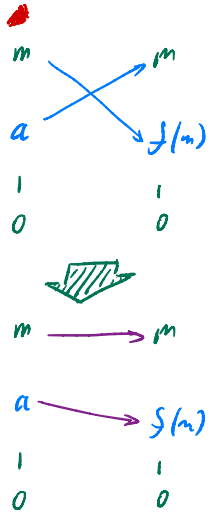
l'ipotesi induttiva, $C = m$. Ma $B = Im(f) =$

$= C \cup \{f(m)\} = m \cup \{m\} = n$.



Se $f(m) \neq m$, allora vediamo che esiste $a < m$ tale che $f(a) = m$. Se così non fosse, infatti, $f|_m$ sarebbe una biiezione fra m e $m \setminus \{f(m)\}$, contro l'ipotesi induttiva. Ora, però, possiamo costruire una nuova biiezione $f' : s(m) \to B$ che ricade nel caso precedente:

$$f'(x) = \begin{cases} m & \text{se } x = m \\ f(m) & \text{se } x = a \\ f(x) & \text{altrimenti} \end{cases}$$

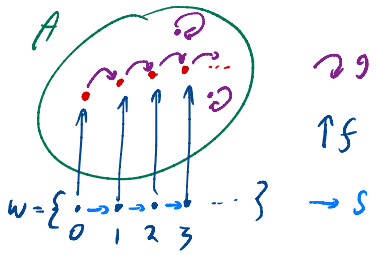
Cor Se A è un insieme finito, allora $\exists!\, n \in \omega$ $|A| = |n|$

Dim Se $|m| = |A| = |n|$, possiamo assumere, senza perdita di generalità $m \leq n$, ossia $m \subseteq n$, quindi $m = n$ per il principio dei cassetti.

Se adesso volessimo dimostrare il viceversa: che un insieme infinito non è Dedekind-finito, quale sarebbe l'ostacolo? Abbiamo già osservato che ω non è finito, poiché la funzione successore stabilisce una corrispondenza biunivoca fra ω e $\omega \setminus \{0\} \subsetneq \omega$. Ne segue la seguente osservazione.

Oss. Se esiste $f : \omega \to A$ iniettiva, allora A non è Dedekind-finito.

Dim Basta considerare la funzione iniettiva



$$g : A \to A$$

$$g(a) = \begin{cases} f(s(f^{-1}(a))) & \text{se } a \in f[w] \\ a & \text{altrimenti} \end{cases}$$

È immediato vedere che $Im(g) = A \setminus \{f(0)\} \subsetneq A$ ☒

Quindi ci basterebbe dimostrare che w si immerge in ogni insieme infinito. Un tentativo di dimostrazione potrebbe andare come segue.

Sia A infinito, costruiamo per ricorsione, seconda forma, una $f : w \to A$ iniettiva. Supponiamo di conoscere $f_{|n}$, il nostro scopo è definire il prossimo valore: $f(n)$. Siccome A è infinito, $f_{|n}$, che è iniettiva per costruzione, non può essere surgettiva, quindi esiste $a \in A$ con $a \notin Im(f_{|n})$. Pongo $f(n) = a$.

Dov'è l'errore? Nell'ultima riga! Noi sappiamo che, data $f_{|n}$, esistono degli $a \in A$ con $a \notin Im(f_{|n})$, questo è corretto. È anche corretto che ci basterebbe porre $f(n) =$ "uno qualunque di questi a". Il guaio è che, per applicare il teorema di ricorsione, ci serve una funzione che fissa uno degli a. A patto di averne una, ne andrebbe bene una qualunque.

Purtroppo, però, a partire dalla mera ipotesi che A è infinito, non abbiamo modo di procurarci nessuna funzione del genere. Potremmo cavarcela se avessimo qualche struttura su A, sulla quale far leva — per esempio per dire "prendo il minimo fra gli $a \notin \mathrm{Im}(f_n)$", o "prendo il più giallo" — ma di A non sappiamo nulla, e non abbiamo modo di indurre una struttura di questo genere.

Accettato che non possiamo dimostrare che ω si immerge in qualsiasi insieme infinito, possiamo però lambire questa soglia: dimostriamo che, in un insieme infinito, si immergono tutti i numeri naturali.

Prop. Sia A infinito. Allora $\forall n \in \omega \quad |n| < |A|$

Dim Basta dimostrare il $\leq$, infatti $|n| < |n+1| \leq |A|$.

Dimostriamo per induzione su n che c'è una funzione iniettiva da n ad A.

