriva come "gli elementi positivi". Ma abbiamo detto che tale ordinamento è unico, quindi in P deve coincidere.

Se $\exists\, c \in R \backslash P$ avremmo che $-c \in P$ per il terzo punto, ma allora $-c \in R$, il che ci dice che $c \notin R$, che è assurdo.

Quindi $R = P$.

□

Dunque in effetti l'insieme dei numeri "positivi" gioca un ruolo fondamentale quando vogliamo porre un ordinamento su un anello.

5.2 Quozienti e Morfismi

Abbiamo dimostrato nei teoremi precedenti che un anello ordinato non ha divisori dello zero, quindi quello che potremmo provare a pensare è di farne il campo dei quozienti. Ma a questo punto il campo dei quozienti è ordinabile?

Grazie alla proposizione appena mostrata abbiamo un modo per ordinare un anello: trovare un sottoinsieme che verifichi le quattro proprietà richieste e definire l'ordinamento sull'anello a partire da questo particolare sottoinsieme. Proviamo dunque ad agire in questa strada.

Preso $(A, \leq)$ anello ordinato consideriamo A' il *campo delle frazioni di* A, ovvero

$$A' = \left\{ \frac{a}{b} \mid a, b \in A,\ b \neq 0 \right\}$$

Definiamo allora il seguente sottoinsieme

$$P := \left\{ \frac{a}{b} \in A' \mid ab > 0 \right\}$$

e verifichiamo che per esso valgono le quattro proprietà enunciate nella proposizione:

1. Se $\frac{a}{b}, \frac{c}{d} \in P$ allora

$$\frac{a}{b} + \frac{c}{d} \in P \iff \frac{ad+bc}{bd} \in P \iff (ad+bc)bd > 0 \iff (ab)d^2 + b^2(cd) > 0$$

e l'ultima espressione è positiva perché prodotto e somma di elementi positivi.

2. Se $\frac{a}{b}, \frac{c}{d} \in P$ allora

$$\frac{a}{b} \cdot \frac{c}{d} \in P \iff \frac{ac}{bd} \in P \iff acbd > 0 \iff (ab)(cd) > 0$$

e di nuovo l'ultima espressione è positiva perché prodotto di elementi positivi.

3. Se $\frac{a}{b} \in P$ allora

$$\frac{a}{b} \in P \iff ab > 0 \iff -ab < 0 \iff -\frac{a}{b} \notin P$$

4. $\frac{0}{1} \notin P$ poiché $0 \cdot 1 = 0 \not\succ 0$.

Quindi abbiamo che in effetti P è proprio il sottoinsieme di A' che ci serviva. Da esso definiamo quindi il seguente ordinamento sul campo A':

$$\frac{a}{b} \leq \frac{c}{d} \iff (ad - bc)bd \leq 0$$

che sappiamo già essere unico e ben definito.

Proposizione 5.2.1 *L'ordinamento appena definito è l'unico ordinamento che rende A' un campo ordinato e che mantiene l'ordinamento di partenza su A.*

Dimostrazione: Sia dato un altro ordinamento $\preceq$ che estenda l'ordinamento $\leq$ definito su A e renda $(A', \preceq)$ campo ordinato.

Poiché estende $\leq$ su A i due ordinamenti devono coincidere. Ne segue che $\frac{a}{1} \succ 0 \iff a > 0$.

Ora passiamo al caso generale:

$$\frac{a}{b} > 0 \iff ab > 0 \iff ab \succ 0 \iff \frac{ab}{b^2} \succ 0 \iff \frac{a}{b} \succ 0$$

Dunque i due ordinamenti coincidono sui positivi, quindi coincidono su tutto l'insieme.

□

Ora che abbiamo definito vari tipi di strutture ordinate e i loro ordinamenti cerchiamo di definire come queste strutture interagiscono tra loro, ovvero studiamone i morfismi.

Definizione 5.2.1 Siano $(G, \leq)$, $(H, \preceq)$ due gruppi ordinati. Si dice che un omomorfismo $f : G \longrightarrow H$ di gruppi è *ordinato* (o *mantiene l'ordine*) quando

$$\forall a, b \in G \text{ vale} \quad a < b \Longrightarrow f(a) \prec f(b)$$

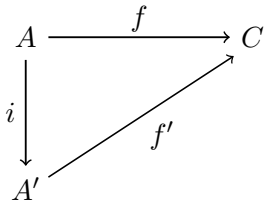
Osservazione $f : G \longrightarrow H$ omomorfismo di gruppi è ordinato se e solo se

$$\forall a \in G \text{ vale} \quad a > 0 \Longrightarrow f(a) \succ 0$$

Proposizione 5.2.2 *Sia $(A, \leq)$ anello ordinato con campo dei quozienti $(A', \leq)$. Sia $(C, \preceq)$ un campo ordinato.*

Ogni omomorfismo ordinato $f : A \longrightarrow C$ si estende ad un omomorfismo ordinato $f' : A' \longrightarrow C$ definito come

$$f'\left(\frac{a}{b}\right) = \frac{f(a)}{f(b)}$$



Dimostrazione: Sappiamo dall'algebra che sicuramente è un morfismo, inoltre se $b \neq 0$ allora $f(b) \neq 0$ perché f è iniettiva.

Ci manca di vedere che f' è ordinato, cioè $\forall a, b \in A, b \neq 0$ con $\frac{a}{b} > 0$ vale che $\frac{f(a)}{f(b)} \succ 0$.

Ma $\frac{f(a)}{f(b)} \succ 0 \iff \frac{f(a)}{f(b)} \cdot f(b)^2 \succ 0$, e sapendo che $\frac{a}{b} > 0 \Rightarrow ab > 0$ e che f mantiene l'ordine abbiamo

$$\frac{f(a)}{f(b)} \cdot f(b)^2 = f(a)f(b) = f(ab) \succ 0 \implies \frac{f(a)}{f(b)} \succ 0$$

Inoltre l'unicità di f' è assicurata dall'unicità della f di partenza.

□

Esempio 5.2.1 Dimostrare che l'applicazione $f : \mathbb{Z} \longrightarrow \mathbb{Z}$, $f(n) = -n$ è un morfismo ma non mantiene l'ordine.

Esercizio 5.2.1 Dimostrare che $(\mathbb{Z}[x], \leq)$ è anello ordinato quando

$$a_n x^n + \ldots + a_1 x + a_0 > 0 \iff a_n > 0$$

Proposizione 5.2.3 *L'ordinamento canonico su $\mathbb{Q}$ è l'unico ordinamento che induce su $\mathbb{N}$ l'ordinamento canonico.*

Dimostrazione: Sicuramente l'ordinamento di $\mathbb{Q}$ induce quello su $\mathbb{N}$ perché abbiamo costruito i miei insiemi $\mathbb{Z}$ e $\mathbb{Q}$ proprio a partire dai numeri naturali[1].

Prendiamo un altro ordinamento $\preceq$ su $\mathbb{Q}$ che induce l'ordinamento canonico su $\mathbb{N}$.

[1] In realtà durante il corso non è mai stato definito $\mathbb{Q}$, ma si può in maniera analoga a quanto fatto per $\mathbb{Z}$: definendo nell'insieme di coppie $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ la relazione di equivalenza $(a, b) = (c, d) \Leftrightarrow a\dot{d} = b\dot{c}$, e definendo $\mathbb{Q}$ come l'insieme delle classi.

Se $\preceq \neq \leq$ allora $(\mathbb{Z}, \preceq)$ ha un ordinamento diverso da quello canonico per ciò che si è visto precedentemente. Ma allora anche su $\mathbb{N}$ non è quello canonico, che è assurdo per ipotesi.

□

Definizione 5.2.2 Un insieme X si dice *denso* in un insieme Y se presi qualsiasi $y_1, y_2 \in Y$ con $y_1 < y_2$ esiste sempre un $x \in X$ tale che $y_1 < x < y_2$.

Esempio 5.2.2 $\mathbb{Q}$ con l'ordinamento canonico è denso in sé stesso, infatti presi $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$, con $\frac{a}{b} < \frac{c}{d}$ posso sempre considerare

$$\frac{a}{b} < \frac{1}{2}\left(\frac{a}{b} + \frac{c}{d}\right) < \frac{c}{d}$$

5.3 Sottoanelli e Sottocampi Fondamentali

Definizione 5.3.1 Sia G gruppo commutativo. Allora $\forall a \in G$, $\forall n \in \mathbb{Z}$ si pone

$$na := \begin{cases} (-n)(-a) & \text{se } n < 0 \\ 0 & \text{se } n = 0 \\ (n-1)a + a & \text{se } n > 0 \end{cases}$$

Proposizione 5.3.1 *$\forall a, b \in G$, $\forall m, n \in \mathbb{Z}$ valgono*

1. $(m+n)a = ma + na$
2. $n(a+b) = na + nb$
3. $n(ma) = (nm)a$

Osservazione Preso un gruppo G, $\forall a \in G$ l'applicazione

$$\begin{array}{rcl} f : \mathbb{Z} & \longrightarrow & G \\ n & \longmapsto & na \end{array}$$

è un omomorfismo di gruppi.

Proposizione 5.3.2 *$(A, \leq)$ anello ordinato. L'omomorfismo*

$$\begin{array}{rcl} f : \mathbb{Z} & \longrightarrow & A \\ n & \longmapsto & n \cdot 1_A \end{array}$$

è iniettivo, ovvero A ha caratteristica 0.

Dimostrazione: Dimostriamo per induzione su n che f è crescente, e come al solito basterà verificarlo per gli elementi positivi.

$\boxed{n = 1}$ $f(1) = 1_A > 0 = f(0)$

$\boxed{n \Rightarrow n+1}$ $f(n+1) = (n+1)1_A = n1_A + 1_A > n1_A = f(n)$

□

Definizione 5.3.2 Se A è un anello ordinato si chiama *sottoanello fondamentale* di A l'anello

$$\mathbb{Z}_A := \{n \cdot 1_A \mid n \in \mathbb{Z}\}$$

Se C è un campo ordinato si chiama *sottocampo fondamentale* di C il campo

$$\mathbb{Q}_C := \left\{ \frac{m \cdot 1_C}{n \cdot 1_C} \in C \;\middle|\; n, m \in \mathbb{Z},\ n \neq 0 \right\}$$

Facciamo alcune osservazioni sulle strutture appena definite: se prendiamo un qualsiasi campo ordinato C, l'applicazione

$$\begin{array}{rcl} \varphi : \mathbb{Q} & \longrightarrow & \mathbb{Q}_C \\ \frac{n}{m} & \longmapsto & \frac{n1_C}{m1_C} \end{array}$$

è un isomorfismo di campi che mantiene l'ordine.

Inoltre se prendiamo due campi ordinati C e C' l'applicazione

$$\begin{array}{rcl} \varphi : \mathbb{Q}_C & \longrightarrow & \mathbb{Q}'_C \\ \frac{n1_C}{m1_C} & \longmapsto & \frac{n1'_C}{m1'_C} \end{array}$$

è anch'essa un isomorfismo di campi che mantiene l'ordine.

Riprendiamo l'esempio dei polinomi $\mathbb{Z}[x]$: il sottoanello fondamentale $\mathbb{Z}_{\mathbb{Z}[x]}$ è formato dai polinomi di grado zero, ovvero semplicemente i numeri interi, poiché $f(n) = n1_{\mathbb{Z}[x]} = n$.

Il campo C dei quozienti di $Z[x]$ sono le frazioni razionali a coefficienti interi, ovvero $\frac{P(x)}{Q(x)}$ con $P(x), Q(x) \in \mathbb{Z}[x]$, $Q[x] \neq 0$ avrà anch'esso un sottocampo fondamentale, che risulta essere semplicemente $\mathbb{Q}$.

Con l'ordinamento che abbiamo definito sui polinomi interi si ha inoltre

$$n < x < x^2 < x^3 < \dots$$
$$\frac{1}{n} > \frac{1}{x} > \frac{1}{x^2} > \frac{1}{x^3} > \dots$$

5.4 Strutture Archimedee

Definizione 5.4.1 Un gruppo/anello/campo ordinato $(G, \leq)$ si dice *archimedeo* se $\forall a, b \in G$ con $a > 0$ $\exists\, n \in \mathbb{N}$ tale che $na > b$.

Proposizione 5.4.1 *Preso un campo ordinato C le seguenti sono equivalenti:*

1. *C è archimedeo*
2. *$\forall b \in C$ $\exists\, n \in \mathbb{N}$ tale che $n \cdot 1_C > b$*
3. *$\forall a \in C$, $a \geq 0$, se $\forall n \in \mathbb{N}\backslash\{0\}$ vale $\frac{1_C}{n} > a$ allora $a = 0$*
4. *il sottoanello fondamentale $\mathbb{Z}_C$ non è superiormente limitato in C*
5. *il sottocampo fondamentale $\mathbb{Q}_C$ è denso in C*

Dimostrazione: $\boxed{1 \Rightarrow 2}$ Poiché C è archimedeo basta sostituire nella definizione a con 1_C.

$\boxed{2 \Rightarrow 3}$ Sia $a \geq 0$ e sia $\frac{1_C}{n} > a$ $\forall n > 0$.
Se $a > 0$ allora abbiamo anche che $\frac{1}{a} > n = n1_C$ $\forall n$, ma questo è assurdo per ipotesi.

$\boxed{3 \Rightarrow 1}$ Siano $a, b \in C$, $a > 0$.
Se $b \leq 0$ vale $a > b$ quindi apposto.
Se $b > 0$ supponiamo per assurdo che $\forall n > 0$ si abbia $na \leq b$, da cui $\frac{a}{b} \leq \frac{1}{n}\, \forall n$. Ma allora per (3) $\frac{a}{b} = 0$, il che è assurdo.

$\boxed{2 \Leftrightarrow 4}$ Basta ricordare la definizione di $\mathbb{Z}_C$.

$\boxed{2 \Rightarrow 5}$ Siano $a, b \in C$, $a < b$.

- Se $a \geq 0$ vale $\frac{1}{b-a} \in C$, quindi per (2) $\exists\, m$ tale che $\frac{1}{b-a} < m1_C$, ovvero $1_C < m(b-a) = mb - ma$, da cui $ma + 1_C < mb$.

  Se consideriamo $\min\{q \in \mathbb{N}^+ \mid ma < q1_C\} = n$, che esiste perché l'insieme è non vuoto, abbiamo che $ma < n1_C$, $ma \geq (n-1)1_C$.

  Allora $n1_C = (n-1)1_C + 1_C \leq ma + 1_C < mb$, da cui $ma < n1_C < mb$, ovvero $a < \frac{n}{m} < b$, che era proprio quello che volevamo dimostrare.

- Se $a < 0 < b$ abbiamo già vinto.

- Se $a < b \leq 0$ abbiamo $0 \leq -b < -a$ e possiamo ripetere il ragionamento di sopra in maniera analoga.

$\boxed{5 \Rightarrow 2}$ Sia $b \in C$, $b > 0$.

Per (5) $\exists\, n, m \in \mathbb{Z}$ tali che $0 < \frac{n}{m} < \frac{1}{b}$ con $n, m > 0$, da cui $0 < 1 < \frac{m}{n}\frac{1}{b}$, perciò $b < \frac{m}{n} < m = m1_C$, che è ciò che volevamo mostrare.

□

Esempio 5.4.1 $\mathbb{Q}$ è archimedeo perché il suo campo dei quozienti, ovvero se stesso, è denso.

Esempio 5.4.2 Sia $(R, \leq)$ un campo ordinato, e sia $(Q, \leq)$ un sottocampo ordinato archimedeo di R ed assumiamo che Q sia denso in R. Allora R è archimedeo.

Esempio 5.4.3 $(\mathbb{Z}\oplus\mathbb{Z}, \leq)$ in cui l'ordine definito è quello *lessico-grafico*[2] non è archimedeo, perché se prendiamo $(0, b)$ abbiamo che $n(0, b) = (0, nb)\ \forall n$, ma allora $n(0, b) < (1, 0)\ \forall n$.

Esempio 5.4.4 $\mathbb{Z}[x]$ non è archimedeo, perché $n \cdot 1 < x\ \forall n$.

Allo stesso modo non è archimedeo nemmeno il campo delle funzioni razionali a coefficienti in $\mathbb{Z}$.

Proposizione 5.4.2 *Sia $(C, \leq)$ un campo ordinato che sia completo per l'ordinamento scelto. Allora $(C, \leq)$ è un campo archimedeo.*

Dimostrazione: Consideriamo $\mathbb{Z}_C$ e supponiamo per assurdo che sia superiormente limitato con $s = \sup_C \mathbb{Z}_C$.

Allora $\exists\, n \in \mathbb{Z}_C$ tale che $s - 1_C < n1_C < s \Longrightarrow s < (n+1)1_C$, che è assurdo.

□

[2]Ricordiamo che l'ordine lessico-grafico è definito come: $(a, b) < (c, d) \Leftrightarrow a < c$ oppure $a = c, b < d$.

Capitolo 6

I Numeri Reali: $\mathbb{R}$

6.1 sezioni di Dedekind

Definizione 6.1.1 Un sottoinsieme S non vuoto di un insieme ordinato $(X, \leq)$ si dice *sezione* se $\forall y \in S$, $\forall x \in X$ vale $x < y \Longrightarrow x \in S$

Definizione 6.1.2 Una sezione di $(\mathbb{Q}, \leq)$ si dice *sezione razionale* se è una sezione e valgono inoltre le seguenti proprietà:

- S è superiormente limitata
- S non ha massimo

A cosa corrispondono queste sezioni se pensate da un punto di vista geometrico? A semirette infinite a sinistra e aperte a destra! Allora a partire da un qualsiasi razionale q possiamo generare una sezione del tipo $S_q := \{x \in \mathbb{Q} \mid x < q\}$.

Ma sono tutte di questo tipo? No, ad esempio la sezione S=$\{x \in \mathbb{Q} \mid x < 0\} \cup \{0\} \cup \{x \in \mathbb{Q} \mid x > 0, x^2 < 2\}$ non si può scrivere in forma S_q con $q \in \mathbb{Q}$.

Essendo queste delle semirette aperte possiamo anche definire un ordinamento sull'insieme delle sezioni razionali sfruttando l'inclusione (insiemistica o geometrica):

$$S \leq S' \quad \Longleftrightarrow \quad S \subseteq S'$$

Teorema 6.1.1 *L'ordinamento appena descritto è totale sull'insieme delle sezioni razionali.*

Dimostrazione: Prese due sezioni razionali $X, Y \in \mathbb{R}$ vogliamo mostrare che vale $X \leq Y$ oppure $Y \leq X$.

Se $X \nleq Y$ allora abbiamo che $X \nsubseteq Y$, quindi possiamo prendere $x \in X$ tale che $x \notin Y$.

Se consideriamo un qualsiasi $y \in Y$ abbiamo che se fosse $x \leq y$ avremmo che $x \in Y$ per definizione di sezione. Ma abbiamo supposto $x \notin Y$, quindi deve essere $x > y$, che implica $y \in X$.

Quindi abbiamo $Y \subseteq X$, che è ciò che volevamo mostrare.

