# Assiomi di Peano

*In una storia di fantascienza noi umani riceviamo un messaggio misterioso da intelligenze aliene. Forse la conversazione fra di loro languisce, ed hanno pensato di invitare al loro salotto il primo pianeta sconosciuto con cui ci si intenda. Ma su che base due intelligenze prese a caso nell'universo possono mai sperare di sintonizzarsi? Che cosa c'è nell'intersezione, nel nocciolo di tutte le intelligenze possibili? Che cosa prendere come stele di Rosetta cosmica? Finalmente il colpo di genio: il messaggio è una versione extraterrestre degli assiomi di Peano.*

## 1. Il conteggio e gli insiemi.

Il nostro primo incontro con la matematica è forse stato il momento in cui ci hanno insegnato a *contare*, cioè a recitare ritmicamente una certa filastrocca

"uno, due, tre, quattro, cinque, ..."

mentre passiamo in rassegna un gruppo di oggetti. Quando poi afferriamo il meccanismo dei numeri grandi e di come si scrivono in cifre, non fatichiamo a capire che *non c'è un ultimo numero*: per quanto mi sia spinto avanti nel gioco del conteggio, posso sempre contare più oltre. Se ho contato fino a duemilaquattrocentoventiquattro, posso benissimo contare anche fino a duemilaquattrocentoventicinque.

Se vogliamo che la teoria degli insiemi possa fare da base alla matematica, bisognerà che in qualche modo contenga una versione della procedura del conteggio. Uno dei primi modi che può venire alla mente è di simulare il conteggio con la singolettazione: pensiamo all'insieme vuoto come allo "zero", al singoletto $\{\varnothing\}$ come all'"uno", al $\{\{\varnothing\}\}$ come al "due", e così via, di modo che il successivo di un "numero" sia semplicemente il suo singoletto $\{\text{numero}\}$. Una proposta più sofisticata, detta degli "numeri ordinali finiti di von Neumann" (Johann von Neumann (1903–1957)), sarebbe questa: partiamo sempre dall'insieme vuoto come "zero", ma arrivati al "numero" della filastrocca "uno, due, tre, quattro, ... , numero" poniamo che il numero successivo sia l'*insieme* delle parole della filastrocca fino a quel punto: {uno, due, tre, quattro, ..., numero}. Facendo i conti risulta

$$\text{zero} := \varnothing, \qquad \text{uno} := \text{zero} \cup \{\text{zero}\} = \{\varnothing\}, \qquad \text{due} := \text{uno} \cup \{\text{uno}\} = \big\{\varnothing, \{\varnothing\}\big\},$$
$$\text{tre} := \text{due} \cup \{\text{due}\} = \Big\{\varnothing, \{\varnothing\}, \big\{\varnothing, \{\varnothing\}\big\}\Big\},$$
$$\text{successivo di un numero} := \text{numero} \cup \{\text{numero}\}.$$

In questa maniera ogni numero $n$ è un insieme di esattamente $n$ elementi, e la relazione di "minore" fra due numeri coincide con l'appartenenza insiemistica: $n < m \iff n \in m$.

Entrambe le proposte sembrano sensate, ma si scontrano subito con due difficoltà:

1) bisognerebbe riuscire a scrivere un predicato insiemistico $N(x)$ che dica se un dato elemento $x$ è un numero naturale oppure no. Per esempio, bisognerà che $N(\varnothing)$ sia vero e che $N(\{\{\varnothing\}, \{\{\varnothing\}\}\})$ sia falso; vorremmo che un tale predicato $N$ fosse una combinazione finita dei predicati insiemistici di base e di operazioni logiche fra questi;
2) sarebbe bello se questo predicato $N(x)$ definisse un insieme, che chiameremmo "insieme dei numeri naturali" e indicheremmo col simbolo $\mathbb{N}$.

Se il primo problema potrebbe ridursi a una questione di ingegnosità, il secondo è in odore di non poter essere dimostrato come teorema, e di abbisognare quindi di un postulato apposito.

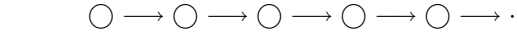
In questa sede, invece di prendere il toro per le corna, gli taglieremo la testa: postuleremo l'esistenza di un insieme $\mathbb{N}$ con certe proprietà, senza sforzarci minimamente di identificare i suoi elementi con oggetti insiemistici già introdotti in precedenza. A tutti gli effetti pratici potremo pensare agli elementi di $\mathbb{N}$ come ad atomi. Le proprietà che imporremo a $\mathbb{N}$ saranno una versione dei famosi assiomi di Peano, che sono stati introdotti alla fine dell'ottocento dal matematico torinese Giuseppe Peano (1858–1932), proprio allo scopo di dare una sistemazione logica rigorosa dei numeri naturali.

**Esercizio.** Per due ordinali finiti di Von Neumann si ha $n \leq m \iff \ldots$ (Non si chiede una dimostrazione rigorosa, ma solo una prova indiziaria).