Caso $n=0$. La funzione vuota.

Caso $n=m+1$. Per ipotesi induttiva esiste $f : m \to A$ iniettiva. Siccome A è infinito, esiste $a \in A \setminus \mathrm{Im}(f)$. La funzione $f' = f \cup \{(m, a)\}$, che si ottiene estendendo f col mandare m in a, è iniettiva $n \to A$. ∎

Cor Un sottoinsieme di un insieme finito è finito.

Dim Sia A finito e $B \subseteq A$. Se, per assurdo, B fosse infinito, avremmo $|A| < |B| \leq |A|$ ↯

Esercizi Dimostra che:
- se $|A| < |n|$ con $n \in \omega$, allora $|A| = |m|$ per qualche $m < n$
- se A è finito e $f : A \to B$, allora $f[A]$ è finito.

Prop Dati $m, n \in \omega$

$$|m| + |n| = |m+n| \qquad |m| \cdot |n| = |m \cdot n| \qquad |m|^{|n|} = |m^n|$$

Dim Dimostriamo, intanto, che $|m| + |1| = |S(m)|$. A sinistra abbiamo, infatti, la cardinalità di $m \times \{0\} \cup \{(1,1)\}$ e a destra quella di $m \cup \{m\}$. Quest'ultimo insieme si mappa biiettivamente nel primo mandando $x \in m$ in $(x,0)$ e m in $(1,1)$.
Ora, le uguaglianze asserite seguono, per induzione su n, dalle proprietà delle operazioni sulle cardinalità e dalla definizione ricorsiva delle operazioni su ω.

$|m| + |n| = |m+n|$

caso $n = 0$. $|m| + |0| = |m| = |m + 0|$

caso $n = S(a)$.
$$\begin{aligned}
|m| + |S(a)| &= |m| + (|a| + |1|) && \text{osservazione iniziale}\\
&= (|m| + |a|) + |1| && \text{proprietà operazioni}\\
&= |m + a| + |1| && \text{ipotesi induttiva}\\
&= |S(m+a)| && \text{di nuovo l'osservazione}\\
&= |m + S(a)| && \text{definizione di } +
\end{aligned}$$

$|m| \cdot |n| = |m \cdot n|$

caso $n = 0$. $|m| \cdot |0| = |0| = |m \cdot 0|$

caso $n = s(a)$.

$$\begin{aligned}
|m| \cdot |s(a)| &= |m| \cdot (|a| + |1|) && \text{osservazione iniziale}\\
&= |m| \cdot |a| + |m| && \text{proprietà operazioni}\\
&= |m \cdot a| + |m| && \text{ipotesi induttiva}\\
&= |m \cdot a + m| && \text{identità per il } +\\
&= |m \cdot s(a)| && \text{definizione di } \cdot
\end{aligned}$$

$|m|^{|n|} = |m^n|$

caso $n = 0$. $|m|^{|0|} = |1| = |m^0|$

caso $n = s(a)$.

$$\begin{aligned}
|m|^{|s(a)|} &= |m|^{|a|+|1|} && \text{osservazione iniziale}\\
&= |m|^{|a|} \cdot |m| && \text{proprietà operazioni}\\
&= |m^a| \cdot |m| && \text{ipotesi induttiva}\\
&= |m^a \cdot m| && \text{identità per il } \cdot\\
&= |m^{s(a)}| && \text{definizione di potenza}
\end{aligned}$$

∎

Nota Questa proposizione ci fornisce una dimostrazione delle proprietà aritmetiche elementari delle operazioni su ω, alternativa a quella per induzione (che è stata lasciata come esercizio). Basta, infatti, applicare le corrispondenti proprietà delle operazioni sulle cardinalità.

Esercizio Dimostra che se $m, n \in \omega$ e $m \leq n$, esiste un unico $n - m \in \omega$ tale che $m + (n - m) = n$. In due modi diversi.

La cardinalità del numerabile — $\aleph_0$.

Def Diciamo che A è *al più numerabile* se $|A| \leq |\omega|$ ed è *numerabile* se $|A| = |\omega|$. Il simbolo $\aleph_0$ — *alef con zero* — è semplicemente un'abbreviazione per $|\omega|$. Per cui $|A| \leq \aleph_0$ si può leggere "A è al più numerabile" e $|A| = \aleph_0$ si può leggere "A è numerabile".

Oss In altri termini, dire che A è al più numerabile significa dire che c'è una funzione iniettiva $A \to \omega$. Dire che è numerabile significa dire che è in biiezione con ω.