□

6.1.1 Operazioni con le sezioni

Sull'insieme delle sezioni razionali $\mathbb{R}$ è possibile definire anche delle operazioni:

⊕ **Somma**

$$X + Y := \{x + y \mid x \in X, y \in Y\}$$

Cerchiamo di verificare le proprietà principali di questa operazione:

- *La somma è ben definita, associativa e commutativa*

  La prima cosa da vedere è che la somma sia ben definita, ovvero che la somma di due sezioni sia ancora una sezione. Per fare questo verifichiamo che vale $z < x + y \implies z \in X + Y$:

  se $z < x + y$ allora $z - y < x$, quindi $(z - y) \in X$. Ma allora $z = (z - y) + y \in X + Y$.

  Inoltre dobbiamo verificare che la somma non abbia massimo. Ma sappiamo già che X, Y sono superiormente limitate, quindi $\exists\, \alpha, \beta \in \mathbb{Q}$ tale che $x < \alpha, y < \beta$ $\forall (x + y) \in X + Y$. Ma allora $x + y < \alpha + \beta$, quindi la somma è ancora superiormente limitata.

  Se avesse un massimo avremmo $m = x' + y' \in X + Y$, il che implicherebbe che $x' = \max X$ perché se x' non fosse massimo troveremmo un $x > x'$, e di conseguenza un $\widehat{m} = x + y' > m$. Ma sappiamo che X non ha massimo, quindi m non può essere massimo per la somma.

  Quindi abbiamo dimostrato che la somma di due sezioni è ancora una sezione. Il fatto che sia associativa e commutativa viene direttamente dalla associatività e commutatività dei numeri razionali.

- *L'elemento neutro per la somma è* $0_{\mathbb{R}} := S_0 = \{x \in \mathbb{Q} \mid x < 0\}$

  Dimostriamo che $X + S_0 = X$:

  $\boxed{\subseteq}$ Preso $x + y \in X + S_0$ abbiamo che $x + y < x + 0 = x \in X \implies x + y \in X$.

  $\boxed{\supseteq}$ Preso $x \in X$ abbiamo che, visto che X non ha massimo $\exists\, a \in X$ con $x < a$, ovvero $x - a \in S_0$, da cui $x = a + (x - a) \in X + S_0 \implies x \in X + S_0$.

$\implies X + S_0 = S_0 + X = X.$

- *L'opposto di una sezione S si esprime come* $-S := \{x \in \mathbb{Q} \mid -x \notin S\}$ [1]

  Dimostriamo innanzitutto che $-S$ è una sezione: prendiamo $x \in -S$, $y < x$ e supponiamo per assurdo che $y \notin -S$. Allora avremmo che $-y \in S$, ma $-x < -y \implies -x \in S$, che è assurdo.

  Dimostriamo che $S + (-S) = S_0$:

  $\boxed{\subseteq}$ Preso $a + b \in S + (-S)$ per definizione di $-S$ abbiamo che $-b \notin S \implies a < -b \implies a + b < 0 \implies a + b \in S_0$.

  $\boxed{\supseteq}$ Preso $k \in S_0$ sappiamo che $k < 0$.

  consideriamo un razionale r tale che $0 < r < -k$ e ricordo che presi due elementi qualsiasi $x \in S$, $y \in -S$ vale che $x < -y$. Ma abbiamo già dimostrato che $\mathbb{Q}$ è archimedeo, ovvero sarà sempre possibile trovare un naturale m tale che $x+mr > -y$, ovvero $x + mr \notin S \Rightarrow x + mr \in -S$, quindi chiamiamo n il minimo dei naturali per cui questo è verificato, abbiamo che: $x + (n-1)r \in S$, $x + nr \in -S$.

  Se chiamiamo $s = x + (n-1)r \in S$ abbiamo che $-k > r \implies -k + s > r + s = x + nr \notin S \implies -k + s \in -S$.

  possiamo quindi scrivere $-k = s + (-k + s) \in S + (-S)$.

  $\implies S + (-S) = -S + S = S_0 = 0_{\mathbb{R}}$.

- *La somma mantiene l'ordinamento*

  Vogliamo dimostrare che prese tre sezioni X, Y, Z vale $X < Y \implies X + Z < Y + Z$:

  Visto che l'ordinamento l'abbiamo definito a partire dall'inclusione questa verifica è in realtà banale perché abbiamo che $X \subset Y$, dunque $X + Z = \{x + z \mid x \in X,\ z \in Z\} \subset \{y + z \mid y \in Y,\ z \in Z\} = Y + Z$.

Con tutte queste proprietà dimostrare per la somma abbiamo dimostrato il seguente risultato:

Teorema 6.1.2 *$(\mathbb{R}, +, \leq)$ è un gruppo ordinato abeliano con elemento neutro S_0.*

Osservazione Valgono le seguenti uguaglianze:

[1] A lezione viene definito come $-S := \{-x \in \mathbb{Q} \mid x \in M,\ x \neq \min M\}$, dove M è l'insieme dei maggioranti di S, ma le definizioni sono equivalenti.

1. $S_{-1} = -S_1$.
2. $-(X+Y) = (-X) + (-Y) := -X - Y$.

Vorremmo ora definire l'operazione prodotto tra due sezioni, ma le sezioni negative ci danno un po' di problemi, quindi lo definiremo inizialmente solo per sezioni positive, per poi estendere la definizione tramite l'utilizzo della **regola dei segni**.

⊗ **Prodotto**

$$X \cdot Y = XY := S_0 \cup \{0\} \cup \{xy \mid x \in X, x > 0, y \in Y, y > 0\} \quad \forall X, Y \geq S_0$$

Per sezioni di segno qualunque definiamo il prodotto per casi:

- $X > S_0$, $Y < S_0 \implies XY := X(-Y)$
- $X < S_0$, $Y > S_0 \implies XY := (-X)Y$
- $X < S_0$, $Y < S_0 \implies XY := (-X)(-Y)$

Per dimostrare le proprietà della moltiplicazione, in modo analogo a quanto fatto per la somma, faremo le verifiche solo per sezioni positive, sapendo che è possibile generalizzare tutto riportandoci ai casi appena scritti.

- *La moltiplicazione è ben definita, associativa e commutativa*

  Dimostriamo innanzitutto che è una buona definizione, ovvero che il prodotto di due sezioni sia ancora una sezione. Se prendiamo $z \in XY$ e un razionale w tale che $w < z$ vorremmo dimostrare che $w \in XY$.

  Se $w \leq 0$: $w \in S_0 \cup \{0\} \subset XY \implies w \in XY$.

  Se $w > 0$: $w < z = xy$, $x, y > 0$, dunque $0 < \frac{w}{x} < \frac{z}{x} = y \in Y \implies w = x\frac{w}{x} \in XY$.

  Ora dovremmo mostrare che XY è superiormente limitato ma non possiede massimo, il che si può dimostrare nello stesso modo della somma, osservando che se avesse un massimo potremmo trovare subito un massimo per X, il che è assurdo perché X è una sezione.

  Dunque la buona definizione è dimostrata. Ancora una volta l'associatività e la commutatività derivano semplicemente dalle proprietà di $\mathbb{Q}$, tramite cui abbiamo definito il prodotto in $\mathbb{R}$.

- *L'elemento neutro per la moltiplicazione è* $1_{\mathbb{R}} := S_1 = \{x \in \mathbb{Q} \mid x < 1\}$

  Dobbiamo dimostrare che $XS_1 = X$:

  $\boxed{\subseteq}$ Preso $ab \in XS_1$ abbiamo che $ab < a \cdot 1 \in XS_1 \implies ab \in XS_1$.

  $\boxed{\supseteq}$ Preso $x \in X$ sappiamo che X non ha massimo, quindi $\exists\ a \in X$ tale che $x < a$, ovvero $\frac{x}{a} \in S_1$, da cui $x = a\frac{x}{a} \in XS_1 \implies x \in XS_1$.

  $\implies XS_1 = S_1X = X$.

- *L'inverso di una sezione* S *è definito come* $S^{-1} := S_0 \cup \{0\} \cup \left\{\frac{1}{x} \mid x \in M\right\}$*, dove* M *è l'insieme dei maggioranti di* X *privato del minimo*[2]*.*

  Dimostriamo innanzitutto che S^{-1} è una sezione: preso $z \in S^{-1}$ e un razionale $y < z$ abbiamo che

  Se $y \leq 0$: $y \in S_0 \cup \{0\} \subset S^{-1} \implies y \in S^{-1}$.

  Se $y > 0$: $y < z = \frac{1}{x}$ con x maggiorante di S, da cui $x < \frac{1}{y} \implies \frac{1}{y} \in M$. Quindi $y = \frac{1}{\frac{1}{y}} \in S^{-1}$.

  Ora dimostriamo che è l'inverso, ovvero che $SS^{-1} = S_1$:

  $\boxed{\subseteq}$ Di sicuro $S_0 \cup \{0\} \subset S_1$, quindi questo caso non lo consideriamo. Se prendiamo $z \in SS^{-1}$, $z > 0$ abbiamo che $z = \frac{x}{y}$ con $x \in S$, $y \in M$, da cui $z < 1 \implies z \in S_1$.

  $\boxed{\supseteq}$ Preso $q \in S_1$, se $q \leq 0 \implies q \in S_0 \subset SS^{-1}$. Allora prendiamo $q > 0$: sappiamo che esiste un razionale r tale che $0 < q < r < 1$. Fisso $t \in M$, e prendiamo $x \in S$ con $x > 0$; $\frac{1}{r} > 1 \implies \exists$[3]$m \in \mathbb{N}$ tc $\left(\frac{1}{r}\right)^m \geq \frac{t}{x}$, da cui $x\left(\frac{1}{r}\right)^m \geq t$.

  consideriamo $\{m \in \mathbb{N} \mid x\left(\frac{1}{r}\right)^m \in M\} \neq \emptyset$ e prendiamo n il minimo. $n > 0$ perché $x \notin M$, così vale che $x\left(\frac{1}{r}\right)^n \in M$ ma $x\left(\frac{1}{r}\right)^{n-1} \notin M$, da cui

  $\frac{1}{r} < \frac{1}{q} \implies x\frac{1}{q}\left(\frac{1}{r}\right)^{n-1} \in S$.

  Allora $q = \left(x\left(\frac{1}{r}\right)^{n-1}\right)\left(x\frac{1}{q}\left(\frac{1}{r}\right)^{n-1}\right)^{-1} \in SS^{-1}$.

  $\implies SS^{-1} = S^{-1}S = S_1$.

  Se avessimo una sezione negativa $S < S_0$ possiamo ripetere tutto il ragionamento con $-S > S_0$, per cui sarebbe ben definita la sezione $-(-S)^{-1}$. Possiamo mostrare

[2] Non è detto che questo insieme abbia minimo, ma se ce l'ha lo togliamo.

[3] Proprietà archimedea per il prodotto. L'idea per dimostrarla è che per dimostrare che $a^n > b$ con $a > 1$ scrivo $a = 1 + x$ con $x > 0$ e sappiamo che $a^n = (1+x)^n \geq q + nx$...

che questo è proprio l'inverso che cerchiamo, perché grazie all'osservazione fatta in precedenza abbiamo

$$S(-(-S)^{-1}) = S(S_{-1}(-S)^{-1}) = (S_{-1}S)(-S)^{-1} = (-S)(-S)^{-1} = S_1$$

- *Il prodotto mantiene l'ordinamento*

  vogliamo dimostrare che prese tre sezioni X, Y, Z vale $X < Y \implies XZ < YZ$:

  Visto che l'ordinamento l'abbiamo definito a partire dall'inclusione questa verifica, come accadeva per la somma, è banale perché abbiamo che $X \subset Y \implies \{xz \mid x \in X, x > 0,\ z \in Z\, z > 0\} \subset \{yz \mid y \in Y, y > 0,\ z \in Z\, z > 0\} \implies XZ \subset YZ$.

Dunque adesso abbiamo le due operazioni definite in $\mathbb{R}$. Con queste possiamo arrivare a dare altre proprietà di $\mathbb{R}$.

Proposizione 6.1.1 *Nell'insieme delle sezioni razionali vale la distributività del prodotto rispetto alla somma, ovvero*

$$Z(X + Y) = ZX + ZY \quad \forall X, Y, Z \in \mathbb{R}$$

Dimostrazione: Dobbiamo procedere per casi sulla positività delle sezioni:

Supponiamo inizialmente che siano $X, Y, Z > S_0$ e dimostriamo la proprietà:

$\boxed{\subseteq}$ Preso $w = z(x + y) \in Z(X + Y)$ abbiamo che:

Se $w \leq 0 \implies w \in S_0 \cup \{0\} \subset ZX + ZY \implies w \in ZX + ZY$ e abbiamo già quello che volevamo.

Altrimenti $w = z(x + y)$ con $z > 0$ e $x + y > 0$. Possiamo supporre $x > 0$ e di sicuro possiamo trovare un $y' > 0$ che verifichi $y' > y$, dunque $w = z(x+y) = zx+zy < zx+zy' \in ZX + ZY \implies w \in ZX + ZY$.

$\boxed{\supseteq}$ ZX e ZY sono contenuti in $Z(X + Y) = S_0 \cup \{0\} \cup \{z(x + y) \mid ...\}$.

Prendiamo $w \in ZX + ZY$, dunque $w = a + b$, con $a \in ZX$, $b \in ZY$.

Se $a, b \leq 0 \implies a + b \in S_0 \cup \{0\} \subset Z(X + Y) \implies w = a + b \in Z(X + Y)$ quindi ok.

Se $a \leq 0$ e $b = zy$ con $z, y > 0$ allora $a + b < b = zy \in ZY \subset Z(X + Y) \implies a + b \in Z(X + Y)$ perché è una sezione.

Se $a = zx$ e $b \leq 0$ si ragiona in maniera analoga.

Se $a = zx$ e $b = z'y$ con $x, y, z, z' > 0$ allora possiamo supporre $z < z'$, da cui $w = zx + z'y < z(x + y) \in Z(X + Y) \implies w \in Z(X + Y)$.

Dunque nel caso di sezioni positive abbiamo dimostrato tutto. Gli altri casi si risolvono riportandoci a sezioni positive:

Se $Z < S_0$ e $X, Y > S_0$ allora $Z(X+Y) = -(-Z)(X+Y) = -(-ZX-XY) = ZX+ZY$, in cui abbiamo usato anche l'osservazione fatta prima di definire il prodotto.

Se Z è di segno qualunque e $X > S_0$, $Y < S_0$ allora abbiamo due casi, che risolveremo usando ciò che si è dimostrato fino ad adesso:
Se $X > -Y$ abbiamo $X + Y > 0$, da cui $ZX = Z(X + Y - Y) = Z(X + Y) + Z(-Y) = Z(X + Y) - ZY \Longrightarrow ZX + ZY = Z(X + Y)$.
Se $X < -Y$ abbiamo che $-X - Y > 0$, da cui $Z(-Y) = Z(-X - Y + X) = Z(-X - Y) + ZX = -Z(X + Y) + ZX \Longrightarrow ZX + ZY = Z(X + Y)$.

Se Z è di segno qualunque e $X < S_0$, $Y > S_0$ si ripete il ragionamento di prima.

Se Z è di segno qualunque e $X, Y < S_0$ allora $-Z(X + Y) = Z(-X - Y) = Z(-X) + Z(-Y) = -ZX - ZY \Longrightarrow Z(X + Y) = ZX + ZY$.

□

6.1.2 Proprietà di $\mathbb{R}$

Ora che abbiamo definito il nostro nuovo insieme in tutto e per tutto, con applicazioni e ordinamento, vediamone le proprietà principali, e soprattutto cosa lo distingue dagli insieme definiti fino ad ora.

Teorema 6.1.3 $(\mathbb{R}, +, \cdot, \leq)$ *è un campo ordinato.*

Dimostrazione: Viene da tutte le proprietà dimostrate fino ad ora.

□

Avendo definito il nostro nuovo insieme $\mathbb{R}$ a partire dai numeri razionali vorremmo ritrovare al suo interno una "copia" di $\mathbb{Q}$, ovvero un suo insieme isomorfo.

Teorema 6.1.4 *L'applicazione*

$$\begin{array}{rcl} S : \mathbb{Q} & \longrightarrow & \mathbb{R} \\ q & \longmapsto & S_q \end{array}$$

è un omomorfismo ordinato di campi.

Dimostrazione: Dimostriamo che si comporta bene con le operazioni e l'ordinamento dei due campi:

$\boxed{+}$ $S_{p+q} = \{x \mid x < p + q\}$, mentre $S_p + S_q = \{x \in \mathbb{Q} \mid x < p\} + \{y \in \mathbb{Q} \mid y < q\}$. Quindi di sicuro $S_p + S_q \subseteq S_{p+q}$.

Viceversa, preso $z \in S_{p+q}$, abbiamo che $z < p+q$, allora $\exists\, c \in \mathbb{Q}^+$ tale che $z+c < p+q$, ovvero $z+c-p < q$, da cui abbiamo che $z+c-p \in S_q$. Ma allora $z = (z+c-p)+(p-c) \in S_q + S_p = S_p + S_q$.

Dunque la somma è mantenuta, quindi è sicuramente un omomorfismo di gruppi.

$\boxed{\cdot}$ Di nuovo sicuramente abbiamo $S_p S_q \subseteq S_{pq}$.

Viceversa, preso $z \in S_{pq}$, abbiamo che $z < pq$, allora $\exists\, c \in \mathbb{Q}$ tale che $\frac{z}{p} < c < q$, da cui $c \in S_q$ e $\frac{z}{c} < p$, quindi $\frac{z}{c} \in S_p$. Ora basta osservare che $z = \frac{z}{c} c \in S_p S_q$.

Dunque anche il prodotto è mantenuto, quindi l'applicazione è un omomorfismo di anelli.

$\boxed{\leq}$ l'ordinamento è banalmente mantenuto per come sono definiti i due ordinamenti negli insiemi.

Dunque in $\mathbb{R}$ possiamo trovare una copia isomorfa di $\mathbb{Q}$ semplicemente considerando l'insieme delle sezioni $\{S_q\}_{q \in \mathbb{Q}}$.

□

C'è una proprietà che caratterizza il nostro nuovo insieme che prima non avevamo: la **completezza**!

Teorema 6.1.5 $\mathbb{R}$ *è completo.*

Dimostrazione: Per dimostrare che è completo dobbiamo mostrare che ogni suo sottoinsieme limitato superiormente ammette un un estremo superiore in $\mathbb{R}$; sia dunque $A \subseteq \mathbb{R}$ con A superiormente limitato. Definiamo

$$\mathcal{E} = \bigcup_{X \in A} X$$

Ovvero l'unione di tutti i razionali che sono contenuti in una qualunque sezione appartenente ad A[4]. Questa è una anche lei una sezione, infatti:

Se $x \in \mathcal{E}$ e prendiamo un razionale $y < x$ abbiamo che $x \in B \in A \Longrightarrow y \in B \Longrightarrow y \in \mathcal{E}$.

Il fatto che A sia superiormente limitato in $\mathbb{R}$ ci dice che $\exists\ T \in \mathbb{R}$ per cui $X \subset T$ $\forall X \in A$, da cui ricaviamo che $\mathcal{E} \subset T$, quindi anche $\mathcal{E}$ è superiormente limitato.

$\mathcal{E}$ non ammette massimo perché se prendiamo $m = \max \mathcal{E} \Longrightarrow m \in X$ per qualche $X \in A$, ovvero $m = \max X$, il che è assurdo perché sappiamo che le sezioni non hanno massimo.

[4]Ricordiamo che A è sottoinsieme di $\mathbb{R}$, quindi è un insieme di sezioni!