## 2. Contare con una catena di perline.

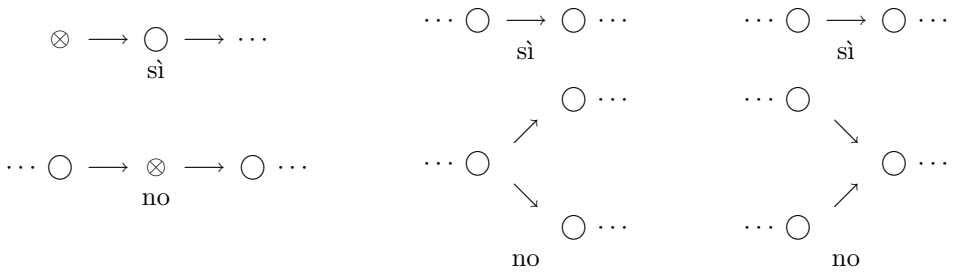
Immaginiamo un pastore che deve tenere il conto delle pecore che escono il mattino dall'ovile e rientrano la sera. Costui è abituato a contare senza addormentarsi sgranando una specie di rosario: una cordicella su cui sono infilzate delle perline; per ogni pecora che passa dalla porta dell'ovile si avanza di una perlina. Facciamo anche finta che questo pastore abbia ambizioni faraoniche nell'espandere la sua attività e che abbia in programma di possedere un giorno un gregge con un numero *finito* di pecore così enorme da non potersi e volersi pronunciare per il momento nemmeno sull'ordine di grandezza. In attesa di diventare super-pastore, ha ordinato alla nostra fabbrica di bigiotteria una catenella così lunga che possa bastare per contare *qualsiasi* gregge finito; per contenere la spesa, però, non vuole che la catenella contenga pezzi superflui.

Come dev'essere fatta una catenella che possa contare tutti i greggi finiti? Cominciamo a farcene un'idea schematizzando la catenella come un allineamento di perline. Delle frecce fra le varie perline mostreranno come deve muoversi il dito al passaggio della pecora:



Dopo approfondita meditazione e discussione, il nostro ufficio tecnico si trova in accordo sui seguenti punti:

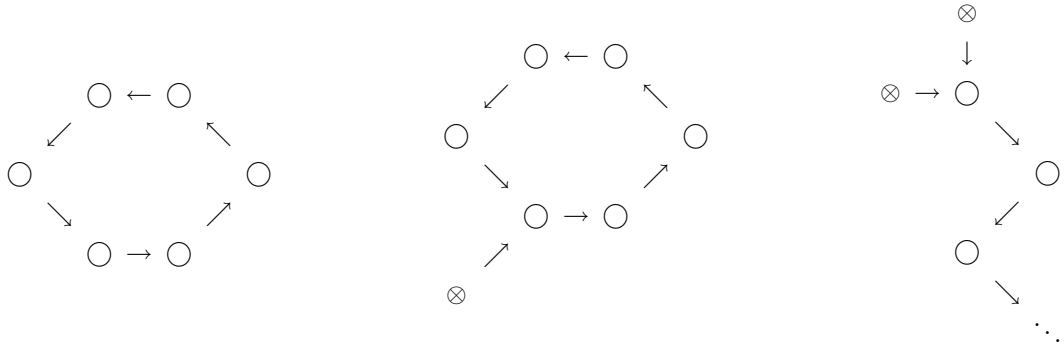
1) il conteggio deve avere un inizio ben preciso: bisogna che ci sia una perlina particolare in cui si posiziona la mano subito prima che il gregge cominci a sfilare; si presume che a quella perlina particolare non si arrivi mai più nel corso di un conteggio, e pertanto ogni altra perlina che per sbaglio fosse stata predisposta a precedere quella speciale è superflua e va eliminata perché nemmeno lei sarà mai raggiunta in alcun conteggio;
2) al passaggio di ogni pecora il movimento della mano sia obbligato: due strade sarebbero uno spreco di risorse;
3) vorremmo che ogni passo del conteggio sia reversibile in modo unico: in questo modo risparmiamo perline e rendiamo possibili conti alla rovescia e correzioni di errori.

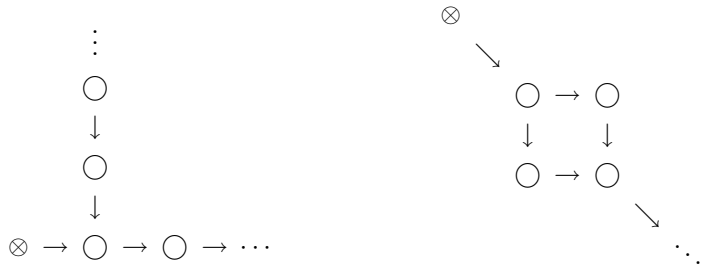



In termini più tecnici possiamo scrivere le seguenti specifiche di progetto:

i) *c'è esattamente una perlina (che chiameremo "la prima"), a cui non arriva alcuna freccia;*
ii) *da tutte le perline parte una e una sola freccia (non ci sono ramificazioni nel verso delle frecce).*
iii) *a tutte le perline, esclusa la prima, arriva una e una sola freccia (non ci sono diramazioni nel senso inverso alle frecce);*