Prop Se A è al più numerabile, allora o A è finito o A è numerabile.
Ossia: $|A| < \aleph_0$ se e solo se A è finito.

Potremmo dimostrare la proposizione direttamente, ma ci conviene, invece, passare attraverso alcune considerazioni che saranno utili in seguito.
In generale, per costruire una biiezione fra due insiemi A e B — ossia per dimostrare $|A| = |B|$ — occorre appoggiarsi a qualche struttura definita sugli insiemi A e B. Per esempio, una funzione successore. In questo

corso, giocheranno un ruolo importante, in questa direzione, le relazioni d'ordine, e, in particolare — l'idea è di Cantor — i buoni ordini. Ricordiamo la definizione.

Def Un insieme totalmente ordinato $(S, <)$ si dice **bene ordinato** se ogni suo sottoinsieme non vuoto ha un minimo.

$$\forall A \subseteq S \quad A \neq \emptyset \to \exists m \in A \ \forall x \in A \ m \leq x$$

Il trucco è che un isomorfismo di ordini è, in particolare, una biiezione, e spesso, per costruire biiezioni, costruiamo isomorfismi di ordini.

Def Due insiemi (parzialmente) ordinati $(A, <_A)$ e $(B, <_B)$ sono **isomorfi**, in simboli $(A, <_A) \sim (B, <_B)$, se esiste una biiezione $f : A \to B$ tale che

$$\forall x, y \in A \quad x <_A y \iff f(x) <_B f(y)$$

Oss Due insiemi TOTALMENTE ordinati $(A, <_A)$ e $(B, <_B)$ sono isomorfi se e solo se esiste una funzione $f : A \to B$ surgettiva e **strettamente crescente** — cioè tale che

$$\forall x, y \in A \quad x <_A y \to f(x) <_B f(y)$$

Rim esercizio.

Oss Sia $(A, <_A)$ totalmente ordinato con $|A| = n \in \omega$. Allora $(A, <_A) \sim (n, <)$, dove $<$ denota l'ordinamento indotto da ω.

Dim Per induzione su n.

caso $n=0$. $A=\emptyset$ quindi $(A, <_a) \sim (\emptyset, \emptyset)$.

caso $n=s(m)$. Se $m=0$, allora $A=\{a\}$ e $(A, <_a) \sim (1, <)$.

Assumiamo quindi $m>0$. Dimostriamo, intanto, che $(A, <_a)$ ha un massimo elemento. Fissiamo una biiezione $f: s(m) \to A$. Allora $|f[m]|=m$, quindi $f[m]$ con l'ordinamento indotto da $<_a$ è isomorfo a $(m, <)$ per ipotesi induttiva, e, in particolare, ha un massimo M. Ora, per la totalità di $<_A$, o $M < f(m)$ oppure $f(m) < M$. Si verifica immediatamente che, nel primo caso, $f(m)$ è il massimo di A, e nel secondo M è il massimo di A.

Stabilito che A ha un massimo N, osserviamo che, detto $A' = A - \{N\}$, siccome $|A'|=m$, usando nuovamente l'ipotesi induttiva abbiamo un isomorfismo $f: A' \to m$ fra A' con l'ordinamento indotto da $<_a$ e $(m, <)$. Si verifica facilmente che

$$f': A \to s(m) \qquad f'(x) = \begin{cases} f(x) & \text{se } x \in A' \\ m & \text{se } x = N \end{cases}$$

è l'isomorfismo cercato. ∎

Possiamo caratterizzare ω in termini delle proprietà del suo ordinamento naturale. Quelle che servono sono le seguenti:

Oss. 1. $(\omega, <)$ è un buon ordine

2. $(\omega, <)$ è illimitato — ossia $\forall x \in \omega \; \exists y \in \omega \;\; x < y$

3. Ogni $A \subseteq \omega$ superiormente limitato e non vuoto ha un massimo, ossia

$$\forall A \subseteq \omega \left(A \neq \emptyset \wedge \underbrace{(\exists L \in \omega \; \forall x \in A \;\; x \leq L)}_{\equiv \text{“}A \text{ è superiormente limitato”}} \right) \dots$$

$$\dots \longrightarrow (\exists M \in A \; \forall x \in A \;\; x \leq M)$$

Dim. 1. è il principio del minimo, e per 2. basta prendere $y = s(x)$. Per 3., osserviamo che, se A è superiormente limitato da $L \in \omega$, allora $A \subseteq s(L)$, quindi A è finito. Sia come A è finito, l'ordinamento totale su A definito da

$$x \preceq y \overset{\text{d.f.}}{\equiv} y < x$$

è buono, quindi, in particolare, c'è il minimo di A secondo l'ordinamento $\preceq$. Questo è il massimo di A. ∎

Prop. Sia $(A, \preceq)$, con $A \neq \emptyset$, un ordinamento

1. buono
2. illimitato
3. tale che ogni sottoinsieme superiormente limitato e non vuoto di A ha un massimo secondo $\preceq$

Allora $(A, \preceq) \sim (\omega, <)$.