$\mathcal{E}$ è maggiorante di A perché se $X \in A \Longrightarrow X \subseteq \mathcal{E}$.

Quindi abbiamo trovato esattamente ciò che cercavamo: $\mathcal{E} = \sup A$.

□

Facciamo un'osservazione su ciò che abbiamo fatto fino ad ora: abbiamo ottenuto $\mathbb{R}$ come estensione di $\mathbb{Q}$ che in più ha la particolarità di essere completo. Ma nel capitolo sulle strutture ordinate avevamo osservato che in ogni campo ordinato C possiamo trovare un insieme $\mathbb{Q}_C$ isomorfo a $\mathbb{Q}$ tramite l'applicazione

$$\begin{array}{rcl} \varphi : \mathbb{Q}_C & \longrightarrow & \mathbb{Q} \\ \frac{n1_C}{m1_C} & \longmapsto & \frac{n}{m} \end{array}$$

Quindi anche un generico campo ordinato C può essere visto come estensione del suo campo fondamentale $\mathbb{Q}_C$. Il fatto che quest'ultimo insieme sia isomorfo a $\mathbb{Q}$ cosa ci può dire sul campo $\mathbb{R}$ che abbiamo costruito lungo tutto questo capitolo?

Formalizzando questa idea possiamo in effetti arrivare a dimostrare un risultato notevole in questo senso, che è il seguente:

Teorema 6.1.6 *Sia $(C, \leq)$ un campo ordinato archimedeo. Allora l'applicazione φ descritta sopra si estende ad omomorfismo ordinato di campi $\Phi : C \longrightarrow \mathbb{R}$.*

Inoltre se C è completo Φ è isomosfismo.

Dimostrazione: Preso $x \in C$ consideriamo $T_x = \{y \in \mathbb{Q}_C \mid y < x\}$.

T_x è sicuramente maggiorato in C perché per archimedeicità sappiamo che $\exists\, n$ tale che $n1_C > x > y \ \ \forall y \in T_x$, dunque anche $\varphi(T_x)$ è maggiorato in $\mathbb{R}$.

Ma sappiamo che $\mathbb{R}$ è completo, quindi è ben definita l'applicazione

$$\begin{array}{rcl} \Phi : C & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \sup_{\mathbb{R}} \varphi(T_x) \end{array}$$

Verifichiamo che Φ è un omomorfismo ordinato che estende φ:

1 Φ estende φ:

Preso $a \in \mathbb{Q}_C$ abbiamo che $\varphi(a)$ è maggiorante di $\varphi(T_a)$ perché sappiamo che φ mantiene l'ordinamento, quindi $\varphi(a) \geq \Phi(a)$.

Se fosse $\varphi(a) > \Phi(a)$ potremmo prendere un $\epsilon \in \mathbb{Q}$ tale che $\Phi(a) < \epsilon < \varphi(a)$, da cui otteniamo $\varphi^{-1}(\epsilon) < a \Longrightarrow \varphi^{-1}(\epsilon) \in T_a \Longrightarrow \epsilon \in \varphi(T_a) \Longrightarrow \epsilon \leq \Phi(a)$, il che è assurdo.

Quindi $\varphi(a) = \Phi(a)$.

2 Φ è un omomorfismo di campi:

Vogliamo dimostrare che $\Phi(x+y) = \Phi(x) + \Phi(y) \ \ \forall x, y \in C$, e lo facciamo dimostrando le due disequazioni

($\leq$) Preso un elemento $z \in \mathbb{Q}_C$ che verifichi $z < x + y$ vorremmo riuscire a scriverlo come somma di due elementi di $\mathbb{Q}_C$ del tipo $z = t + w$ con $t < x$, $w < y$, perché se riusciamo a fare questo avremo che un elemento qualsiasi di $\varphi(T_{x+y})$, quindi della forma $\varphi(z)$, lo scriviamo come somma di due elementi $\varphi(t) \in \varphi(T_x)$, $\varphi(w) \in \varphi(T_y)$; Visto come abbiamo definito la funzione Φ questo proverebbe che $\Phi(x + y) \leq \Phi(x) + \Phi(y)$.

Allora preso $z < x + y$ sappiamo che esiste $w \in \mathbb{Q}_C$ tale che $z - x < w < y$, quindi se chiamiamo $t = z - w$ abbiamo che $z = t + w$, $t < x$, $w < y$, che è proprio quello che volevamo.

($\geq$) Per dimostrare quest'altra disequazione agiremo su $\mathbb{R}$: preso un qualunque $q < \Phi(x) + \Phi(y)$ vogliamo trovare due elementi $a \in T_x$, $b \in T_y$ per cui $q \leq \varphi(a + b)$.

Allora preso $q < \Phi(x) + \Phi(y)$ sappiamo che esiste un razionale $\overline{b}$ tale che $q - \Phi(x) < \overline{b} < \Phi(y)$, quindi preso $\overline{a} = q - \overline{b}$ vale $q = \overline{a} + \overline{b}$. Dunque se chiamiamo $a = \varphi^{-1}(\overline{a}) < x$, $b = \varphi^{-1}(\overline{b}) < y$ abbiamo che $a \in T_x$, $b \in T_y$ e $q = \overline{a} + \overline{b} = \varphi(a) + \varphi(b) = \varphi(a + b)$, che prova la nostra tesi.

Dovremmo poi dimostrare che $\Phi(xy) = \Phi(x)\Phi(y) \ \ \forall x, y \in C$, ma si fa sostanzialmente come abbiamo fatto per la somma, quindi lasciamo la prova al lettore.

3 Φ mantiene l'ordine:

Preso $x \in C$, $x > 0$ dobbiamo verificare che $\Phi(x) > 0$.

Sappiamo che $\exists\, u \in \mathbb{Q}_C$ con $0 < u < x$. Certo $u \in T_x$, ovvero $\varphi(u) \in \varphi(T_x)$, da cui ricaviamo che $\Phi(x) \geq \varphi(u)$. Ma φ mantiene l'ordine, quindi $0 < \varphi(u) \leq \Phi(x)$.

4 Se C è completo Φ è un isomorfismo:

Basta vedere che è surgettivo: preso $w \in \mathbb{R}$ cerchiamo $x \in C$ con $\Phi(x) = w$.

Definiamo $Y := \{y \in \mathbb{Q} \mid y < w\}$ e consideriamo $\varphi^{-1}(Y) \subset \mathbb{Q}_C$. Sapendo che $\varphi^{-1}(Y)$ è maggiorato in C e che C è completo definiamo

$$x := \sup_C \left(\varphi^{-1}(Y)\right)$$

e verifichiamo che vale proprio $\Phi(x) = w$:

Se fosse $\Phi(x) < w$ potremmo prendere un certo $\epsilon \in \mathbb{Q}$ tale che $\Phi(x) < \epsilon < w$. Allora varrebbe $\epsilon \in Y$, da cui $\varphi^{-1}(\epsilon) \in \varphi(Y) \subseteq T_x$, ovvero $\Phi(\epsilon) = \varphi(\epsilon) < x \Longrightarrow \epsilon < \Phi(x)$, il che è assurdo.

Viceversa, se fosse $\Phi(x) > w$ potremmo prendere come al solito un $\epsilon \in \mathbb{Q}$ tale che $w < \epsilon < \Phi(x)$. Visto che abbiamo già verificato che Φ mantiene l'ordine ciò implica che $\Phi^{-1}(\epsilon) = \varphi^{-1}(\epsilon) < x$. Allora per definizione di x sappiamo che esiste $r \in \varphi^{-1}(Y)$ tale che $\varphi^{-1}(\epsilon) < r < x$, ma sapendo che $\varphi r \in Y$ ricaviamo che $\epsilon < \varphi r < w$, il che è assurdo.

Dunque l'unica possibilità è che si abbia $\Phi(x) = w$.

□

Corollario *Siano C, C' due campi ordinati completi. L'applicazione $f : \mathbb{Q}_C \longrightarrow \mathbb{Q}_{C'}$ si estende ad una applicazione $F : C \longrightarrow C'$ che è isomorfismo ordinato di campi.*

6.2 Successioni di Cauchy

Definizione 6.2.1 Sia $(A, \leq)$ un anello ordinato. $\forall a \in A$ il *valore assoluto* di a è definito come

$$|a| = \begin{cases} a & \text{se } a \geq 0 \\ -a & \text{se } a < 0 \end{cases}$$

Proposizione 6.2.1 *Valgono le seguenti proprietà:*
$|a + b| \leq |a| + |b|$
$|ab| = |a||b|$
$||a| - |b|| \leq |a - b|$

Definizione 6.2.2 Sia $(A, \leq)$ un anello ordinato. Una successione $\{a_n\}_{n\geq 1}$ di elementi di A si dice *di Cauchy* in A quando

$$\forall \epsilon > 0,\ \epsilon \in A,\ \exists\, k > 0 \text{ per cui } |a_n - a_m| < \epsilon\ \ \forall n, m \geq k$$

Definizione 6.2.3 Si dice che la successione è *limitata* se

$$\exists\, a \in A, a > 0,\ \text{per cui } |a_n| \leq a\ \forall n > 0$$

Definizione 6.2.4 Si dice che la successione $\{a_n\}$ *converge* (in A) all'elemento $a \in A$ quando

$$\forall \epsilon > 0, \epsilon \in A,\ \exists\, k \text{ per cui } |a_n - a| < \epsilon\ \forall n \geq k$$

$$\text{e si scrive} \quad \lim_{n\to\infty} a_n = a$$

Definizione 6.2.5 Sia $(A, \leq)$ anello ordinato, allora $\forall a, b \in A$, $a \leq b$ definiamo

$$[a, b] := \{x \in A \mid a \leq x \leq b\}$$

Definizione 6.2.6 Una successione $\{a_n\}$ si dice *infinitesima* se converge a 0.

Definizione 6.2.7 Un anello ordinato A si dice *Cauchy completo* se ogni successione di Cauchy converge.

Definizione 6.2.8 Una successione $\{a_n\}$ si dice *definitivamente positiva* se

$$\exists\, k \text{ per cui } a_n > 0\ \forall n \geq k$$

si dice invece *definitivamente negativa* se

$$\exists\, k \text{ per cui } a_n < 0\ \forall n \geq k$$

Definizione 6.2.9 Una successione $\{a_n\}$ si dice *strettamente positiva* se

$$\exists\, \epsilon \in A, \epsilon > 0 \text{ per cui } \exists\, k \text{ tale che } a_n > \epsilon\ \forall n \geq k$$

si dice invece *strettamente negativa* se

$$\exists\, \epsilon \in A, \epsilon > 0 \text{ per cui } \exists\, k \text{ tale che } a_n < -\epsilon\ \forall n \geq k$$

Osservazione 1. Tutte le successioni di Cauchy sono limitate.

2. Tutte le successioni convergenti sono di Cauchy.

Osservazione Sia $(Q, \leq)$ un campo ordinato, e sia $\mathcal{C}(Q)$ l'insieme delle successioni di Cauchy a coefficienti in Q. Presa $a = \{a_n\} \in Q$ non infinitesima valgono le seguenti proprietà:

1. $\exists\, \lambda \in Q$, $\lambda > 0$, ed $\exists\, p$ tali che $a_n > \lambda\ \ \forall n \geq p$ oppure $a_n < -\lambda\ \ \forall n \geq p$.
2. $\exists\, \lambda > 0$ tale che $\forall\, b = \{b_n\} \in \mathcal{C}(Q)$ se $a - b = \{a_n - b_n\}$ è infinitesima allora

$$\begin{cases} b_n > \lambda\ \ \forall n > p & \text{se} \quad a_n > \lambda\ \ \forall n \geq s \\ b_n < -\lambda\ \ \forall n \geq p & \text{se} \quad a_n < -\lambda\ \ \forall n \geq s \end{cases}$$

6.2.1 Operazioni con le Successioni

Facciamo adesso un piccolo ragionamento: prendiamo $(Q, \leq)$ un campo ordinato e definiamo $\mathcal{C}(Q) = \mathcal{C}$ lo spazio delle successioni di Cauchy a coefficienti in Q.

Su $\mathcal{C}$ possiamo definire le operazioni di somma e prodotto semplicemente termine a termine in modo da renderlo un anello:

$\oplus$ **Somma**

$$\{a_n\} + \{b_n\} := \{a_n + b_n\}$$

$\otimes$ **Prodotto**

$$\{a_n\} \cdot \{b_n\} := \{a_n \cdot b_n\}$$

Dobbiamo verificare che queste operazioni siano ben definite, ovvero che somma e prodotto di successioni di Cauchy siano ancora successioni di Cauchy.

Per la somma è abbastanza semplice: sappiamo che $\{a_n\}$ e $\{b_n\}$ sono di Cauchy, dunque $\forall \epsilon \; \exists \, k_1, k_2$ tali che $|a_n - a_m| < \epsilon \; \forall m, n > k_1$ e $|b_n - b_m| < \epsilon \; \forall m, n > k_2$.

Ma allora presi $m, n > \max\{k_1, k_2\}$ abbiamo che

$|(a_n + b_n) - (a_m + b_m)| < |a_n - a_m| + |b_n - b_m| < 2\epsilon$

il che prova che $\{a_n + b_n\} = \{a_n\} + \{b_n\}$ è di Cauchy.

Per il prodotto dovremo lavorare un attimo di più: sappiamo che $\forall \epsilon > 0 \; \exists \, \nu$ tale che $\forall m, n \geq \nu$ vale $|a_n - a_m| < \epsilon$, $|b_n - b_m| < \epsilon$.

$|a_n b_n - a_m b_m| = |(a_n - a_m)b_n - a_m(b_m - b_n)| \leq |a_n - a_m||b_n| + |a_m||b_m - b_n| \leq \epsilon c + \epsilon d$, visto che le successioni sono limitate, il che prova che anche $\{a_n b_n\} = \{a_n\}\{b_n\}$ è di Cauchy.

Ora se chiamiamo $\mathcal{S}(Q) = \mathcal{S}$ lo spazio delle successioni infinitesime a coefficienti in Q abbiamo che $\mathcal{S}$ è un ideale di $\mathcal{C}$.

Infatti sappiamo già che $\mathcal{S} \subset \mathcal{C}$, inoltre se prendiamo $a \in \mathcal{C}$ e $b \in \mathcal{S}$ vale $ab \in \mathcal{S}$, semplicemente perché moltiplichiamo una successione infinitesima per una limitata, quindi il prodotto non può che essere una successione infinitesima!

Ora, sapendo che $\mathcal{C}$ è un anello e $\mathcal{S}$ un suo ideale, possiamo considerare l'insieme quoziente

$$\mathcal{C}/_{\mathcal{S}}$$

che possiamo verificare essere un campo, e definire su di esso anche un ordinamento, così da renderlo un **campo ordinato**.

L'ordinamento non lo definiremo in modo esplicito, ma daremo una caratterizzazione degli elementi *positivi*, da cui l'ordinamento è totalmente determinato[5].

Verifichiamo innanzitutto che è un campo:

Dato un elemento $\{a_n\}$ non nullo[6] di $\mathcal{C}/_{\mathcal{S}}$ vorremmo trovare il suo inverso moltiplicativo, ma per fare ciò dobbiamo prima capire chi è l'elemento neutro per il prodotto, che visto che siamo in un quoziente è una qualsiasi successione del tipo:

$$\{\theta_n\} \text{ tale che } \theta_n = 1 \;\; \forall n \geq k$$

[5] Avevamo infatti visto nel capitolo sulle strutture ordinate che una volta definiti gli elementi positivi di un insieme esiste un modo canonico di costruire un ordinamento su tutto l'insieme!

[6] Ovvero tale che $\{a_n\}$ non sia infinitesima.

Questo perché se consideriamo $\{a_n\}, \{a_n\}\{\theta_n\} \in \mathcal{C}$ vale che $a_n\theta_n = a_n \ \ \forall n \geq k$, quindi $\{a_n\} - \{a_n\theta_n\} = \{a_n - a_n\theta_n\}$ risulta infinitesima in $\mathcal{C}$ e dunque nulla in $\mathcal{C}/_{\mathcal{S}}$, il che ci dice che in $\mathcal{C}/_{\mathcal{S}}$ abbiamo $\{a_n\} = \{a_n\theta_n\}$, ovvero $\{\theta_n\}$ è l'elemento neutro che cerchiamo.

Ma una volta trovato l'elemento neutro è semplicissimo trovare l'inverso di una successione $\{a_n\}$ non infinitesima, visto che se una successione non è infinitesima allora $a_n > \delta > 0 \ \ \forall n \geq N$, quindi definiamo l'inverso

$$\{a_n\}^{-1} := \begin{cases} \frac{1}{a_n} & \forall n \geq N \\ 1 & \forall n < N \end{cases}$$

Tenendo presente che in realtà il fatto di definire uguali a 1 gli elementi fino all'N-esimo è del tutto irrilevante, avremmo potuto mettere un qualsiasi valore e sarebbe ancora stato un inverso valido.

Ma allora l'inverso non è unico? In realtà è *unico a meno di successioni infinitesime*, visto che abbiamo dimostrato poco fa che due successioni che differiscono solo per un numero finito di termini iniziali sono la stessa nell'insieme $\mathcal{C}/_{\mathcal{S}}$.

Definiamo allora l'insieme dei positivi, da cui poi avremo di conseguenza un ordinamento: Diciamo che in $\mathcal{C}/_{\mathcal{S}}$ gli elementi positivi sono le classi indotte da successioni strettamente positive in $\mathcal{C}$.

Questa è una buona definizione perché somma e prodotto di positivi rimane positiva.

Teorema 6.2.1 *$(\mathcal{C}/_{\mathcal{S}}, +, \cdot, \leq)$ è un campo ordinato e l'applicazione*

$$\begin{array}{rcl} j : Q & \longrightarrow & \mathcal{C}/_{\mathcal{S}} \\ q & \longmapsto & \{q, q, q, ...\} \end{array}$$

è un omomorfismo iniettivo che conserva l'ordine.

Dimostrazione: La dimostrazione è già praticamente fatta perché abbiamo già mostrato che $\mathcal{C}/_{\mathcal{S}}$ è un campo ordinato, e per come abbiamo definito operazioni e ordinamento è ovvio che j sia un morfismo iniettivo ordinato.

□

Il campo $\mathcal{C}/_{\mathcal{S}}$ così costruito lo chiamiamo **Completamento di Cantor** di Q e lo indichiamo $\mathbb{R}(Q)$. Nel caso in cui $Q = \mathbb{Q}$ allora chiamiamo $\mathbb{R} := \mathbb{R}(\mathbb{Q})$ **Reali di Cantor**.

6.2.2 Proprietà di $\mathbb{R}(Q)$

Nota: In questo paragrafo faremo alcune considerazioni sul nuovo campo che abbiamo definito in questo paragrafo, durante le quali verranno usate disequazioni di elementi che

sono talvolta in Q e talvolta in $\mathbb{R}(Q)$. Per correttezza dovremmo indicare i simboli con "$<_Q$" e "$<_{\mathbb{R}}$", ma per non appesantire troppo la notazione useremo sempre lo stesso simbolo "$<$" che dovrà essere contestualizzato dal lettore a seconda degli elementi che stiamo considerando.

Osservazione Sia $(\mathbb{Q}, \leq)$ un campo ordinato e sia $A \in \mathbb{R}(Q)$.

Se $A > 0$ allora $\exists\, \delta \in Q$ tale che $A > j(\delta) > 0$.