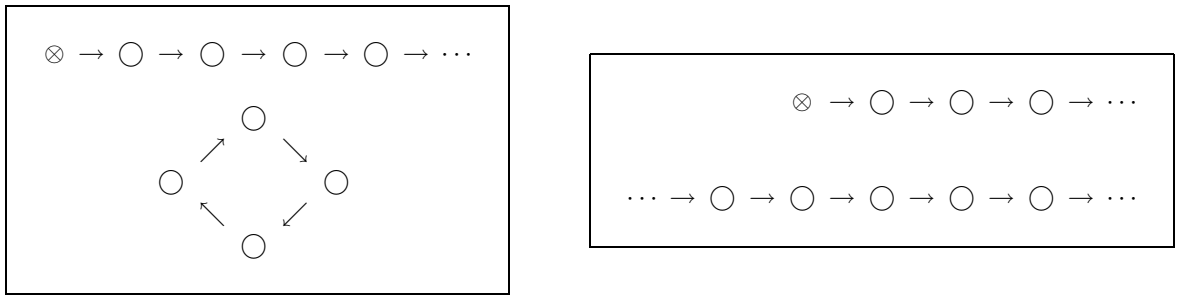
**Esercizio.** I seguenti schemi di catena sono accettabili?





Una catena che rispetti le nostre tre specifiche riesce a contare qualsiasi gregge finito. Infatti il movimento delle dita a ogni passaggio di pecora è obbligato, e ogni volta la mano si sposta su una perlina *nuova*, che non era stata usata né sarà più usata ancora per un'altra pecora nella stessa seduta. Supponiamo infatti di accorgerci di essere passati due volta sulla stessa perlina. Ritorniamo allora sui nostri passi per vedere se per caso un doppio conteggio non fosse già successo anche prima per altre perline. Individuiamo la *prima* perlina che è stata contata più di una volta, e chiamiamola $x$. Questa $x$ non può essere la perlina d'inizio conto, perché una volta contata quella non c'è modo di ritornarci (per la regola i non vi arrivano frecce). Dunque la $x$ deve essere una delle altre perline, alle quali arriva una e una sola freccia (per la regola iii). Sia $y$ la perlina da cui parte la freccia che arriva a $x$. Ma allora ogni volta che contiamo $x$ dobbiamo aver contato la pecora precedente su $y$. Questo va contro la nostra supposizione che $x$ fosse la primissima perlina contata due volte.

Il lavoro però non è terminato. Proviamo ad aggiungere a una catena "a semiretta" una seconda catena "a collana", oppure "a retta" (infinita in entrambe le direzioni). Otteniamo così delle catene *sconnesse*, che



verificano le tre regole, ma che non saranno accettate dal cliente, perché contengono dei pezzi inutili, che non serviranno mai nel conteggio di alcun gregge finito.

Non è così facile formalizzare l'idea di connessione o sconnessione di una catena, perché per decidere può essere necessario guardare la catena nel suo complesso, a volo d'uccello, e non basta andare col microscopio a contare quante frecce entrano ed escono da ogni singola perlina, come invece fanno le regole i, ii e iii. Un grosso aiuto alla soluzione del problema viene dalla nozione di *insieme ereditario*: *un insieme $A$ di perline di una catena si dice ereditario se ogniqualvolta $x$ e $y$ sono perline della catena succede la seguente cosa: se $x \in A$ e c'è una freccia che va da $x$ a $y$, allora anche $y \in A$.* Si capirà perché si parla di ereditarietà se si interpreta la catena come una albero genealogico: un insieme $A$ è ereditario se la proprietà '$x \in A$' si trasmette di padre in figlio. Potremmo anche pensare a un insieme ereditario come al "bacino di infezione" di una malattia che si trasmetta istantaneamente lungo le frecce (ma non le risale): in insieme è ereditario se un'infezione iniziata nel suo interno non ne può uscire.

Una catena fatta a collana, per esempio, ha solo due sottinsiemi ereditari: l'insieme vuoto e la collana stessa. Infatti l'insieme vuoto e la catena tutta sono sempre insiemi ereditari, e lungo una collana basta una perlina malata per trasmettere l'infezione via via a tutte le altre, fino a tornare al punto di partenza. Una catena a semiretta, invece, ha infiniti sottinsiemi ereditari diversi dal vuoto e dalla catena stessa: infatti se infettiamo una qualsiasi perlina, la malattia si trasmette a tutta la semiretta delle perline seguenti, ma non risale a quelle precedenti.

**Esercizio.** Individuare sottinsiemi ereditari delle due catene sconnesse introdotte poco fa. Attenzione: un insieme ereditario può benissimo avere più di un focolaio di infezione, o anche infiniti.