Dimostriamo prima un facile lemma.

Lemma Sia $(A, \prec)$ un ordine, e sia $f : \omega \to A$ tale che

$$\forall n \in \omega \quad f(n) \prec f(s(n))$$

Allora f è strettamente crescente, $\forall m, n \in \omega \quad m < n \to f(m) \prec f(n)$, e, in particolare, iniettiva.

Dim Consideriamo, per assurdo, $m < n$ tali che $f(m) \not\prec f(n)$, con n minimo. Siccome $0 \leq m < n$, esiste n' tale che $n = s(n')$. O $n' = m$ o $m < n'$. Nel primo caso $f(m) \prec f(s(n')) = f(n)$ contraddicendo $f(m) \not\prec f(n)$. Nel secondo, per la minimalità di n, $f(m) \prec f(n')$, ma $f(n') \prec f(s(n')) = f(n)$, quindi abbiamo di nuovo la contraddizione $f(m) \prec f(n)$. ∎

Dim (proposizione) Costruiamo per ricorsione un isomorfismo f da $(\omega, <)$ a $(A, \prec)$.

$$f(0) = \min_{\prec} A \qquad f(s(n)) = \min_{\prec} \{a \in A \mid f(n) \prec a\}$$

dove $\min_{\prec}$ denota il minimo secondo $\prec$.

Occorre dimostrare, intanto, che f è ben definita.

$f(0)$ è ben definita perché $A \neq \emptyset$, quindi ha un minimo.

Per dire che $f(s(n))$ è ben definita, occorre dire che la funzione $h : A \to A$, $h(x) = \min_{\prec} \{a \in A \mid x \prec a\}$ è ben definita, ossia che $\{a \in A \mid x \prec a\}$ è non vuoto. Ma questo avviene, qualsiasi sia $x \in A$, perché altrimenti A sarebbe limitato da x.

Per come è costruita, e per il lemma, f è crescente, quindi

iniettiva. Di conseguenza, ci basta dimostrare la suriettività. Prendiamo $y \in A$ e cerchiamo x tale che $f(x) = y$.
Se, per ogni $x \in \omega$, avessimo $f(x) \prec y$, allora $f[\omega]$ sarebbe superiormente limitato da y, e tuttavia non avrebbe massimo perché ogni $f(x)$ è $\prec$ di $f(s(x))$. Quindi c'è il minimo $x \in \omega$ tale che $y \preceq f(x)$. Dimostriamo che $f(x) \preceq y$, da cui l'uguaglianza cercata.
Se $x = 0$, allora $f(x)$ è il minimo di A, quindi $f(x) \preceq y \in A$.
Se $x = s(x')$, $f(x') \prec y$ per la minimalità di x, ma allora, $y \in \{a \in A \mid f(x') \prec a\}$ quindi $f(x) = f(s(x')) = \min_{\prec}\{\dots\} \preceq y$ ∎

Tornando alla proposizione iniziale

Prop. Se A è al più numerabile, allora o A è finito o A è numerabile.

Dim Per ipotesi esiste $f : A \to \omega$ iniettiva, per cui abbiamo $|A| = |f[A]|$, e, siccome $f[A] \subseteq \omega$, ci basta dimostrare che dato $B \subseteq \omega$, o B è finito o è numerabile.

Sia $B \subseteq \omega$ infinito, dimostriamo che B, con l'ordinamento indotto dall'ordine naturale di ω, soddisfa le ipotesi della proposizione precedente.
1. e 2. valgono in quanto ogni sottoinsieme di B è, in particolare, sottoinsieme di ω. Per ottenere 3. dobbiamo dire

che $\mathcal{B}$ non ha un massimo elemento. Se, infatti, ci fosse un $M \in \mathcal{B}$ tale che $\forall b \in \mathcal{B}\ b \subseteq M$, allora avremmo che $\mathcal{B} \subseteq S(M)$. $\mathcal{B}$ sarebbe dunque finito, contro l'ipotesi. ∎