Se $A < 0$ allora $\exists\, \delta \in Q$ tale che $A < -j(\delta) < 0$.

Dimostrazione: Poiché $A > 0$, se A è rappresentato da una successione $\{a_n\}$ non infinitesima, quindi sappiamo che $\exists\, \delta > 0$, $\delta \in Q$ con $a_n > \delta > 0 \ \ \forall n \geq p$.

Allora se consideriamo la successione $j(\delta) \in \mathbb{R}(Q)$ abbiamo immediatamente che $A > j(\delta) > 0$.

□

Proposizione 6.2.2 *Presa $\{a_n\} = A \in \mathbb{R}(Q)$ vale*

$$\lim_{n\to\infty} j(a_n) = A$$

Dunque in particolare Q è denso in $\mathbb{R}(Q)$.

Dimostrazione: Dobbiamo verificare che $\forall \sigma > 0\ \exists p$ tale che $|j(a_n) - A| < \sigma \ \ \forall n \geq p$.

Vista l'osservazione precedente ci basta dimostrare la disequazione per σ del tipo $\sigma = j(\delta)$ con $\delta \in Q$.

La successione $\{a_n\}$ è di Cauchy, così $\exists p$ tale che $|a_m - a_n| < \delta \ \ \forall m, n \geq p$, e vorrei dimostrare che $|j(a_n) - A| \leq j(\delta) \ \ \forall n \geq p$.

Ma in effetti la successione associata a $(j(a_n) - A)$ è proprio $\{a_n - a_m\}_{m\geq 1}$, così la disuguaglianza è data semplicemente dal fatto che $\{a_n\}$ è di Cauchy.

□

Teorema 6.2.2 *Preso Q campo ordinato $\mathbb{R}(Q)$ è Cauchy-completo. Inoltre se Q è archimedeo lo è anche $\mathbb{R}(Q)$.*

Dimostrazione: Dimostriamo la Cauchy completezza di $\mathbb{R}(Q)$: presa $\{A_n\}$ una successione di Cauchy in $\mathbb{R}(Q)$ dimostriamo che $\{A_n\}$ converge. Per fare questo dovremo prima capire a cosa potrebbe convergere, per poi dimostrare che la convergenza c'è davvero.

Fissato $\epsilon \in Q$, $\epsilon > 0\ \exists n' = n'(\epsilon)$ tale che $\forall m, n \geq n'(\epsilon)$ vale $|A_n - A_m| < \frac{j(\epsilon)}{3}$.

Sia $b_n \in Q$ tale che $|A_n - j(b_n)| < \frac{j(\epsilon)}{3}$, allora abbiamo che

$$|j(b_n) - j(b_m)| \leq |j(b_n) - A_n| + |A_n - A_m| + |A_m - j(b_m)| < j(\epsilon)$$

Dunque la successione $\{b_n\}$ è ancora di Cauchy perché $|j(b_n) - j(b_m)| = j(|b_n - b_m|)$, quindi definisce una successione $\mathcal{A} \in \mathbb{R}(Q)$ a cui $\{j(b_n)\}$ converge.

Allora se consideriamo il comportamento della successione $\{A_n\}$ rispetto a $\mathcal{A}$ abbiamo che

$$|A_n - \mathcal{A}| \leq |A_n - j(b_n)| + |j(b_n) - \mathcal{A}| < j(\epsilon)$$

Dunque $\{A_n\}$ converge proprio ad $\mathcal{A}$.

Il fatto che sia archimedeo è già dimostrato perché sappiamo che Q è denso in $\mathbb{R}(Q)$.

□

6.3 Completezza Secondo Dedekind e Secondo Cauchy

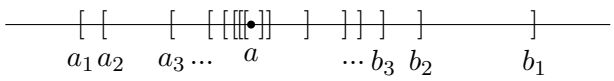
Quello che vorremmo dimostrare adesso è che la completezza enunciata nel paragrafo sulle sezioni di Dedekind è equivalente alla Cauchy completezza enunciata in questo paragrafo. Per fare ciò dovremo fare diversi passaggi che ci porteranno via un po' di tempo.

Lemma (Proprietà degli intervalli imbottigliati) *Sia $(Q, \leq)$ un campo ordinato Cauchy-completo. Allora per ogni successione decrescente di intervalli $[a_n, b_n]$ di Q con lunghezze tendenti a zero vale*

$$\bigcap_{n\geq 1} [a_n, b_n] = a \in Q$$

in cui si ha $a_n \leq a \leq b_n \ \ \forall n$.

Dimostrazione: I nostri intervalli sono disposti in una posizione generica di questo tipo:



In cui notiamo che $\forall n$ si hanno le seguenti proprietà:

1) $a_n < b_n$ 2) $a_n < a_{n+1}$ 3) $b_{n+1} < b_n$ 4) $\lim_{n\to\infty} (b_n - a_n) = 0$

Dimostriamo innanzitutto che le successioni $\{a_n\}$ e $\{b_n\}$ sono di Cauchy: dalla (4) ricaviamo che preso $\epsilon > 0$ $\exists\, n'$ tale che $\forall n \geq n'$ vale $|a_n - b_n| = b_n - a_n < \epsilon$.

Quindi $\forall m \geq n \geq n'$ vale $0 < b_n - a_n < \epsilon$ e $-\epsilon < a_m - b_m < 0$, dunque sommiamo e otteniamo

$$-\epsilon < (a_m - b_m) + (b_n - a_n) < \epsilon \quad \Longrightarrow \quad -\epsilon < (a_m - a_n) + (b_n - b_m) < \epsilon$$

Dunque $|a_m - a_n| < \epsilon$ e $|b_n - b_m| < \epsilon$, che è ciò che volevamo.

Vediamo ora che l'intersezione di tutti è non vuota: questo è abbastanza semplice, perché da quello che sappiamo ricaviamo subito

$$\begin{cases} \lim_{n\to\infty} a_n = a \\ \lim_{n\to\infty} b_n = b \\ \lim_{n\to\infty}(b_n - a_n) = 0 \end{cases} \implies a = b \in \bigcap_n [a_n, b_n]$$

Adesso dimostriamo che $a_n < a < b_n \ \forall n$: se esistesse un m per cui $a_m > a$ avremmo $a_m - a > \epsilon > 0$. Ma allora $\forall s > m$ vale $a_s - a > \epsilon > 0$, che è un assurdo.

Lo stesso per b_n.

Per ultima dimostriamo l'unicità: siano $c, d \in \bigcap[a_n, b_n]$, e supponiamo $c < d$.

Abbiamo $a_n \leq c < d \leq b_n \ \forall n$, ma noi sappiamo che $b_n - a_n \to 0$, dunque $b_n - a_n < d - c$ da un certo $\overline{n}$ in poi, da cui ricaviamo

$$b_n - c \leq b_n - a_n < d - c \leq b_n - c$$

che è un assurdo.

□

Teorema 6.3.1 (Metodo della Dicotomia) *Se $(Q, \leq)$ è un campo ordinato, archimedeo e Cauchy-completo allora $(Q, \leq)$ è completo.*

Dimostrazione: Preso un sottoinsieme X di Q superiormente limitato vorremmo trovarne l'estremo superiore.

diciamo che è possibile costruire una successione decrescente di intervalli chiusi $[a_n, b_n]$ con queste proprietà:

1. b_n è maggiorante di X.
2. $([a_n, b_n] \cap X) \neq \emptyset \ \ \forall n$.
3. $b_n - a_n = \frac{1}{2}(b_{n-1} - a_{n-1}) \ \ \forall n \geq 2$.

Infatti: sia $a_1 \in X$ e sia b_1 un maggiorante di X. Certo $([a_1, b_1] \cap X) \neq \emptyset$. Per costruire l'intervallo successivo consideriamo $m_1 = \frac{1}{2}(a_1 + b_1)$ il punto medio di $[a_1, b_1]$.

Se m_1 è maggiorante di X scegliamo $[a_2, b_2] := [a_1, m_1]$, mentre se $m_1 \in X$ scegliamo $[a_2, b_2] := [m_1, b_1]$.

Questo processo lo possiamo fare per ogni n, quindi abbiamo costruito la successione che cercavo.

Ora vogliamo mostrare che $\cap[a_n, b_n]$ è proprio l'estremo superiore che cerchiamo!

Per il lemma precedente sappiamo che $\cap[a_n, b_n] = a$, ovvero l'intersezione è composta di un solo punto $a \in Q$.[7]

Vediamo che a è maggiorante: se esistesse $x \in X$ con $x > a$ avremmo che $\exists\, n$ tale che $2^n(x-a) > b_1 - a_1 = 2^n(b_n - a_n)$ perché Q è archimedeo. Ma allora $x > b_n + (a - a_n) \geq b_n$, il che è assurdo perché b_n è maggiorante di X.

E verifichiamo che sia il più piccolo dei maggioranti: se prendiamo $q \in Q$, $q < a$ vogliamo dimostrare che possiamo sempre trovare $x \in X$ tale che $q < x$: poiché Q è archimedeo esiste un n tale che $2^n(a - q) > b_1 - a_1 = 2^n(b_n - a_n)$, da cui $q < a - b_n + a_n < a_n$, il che è assurdo.

□

Lemma *Sia $(Q, \leq)$ un campo ordinato completo. Allora per ogni successione di intervalli decrescenti $[a_n, b_n]$ con lunghezze tendenti a zero vale*

$$\bigcap_{n \geq 1} [a_n, b_n] = a \in Q$$

Dimostrazione: Che l'intersezione non contenga più di un punto l'abbiamo già dimostrato, perché la precedente dimostrazione non usa la proprietà di essere un campo archimedeo per dimostrare questo, quindi possiamo ripeterla senza problemi. Dunque tutto quello che vogliamo dimostrare è che l'intersezione sia non vuota.

Siano allora $A = \{a_n\}$ e $B = \{b_n\}$.

A è superiormente limitato perché $a_n < b_n\ \forall n$, e B è inferiormente limitato per lo stesso motivo[8]. Quindi $\exists\, a, b \in Q$ tali che $a = \sup_Q A$, $b = \inf_Q B$.

Se prendiamo $x \in [a, b]$ abbiamo allora $x \in [a, b] \subset [a_n, b_n]$, quindi $\cap[a_n, b_n] \neq \emptyset$, che completa la dimostrazione.

□

Siamo finalmente pronti a dimostrare il teorema che volevamo:

Teorema 6.3.2 *Sia $(Q, \leq)$ un campo ordinato. Allora vale*

$$Q \text{ è completo} \quad \Longleftrightarrow \quad Q \text{ è archimedeo e Cauchy-completo}$$

Dimostrazione: $\boxed{\Longleftarrow}$ Già dimostrato precedentemente.

[7] Questo lo possiamo dire solo perché il campo è archimedeo, altrimenti $\lim_{n\to\infty}(b_n - a_n) = \lim_{n\to\infty} \frac{1}{2^n} = 0$ non sarebbe vero!

[8] Ricordiamo che siamo nella stessa situazione del lemma precedente, quindi valgono ancora le quattro proprietà enunciate.

$\boxed{\Longrightarrow}$ Abbiamo già dimostrato che se un campo è completo allora è archimedeo, quindi rimane da dimostrare che è anche Cauchy-completo, ovvero che ogni successioni di Cauchy è convergente.

Presa $\{a_n\}$ di Cauchy consideriamo $A_p = \{a_n \mid n \geq p\}$.

Certamente A_p è limitato in Q per ogni p perché $\{a_n\}$ stessa è limitata.

Poiché Q è completo esistono

$$\alpha_p = \inf_Q A_p \qquad \beta_p = \sup_Q A_p$$

su cui facciamo alcune considerazioni:

- $\forall p$ vale $\alpha_p \leq \beta_p$;
- La successione $\{\alpha_p\}_{p\geq 1}$ è crescente;
- La successione $\{\beta_p\}_{p\geq 1}$ è decrescente.

Quindi vale

$$\beta_1 - \alpha_1 \geq \beta_2 - \alpha_2 \geq \ldots \geq \beta_p - \alpha_p \geq \ldots$$

Sia dunque $\epsilon > 0$, $\epsilon \in Q$. Visto che $\{a_n\}$ è di Cauchy sappiamo che $\exists\, p$ con $|a_n - a_m| \leq \frac{\epsilon}{3}$ $\forall n, m \geq p$.

Per definizione di estremo inferiore e superiore $\exists\, n \geq p$ tale che $0 \leq a_n - \alpha_p < \frac{\epsilon}{3}$, ed $\exists\, m \geq p$ tale che $0 \leq \beta_p - a_m < \frac{\epsilon}{3}$, che implica subito $\beta_p - \alpha_p < \epsilon$.

E quindi dalle considerazioni fatte prima abbiamo subito che

$$\beta_q - \alpha_q < \epsilon \quad \forall q \geq p$$

Per il lemma degli intervalli imbottigliati sappiamo quindi che $\exists\, a \in Q$ con

$$a \in \bigcap_{p\geq 1} [\alpha_p, \beta_p] \qquad \alpha_p \leq a \leq \beta_p \ \ \forall p$$

Vorremmo dimostrare che a è proprio il limite della successione $\{a_n\}$.

Fissato $\eta > 0$ $\exists\, p > 0$ tale che $\beta_p - \alpha_p < \eta$, cioè $(\beta_p - a) + (a - \alpha_p) < \eta$, che implica

$$\begin{array}{l} \beta_p - a \leq \eta \\ a - \alpha_p \leq \eta \end{array} \implies \begin{array}{l} a - \eta \leq \alpha_p \\ a + \eta \geq \beta_p \end{array}$$

Vale quindi $\alpha_p \leq a_n \leq \beta_p \ \ \forall n > p$, da cui

$$\forall n > p \ \text{ vale } \ a - \eta \leq \alpha_p \leq a_n \leq \beta_p \leq a + \eta \quad \Longrightarrow \quad |a_n - a| \leq \eta$$

□

Corollario *I reali di Dedekind e i reali di Cantor sono campi ordinati isomorfi.*

Esercizio 6.3.1 Preso un campo Q possiamo sempre creare $\mathbb{R}(Q)$. Dimostrare che $\mathbb{R}(\mathbb{R}(Q))$ è isomorfo a $\mathbb{R}(Q)$.

6.4 Considerazioni sugli Spazi Metrici

Facciamo alcune considerazioni sugli spazi metrici in generale, di cui $\mathbb{R}$ è un esempio. Prendiamo uno spazio metrico (X, d) (dove d è una *distanza*).

In questo spazio una successione $\{a_n\}$ si dice *di Cauchy* se $\forall \epsilon > 0$ ($\epsilon \in \mathbb{R}$) $\exists p$ tale che $\forall n, m \geq p$ vale $d(a_n, a_m) < \epsilon$.

La successione $\{a_n\}$ *converge* ad $a \in X$ se $\forall \epsilon > 0$ $\exists p$ tale che $\forall n \geq p$ vale $d(a_n, a) < \epsilon$.

Lo spazio (X, d) si dice *Cauchy-completo* se ogni successione di Cauchy converge.

Consideriamo $\mathcal{C}$ lo spazio delle successioni di Cauchy di X. Prese $a = \{a_n\}$, $b = \{b_n\}$ poniamo

$$\widehat{d}(a, b) = \lim_{n \to \infty} d(a_n, b_n)$$

questa è una distanza? In realtà no, ma quasi; Valgono infatti le seguenti proprietà:

- $\widehat{d}(a, b) \geq 0$
- $\widehat{d}(a, b) = \widehat{d}(b, a)$
- $\widehat{d}(a, c) \leq \widehat{d}(a, b) + \widehat{d}(b, c)$

Ma non vale l'importante proprietà che
$\widehat{d}(a, b) = 0 \iff a = b$.

Come risolvo questo problema? Come avevamo già fatto prima: quoziento il campo per la relazione di equivalenza

$$\{a_n\} \sim \{b_n\} \quad \iff \quad \lim_{n \to \infty} |a_n - b_n| = 0$$

ovvero quoziento $\mathcal{C}$ per l'ideale delle successioni infinitesime come avevamo fatto nella costruzione di $\mathbb{R}$ da parte di Cantor, e tutto funziona!

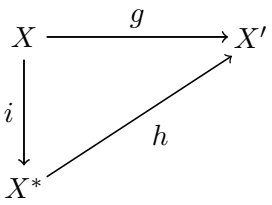
A questo punto $\widehat{d}$ induce una distanza su $\mathcal{C}/_\sim$. Tale spazio metrico è indicato con (X^*, d^*) ed è chiamato *completamento di* X.

(X, d) si immerge isometricamente[9] in (X^*, d^*) con l'applicazione

$$\begin{array}{rcl} i : X & \longrightarrow & X^* \\ x & \longmapsto & [\{x, x, x, \ldots\}] \end{array}$$

Teorema 6.4.1 *Sia (X', d') uno spazio metrico, e sia $g : X \longrightarrow X'$ una isometria tra i due spazi metrici. Allora $\exists! \, h : X^* \longrightarrow X'$ tale che $h \circ i = g$.*

[9] Nel senso che l'applicazione $i : X \longrightarrow X^*$ di immersione le distanze.


X
g
X′
i
h
X*

Capitolo 7

Parte Intera

7.1 Definizione e Prime Proprietà in $\mathbb{R}$

Definizione 7.1.1 Sia $r \in \mathbb{R}$. Chiamiamo *parte intera* di r il numero intero descritto come

$$\lfloor r \rfloor := \max\{n \in \mathbb{Z} \mid n \leq r\}$$

Oppure equivalentemente $\lfloor r \rfloor$ è l'unico intero per cui vale

$$\lfloor r \rfloor \leq r < \lfloor r \rfloor + 1$$

Si dice *parte frazionaria* di r il numero reale

$$r - \lfloor r \rfloor \geq 0$$

Domanda: ma siamo sicuri che la parte intera esiste? Dovremmo sapere di poter estrarre il massimo da un sottoinsieme di $\mathbb{Z}$, quindi cerchiamo di dimostrarlo.

Lemma *Sia $S \subseteq \mathbb{Z}$, $S \neq \emptyset$. Se S è inferiormente (superiormente) limitato in $\mathbb{Z}$ allora S ha minimo (massimo) in $\mathbb{Z}$.*

Dimostrazione: Supponiamo che S sia inferiormente limitato e prendiamo $a \in \mathbb{Z}$ un minorante di S.

Consideriamo $S_{-a} := \{n - a \mid n \in S\}$: $S_{-a} \subseteq \mathbb{N}$ perché $a \leq n \; \forall n \in S$.

Ma in $\mathbb{N}$ sappiamo di poter considerare $m = \min(S_{-a})$, dunque avrò $m = \widehat{n} - a$, da cui $\widehat{n} = \min S$.

Si fa un discorso analogo per S superiormente limitato.

□

Proposizione 7.1.1 *Sia $r \in \mathbb{R}$. Allora $\lfloor r \rfloor$ esiste ed è unica.*

Dimostrazione: Essendo definita come un massimo, se esiste deve essere unica.

Considero $S = \{n \in \mathbb{Z} \mid n \leq r\}$: esso è sicuramente non vuoto e superiormente limitato perché $\mathbb{R}$ è archimedeo, quindi S ha massimo.

□

Benissimo, ora che abbiamo dimostrato che in effetti questa "parte intera" di un reale esiste possiamo iniziare a fare alcune considerazioni su di essa. Iniziamo a capire le principali proprietà di questo numero.