Supponiamo ora di inoculare il virus alla perlina d'inizio conto. La zona che ne risulta infettata *non* comprende eventuali pezzi della catena sconnessi, giacché l'unica via che il virus può seguire è quella segnata dalle frecce. Una catena sconnessa ha la proprietà di possedere almeno *due sottinsiemi ereditari distinti comprendenti l'inizio catena*: (1) la zona d'influenza dell'inizio catena e (2) la catena nel suo complesso. Abbiamo dunque una semplice regola anti-sconnessione:

iv) la catena nel suo complesso deve essere l'unico sottinsieme ereditario comprendente l'inizio catena.

## 3. Un insieme su cui possiamo contare.

Vediamo come tradurre i discorsi su frecce e catene in termini di insiemi: avremo un insieme di elementi che staranno per le perline e un insieme di coppie ordinate $(x, y)$ che staranno per le frecce $x \to y$. Una catena sarà un insieme di perline accoppiato a un insieme di frecce. Un sottinsieme $E$ dell'insieme delle perline sarà detto ereditario se ogniqualvolta $x \in E$ e $(x, y)$ è nell'insieme di frecce, allora anche $y \in E$. Le regole sviluppate nel paragrafo precedente si possono tradurre così:

• **Postulato dell'insieme dei numeri naturali.** *Esiste un insieme, chiamato insieme dei numeri naturali e indicato con* $\mathbb{N}$*, e un sottinsieme* $s \subset \mathbb{N} \times \mathbb{N}$ *con le seguenti proprietà:*

*1) esiste un unico elementi di* $\mathbb{N}$*, chiamato "zero" e indicato con '*$0$*', tale che* $\forall n \in \mathbb{N}$*:* $(n, 0) \notin s$*;*
*2)* $\forall n \in \mathbb{N}\ \exists! m \in \mathbb{N}$*:* $(n, m) \in s$*;*
*3)* $\forall m \in \mathbb{N} \setminus \{0\}\ \exists! n \in \mathbb{N}$*:* $(n, m) \in s$*;*
*4) se un sottinsieme* $E$ *di* $\mathbb{N}$ *è ereditario e tale che* $0 \in E$*, allora* $E = \mathbb{N}$*.*

Non c'è accordo generale se includere lo zero o no fra i numeri naturali. Qui abbiamo scelto di farlo, ma a scanso di equivoci converrà dire esplicitamente se si considera lo zero in $\mathbb{N}$ in un dato contesto.

Se interpretiamo discorsivamente il predicato '$(n, m) \in s$' come "$m$ è un successivo di $n$" oppure "$n$ è un precedente di $m$", possiamo ricordare più facilmente i quattro punti del postulato, che sono la nostra versione degli *assiomi di Peano*:

$1'$) lo zero non ha precedenti;
$2'$) ogni numero naturale ha un unico successivo;
$3'$) ogni numero naturale escluso lo zero ha un unico precedente;
$4'$) se un insieme $E \subset \mathbb{N}$ è ereditario (cioè ogniqualvolta ha un numero naturale ha anche tutti i suoi successivi) e gli appartiene lo zero, allora $E = \mathbb{N}$.

La condizione 2 significa che $s$ è una *funzione* da $\mathbb{N}$ in se stesso, che merita il nome di "passaggio al successivo". Indicheremo il successivo di un numero naturale $n$ con $s(n)$. (Verrebbe da scrivere $s(n) = n+1$, ma ancora non abbiamo parlato di addizione).

**Esercizio.** possiamo riformulare il postulato così: esiste un insieme $\mathbb{N}$, un elemento $0 \in \mathbb{N}$ e una funzione $s\colon \mathbb{N} \to \mathbb{N}$ iniettiva tali che $s(\mathbb{N}) = \mathbb{N} \setminus \{0\}$, e inoltre ogniqualvolta $E \subset \mathbb{N}$ è ereditario (cioè $\forall n \in E$: $n \in E \Rightarrow s(n) \in E$) e $0 \in E$, allora $E = \mathbb{N}$.

**Esercizio.** Se $\mathcal{E}$ è una famiglia non vuota di sottinsiemi ereditari di una catena, allora anche $\bigcap \mathcal{E}$ è un sottinsieme ereditario. Far vedere come conseguenza che il postulato dei numeri naturali poteva anche richiedere l'esistenza di una coppia $(N, s)$ che verificasse soltanto le proprietà 1, 2 e 3, poiché allora $\mathbb{N}$ si potrebbe ricavare facendo l'intersezione di *tutti* quei sottinsiemi ereditari di $N$ a cui appartiene lo zero.

Invece di insiemi ereditari parleremo spesso di *predicati ereditari*: un predicato $P(n)$ che abbia senso per tutti gli $n \in \mathbb{N}$ si dirà ereditario se il sottinsieme di $\mathbb{N}$ definito da $P$ è ereditario, cioè se

$$\forall n \in \mathbb{N}: \qquad P(n) \Rightarrow P(s(n))\,.$$

Con questa convenzione l'assioma 4 si può riformulare come

$4''$) *se un predicato* $P$ *definito su* $\mathbb{N}$ *è ereditario e tale che* $P(0)$ *è vero, allora* $P(n)$ *è vero per tutti gli* $n \in \mathbb{N}$*.*

Nota: una coppia ordinata $(A, s)$, in cui $A$ è un insieme e $s \subset A \times A$ è un insieme di frecce, è chiamata qui *"catena"* perché quello a cui vogliamo arrivare è una catenella di perline su cui contare, però il termine usuale in matematica per questo concetto generale è *"grafo orientato"*.

Ci si potrà chiedere se l'insieme $\mathbb{N}$ è unico: la risposta è che non c'è nessun motivo perché lo sia. Se abbiamo un insieme di numeri naturali, potremo trovarne un altro semplicemente "cambiando nome" a qualche elemento, o a tutti. Quando si introducono i numeri interi, razionali, reali o complessi, ogni volta all'interno del nuovo insieme riconosceremo una "copia" di $\mathbb{N}$, che a rigore non è lo stesso insieme. Però potremo usare tranquillamente uno qualsiasi di questi insiemi di numeri naturali, perché "sono tutti fatti allo stesso modo" (con significato da precisare).

**Esercizio.** Dimostrare che il postulato 4 è equivalente al seguente:

4‴) *Non esistono due sottinsiemi $A, B$ di $\mathbb{N}$ che siano contemporaneamente ereditari, non vuoti, disgiunti e tali che $A \cup B = \mathbb{N}$.*

## 4. Prime conseguenze degli assiomi (Non svolto a lezione; facoltativo).

**Definizione.** *Il successivo dello zero è chiamato "uno" e è indicato con '1'. Dato $n \in \mathbb{N}$ indicheremo con $[n, +\infty[$ l'intersezione di tutti i sottinsiemi ereditari di $\mathbb{N}$ a cui appartiene $n$. Dati $n, m \in \mathbb{N}$ scriveremo indifferentemente '$n \le m$' o '$m \ge n$' se $m \in [0, +\infty[$ e porremo $[n, m] := \{x \in \mathbb{N} \,:\, n \le x \le m\}$.*

Quando scriviamo $[n, +\infty[$, il simbolo '$+\infty$' non è un numero naturale, ma sta semplicemente a suggerire una 'direzione' (quella in cui si propaga il contagio), così come "sud, nord, est, ovest" sono direzioni e non punti della superficie terrestre. $[n, +\infty[$ è la zona contagiata da un focolaio posto in $n$. Invece $[n, m]$ è la zona contagiata da un focolaio in $n$ quando però il successivo di $m$ sia stato vaccinato e non trasmetta la malattia.

**Lemma.** *L'intersezione di una famiglia non vuota di sottinsiemi ereditari di $\mathbb{N}$ è anch'essa un sottinsieme ereditario di $\mathbb{N}$.*

**Dimostrazione.** Sia $\mathcal{F}$ una famiglia non vuota di sottinsiemi ereditari di $\mathbb{N}$ e supponiamo che sia $n \in \bigcap \mathcal{F}$. Dobbiamo dimostrare che anche il successivo di $n$ appartiene all'intersezione: $s(n) \in \bigcap \mathcal{F}$. Sia $E \in \mathcal{F}$. Per definizione di intersezione di una famiglia di insiemi si ha $n \in E$. Ma $E$ è ereditario, per cui $s(n) \in E$. Essendo $E$ arbitrario, si ha $\forall E \in \mathcal{F}$: $s(n) \in E$, cioè $s(n) \in \bigcap \mathcal{F}$, ancora per la definizione di intersezione di una famiglia di insiemi. □

A uso e consumo dei lemmi seguenti, introduciamo la notazione

$$\forall n \in \mathbb{N}: \qquad \mathcal{F}(n) := \big\{E \in \mathcal{P}(\mathbb{N}) \,:\, E \text{ è ereditario e } n \in E\big\}\,,$$

di modo che $[n, +\infty[ = \bigcap \mathcal{F}(n)$.

**Esercizio.** Dimostrare che $n \le m \iff \mathcal{F}(n) \subseteq \mathcal{F}(m) \iff [n, +\infty[ \supseteq [m, +\infty[$.