Proposizione 7.1.2 *Siano $r, s \in \mathbb{R}$ e $n \in \mathbb{N}$. Valgono le seguenti proprietà:*

1. $\lfloor r \rfloor + \lfloor s \rfloor \leq \lfloor r + s \rfloor$
2. $\lfloor r \rfloor + \lfloor n \rfloor = \lfloor r + n \rfloor$
3. *se $m > 0$ allora* $0 \leq \lfloor nr \rfloor - n\lfloor r \rfloor \leq n - 1$
4. *se $s > 0$ allora* $\frac{\lfloor sr \rfloor}{s} \leq r \leq \frac{\lfloor sr \rfloor}{s} + \frac{1}{s}$

Dimostrazione: 1. Ovvio.

2. Visto che $n \in \mathbb{N}$ sappiamo che $\lfloor n \rfloor = n$, da cui $\lfloor r \rfloor + \lfloor n \rfloor \leq \lfloor r + n \rfloor$. Supponiamo per assurdo che si abbia $\lfloor r \rfloor + \lfloor n \rfloor < \lfloor r + n \rfloor$.

$$\lfloor r \rfloor + n = \lfloor r \rfloor + \lfloor n \rfloor \leq \lfloor r + n \rfloor - 1 \leq r + n - 1 \Longrightarrow \lfloor r \rfloor \leq r - 1$$

che è un assurdo, quindi l'unica possibilità è che si abbia $\lfloor r \rfloor + \lfloor n \rfloor = \lfloor r + n \rfloor$.

3. Poiché $n\lfloor r \rfloor$ è intero si ha

$$\lfloor r \rfloor \leq r \Longrightarrow n\lfloor r \rfloor \leq nr \Longrightarrow n\lfloor r \rfloor \leq \lfloor nr \rfloor \Longrightarrow 0 \leq \lfloor nr \rfloor - n\lfloor r \rfloor$$

Inoltre $r < \lfloor r \rfloor + 1 \Longrightarrow \lfloor nr \rfloor \leq nr < n\lfloor r \rfloor + n$, e visto che sono tutti interi vale che

$$\lfloor nr \rfloor \leq n\lfloor r \rfloor + n - 1 \Longrightarrow 0 \leq \lfloor nr \rfloor - n\lfloor r \rfloor \leq n - 1$$

4. Di sicuro $\lfloor sr \rfloor \leq sr \leq \lfloor sr \rfloor + 1$, da cui otteniamo la tesi dividendo tutto per s.

□

Facciamo una piccola osservazione: quando consideriamo la parte intera di una frazione di numeri reali $\frac{x}{y}$ cosa otteniamo? Per definizione abbiamo

$$\left\lfloor \frac{x}{y} \right\rfloor = \max \left\{ n \in \mathbb{Z} \;\middle|\; n \leq \frac{x}{y} \right\} = \max\{n \in \mathbb{Z} \mid ny \leq x\}$$

che corrisponde esattamente al *quoziente della divisione euclidea di x per y*. Quindi individuando la parte intera di una frazione non facciamo altro che operare la già conosciuta divisione euclidea.

7.2 Parte Intera nei Gruppi

La nozione di parte intera che abbiamo introdotto nel paragrafo precedente può essere estesa nel caso di gruppi **abeliani**, **ordinati** e **archimedei** nel seguente modo:

Definizione 7.2.1 Sia $(G, \leq)$ un gruppo abeliano ordinato archimedeo. Presi due elementi $x, u \in G$, con $u > 0$, definiamo la *parte intera di x rispetto a u* come

$$\lfloor x : u \rfloor := \max\{n \in \mathbb{Z} \mid nu \leq x\}$$

Oppure equivalentemente $\lfloor x : u \rfloor$ è l'unico intero per cui vale

$$\lfloor x : u \rfloor u \leq x < (\lfloor x : u \rfloor + 1)u$$

Oppure ancora possiamo dire che $\lfloor x : u \rfloor$ è l'unico intero per cui vale

$$x = \lfloor x : u \rfloor u + r \quad \text{con} \quad r \in G,\ 0 \leq r < u$$

In particolare nell'ultima definizione data si pone l'accento nella possibilità di vedere $\lfloor x : u \rfloor$ come *quoziente della divisione euclidea di x per u*.

Esercizio 7.2.1 Dimostrare l'equivalenza tra le definizioni date.

Osservazione Se provassimo a riportare questa definizione nel gruppo dei numeri reali otterremmo quello che avevamo osservato, ovvero che $\lfloor x : u \rfloor = \lfloor \frac{x}{u} \rfloor$. Mentre se lo volessimo riportare al gruppo dei numeri naturali (o interi) otterremmo che $\lfloor x : u \rfloor$ è semplicemente il quoziente euclideo di x diviso u.

Per come è stato definito anche stavolta la parte intera se esiste è unica, e il fatto che esista è assicurato proprio dalle proprietà che sono state richieste sul gruppo G.

Proposizione 7.2.1 *Sia $(G, \leq)$ un gruppo abeliano ordinato archimedeo. Presi $x, y, u \in G$ con $y, u > 0$ valgono le seguenti proprietà:*

1. $\lfloor x : y \rfloor \lfloor y : u \rfloor \leq \lfloor x : u \rfloor$
2. $(\lfloor x : y \rfloor + 1)(\lfloor y : u \rfloor + 1) \geq \lfloor x : u \rfloor + 1$

Dimostrazione: 1 Dalla definizione data si ottiene

$$\lfloor x : y \rfloor \lfloor y : u \rfloor u \leq \lfloor x : y \rfloor y \leq x$$

ma visto che $\lfloor x : u \rfloor$ è definito come il massimo intero tale che $nu \leq x$ si deve avere necessariamente $\lfloor x : y \rfloor \lfloor y : u \rfloor \leq \lfloor x : u \rfloor$.

2 Di nuovo usando una delle definizioni date si ottiene

$$(\lfloor x : y \rfloor + 1)(\lfloor y : u \rfloor + 1)u > (\lfloor x : y \rfloor + 1)y > x \geq \lfloor x : u \rfloor u$$

visto che il gruppo è abeliano e ordinato[1] questo si traduce in $(\lfloor x : y \rfloor + 1)(\lfloor y : u \rfloor + 1) > \lfloor x : u \rfloor$, ovvero $(\lfloor x : y \rfloor + 1)(\lfloor y : u \rfloor + 1) \geq \lfloor x : u \rfloor + 1$.

□

[1] In caso di dubbio si riveda la definizione di nx con $n \in \mathbb{Z}$ e $x \in G$ data nel capitolo sui gruppi ordinati.

Capitolo 8

Rappresentazione Decimale

In questo capitolo vedremo una diversa rappresentazione dei numeri che ha facilitato non poco l'uso dei numeri e delle operazioni nella storia dell'uomo: la **Rappresentazione Decimale**.

Grazie ad essa infatti sono stati resi possibili tutti gli algoritmi di calcolo delle operazioni che ad oggi conosciamo e usiamo abitualmente. Prima dell'utilizzo di una rappresentazione di questo tipo risultava abbastanza difficile compiere operazioni tra numeri grandi, basti pensare a cosa volesse dire sommare o moltiplicare numeri dell'ordine delle migliaia con le cifre romane.

Non bisogna pensare che una rappresentazione di questo tipo non venisse usata perché non se ne sentiva la necessità, tutt'altro: gli spostamenti militari delle grandi quantità di truppe di cui disponeva l'impero romano richiedeva necessariamente un conteggio complesso di divisione dei reparti, dei viveri e quant'altro anche per decine di migliaia di soldati, quindi calcoli di questo tipo erano piuttosto frequenti (poiché lo erano le guerre).

L'introduzione di una rappresentazione dei numeri in base dieci in occidente venne durante la ripresa economica-scientifica del 1400 in cui i commerci con i regni arabi permisero l'importazione da questi popoli delle cifre che usiamo tutt'ora e del sistema di numerazione in base dieci.

Vediamo adesso matematicamente come si definisce e si utilizza questa rappresentazione.

8.1 Numeri Interi

Definizione 8.1.1 Fissiamo un numero naturale $B > 1$ (chiamato *base*) consideriamo un numero intero M per cui vale che

$$\begin{aligned} &M = a_m B^m + a_{m-1} B^{m-1} + \ldots + a_1 B + a_0 \\ &a_i \in \{0, 1, \ldots, B-1\} \ \ \forall i \\ &a_m \neq 0 \end{aligned}$$

Chiamiamo *rappresentazione di M in base B* il seguente simbolo:

$$(a_m a_{m-1} \ldots a_1 a_0)_B$$

E gli interi a_i sono detti *cifre* di M.
Nel caso in cui $B = 10$ scriveremo semplicemente il numero senza parentesi:

$$a_m a_{m-1} \ldots a_1 a_0 := (a_m a_{m-1} \ldots a_1 a_0)_{10}$$

Nota: il simbolo $a_m a_{m-1} \ldots a_1 a_0$ appena introdotto potrebbe essere inteso come rappresentazione decimale di un numero o anche come prodotto degli n termini a_i. Il significato dovrebbe essere chiaro dal contesto ma quando potrebbe esserci confusione indicheremo il prodotto con il solito simbolo " $\cdot$ ", in modo da eliminare fraintendimenti.

Ma siamo sicuri che questa scrittura abbia senso? Cioè un numero naturale (o intero) si può davvero scrivere in questo modo?

Proposizione 8.1.1 *Ogni naturale $M \neq 0$ può essere scritto nella forma $M = a_m a_{m-1} \ldots a_1 a_0$, in cui $m \in \mathbb{N}$, $0 \leq a_i \leq 9 \ \forall i$, $a_m \neq 0$, e i coefficienti a_i sono univocamente determinati da M.*

Dimostrazione: Visto che $\mathbb{N}$ è archimedeo sappiamo che esiste un naturale m per cui vale $10^m \leq M < 10^{m+1}$.

Allora applicando la divisione euclidea sappiamo che esistono due naturali r_m e a_m tali che

$$M = a_m \cdot 10^m + r_m \qquad \text{con } r_m < 10^m,\ 1 \leq a_m \leq 9$$

in cui a_m è compreso tra 1 e 9 perché M è compreso tra 10^m e 10^{m+1}.

Questi due numeri a_m e r_m sono univocamente determinati perché sappiamo che il quoto e il resto della divisione euclidea sono unici.

Possiamo allora applicare di nuovo la divisione euclidea tra r_m e 10^{m-1} ed ottenere

$$r_m = a_{m-1} \cdot 10^{m-1} + r_{m-1} \qquad \text{con } r_{m-1} < 10^{m-1},\ 0 \leq a_{m-1} \leq 9$$

in cui anche stavolta a_{m-1} e r_{m-1} sono univocamente determinati.
Possiamo iterare questo processo fino ad arrivare a

$$r_1 = a_1 \cdot 10 + r_0 = a_1 \cdot 10 + a_0$$

ottenendo così gli interi $a_1, a_2, \dots a_m$ compresi fra 0 e 9 (in cui $a_m \neq 0$) che sono univocamente determinati dall'intero di partenza M tramite divisioni intere delle potenze di 10.

□

Guardando bene questa dimostrazione ci accorgiamo che non abbiamo solamente dimostrato che le cifre di una rappresentazione sono univocamente determinate dal numero di partenza, ma abbiamo anche fornito un *algoritmo* per trovare tali cifre!

L'algoritmo inoltre non dipende in alcun modo dalla base 10 che abbiamo usato e può essere usato per determinare le cifre di un numero in qualsiasi base B, basta sostituire il numero B nelle divisioni euclidee ovunque compaia un 10.

Proposizione 8.1.2 *Preso un naturale $M = a_m \dots a_1 a_0$ per ogni $i = 0, \dots, m$ vagono le seguenti uguaglianze:*

$$\left\lfloor \frac{M}{10^i} \right\rfloor = a_m \dots a_{i+1} a_i$$

$$a_i = \left\lfloor \frac{M}{10^i} \right\rfloor - 10 \cdot \left\lfloor \frac{M}{10^{i+1}} \right\rfloor$$

Dimostrazione: Per definizione della rappresentazione decimale possiamo scrivere M come somma delle sue cifre:

$$\begin{aligned} &M = a_m \cdot 10^m + \dots + a_i \cdot 10^i + a_{i-1} \cdot 10^{i-1} + \dots + a_1 \cdot 10 + a_0 = \\ &= (a_m \cdot 10^{m-i} + \dots + a_{i+1} \cdot 10 + a_i) \cdot 10^i + (a_{i-1} \cdot 10^{i-1} + \dots + a_1 \cdot 10 + a_0) \end{aligned}$$

dal fatto che $0 \leq a_i \leq 9$ otteniamo che $a_{i-1} \cdot 10^{i-1} + \dots + a_1 \cdot 10 + a_0 < 10^i$, da cui otteniamo subito

$$\left\lfloor \frac{M}{10^i} \right\rfloor = a_m \dots a_{i+1} a_i$$

Grazie a questa scrittura la seconda equazione si dimostra subito:

$$\left\lfloor \frac{M}{10^i} \right\rfloor - 10 \cdot \left\lfloor \frac{M}{10^{i+1}} \right\rfloor = (a_m \cdot 10^{m-i} + \dots + a_i) - 10 \cdot (a_m \cdot 10^{m-i-1} + \dots + a_{i+1}) = a_i$$

□

Proposizione 8.1.3 *Presi due naturali $M = a_m \dots a_0$ e $N = b_n \dots b_0$ si ha che $M > N$ se e solo se vale una delle seguenti affermazioni:*

- $m > n$
- $m = n$, $\exists\, k \in \mathbb{N}$ *tale che* $\begin{cases} a_i = b_i & \forall i > k \\ a_k > b_k \end{cases}$

Dimostrazione: $\boxed{\Rightarrow}$ Sappiamo che vale $M > N$.

Se si avesse $m < n$ allora troveremmo che $N \geq 10^n \geq 10^{m+1} > M$, che è assurdo. Quindi di certo $m \geq n$.

Se vale $m > n$ abbiamo la prima tesi; Analizziamo il caso $m = n$: visto che $M \neq N$ deve esistere un indice k per cui si abbia $a_i = b_i \; \forall i > k$ e $a_k \neq b_k$.

Supponiamo per assurdo che valga $a_k < b_k$, ovvero $b_k \geq a_k + 1$. Allora possiamo scrivere

$$\begin{aligned} &N = b_n \cdot 10^n + \dots + b_1 \cdot 10 + b_0 = \\ &= a_m \cdot 10^m + \dots + a_{k+1} \cdot 10^{k+1} + b_k \cdot 10^k + \dots + b_0 \geq \\ &\geq (a_m \cdot 10^m + \dots + a_{k+1} \cdot 10^{k+1}) + (a_k \cdot 10^k + 10^k) + (b_{k-1} \cdot 10^{k-1} + \dots + b_0) \end{aligned}$$

Ma noi sappiamo che $10^k > 9 \cdot 10^{k-1} + \dots + 9 \cdot 10 + 9$, quindi a maggior ragione si avrà $10^k + (b_{k-1} \cdot 10^{k-1} + \dots + b_0) > 9 \cdot 10^{k-1} + \dots + 9 \cdot 10 + 9$. Quindi considerando la disequazione sopra scritta possiamo scrivere che

$$N > (a_m \cdot 10^m + \dots + a_{k+1} \cdot 10^{k+1}) + (a_k \cdot 10^k) + (9 \cdot 10^{k-1} + \dots + 9) \geq M$$

che è assurdo per ipotesi di partenza $M > N$.

Quindi $a_k < b_k$ è assurdo, che dimostra che si debba avere $a_k > b_k$, ovvero la tesi.

$\boxed{\Leftarrow}$ Sappiamo che vale una delle due proprietà scritte sopra.

Se supponiamo che valga $m > n$ allora la tesi si ha subito perché

$$M \geq 10^m \geq 10^{n+1} > N$$

Dunque supponiamo che sia vera la seconda, cioè che si abbia $m = n$ e un indice k per cui $a_i = b_i \; \forall i > k$ e $a_k > b_k$. Anche stavolta la dimostrazione si basa semplicemente nel riscrivere i numeri come somma delle proprie cifre:

$$\begin{aligned} &M = a_m \cdot 10^m + \dots + a_0 = b_n \cdot 10^n + \dots + b_{k+1} \cdot 10^{k+1} + a_k \cdot 10^k + \dots + a_0 \geq \\ &\geq (b_n \cdot 10^n + \dots + b_{k+1} \cdot 10^{k+1}) + (b_k \cdot 10^k + 10^k) + (a_{k-1} \cdot 10^{k-1} + \dots + a_0) > \\ &> (b_n \cdot 10^n + \dots + b_{k+1} \cdot 10^{k+1}) + (b_k \cdot 10^k) + (9 \cdot 10^{k-1} + \dots + 9 \cdot 10 + 9) \geq N \end{aligned}$$

□

Anche stavolta ciò che abbiamo dimostrato è particolarmente significativo: presi due numeri qualsiasi abbiamo individuato un modo molto semplice e veloce per individuare quale dei due è il più grande, cosa in generale abbastanza difficile se si considerano altri tipi di scritture dei numeri!

Osservazione Il fatto di aver usato la base 10 non influisce minimamente nel metodo dimostrativo che abbiamo usato in queste prime tre dimostrazioni, che possono quindi essere ripetute pari pari per qualsiasi base B sostituendo opportunamente in ogni punto 10 con B e 9 con $B-1$.

Fino ad ora abbiamo dunque ottenuto, tra le altre cose, un algoritmo abbastanza efficiente per determinare le cifre di un numero in una qualsiasi base B mostrato nella Proposizione 8.1.1.

Ma ci sono altri modi per fare la stessa cosa e ne possiamo individuare facilmente almeno un altro:

Preso un numero naturale M sappiamo di poterlo scrivere nella forma

$$M = a_m \cdot B^m + \ldots a_1 \cdot B + a_0$$

che è equivalente a scriverlo nella forma

$$M = (a_m \cdot B^{m-1} + \ldots + a_2 \cdot B + a_1) \cdot B + a_0$$

Dunque questo secondo modo di scriverlo ci dà una nuova idea per individuare la prima cifra di M: a_0 può essere individuata direttamente come resto della divisione euclidea di M per B:

$$M = Q_0 \cdot B + a_0$$

in cui il quoziente Q_0 è scritto sopra: $Q_0 = (a_m \cdot B^{m-1} + \ldots + a_2 \cdot B + a_1)$.

A questo punto possiamo riscrivere Q_0 nella forma

$$Q_0 = (a_m \cdot B^{m-2} + \ldots + a_2) \cdot B + a_1$$

Dunque a_1 può essere individuato come resto della divisione euclidea di Q_0 per B:

$$Q_0 = Q_1 \cdot B + a_1$$

in cui il quoziente Q_1 è scritto sopra: $Q_1 = (a_m \cdot B^{m-2} + \ldots + a_3 \cdot B + a_2)$.

Iterando il processo fino a raggiungere a_m abbiamo un nuovo modo di ottenere le cifre di M "inverso" rispetto a prima, ovvero che individua le cifre a partire da a_0 invece che da a_m.

I due algoritmi hanno alla base sempre l'utilizzo della divisione euclidea intera con resto, quindi sono equivalenti dal punto di vista della complessità[1], e possono essere quindi usati a seconda delle necessità.