**Lemma.** *Si ha $\mathcal{F}(0) = \{\mathbb{N}\}$ e $\mathcal{F}(1) = \{\mathbb{N}, \mathbb{N} \setminus \{0\}\}$. Di conseguenza $[0, +\infty[ = \mathbb{N}$ e $[1, +\infty[ = \mathbb{N} \setminus \{0\}$. Quindi '$0 \le 0$', '$1 \le 1$' e '$0 \le 1$' sono vere mentre '$1 \le 0$' è falsa.*

**Dimostrazione.** Per l'assioma 4 l'unico sottinsieme ereditario di $\mathbb{N}$ a cui appartiene 0 è $\mathbb{N}$ stesso. Quindi $\mathcal{F}(0) = \{\mathbb{N}\}$ e $[0, +\infty[ = \bigcap\{\mathbb{N}\} = \mathbb{N}$.
Quali sono i sottinsiemi ereditari contenenti l'1? Di sicuro c'è $\mathbb{N}$ stesso. Poi $\mathbb{N} \setminus \{0\}$ è ereditario perché se $n \in \mathbb{N} \setminus \{0\}$ allora $s(n)$ è un numero naturale ma non può essere zero, perché zero non è successivo di alcun numero naturale, dunque pure $s(n) \in \mathbb{N} \setminus \{0\}$. Inoltre $1 \in \mathbb{N} \setminus \{0\}$ perché $1 \neq 0$ (di nuovo, lo zero non è successivo di alcun numero naturale mentre l'uno sì). Perciò i due insiemi $\mathbb{N}$ e $\mathbb{N} \setminus \{0\}$ sono ereditari e

comprendono l'1. Dimostriamo che non ci sono altri insiemi con queste proprietà. Sia $E$ un insieme ereditario comprendente 1. Allora $E \cup \{0\}$ è pure ereditario; sia infatti $n \in E \cup \{0\}$;

$$
\begin{array}{cl}
n \in E \cup \{0\} & \\
\Updownarrow & \text{definizione di unione} \\
\big(n \in E\big) \vee \big(n \in \{0\}\big) & \\
\Downarrow & \begin{array}{l} E \text{ è ereditario e} \\ \text{definizione di singoletto} \end{array} \\
\big(s(n) \in E\big) \vee \big(n = 0\big) & \\
\Downarrow & \begin{array}{l} E \subset E \cup \{0\} \text{ e} \\ \text{definizione di } 1 \end{array} \\
\big(s(n) \in E \cup \{0\}\big) \vee \big(s(n) = 1\big) & \\
\Downarrow & 1 \in E \\
\big(s(n) \in E \cup \{0\}\big) \vee \big(s(n) \in E\big) & \\
\Downarrow & \begin{array}{l} E \subset E \cup \{0\} \text{ e} \\ \text{se } q \Rightarrow p \text{ allora } (p \vee q) \Rightarrow p \end{array} \\
s(n) \in E \cup \{0\}\,. &
\end{array}
$$

Inoltre ovviamente $E \cup \{0\}$ comprende lo zero, da cui $E \cup \{0\} = \mathbb{N}$ per l'assioma 4. Ma allora necessariamente o $E = \mathbb{N}$ oppure $E = \mathbb{N} \setminus \{0\}$. Finalmente abbiamo $\mathcal{F}(1) = \{\mathbb{N}, \mathbb{N} \setminus \{0\}\}$ e quindi anche $[1, +\infty[ = \bigcap\{\mathbb{N}, \mathbb{N} \setminus \{0\}\} = \mathbb{N} \setminus \{0\}$.
Che ora '$0 \le 0$', '$1 \le 1$' e '$0 \le 1$' valgano e che '$1 \le 0$' non valga segue direttamente dalla definizione di '$\le$'. □

**Lemma.** *Per ogni $n \in \mathbb{N}$ ed $E \in \mathcal{P}(\mathbb{N})$ ereditario si ha $E \in \mathcal{F}(s(n)) \iff E \cup \{n\} \in \mathcal{F}(n)$. Quindi in particolare $[s(n), +\infty[ = [n, +\infty[ \setminus \{n\}$.*

**Dimostrazione.** Consideriamo il predicato

$$\boxed{(\textit{da dimostrare vero } \forall n) \qquad P(n) := \text{'}\forall E \in \mathcal{P}(\mathbb{N}) \text{ ereditario: } E \in \mathcal{F}\big(s(n)\big) \iff E \cup \{n\} \in \mathcal{F}(n)\text{'}.}$$

Il lemma precedente dice fra l'altro che

$$\boxed{P(0) \text{ è vero,}}$$

perché $E \in \mathcal{F}(s(0)) \iff E \in \mathcal{F}(1) \iff E \in \{\mathbb{N}, \mathbb{N} \setminus \{0\}\} \iff E \cup \{0\} \in \{\mathbb{N}\} \iff E \cup \{0\} \in \mathcal{F}(0)$. Per l'assioma 4 (nella versione 4″) ora basterà dimostrare che

$$\text{per ogni } n \in \mathbb{N} \text{ vale l'implicazione '} P(n) \Rightarrow P\big(s(n)\big)\text{'},$$

e avremo così che il predicato vale per tutti i numeri naturali, che è quello che vogliamo:

$$\forall n \in \mathbb{N}\colon\ P(n)$$

(il nostro primo esempio di *"dimostrazione per induzione"*). Dell'implicazione $P(n) \Rightarrow P(s(n))$ supponiamo dunque che valga l'antecedente:

$$\boxed{P(n)\ (\textit{ipotesi induttiva}): \qquad \forall E \in \mathcal{P}(\mathbb{N}) \text{ ereditario:} \quad E \in \mathcal{F}\big(s(n)\big) \iff E \cup \{n\} \in \mathcal{F}(n),}$$

e proponiamoci di dedurne il conseguente:

$$\boxed{P\big(s(n)\big)\ (\textit{tesi induttiva}): \qquad \forall G \in \mathcal{P}(\mathbb{N}) \text{ ereditario:} \quad G \in \mathcal{F}\big(s(s(n))\big) \iff G \cup \{s(n)\} \in \mathcal{F}\big(s(n)\big)}$$

(abbiamo cambiato la variabile muta $E$ in $G$ per non confonderci nel seguito).