Fino ad ora abbiamo parlato solo di interi positivi, ma è facile estendere i concetti illustrati fino ad ora agli interi negativi usando una nuova definizione che si rifaccia ai positivi, come abbiamo fatto anche nei capitoli precedenti.

Definizione 8.1.2 Sia M un intero negativo.

Se la rappresentazione di $-M$ (intero positivo) in base B è

$$-M = (a_m a_{m-1} \dots a_1 a_0)_B$$

Allora chiamiamo *rappresentazione di M in base B* il seguente simbolo:

$$-(a_m a_{m-1} \dots a_1 a_0)_B$$

8.2 Numeri Decimali

Definizione 8.2.1 Chiamiamo *numero decimale* un qualsiasi numero razionale D che si possa scrivere nella forma

$$D = \frac{d}{10^n} \qquad d \in \mathbb{Z},\ n \in \mathbb{Z}$$

È importante osservare che tale rappresentazione non è affatto unica, ad esempio $\frac{1}{10} = \frac{10}{100} = \frac{100}{1000} = \dots$, ma se fissiamo l'intero n allora l'intero d è univocamente determinato da D secondo la formula $d = D \cdot 10^n$.

Proposizione 8.2.1 *Sia D un razionale positivo. Allora le seguenti sono equivalenti:*

1. *D è un numero decimale*
2. *D può essere scritto nella forma*

$$D = a_m \cdot 10^m + \dots + a_1 \cdot 10 + a_0 + \frac{a_{-1}}{10} + \dots + \frac{a_{-t}}{10^t}$$

   in cui $a_i \in \{0, 1, \dots, 9\}$ e $m, t \in \mathbb{N}$.

3. *$\forall m, n$ coprimi tali che $D = \frac{m}{n}$ deve valere $n = 2^h 5^k$.*

[1] Non stiamo parlando di *costo computazionale* dei due algoritmi, per cui servirebbe un'analisi più profonda delle operazioni usate, ma solo della complessità dei concetti matematici usati.

Dimostrazione: $\boxed{1 \Rightarrow 2}$ Sappiamo scrivere D nella forma $D = \frac{d}{10^t}$, con $d, t \in \mathbb{N}$.

Ma per i numeri naturali sappiamo scrivere una rappresentazione in base 10, quindi abbiamo

$$D = \frac{d_s \cdot 10^s + \ldots + d_0}{10^t} = d_s \cdot 10^{s-t} + \ldots + d_0 \cdot 10^{-t}$$

Basta quindi porre $m = s - t$ e prendere $a_i = d_{i+t}$ per avere la tesi.

$\boxed{2 \Rightarrow 3}$ Presi due interi p, n coprimi tali che $D = \frac{p}{n}$ possiamo eguagliare questa scrittura con quella che abbiamo per ipotesi ed ottenere:

$$a_m \cdot 10^m + \ldots + a_1 \cdot 10 + a_0 + \frac{a_{-1}}{10} + \ldots + \frac{a_{-t}}{10^t} = \frac{p}{n}$$

$$\frac{a_m \cdot 10^{m+t} + \ldots + a_{-t}}{10^t} = \frac{p}{n}$$

Da cui

$$n \cdot (a_m \cdot 10^{m+t} + \ldots + a_{-t}) = p \cdot 10^t$$

Ma n ed p sono coprimi, quindi se n divide $p \cdot 10^t$ deve necessariamente dividere 10^t, i cui unici divisori sono 2 e 5, da cui abbiamo la tesi.

$\boxed{3 \Rightarrow 1}$ Sappiamo che D si scrive nella forma $D = \frac{d}{2^h 5^k}$, ma allora semplicemente riscriviamo

$$D = \frac{d}{2^h 5^k} = \frac{d \cdot 2^{t-h} 5^{t-k}}{10^t}$$

ed otteniamo la tesi.

□

Osservazione Ancora una volta la dimostrazione proposta non dipende dalla base 10 scelta, quindi può essere ripetuta per una qualunque base B (sostituendo 10 con B dove necessario) se consideriamo invece di "numero decimale" un numero che si scriva nella forma $D = \frac{d}{B^t}$ e invece che potenze di 2 e 5 potenze di tutti i divisori di B.

Avendo caratterizzato i numeri decimali con una scrittura simile a quella che abbiamo introdotto nel paragrafo precedente per i numeri naturali definiamo anche in questo caso una notazione specifica per rappresentarli più comodamente.

Definizione 8.2.2 Sia D un numero razionale scrivibile nella forma

$$D = a_m \cdot B^m + \ldots + a_1 \cdot B + a_0 + \frac{a_{-1}}{B} + \ldots + \frac{a_{-t}}{B^t}$$

Allora chiamiamo *rappresentazione di D in base B* il seguente simbolo:

$$(a_m \ldots a_0, a_{-1} \ldots a_{-t})_B$$

Nel caso in cui la base B sia uguale a 10 scriveremo più brevemente

$$a_m \dots a_0, a_{-1} \dots a_{-t}$$

Ancora una volta le cifre della rappresentazione sono univocamente determinate da D.

Basta infatti considerare l'intero $M = D \cdot 10^t$ e trovare la sua rappresentazione in base B, che sappiamo già essere unica, e riportarla successivamente in D tramite una semplice traslazione di $-t$ degli indici delle cifre.

8.3 Numeri Reali

In questo paragrafo cercheremo di approssimare un numero reale usando i numeri decimali che abbiamo definito nei paragrafi precedenti. Per fare questo ci sono due approcci possibili che hanno alla base lo stesso tipo di ragionamento.

Preso un reale positivo R per la proprietà archimedea sappiamo che esiste un intero m tale che $10^m \leq R < 10^{m+1}$. Pensando alla divisione euclidea dei naturali potremmo dire che "10^m sta $\left\lfloor \frac{R}{10^m} \right\rfloor$ volte in R", dunque se definiamo

$$a_m := \left\lfloor \frac{R}{10^m} \right\rfloor$$

abbiamo che $1 \leq a_m \leq 9$.

Ma allora sicuramente vale $R - a_m 10^m < 10^m$, quindi possiamo definire un nuovo

$$a_{m-1} := \left\lfloor \frac{R - a_m 10^m}{10^{m-1}} \right\rfloor = \left\lfloor \frac{R}{10^{m-1}} - a_m 10 \right\rfloor = \left\lfloor \frac{R}{10^{m-1}} \right\rfloor - a_m 10 =$$

$$= \left\lfloor \frac{R}{10^{m-1}} \right\rfloor - 10 \left\lfloor \frac{R}{10^m} \right\rfloor$$

Iterando questo processo possiamo continuare a definire una successione di termini

$$a_j := \left\lfloor \frac{R}{10^j} \right\rfloor - 10 \left\lfloor \frac{R}{10^{j+1}} \right\rfloor$$

fino ad arrivare al termine $a_0 := \lfloor R \rfloor - 10 \left\lfloor \frac{R}{10} \right\rfloor$.

Ma ci dobbiamo davvero fermare? Nel caso degli interi si, ma coi reali nessuno ci impedisce di proseguire nel nostro ragionamento e definire ancora

$$a_{-1} = \lfloor 10\, R \rfloor - 10 \lfloor R \rfloor$$

E così altri termini a_i con i negativo.

Proseguendo fino ad un certo indice $i = -h$ otterremo una *approssimazione* di R:

$$R - \left(a_m 10^m \ldots + a_0 + \frac{a_{-1}}{10} + \ldots + \frac{a_{-h}}{10^h}\right) < \frac{1}{10^h}$$

E riscrivendo il numero nella scrittura decimale avremo:

$$R - a_m \ldots a_0, a_{-1} \ldots a_{-h} < \frac{1}{10^h}$$

Dunque abbiamo ottenuto di saper scrivere un numero decimale univocamente determinato da R che si "avvicina abbastanza" ad R, dove per "avvicinarsi" intendiamo che la differenza tra i due può essere resa sempre più piccola considerando approssimazioni sempre più precise, ovvero aumentando l'indice h.

Vediamo ora un approccio leggermente diverso, che cerca di approssimare un numero reale in modo differente da quello appena visto.

Definizione 8.3.1 Preso un reale R possiamo chiamare *troncamento* del reale R alla h-esima cifra il numero

$$R_{[h]} := \left\lfloor \frac{R}{10^h} \right\rfloor 10^h$$

La motivazione di tale nome risulta chiara non appena si provi a pensare ad un esempio: preso R=5864,01749 avrò per h=2:

$$R_{[2]} = \left\lfloor \frac{5864,01749}{10^2} \right\rfloor 10^2 = \lfloor 58,6401749 \rfloor \, 10^2 = 5800$$

invece per $h = -3$:

$$R_{[-3]} = \left\lfloor \frac{5864,01749}{10^{-3}} \right\rfloor 10^{-3} = \lfloor 5864017,49 \rfloor \, 10^{-3} = 5864,017$$

Anche stavolta quello che facciamo è scrivere un numero decimale "vicino" al numero reale di partenza R, ma usando un metodo leggermente diverso.

Osservazione La successione dei troncamenti $\left\{R_{[-j]}\right\}_{j\in\mathbb{N}}$ è una successione crescente:

$$R_{[0]} \leq R_{[-1]} \leq \ldots \leq R_{[-h]} \leq \ldots$$

di numeri decimali che approssimano R con precisione determinata dall'indice, infatti

$$0 < R - R_{[-h]} < \frac{1}{10^h}$$

Da ciò possiamo subito dire che

$$\lim_{h\to+\infty} R_{[-h]} = R$$

Proposizione 8.3.1 *Presi $R \in \mathbb{R}$ e $h \in \mathbb{N}$ valgono le seguenti proprietà:*

1. *$R_{[-h]}$ è univocamente determinato da R ed h*
2. *$\forall j$ tale che $1 \leq j \leq h$ vale $\lfloor R \cdot 10^j \rfloor = \lfloor R_{[-h]} \cdot 10^j \rfloor$*
3. *$\forall j$ tale che $1 \leq j \leq h$ vale $a_{-j} = \lfloor R \cdot 10^j \rfloor - 10 \lfloor R \cdot 10^{j-1} \rfloor$*
4. *$\forall j$ tale che $1 \leq j \leq h$ vale che $(R_{[-h]})_{[-j]} = R_{[-j]}$*

Dimostrazione: 1 Questo fatto è dimostrato esattamente come fatto precedentemente: essendo $R_{[-h]}$ ottenuto da R tramite h divisioni euclidee, esso deve per forza essere unico.

2 Dalla disequazione $R \geq R_{[-h]}$ otteniamo subito che $\lfloor R \cdot 10^j \rfloor \geq \lfloor R_{[-h]} \cdot 10^j \rfloor$.
Per ottenere l'altra disequazione partiamo da $R < R_{[-h]} + \frac{1}{10^h}$ e otteniamo

$$\lfloor R \cdot 10^j \rfloor \leq R \cdot 10^j < R_{[-h]} \cdot 10^j + \frac{1}{10^{h-j}} =$$

$$= a_m \dots a_0 a_{-1} \dots a_{-j}, a_{-(j+1)} \dots a_{-h} + \frac{1}{10^{h-j}} =$$

$$= a_m \dots a_0 a_{-1} \dots a_{-j} + 0, a_{-(j+1)} \dots a_{-h} + \frac{1}{10^{h-j}} \leq$$

$$\leq a_m \dots a_0 a_{-1} \dots a_{-j} + 1$$

Da cui otteniamo la disequazione richiesta:

$$\lfloor R \cdot 10^j \rfloor \leq a_m \dots a_0 a_{-1} \dots a_{-j} = \lfloor R_{[-h]} \cdot 10^j \rfloor$$

3 Abbiamo già visto che le cifre a_i possono essere trovate tramite la formula

$$a_i = \left\lfloor \frac{R}{10^i} \right\rfloor - 10 \left\lfloor \frac{R}{10^{i+1}} \right\rfloor$$

quindi sostituendo $i = -j$ otteniamo la tesi.

4 Visto che abbiamo dimostrato che la scrittura è unica questa proprietà è automaticamente verificata se $j \leq h$.

□

Ora possiamo finalmente dare la definizione cardine per quanto riguarda i numeri reali:

Definizione 8.3.2 Si dice *allineamento decimale* un simbolo della forma

$$a_m \dots a_0, a_{-1} a_{-2} \dots$$

in cui $\forall j$ vale $a_j \in \{0, 1, \dots, 9\}$ e $a_m \neq 0$.

Un allineamento si dice poi *improprio* se $\exists\, k \in \mathbb{N}$ tale che $a_{-j} = 9\ \forall j > k$, altrimenti si dice *proprio*.

Esempio 8.3.1 L'allineamento decimale 729,082599999... è improprio;
Mentre 729,082591919191... è proprio.

Proposizione 8.3.2 *Dato un allineamento* $a_m \dots a_0, a_{-1} \dots$ *, la serie*

$$\sum_{j=0}^{m} a_j 10^j + \sum_{j=1}^{\infty} \frac{a_{-j}}{10^j}$$

converge ad un numero reale R *compreso tra 0 e* 10^{m+1}*.*

Dimostrazione: È sufficiente osservare che la serie considerata è maggiorata dalla serie geometrica di ragione $\frac{9}{10}$ che sappiamo essere convergente.

□

Definizione 8.3.3 L'allineamento decimale $a_m \dots a_0, a_{-1} \dots$ si dice *rappresentazione decimale* (o *sviluppo decimale*) di un numero reale R se vale

$$R = \sum_{j=0}^{m} a_j 10^j + \sum_{j=1}^{\infty} \frac{a_{-j}}{10^j}$$

Lemma *Sia* $R > 0$ *un reale positivo, e* $a_m \dots a_0, a_{-1} \dots$ *una sua rappresentazione decimale. Se consideriamo* $\forall h \in \mathbb{N}$ *il decimale*

$$R'_{[-h]} = a_m \dots a_0, a_{-1} \dots a_{-h}$$

le seguenti sono equivalenti:

1. *La rappresentazione è propria*
2. $R'_{[-h]} = R_{[-h]}$
3. *Vale* $0 < R - R'_{[-h]} < \frac{1}{10^h}$

Inoltre R *ammette rappresentazione unica, e se* R *ha una rappresentazione impropria allora è decimale.*

Dimostrazione: Prima di iniziare la dimostrazione osserviamo che vale $R'_{[-h]} = \sum_{j=0}^{m} a_j 10^j + \sum_{j=1}^{h} a_{-j} 10^j$, quindi

$$R - R'_{[-h]} = \sum_{j=h+1}^{\infty} a_{-j} 10^{-j} = \frac{1}{10^h} \left(\sum_{j=1}^{\infty} \frac{a_{-(h+j)}}{10^j} \right) \leq \frac{1}{10^h} \left(\sum_{j=1}^{\infty} \frac{9}{10^j} \right) = \frac{1}{10^h}$$

$\boxed{1 \Rightarrow 2}$ Se non valesse (2) vorrebbe dire che $\exists\, h$ con $R_{[-h]} \neq R'_{[-h]}$.

Ora $R'_{[-h]}$ è un decimale che approssima R per difetto, ma abbiamo già mostrato che $R_{[-h]}$ è l'unico decimale tale che $R - R_{[-h]} < \frac{1}{10^h}$.

Allora deve valere $R - R'_{[-h]} = \frac{1}{10^h}$, ovvero $R = a_m \dots a_0, a_{-1} \dots a_{-h} + \frac{1}{10^h}$, cioè $a_{-(h+1)}10^{-(h+1)} + a_{-(h+2)}10^{-(h+2)} + \dots = \frac{1}{10^h}$.

Ma questo accade solo se $a_{-j} = 9 \ \forall j \geq h+1$, da cui abbiamo che la rappresentazione è impropria, che è assurdo per ipotesi.

$\boxed{2 \Rightarrow 3}$ Niente da dimostrare, visto che $R'_{[-h]} = R_{[-h]}$ e sappiamo che la proprietà vale per $R_{[-h]}$.

$\boxed{3 \Rightarrow 1}$ Se non valesse (1) avremmo che la rappresentazione è impropria, ovvero $\exists\, h$ tale che $a_{-j} = 9 \ \forall j > h$.

Ma allora

$$R - R'_{[-h]} = \sum_{j=h+1}^{\infty} 9 \cdot 10^{-j} = \frac{1}{10^h} \left(\sum_{j=1}^{\infty} 9 \cdot 10^{-j} \right) = \frac{1}{10^h}$$

che è assurdo.

Da tutto ciò abbiamo che se R ha una rappresentazione impropria allora è decimale. Se la rappresentazione è propria è unica perché i coefficienti sono univocamente determinati come al solito.

□

Tutto ciò che abbiamo discusso fino ad ora può essere riassunto in un unico grande teorema di rappresentazione.

Teorema 8.3.1 (Rappresentazione Decimale dei Numeri Reali) *Sia R un reale positivo, e $a_m \dots a_0, a_{-1} \dots$ un allineamento decimale in cui $\forall h$ $a_m \dots a_0, a_{-1} \dots a_{-h}$ è la rappresentazione decimale del troncamento $R_{[-h]}$.*

Valgono allora le seguenti affermazioni:

- *$a_m \dots a_0, a_{-1} \dots$ è una rappresentazione decimale propria di R.*
- *$\forall j = m, m-1, \dots 0, -1, \dots$ vale $a_j = 10^j \left\lfloor \frac{R}{10^j} \right\rfloor - 10 \left\lfloor \frac{R}{10^{j+1}} \right\rfloor$.*
- *Se R non è decimale questa è l'unica rappresentazione decimale di R.*
- *Se $R \neq 0$ è decimale allora ammette un'unica rappresentazione decimale finita a patto di eliminare scritture in cui $a_{-j} = 0 \ \forall j > h$ fissato.*
- *L'applicazione che manda un reale R positivo nella sua rappresentazione decimale propria è una bigezione.*

Dimostrazione: Innanzitutto la definizione è ben posta per ciò che abbiamo dimostrato finora. Anche il fatto che l'allineamento sia proprio è già dimostrato, e che la rappresentazione è unica ed ha quelle cifre lì.

Se R non è decimale allora non ha rappresentazione decimali improprie, quindi la rappresentazione definita è unica. Se R è decimale, oltre alla rappresentazione definita sopra, ammette un'unica rappresentazione impropria.

Infine ogni reale positivo ammette una ed una sola rappresentazione propria, così la funzione è iniettiva, ma ogni decimale proprio converge ad un reale positivo, quindi l'applicazione è anche surgettiva.

□

Attenzione! Non bisogna confondere il numero con la sua rappresentazione!

Nota: tutto ciò che si è dimostrato poteva essere detto senza problemi in una base generica B, cosicché tutti i teoremi possono essere considerati validi in ogni base.

Capitolo 9

Allineamenti Periodici

9.1 Definizioni

Anche i numeri razionali, come i reali, possono essere approssimati in vari modi. Una delle prime idee che possono sorgere è suggerita dalla divisione euclidea, vediamone un esempio.

Il razionale $\frac{7}{4}$ si può calcolare così:

$$7 = 4 \cdot 1 + 3 \Longrightarrow \frac{7}{4} = 1 + \frac{3}{4}$$

quindi ad un primo approccio approssimiamo $\frac{7}{4}$ con 1 scartando il resto $\frac{3}{4}$, che non è un granché come approssimazione...

Proviamo allora così:

$$7 \cdot 10 = 4 \cdot 17 + 2 \Longrightarrow 7 = 4 \cdot \frac{17}{10} + \frac{2}{10} \Longrightarrow \frac{7}{4} = \frac{17}{10} + \frac{2}{4 \cdot 10}$$

quindi lo approssimiamo con $\frac{17}{10}$, che già va meglio.