Sia dunque $G \in \mathcal{P}(\mathbb{N})$ ereditario. L'implicazione verso destra $G \in \mathcal{F}(s(s(n))) \Rightarrow G \cup \{s(n)\} \in \mathcal{F}(s(n))$ è facile e non richiede di usare l'ipotesi induttiva: se $G \in \mathcal{F}(s(s(n)))$ si ha che $E := G \cup \{s(n)\}$ è ereditario, perché $m \in G \Rightarrow s(m) \in G \subset E$ e $m \in \{s(n)\} \iff m = s(n) \Rightarrow s(m) = s(s(n)) \in G \subset E$: riunendo i due casi $m \in E \Rightarrow s(m) \in E$.
Per l'implicazione inversa $G \in \mathcal{F}(s(s(n))) \Leftarrow G \cup \{s(n)\} \in \mathcal{F}(s(n))$ ci vuole invece l'ipotesi induttiva:

$$
\begin{array}{rl}
G \cup \{s(n)\} \in \mathcal{F}\big(s(n)\big) & \\
\Updownarrow & \text{ipotesi induttiva applicata con } E{=}G{\cup}\{s(n)\} \\
& \text{che è ereditario} \\
\big(G \cup \{s(n)\}\big) \cup \{n\} \in \mathcal{F}(n) & \\
\Updownarrow & \text{definizione di unione e coppia non ordinata} \\
G \cup \{n, s(n)\} \in \mathcal{F}(n) & \\
\Updownarrow & \text{definizione di } \mathcal{F}(n) \\
G \cup \{n, s(n)\} \text{ è ereditario e gli appartiene } n & \\
\Downarrow & \text{ereditarietà due volte} \\
G \cup \{n, s(n)\} \text{ è ereditario e gli appartiene } s(s(n)) & \\
\Downarrow & s(s(n)){\notin}\{n,s(n)\} \\
s\big(s(n)\big) \in G & \\
\Downarrow & G \text{ è ereditario} \\
G \in \mathcal{F}\big(s(s(n))\big)\,. &
\end{array}
$$

□

**Lemma.** *Per ogni $n, m \in \mathbb{N}$ si ha $n \le m \iff s(n) \le s(m)$.*

**Dimostrazione.** Dimostriamo dapprima la freccia '⇒'. Sia $n \le m$. Allora $m \in [n, +\infty[$ e, per l'ereditarietà e per il lemma precedente, si ha $s(m) \in [n, +\infty[ \,=\, [s(n), +\infty[ \cup \{n\}$. L'elemento $s(m)$ deve dunque appartenere a uno dei due insiemi $[s(n), +\infty[$ e $\{n\}$, ma non può essere che $s(m) = n$, perché $m \in [n, +\infty[$ mentre $m \notin [s(m), +\infty[ = [m, +\infty[ \setminus \{m\}$. Quindi $s(m) \in [s(n), +\infty[$, cioè $s(n) \le s(m)$.
Passiamo alla freccia '⇐'. La dimostrazione sarà per induzione. Sia $P(n)$ il predicato

$$P(n) := \text{“}\forall m \in \mathbb{N} \quad s(n) \le s(m) \Rightarrow n \le m\text{”}.$$

La $P(0)$ vuol dire “$\forall m \in \mathbb{N}\ 1 \le s(m) \Rightarrow 0 \le m$”, che è vera perché il secondo membro dell'implicazione è '$0 \le m$', che equivale a '$m \in [0, +\infty[ = \mathbb{N}$, che a sua volta è vero per ogni $m \in \mathbb{N}$. Supponiamo ora che $P(n)$ sia vera per un qualche $n \in \mathbb{N}$ e cerchiamo di dimostrare che vale anche $P(s(n))$, che si scrive

$$P\big(s(n)\big) = \text{“}\forall m \in \mathbb{N} \quad s\big((n)\big) \le s(m) \Rightarrow s(n) \le m\text{”}.$$