Potremmo procedere in questo modo per fare approssimazioni via via sempre migliori, l'idea l'abbiamo capita.

Questo metodo si chiama il **Metodo delle Approssimazioni Successive**.

Definizione 9.1.1 Presi $M, N \in \mathbb{N}$, $N \neq 0$ associamo al numero razionale $\frac{M}{N}$ l'allineamento decimale

$$q_k \dots q_0, q_{-1} \dots$$

in cui per ogni h l'allineamento $q_k \dots q_0 q_{-1} \dots q_{-h}$ rappresenta il quoziente della divisione euclidea di $M \cdot 10^h$ per N.

Proposizione 9.1.1 *Preso $R = \frac{M}{N}$ con $M, N \in \mathbb{N}$, $N \neq 0$, la rappresentazione propria di R è nella forma $q_k \dots q_0, q_{-1} \dots$ dove $\forall h$ $q_k \dots q_0 q_{-1} \dots q_{-h}$ è la rappresentazione decimale finita del quoto euclideo della divisione tra $M \cdot 10^h$ ed N.*

Dimostrazione: Abbiamo detto che vale $\left\lfloor \frac{M \cdot 10^h}{N} \right\rfloor = q_k \dots q_0 q_{-1} \dots q_{-h}$

Allora se $R = \frac{M}{N}$:

$$R_{[-h]} = \frac{\left\lfloor \frac{M}{N} 10^h \right\rfloor}{10^h} = q_k \dots q_0, q_{-1} \dots q_{-h}$$

□

Vediamo qual'è in generale l'algoritmo per rappresentare il razionale $R = \frac{M}{N}$:

Sia $q_k \dots q_0$ la rappresentazione decimale della parte intera di R, cioè il quoto euclideo di M per N.

Vale $M = N \left\lfloor \frac{M}{N} \right\rfloor + r_0$

Ora consideriamo la divisione euclidea $r_0 \cdot 10 = N \cdot q_{-1} + r_{-1}$, così da trovare q_{-1} come quoziente e r_{-1} come resto per cui vale $0 \leq r_{-1} \leq N - 1$.

Possiamo continuare e trovare q_{-2} con lo stesso metodo: $r_{-1} \cdot 10 = N \cdot q_{-2} + r_{-2}$, in cui di nuovo $0 \leq r_{-2} \leq N - 1$.

Possiamo proseguire ancora con lo stesso metodo, ma otterremo sempre resti che stanno tra 0 e $N - 1$, quindi al massimo dopo N passaggi riotterremo un resto già avuto, che ci porta ad un quoziente già visto, ovvero si ottiene un *periodo*.

Vediamo un esempio per chiarire le cose: consideriamo il razionale $R = \frac{M}{N} = \frac{57}{11}$.

La divisione euclidea ci da come risultato $57 = 11 \left\lfloor \frac{57}{11} \right\rfloor + r_0 = 11 \cdot 5 + 2$.

Ora possiamo considerare la divisione di $r_0 \cdot 10$ per N ed ottenere $2 \cdot 10 = 11 \cdot 1 + 9$. Quindi abbiamo trovato la prima cifra dopo la virgola, ovvero il quoziente di questa divisione: $q_{-1} = 1$, e il resto con cui faremo la prossima divisione: $r_{-1} = 9$.

Ora proseguiamo considerando la divisione di $r_{-1} \cdot 10$ per N, che ci individua la prossima cifra decimale: $9 \cdot 10 = 11 \cdot 8 + 2$. Quindi abbiamo $q_{-2} = 8$ e $r_{-2} = 2$

Proviamo a proseguire ancora: la divisione di $r_{-2} \cdot 10$ per N sarà $2 \cdot 10 = 11 \cdot 1 + 9$, quindi la terza cifra decimale sarà $q_{-3} = 1$ e il resto $r_{-3} = 9$.

E ancora: la divisione di $r_{-3} \cdot 10$ per N sarà $9 \cdot 10 = 11 \cdot 8 + 2$, quindi $q_{-4} = 8$.

Dobbiamo proseguire ancora? In realtà no, perché continueremo ad ottenere gli stessi quozienti 1 e 8 con gli stessi resti 9 e 2. Quindi diremo che "18 è il *periodo* della divisione".

Tutto questo possiamo riassumerlo in una definizione:

Definizione 9.1.2 Consideriamo l'allinamento decimale $a_m \dots a_0, a_{-1} \dots$.

Se $\exists\, s, k \in \mathbb{N}$ tali che $\forall j > 0$ si ha $a_{-(s+j)} = a_{-(s+j+n)}$ si dice che l'allineamento è *periodico* di periodo $a_{-(s+1)} \dots a_{-(s+k)}$.

In questo caso k è detta *lunghezza* del periodo, e $a_{-1} \dots a_{-s}$ è chiamato *antiperiodo*.

Osservazione Con le definizioni date il periodo e l'antiperiodo sono assolutamente non unici: il numero 0,7151515... può avere periodo 15 e antiperiodo 0,7 , oppure periodo 1515 e antiperiodo 0,7 , o ancora periodo 5151 e antiperiodo 0,71.

Definizione 9.1.3 Consideriamo un allineamento periodico $a_m \dots a_0, a_{-1} \dots$.

Sia p la lunghezza minima di tutti i possibili periodi. Il *periodo minimo* dell'allineamento è il periodo di lunghezza p che ha antiperiodo di lunghezza s minima tra tutti i possibili antiperiodi connessi con i periodi di lunghezza p.

Se $s = 0$ l'allineamento si dice periodico *semplice*, altrimenti periodico *misto*.

Esempio 9.1.1 Riprendendo l'esempio di prima, il numero 0,7151515... ha molti periodi possibili: 15, 1515, 51, 515151, e così via.

La lunghezza minima in questo caso sarà p=2, e ad ogni periodo di lunghezza 2 potremmo associare un antiperiodo diverso, ad esempio possiamo considerare il periodo 15 con antiperiodo 0,71515 , oppure il periodo 51 con antiperiodo 0,71 o 0,7151 e molti altri ancora.

Tra tutti questi antiperiodi quello di lunghezza minima è 0,7 , in cui consideriamo il periodo 15.

Quindi per il numero 0,71515... il "periodo minimo" sarà 15 con antiperiodo 0,7.

Proposizione 9.1.2 *Preso un allineamento periodico $a_m \dots a_0, a_{-1} \dots$ di antiperiodo lungo s. Se $a_{-(S+1)} \dots a_{-(S+k)}$ è un periodo allora $s \leq S$.*

Dimostrazione: Visto che la lunghezza dell'antiperiodo è s prendiamo $a_{-(s+1)} \dots a_{-(s+p)}$ il periodo minimo.

Supponiamo per assurdo che $s > S$; Basterà verificare che $a_{-s} = a_{-(s+p)}$, infatti in tal caso $a_{-s} \dots a_{-(s+p-1)}$ è periodo di lunghezza minore del minimo, che porta ad un assurdo.

Certo $k \geq p$, dunque possiamo applicare la divisione euclidea e ottenere $k = mp + r$ con $m > 0$ e $0 \leq r < p$.

$\forall j > 0$ abbiamo che $a_{-(s+j)} = a_{-(s+j+p)}$ e inoltre $a_{-(S+j)} = a_{-(S+j+k)} = a_{-(S+j+mp+r)}$.

Poiché $s - S > 0$ per $j = s - S$ dalla seconda equazione abbiamo che

$$a_{-s} = a_{-(S+j)} = a_{-(S+j+mp+r)} = a_{-(S+s-S+mp+r)} = a_{-(s+mp+r)}$$

mentre per $j = s - S + p$ da entrambe le equazioni otteniamo

$$a_{-(s+p)} = a_{-(S+j)} = a_{-(S+s-S+p+mp+r)} = a_{-(s+mp+r+p)} = a_{-(s+mp+r)}$$

Da cui $a_{-s} = a_{-(s+p)}$, che è un assurdo per quanto detto prima.

□

Esercizio 9.1.1 Dimostrare che $\frac{286}{999}$=0,286286286286=0,$\overline{286}$.

Svolgimento: Dimostriamolo in forma generale: ogni allineamento periodico semplice $0,\overline{a_{-1}\dots a_{-k}}$ rappresenta il numero razionale

$$R = \frac{a_{-1}\dots a_{-k}}{10^k - 1} = \frac{a_{-1}\dots a_{-k}}{\underbrace{9\dots 9}_{k\ volte}}$$

Questo perché la prima divisione da fare nell'algoritmo è $(a_{-1}\dots a_{-k})\cdot 10$ diviso 10^k-1, che darà quoziente a_{-1} e resto $a_{-2}\dots a_{-k}a_{-1}$.

Poi dovremo fare $(a_{-2}\dots a_{-k}a_{-1})\cdot 10$ diviso 10^k-1, che stavolta darà quoziente a_{-2} e resto $a_{-3}\dots a_{-k}a_{-1}a_{-2}$.

Andando avanti così otterremo esattamente l'allineamento $0,\overline{a_{-1}\dots a_{-k}}$.

□

Osservazione Seguendo ciò che abbiamo dimostrato poco fa otteniamo

$$0,9999999 = 0,\overline{9} = \frac{9}{9} = 1$$

Che è una semplice dimostrazione di un fatto notoriamente ostico da digerire per moltissimi studenti!

9.2 Frazione Generatrice

Con quello che abbiamo trovato fin'ora possiamo già pensare a trovare un metodo per associare ad un allineamento decimale qualsiasi un numero razionale, che è la famosa **Frazione Generatrice**.

Proposizione 9.2.1 *Sia $a_q\dots a_0, a_{-1}\dots a_{-s}\overline{a_{-(s+1)}\dots a_{-(s+k)}}$ un allineamento decimale periodico.*

L'allineamento rappresenta il razionale $R = \frac{a}{b}$ con

$$a = a_q\dots a_0a_{-1}\dots a_{-s}\dots a_{-(s+k)} - a_q\dots a_0a_{-1}\dots a_{-s}$$
$$b = 10^s(10^k-1)$$

Dimostrazione: Scrivo il numero R nella forma:

$$R = a_q\dots a_0, a_{-1}\dots a_{-s} + 10^{-s}\cdot\left(0,\overline{a_{-(s+1)}\dots a_{-(s+k)}}\right)$$

Da ciò che abbiamo dimostrato nell'esercizio precedente (3.1.1) otteniamo che

$$R = 10^{-s}(a_q\dots a_0a_{-1}\dots a_{-s}) + 10^{-s}\frac{a_{-(s+1)}\dots a_{-(s+k)}}{10^k-1}$$

Da cui otteniamo subito

$$R \cdot 10^s(10^k - 1) = (10^k - 1)(a_q \dots a_0 a_{-1} \dots a_{-s}) + a_{-(s+1)} \dots a_{-(s+k)} =$$

$$= a_q \dots a_0 a_{-1} \dots a_{-s} \overbrace{0 \dots 0}^{k \text{ volte}} + a_{-(s+1)} \dots a_{-(s+k)} - a_q \dots a_0 a_{-1} \dots a_{-s} =$$

$$= a_q \dots a_0 a_{-1} \dots a_{-s} a_{-(s+1)} \dots a_{-(s+k)} - a_q \dots a_0 a_{-1} \dots a_{-s}$$

che è proprio quello che dovevamo mostrare.

□

Definizione 9.2.1 La frazione $\frac{a}{b}$ trovata nella precedente proposizione (9.2.1) è detta *frazione generatrice* dell'allineamento periodico dato.

Proposizione 9.2.2 *Sia $a_q \dots a_0, a_{-1} \dots a_{-n} \dots$ un allineamento periodico di periodo $a_{-(s+1)} \dots a_{-(s+k)}$ e antiperiodo lungo s. Allora posso scrivere l'allinemento nella forma*

$$a_q \dots a_0, a_{-1} \dots a_{-s} + 10^{-s} \left(0, a_{-(s+1)} \dots a_{-(s+k)}\right) \left(1 + \frac{1}{10^k} + \frac{1}{10^{2k}} + \dots\right)$$

Dimostrazione: Vale

$$a_q \dots a_0, a_{-1} \dots a_{-n} \dots =$$

$$= a_q \dots a_0, a_{-1} \dots a_{-s} + 10^{-s} \left(\left(0, a_{-(s+1)} \dots a_{-(s+k)}\right) + \frac{1}{10^k} \left(0, a_{-(s+1)} \dots a_{-(s+k)}\right) + \right.$$

$$\left. + \frac{1}{10^{2k}} \left(0, a_{-(s+1)} \dots a_{-(s+k)}\right) + \quad \dots \right) =$$

$$= a_q \dots a_0, a_{-1} \dots a_{-s} + 10^{-s} \left(\sum_{j=1}^{\infty} \left(\frac{1}{10^k}\right)^j \right) \left(0, a_{-(s+1)} \dots a_{-(s+k)}\right)$$

Ma sappiamo che la serie converge

$$\sum_{j=1}^{\infty} \left(\frac{1}{10^k}\right)^j = \frac{1}{1 - \frac{1}{10^k}} = \frac{10^k}{10^k - 1}$$

da cui otteniamo la tesi.

□

Proposizione 9.2.3 *Sia $R \in \mathbb{R}$, $R > 0$ con allineamento decimale $a_q \dots a_0, a_{-1} \dots$. Allora vale che*

$$R \text{ è razionale } \iff a_q \dots a_0, a_{-1} \dots \text{ è allineamento periodico}$$

Se $R = \frac{a}{b} \in \mathbb{Q}$ la somma del numero delle cifre del periodo minimo e dell'antiperiodo dell'allineamento non supera b.

Dimostrazione: $\boxed{\Leftarrow}$ Se l'allineamento è periodico abbiamo già mostrato nella proposizione 9.2.1 che è possibile trovare una frazione che rappresenti R (la frazione generatrice).

$\boxed{\Rightarrow}$ Abbiamo $R = \frac{a}{b}$.

La rappresentazione $a_q \dots a_0, a_{-1} \dots$ è quella data dall'algoritmo di divisione euclidea con divisore b ad ogni passo. Ma allora i possibili resti variano tra 0 e $b-1$, quindi al più dopo b passi i resti si ripetono: $\exists\, m, n$ tali che $r_{-m} = r_{-(m+n)}$.

Chiamiamo j e k i minimi indici m, n per cui vale questo fatto.

Dall'algoritmo di divisione euclidea abbiamo che

$$r_{-j} \cdot 10 = b \cdot a_{-(j+1)} + r_{-(j+1)}$$
$$r_{-(j+k)} \cdot 10 = b \cdot a_{-(j+k+1)} + r_{-(j+k+1)}$$

Ma se $r_{-j} = r_{j+k}$ vale anche $r_{-(j+1)} = r_{-(j+k+1)}$.

Allo stesso modo si ripeterà che $r_{-(j+2)} = r_{-(j+k+2)}$ e così via, quindi otteniamo che l'allineamento è necessariamente periodico.

In particolare l'allineamento avrà periodo lungo k e antiperiodo lungo $s = j - 1$

Sapendo che i primi $k + s$ resti assumono tutti valori differenti abbiamo che $k + s \leq b$.

□

9.3 Proprietà degli Allineamenti Periodici

Proposizione 9.3.1 *Siano $a, b \in \mathbb{N}$ primi tra loro con $b > 1$. Sia $R = \frac{a}{b}$. Valgono le seguenti proprietà:*

1. *Se $b = 2^r 5^t$ allora R è decimale con $s := \max\{r, t\}$ cifre dopo la virgola*
2. *Se né 2 né 5 dividono b allora R non è decimale e la rappresentazione decimale è periodica semplice*
3. *Se b ammette tra i divisori 2 o 5 ed altri primi allora R non è decimale e la sua rappresentazione decimale è periodica mista*

Dimostrazione: $\boxed{1}$ Poniamo che $s > 0$ (altrimenti $b = 1$ e tutto è banale). Allora

$$\frac{a}{b} = \frac{2^{s-r} 5^{s-t} a}{10^s}$$

quindi R è sicuramente decimale.

Se chiamiamo $d = 2^{s-r} 5^{s-t} a$ possiamo scrivere $d = d_q \dots d_0$, in cui deve essere $d_0 \neq 0$, altrimenti d sarebbe multiplo di 10, che non è possibile per come è definito s.

Visto che dividiamo d per 10^s otterremo quindi un numero decimale con s cifre dopo la virgola.

2 Supponiamo per assurdo che lo sviluppo non sia semplice. Ne segue che

$$\frac{a}{b} = a_q \dots a_0, a_{-1} \dots a_{-s}\overline{a_{-(s+1)} \dots a_{-(s+k)}}$$

Sia $\frac{m}{n}$ la frazione generatrice di tale sviluppo, per cui

$$\begin{aligned} m &= a_q \dots a_0, a_{-1} \dots a_{-s} a_{-(s+1)} \dots a_{-(s+k)} - a_q \dots a_0, a_{-1} \dots a_{-s} \\ n &= 10^s(10^k - 1) \end{aligned}$$

Dunque abbiamo

$$\frac{a}{b} = \frac{m}{n} \quad \Longrightarrow \quad bm = an = a\,10^s(10^k - 1)$$

Poiché b è coprimo con 10 ne segue che 10 deve dividere m, che equivale a dire che m ha ultima cifra uguale a zero. Ma sappiamo che l'ultima cifra di m è data dalla differenza $a_{-(s+k)} - a_{-s}$. Allora

$$a_{-(s+k)} - a_{-s} = 0 \Longrightarrow a_{-(s+k)} = a_{-s} \Longrightarrow a_{-s} \dots a_{-(s+k-1)} \text{ è un periodo}$$

il che è assurdo.

3 Supponiamo per assurdo che R ammetta una rappresentazione decimale semplice, e sia $\frac{m}{n}$ la sua frazione generatrice, da cui di nuovo otteniamo che

$$\frac{a}{b} = \frac{m}{n} = \frac{m}{10^k - 1} \quad \Longrightarrow \quad mb = an = a(10^k - 1)$$

Il che ci dice che b divide $10^k - 1$, che non può essere vero perché né 2 né 5 dividono $10^k - 1$, ma almeno uno dei due divide b.

□

Ora vogliamo riformulare il Teorema di Rappresentazione dimostrato nel capitolo sui numeri reali nel caso dei numeri razionali. Per farlo dimostreremo prima un lemma che semplifica notevolmente la dimostrazione del teorema stesso.

Lemma *Siano a, b naturali coprimi con $b > a$ tali che $b = 2^r 5^t b'$ con b' non divisibile per 2 e 5.*

Allora $\frac{a}{b}$ ammette una rappresentazione decimale con antiperiodo lungo $s = \max\{r, t\}$ e periodo minimo lungo $p = \min_n\{10^n \equiv 1 \pmod{b'}\}$.

Inoltre il periodo minimo di $\frac{a}{b}$ è il periodo minimo di $\frac{r'}{b'}$ dove r' è il resto della divisione di $2^{s-r}5^{s-t}a$ per b'.