Sia dunque $m \in \mathbb{N}$ tale che $s(s(n)) \le s(m)$, cioè $s(m) \in [s(s(n)), +\infty[ = [s(n), +\infty[ \setminus \{s(n)\}$. Da qui segue in particolare che $s(m) \ne s(n)$ e quindi che $m \ne n$ (per il postulato 2). Inoltre da $s(m) \in [s(n), +\infty[$ segue che $s(n) \le s(m)$. Dall'ipotesi induttiva $P(n)$ si trae che $n \le m$, ossia $m \in [n, +\infty[$. Ma $m \ne n$, e quindi $m \in [n, +\infty[ \setminus \{n\} = [s(n), +\infty[$, cioè $s(n) \le m$, che è proprio il secondo membro dell'implicazione di $P(s(n))$. □

**Proposizione.** *La relazione '$n \le m$' è una relazione d'ordine debole totale su $\mathbb{N}$.*

**Dimostrazione.** Per dimostrare che si tratta di una relazione d'ordine debole bisogna verificare le proprietà riflessiva, antisimmetrica e transitiva.
*Riflessiva*: sia $n \in \mathbb{N}$. È evidente che $n$ appartiene a ogni insieme ereditario a cui appartenga $n$ stesso. Quindi $n \in [n + \infty[$, cioè $n \le n$.

*Antisimmetrica*: per induzione. Sia $P(n)$ il predicato

$$P(n) := \text{`}\forall m \in \mathbb{N} \quad \Big((n \le m) \wedge (m \le n)\Big) \Rightarrow n = m\text{'}.$$

La $P(0) = \text{`}\forall m \in \mathbb{N} \quad ((0 \le m) \wedge (m \le 0)) \Rightarrow 0 = m\text{'}$ 'e vera perché $m \le 0$ vuol dire che 0 appartiene all'insieme ereditario $[m, +\infty[$, il quale viene quindi a coincidere con $\mathbb{N}$ (per il postulato 4); se fosse $m \neq 0$, $m$ sarebbe il successivo di un $m' \in \mathbb{N}$ e quindi $[m, +\infty[ = [m', +\infty[ \setminus \{m'\} \neq \mathbb{N}$, contro quanto già stabilito. Quindi in effetti $m = 0$.
Supponiamo ora che valga $P(n)$ per un qualche $n \in \mathbb{N}$ e proponiamoci di dimostrare $P(s(n))$:

$$P\big(s(n)\big) := \text{`}\forall m \in \mathbb{N} \quad \Big((s(n) \le m) \wedge (m \le s(n))\Big) \Rightarrow s(n) = m\text{'}.$$

Supponiamo dunque che $s(n) \le m$ e che $m \le s(n)$. Dalla prima segue che $m \neq 0$, e quindi $m$ ha un (solo) predecessore, che indichiamo con $m'$. Usando l'uguaglianza $m = s(m')$ si ha $s(n) \le s(m')$ e $s(m') \le s(n)$, che per il lemma precedente implicano $n \le m'$ e $m' \le m$. Possiamo applicare ora l'ipotesi induttiva $P(n)$ con $m'$ al posto di $m$ e ottenere $n = m'$, da cui segue $s(n) = s(m') = m$, che era il secondo membro dell'implicazione di $P(s(n))$.
*Transitiva*: facillima. Supponiamo infatti che $n \le m$ e $m \le p$. Allora ogni insieme induttivo che contiene $n$ deve anche contenere $m$, e ogni insieme induttivo che contiene $m$ deve contenere anche $p$. Di conseguenza ogni insieme induttivo che contiene $n$ deve contenere anche $p$, cioè $n \le p$.
*Ordinamento totale*: per induzione. Sia $P(n)$ il predicato

$$P(n) := \text{`}\forall m \in \mathbb{N} \quad (n \le m) \vee (m \le n)\text{'}$$

La $P(0)$ è '$\forall m \in \mathbb{N} \quad (0 \le m) \vee (m \le 0)$', che è vera perché '$0 \le m$' è vera per ogni $m \in \mathbb{N}$. Supponiamo quindi che la $P(n)$ sia vera per un qualche $n$ e dimostriamo che vale anche

$$P\big(s(n)\big) := \text{`}\forall m \in \mathbb{N} \quad \big(s(n) \le m\big) \vee \big(m \le s(n)\big)\text{'}$$

Sia dunque $m \in \mathbb{N}$. Dall'ipotesi induttiva $P(n)$ segue che o $n \le m$ oppure $m \le n$. Mettiamoci nel primo caso: $n \le m$. Allora $m \in [n, +\infty[ = [s(n), +\infty[ \cup \{n\}$. Possono accadere due cose: o $m \in [n, +\infty[ = [s(n), +\infty[$, che equivale a $s(n) \le m$, che è proprio uno dei membri della disgiunzione di $P(s(n))$, oppure $m = n$, il quale implica che $s(n) = s(m) \in [m, +\infty[$ e quindi $m \le s(n)$, che è l'altro membro della disgiunzione. Nel secondo caso abbiamo $m \le n$, che significa che $n$ appartiene all'insieme ereditario $[m, +\infty[$. Ma allora anche il suo successivo $s(n)$ gli appartiene, ossia $m \le s(n)$, che è di nuovo uno dei due membri della disgiunzione da dimostrare. □