Dimostrazione: Sia s la lunghezza dell'antiperiodo di $\frac{a}{b}$, e P la lunghezza del periodo minimo. Scriviamo quindi $\frac{a}{b}$ in forma di allineamento:

$$\frac{a}{b} = a_q \dots a_0, a_{-1} \dots a_{-s} a_{-(s+1)} \dots a_{-(s+P)} \dots$$

Se prendiamo la frazione generatrice $\frac{m}{n}$ dell'allineamento appena scritto sappiamo che

$$\begin{aligned} m &= a_q \dots a_0 a_{-1} \dots a_{-s} a_{-(s+1)} \dots a_{-(s+P)} - a_q \dots a_0 a_{-1} \dots a_{-s} \\ n &= 10^s(10^P - 1) \end{aligned}$$

Procediamo ora in questo modo: mostriamo innanzitutto che il periodo minimo di $\frac{r'}{b'}$ è il periodo di $\frac{a}{b}$:

Sia $d = \max\{r, t\}$. Allora scriviamo

$$\frac{a}{b} = \frac{a}{2^r 5^t b'} = \frac{2^{d-r}5^{d-t}a}{10^d b'}$$

Consideriamo la divisione euclidea $2^{d-r}5^{d-t}a = q' \cdot b' + r'$, in cui $r' < b'$. Ne segue che

$$\frac{a}{b} = \frac{2^{d-r}5^{d-t}a}{10^d b'} = \frac{q'b' + r'}{10^d b'} = \frac{q'}{10^d} + \frac{r'}{10^d b'}$$

Supponiamo di avere k divisore primo di b' e r'. Certo $k \neq 2$, $k \neq 5$, inoltre k divide $2^{d-r}5^{d-t}a$, quindi deve necessariamente dividere a. Ma k divide anche b, il che è assurdo perché a e b sono coprimi per ipotesi.

Quindi in realtà b' e r' sono coprimi.

Sia ora p la lunghezza del periodo minimo di $\frac{r'}{b'}$. Essendo r' e b' coprimi la rappresentazione decimale di questo razionale è semplice:

$$\frac{r'}{b'} = 0, \overline{c_{-1} \dots c_{-p}}$$

Dunque

$$\frac{r'}{10^d b'} = 0, \overbrace{0 \dots 0}^{d \text{ volte}} \overline{c_{-1} \dots c_{-p}}$$

A questo punto consideriamo $\frac{q'}{10^d}$: esso è un decimale con non più di d cifre dopo la virgola.

Se $q' = q_g \dots q_d \dots q_0$ abbiamo che

$$\frac{a}{b} = \frac{q'}{10^d} + \frac{r'}{10^d b'} = q_g \dots q_d, q_{d-1} \dots q_0 + 0, \overbrace{0 \dots 0}^{d \text{ volte}} \overline{c_{-1} \dots c_{-p}} =$$

$$= q_g \dots q_d, q_{d-1} \dots q_0 \overline{c_{-1} \dots c_{-p}}$$

Quindi $c_{-1} \dots c_{-p}$ è un periodo di $\frac{a}{b} \Longrightarrow p \geq P$.

Ora dimostriamo che $s = d$:

Sappiamo già che $s \leq d = \max\{r, t\}$, e possiamo supporre senza perdita di generalità che sia $t = d > 0$, da cui $d - r \geq 0$.

Vale $\frac{a}{b} = \frac{m}{n} \Longrightarrow na = mb \Longrightarrow 10^s(10^P - 1)a = m2^r 5^t b'$.

Allora abbiamo che $10^s(10^P - 1)2^{d-r}5^{d-t}a = m10^d b'$, ma abbiamo posto $d = t$, quindi

$$(10^P - 1)2^{d-r}a = m10^{d-s}b'$$

A questo punto abbiamo che se $d \neq s$ nel membro di destra compare un fattore 10, e l'unica possibilità che questo divida il membro di sinistra è che divida a, il che non è possibile perché a e b sono coprimi.

Quindi $s = d$.

Terzo passo: Dimostriamo che i periodi sono gli stessi, ovvero che $c_{-1} \dots c_{-p}$ è periodo minimo di $\frac{a}{b}$.

Per fare ciò dobbiamo mostrare che $p = P$ e che $c_{-1} \dots c_{-p} = a_{-(s+1)} \dots a_{-(s+P)}$.

Eguagliando le due scritture di $\frac{a}{b}$ che abbiamo trovato otteniamo

$$a_q \dots a_0, a_{-1} \dots a_{-s} \overline{a_{-(s+1)} \dots a_{-(s+P)}} = q_g \dots q_d, q_{d-1} \dots q_0 \overline{c_{-1} \dots c_{-p}}$$

Ma abbiamo mostrato che $s = d$, quindi $a_{-1} \dots a_{-s} = q_{d-1} \dots q_0$ e $\overline{a_{-(s+1)} \dots a_{-(s+P)}} = \overline{c_{-1} \dots c_{-p}}$. Inoltre questi due sono periodi minimi, quindi si deve avere necessariamente $p = P$.

Quarto passo: Esplicitiamo p.

Vale

$$\frac{r'}{b'} = 0, \overline{c_{-1} \dots c_{-p}} = \frac{c_{-1} \dots c_{-p}}{10^p - 1}$$

Da cui $r'(10^p - 1) = b' \cdot c_{-1} \dots c_{-p}$.

Ma abbiamo dimostrato che r' e b' sono coprimi, quindi dall'ultima equazione abbiamo che b' divide $10^p - 1$.

Ora vorremmo dimostrare che p è il più piccolo naturale per cui $b' \big| 10^p - 1$.

Supponiamo per assurdo che $\exists\, j < p$ tale che $b' \big| 10^j - 1$. Da ciò scriviamo $kb' = 10^j - 1$, quindi

$$\frac{r'}{b'} = \frac{kr'}{kb'} = \frac{kr'}{10^j - 1}$$

Visto che $r' < b'$ si avrà $kr' < 10^j - 1$, il che ci dice che il numero di cifre di kr' è $\leq j$. Allora è possibile identificare un periodo di $\frac{r'}{b'}$ di j cifre, ma p è la lunghezza del periodo minimo, quindi $p \leq j$, il che contrasta con l'ipotesi di partenza.

Quindi abbiamo $p = \min_n\{10^n \equiv 1 \pmod{b'}\}$ come volevamo, che conclude la nostra dimostrazione.

□

Una volta dimostrato questo grosso lemma siamo pronti per enunciare il teorema principale di questo capitolo.

Teorema 9.3.1 (Rappresentazione Decimale dei Numeri Razionali) *Siano $a, b \in \mathbb{N}$ coprimi, con $b > 1$. Sia $R = \frac{a}{b}$, $b = 2^r 5^t b'$, con b' coprimo con 10, $s = \max\{r, t\}$ e p la lunghezza del periodo minimo di R. Valgono le seguenti:*

1. *Se b ammette per diviori primi 2,5 e nessun altro allora R è decimale con s cifre significative dopo la virgola.*

2. *Se b non ammette per divisori primi né 2 né 5 allora R non è decimale e la sua rappresentazione decimale propria è semplice.*

3. *Se b ammette 2 o 5 come divisori primi e ne ammette altri, R non è decimale e la sua rappresentazione decimale è mista con antiperiodo di lunghezza s e periodo minimo di lunghzza p. Il periodo minimo di R è il periodo minimo di $\frac{r'}{b'}$ quando r' sia il rest della divisione di $2^{s-r}5^{s-t}a$ per b'.*

Dimostrazione: Possiamo assumere $a < b$, poiché se si avesse $a \geq b$ potremmo considerare $c = a - \left\lfloor \frac{a}{b} \right\rfloor b < b$ per cui vale

$$\frac{c}{b} = \frac{a}{b} - \left\lfloor \frac{a}{b} \right\rfloor b$$

Il teorema a questo punto è dimostrato dal lemma precedente.

□

Esercizio 9.3.1 Dimostrare che preso un qualsiasi b coprimo con 10 esiste sempre $p \in \mathbb{N}$ tale che $b \big| 10^p - 1$.

9.4 Allineamenti Periodici in Base B

Estendiamo tutto ciò che abbiamo fatto in questo capitolo ad una base qualsiasi B:

Consideriamo $\frac{M}{N}$ con M, N interi in base B: $\frac{M}{N} = (q_n \dots q_0, q_{-1} \dots q_{-h} \dots)_B$.

Se r_0 è il resto della divisione di M per N l'algoritmo è sempre il solito:

$$\begin{aligned} r_0 B &= N q_{-1} + r_{-1} && 0 \le r_{-1} < N \\ r_{-1} B &= N q_{-2} + r_{-2} && 0 \le r_{-2} < N \\ &\vdots \\ r_{-h} B &= N q_{-(h-1)} + r_{-(h-1)} && 0 \le r_{-(h-1)} < N \end{aligned}$$

Dato l'allineamento $\left(a_q \dots a_0, a_{-1} \dots a_{-s}\overline{a_{-(s+1)} \dots a_{-(s+k)}}\right)_B$ esso rappresenta il numero $\frac{m}{n}$ con

$$\begin{aligned} m &= (a_q \dots a_0 a_{-1} \dots a_{-s} a_{-(s+1)} \dots a_{-(s+k)})_B - (a_q \dots a_0, a_{-1} \dots a_{-s})_B \\ n &= (10)_B^s ((10)_B^k - (1)_B) \end{aligned}$$

Prendiamo ora un naturale $B > 1$ e la sua decomposizione in fattori primi: $B_1^{r_1} \dots B_n^{r_n}$. Sia b un altro naturale che scriviamo come $b = B_1^{t_1} \dots B_n^{t_n} b'$, dove b' è coprimo con B e gli esponenti possono anche essere nulli.

Se ora indichiamo con $s = s(B, b) \ge 0$ il più piccolo naturale non nullo per cui B^s sia multiplo di $B_1^{t_1} \dots B_n^{t_n}$ vale un interessante teorema (che non dimostreremo):

Teorema 9.4.1 *Sia B naturale con scomposizione in fattori primi del tipo: $B_1^{r_1} \dots B_n^{r_n}$. Siano a, b due naturali coprimi con $b > 1$ tale che esistano b' e s come definiti sopra, e sia $R = \frac{a}{b}$.*

Il periodo minimo di R (indicato con p) è il più piccolo naturale tale che $B^p \equiv 1 \ mod\ b'$.

Vale allora una ed una sola delle seguenti affermazioni:

1. *Se $b' = 1$ allora R è un numero B-adico con s cifre dopo la virgola nella sua rappr B-adica.*
2. *Se $b = b'$ R non è B-adico e la sua rappr B-adica infinita propria è semplice di periodo lungo p.*
3. *Se $b \ne b' \ne 1$ allora R non è B-adico e la sua rappr B-adica infinita propria è mista con antiperiodo di lunghezza s e periodo di lunghezza p.*

Esempio 9.4.1 Se prendiamo $b = 3$ e $B = 7$ abbiamo che $p = 1$, quindi $R = (0, \overline{2})_7$.

Se prendiamo $b = 7$ e $B = 3$ abbiamo che $p = 6$, quindi $R = (0, 0\overline{102120})_3$.

Appendice A

Il Piccolo Teorema di Fermat

Fermat fu uno dei più grandi matematici del diciasettesimo secolo. Chiamato anche "il principe dei dilettanti" studiò a fondo le proprietà dei numeri primi, sviluppando metodi nuovi che sono serviti alla matematica in tutti i secoli successivi.

In questa appendice richiameremo uno dei teoremi che portano il suo nome e cercheremo di darne un cenno della dimostrazione, senza però concluderla. Le dimostrazioni disponibili per questo teorema sono molteplici; quella che enunceremo qui è ricollegabile ai contenuti di questo corso.

Definizione A.0.1 Due numeri interi si dicono *coprimi* se non hanno divisori comuni primi diversi da 1 e -1.

Se $c \in \mathbb{N}^+$, la *funzione di Eulero* φ su c (indicata con $\varphi(c)$) è uguale al numero dei naturali minori di c coprimi con c.

Osservazione Se c è primo $\varphi(c) = c - 1$.

C'è anche un metodo comodo per calcolare questa funzione:

$$\varphi(c) = c \cdot \left[\prod_{p|c,\ p \text{ primo}} \left(1 - \frac{1}{p}\right) \right]$$

La funzione di Eulero ha molte interessanti proprietà. Quella che a noi serve per poter enunciare e dimostrare il teorema è la seguente:

Proposizione A.0.1 *La lunghezza p del periodo dello sviluppo B-adico di $\frac{a}{b}$ (con a, b coprimi) è divisore di $\varphi(b)$ $\forall B$.*

Teorema A.0.2 (Piccolo Teorema di Fermat) *Se b, B sono naturali coprimi allora vale*

$$B^{\varphi(b)} \equiv 1 \ \ mod\ b$$

Cenno della dimostrazione: Sia p la lunghezza del periodo dello sviluppo B-adico di $\frac{1}{b}$: allora $\exists\, q$ tale che $\varphi(b) = pq$.

Considero l'identità $B^{\varphi(b)} - 1 = (B^p)^q - 1 = (B^p - 1)(1 + B^p + B^{2p} + \ldots B^{(q-1)p})$, da cui segue che $b \,|\, B^{\varphi(b)} - 1$ perché $b \,|\, B^p - 1$.

Quindi una volta accertato che b divide $B^p - 1$ il teorema è praticamente dimostrato.

□

Appendice B

Ancora Sezioni di Dedekind

Nel capitolo 6 abbiamo definito i numeri reali con una relazione di equivalenza sull'insieme delle Sezioni Razionali (o Sezioni di Dedekind).

La definizione di Sezione Razionale che abbiamo dato in quel capitolo non è l'unica possibile, ce ne sono molte altre. Come sempre accade in questi casi ogni diversa definizione risulta più comoda per fare alcune cose e meno comoda per farne delle altre.

In questa appendice daremo una diversa definizione di Sezione Razionale e mostreremo come si arriva agli stessi risultati mostrati nel capitolo 6.

Definizione B.0.2 Una *sezione razionale* è una coppia (A, B) di insiemi $A, B \subseteq \mathbb{Q}$ non vuoti tali che

1. $A \cup B = \mathbb{Q}$ e $A \cap B = \emptyset$.
2. $\forall a \in A$, $\forall b \in B$ vale $a < b$.
3. A non ha massimo.

Osservazione

- Se (A, B) è una sezione razionale (o sezione di Dedekind), A è un segmento razionale.
- Se A è un segmento razionale $(A, \mathbb{Q} \setminus A)$ è una sezione razionale.
- Se $\mathbb{R}$ sono i reali di Dedekind l'applicazione

$$\begin{array}{rccc} f: & \mathbb{R} & \longrightarrow & \mathcal{S} \\ & A & \longmapsto & (A, \mathbb{Q}\setminus A) \end{array}$$

  dove $\mathcal{S}$ è l'insieme delle sezioni razionali, è bigettiva.

Dobbiamo quindi definire le operazioni sul nuovo insieme $\mathcal{S}$ che abbiamo definito: presi $(A_1, B_1), (A_2, B_2) \in \mathcal{S}$

$$(A_1, B_1) + (A_2, B_2) := (A_1 + A_2, B_1 + B_2)$$

$$(A_1, B_1) \cdot (A_2, B_2) := (A_1 \cdot A_2, B_1 \cdot B_2)$$

dove $A_1 + A_2$ e $A_1 \cdot A_2$ sono operazioni sui segmenti come avevamo già definito nel capitolo 6.

Esercizio B.0.1 Dimostrare che le operazioni sono ben definite, e che con esse l'insieme $\mathcal{S}$ ha la struttura di campo ordinato.

Definizione B.0.3 Sia $(A, B) \in \mathcal{S}$. L'*elemento separatore* di (A, B) è quel razionale e per cui $a \leq e \leq b \quad \forall a \in A, \forall b \in B$.

Definizione B.0.4 Due insiemi razionali $A \subseteq \mathbb{Q}$, $B \subseteq \mathbb{Q}$ non vuoti si dicono *contigui* se

1. $\forall a \in A, \forall b \in B$ vale $a \leq b$.
2. $\forall \epsilon \in \mathbb{Q}^+ \quad \exists\, a \in A, \exists\, b \in B$ tali che $b - a < \epsilon$.

Osservazione Se (A, B) è una sezione di Dedekind sicuramente (A, B) è una coppia di insiemi contigui.

Un modo naturale per associare ad una coppia di insiemi contigui una sezione razionale è di associare ad (A, B) la sezione $(S(A), S(B))$, dove
$S(A) := \{x \in \mathbb{Q} \mid \exists\, a \in A \text{ tale che } x < a\}$
$S(B) := \mathbb{Q} \backslash A$
Questa è ancora una sezione perché presi $a' \in S(A)$ e $y < a'$ abbiamo che $\exists\, a \in A$ tale che $a' < a \Longrightarrow y < a \Longrightarrow y \in S(A)$.
Domanda: ma individuo sempre un solo reale? no, ci serve una relazione di equivalenza!

Definizione B.0.5 Si dice che coppie di insiemi contigui sono *equivalenti* quando $\forall a \in A_1, \forall b \in B_2$ vale $a < b$ e $\forall a \in A_2, \forall b \in B_1$ vale $a < b$.

Questa è una buona definizione e si può dire che (A_1, B_1) è equivalente a (A_2, B_2) se e solo se $(A_1 \cup A_2, B_1 \cup B_2)$ è ancora una coppia di insiemi contigui.

L'insieme delle coppie di insiemi contigui quozientato con la precedente relazione di equivalenza dà luogo all'insieme $\mathcal{C}$ delle classi contigue.

Osservazione Se $\mathbb{R}$ è lo spazio delle sezioni di Dedekind, l'applicazione

$$\begin{array}{rccc} \sigma: & \mathbb{R} & \longrightarrow & \mathcal{C} \\ & (A, B) & \longmapsto & (S(A), S(B)) \end{array}$$

è bigettiva.

Le operazioni e l'ordinamento in $\mathcal{C}$ si definiscono come segue:
La somma:

$$[A, B] + [A', B'] := [A + A', B + B']$$

L'ordinamento:

$$[A_1, B_1] < [A_2, B_2] \text{ se } \exists\, b \in B_1 \text{ e } \exists\, a \in A_2 \text{ con } b < a$$

Il prodotto: se $[A, B] > 0$ e $[A', B'] > 0$ definiamo[1]

$$[A, B] \cdot [A', B'] := [A^+ \cdot A'^+, B \cdot B']$$

Con queste operazioni $\mathcal{C}$ è un campo ordinato completo, e la funzione σ definita prima è un isomorfismo di campi ordinato.
Con queste operazioni e questo ordinamento definiamo $\mathbb{R} := \mathcal{C}$.

Avendo definito l'insieme $\mathbb{R}$ potremmo pensare di ripetere questa costruzione per trovare un nuovo insieme. Ovvero ridefiniamo le sezioni, non più sui razionali ma direttamente sui reali:

Definizione B.0.6 Una *sezione reale* è una coppia (A, B) tale che

1. $A \cup B = \mathbb{R}$ e $A \cap B = \emptyset$.
2. $\forall a \in A$, $\forall b \in B$ vale $a < b$.
3. A non ha massimo.

Definizione B.0.7 Sia $(A, B) \in \mathcal{S}$. L'*elemento separatore* di (A, B) è quel reale e per cui $a \leq e \leq b \quad \forall a \in A$, $\forall b \in B$.

La differenza è che stavolta l'elemento separatore esiste sempre e non è altro che $\sup_{\mathbb{R}} A$.
Quindi la costruzione che facciamo in realtà non porta da nessuna parte perché rimaniamo ancora dentro $\mathbb{R}$.

[1] Ricordando che indichiamo $A^+ := \{a \in A \mid a > 0\}$.