Ordini densi numerabili

Il prossimo risultato che vedremo è, come al solito, dovuto a Cantor, e caratterizza l'ordine di $\mathbb{Q}$ a meno di isomorfismi.

Def Sia $(A, <)$ totalmente ordinato, e $B \subseteq A$.

B è denso in $(A, <)$ $\overset{def.}{\equiv}$ $\forall x, y \in A \quad x < y \to \exists z \in B \quad x < z < y$

$(A, <)$ è denso $\overset{def.}{\equiv}$ A è denso in se stesso, cioè

$\forall x, y \in A \quad x < y \to \exists z \in A \quad x < z < y$

Esempio Abbiamo già osservato, in un esercizio, che $\mathbb{Q}$ è denso, infatti $x < y \to x < \frac{x+y}{2} < y$.

NON Esempio L'insieme ω con il suo ordinamento naturale non è denso, perché $\nexists z \in \omega \quad 0 < z < 1$.

Teorema (di isomorfismo di Cantor)

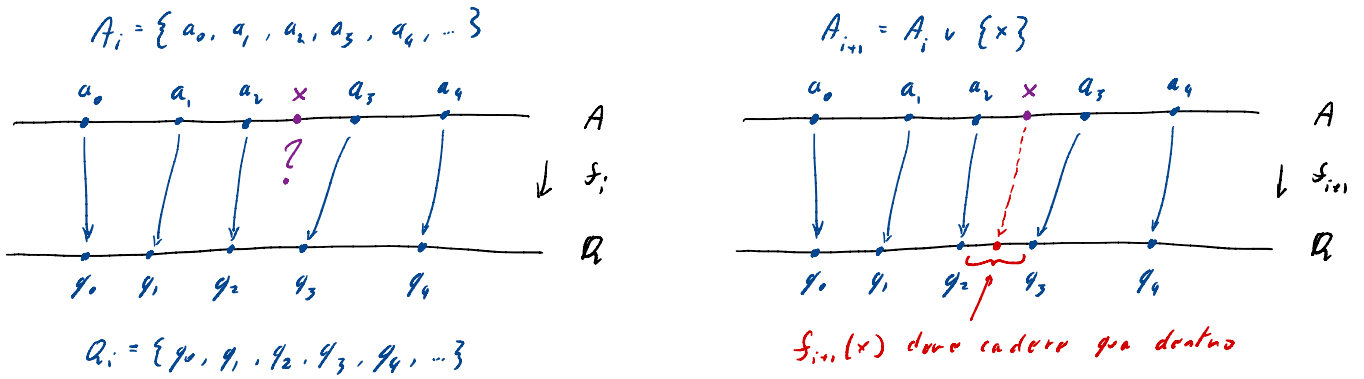
Sia $(A, <)$ un insieme totalmente ordinato tale che

- $|A| = \aleph_0$
- $(A, <)$ è denso
- $(A, <)$ non ha estremi, ossia non ha né massimo né minimo elemento.

Allora $(A, <) \sim (\mathbb{Q}, <)$.

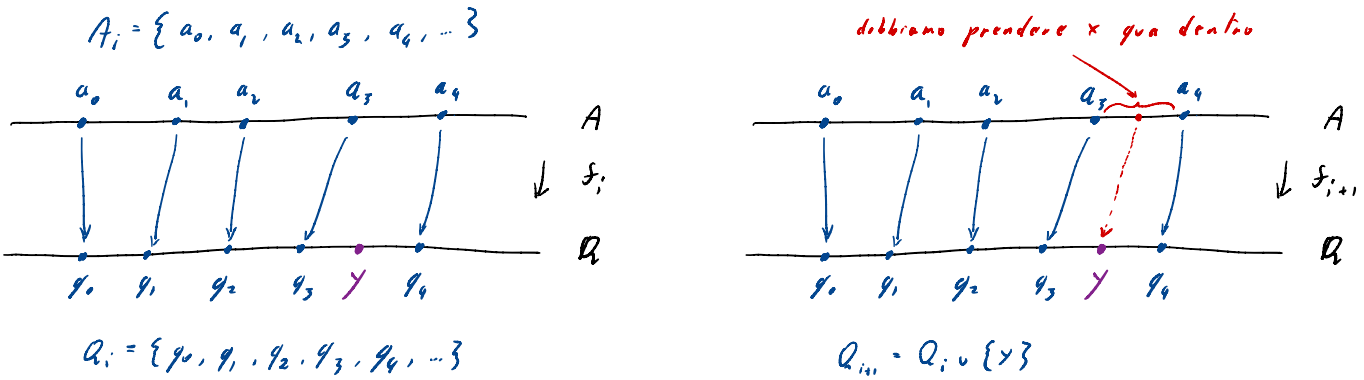
L'idea è di costruire l'isomorfismo per ricorsione. Ad

ogni passo della ricorsione avremo $f_i : A_i \to Q_i$ isomorfismo con $A_i \subseteq A$ finito e $Q_i \subseteq \mathbb{Q}$. Dovremo quindi estendere f_i ingrandendo il suo dominio. Supponiamo, per esempio, di



voler definire $f_{i+1}(x)$ con $x \notin A_i$. Allora, siccome A_i è finito, per sapere la posizione di x rispetto a ciascuno degli elementi di A_i, ci basta sapere quale sia l'ultimo elemento prima di x, e quale sia il primo dopo x — diciamo che, per esempio, sono a_2 e a_3 rispettivamente. Dovremo allora mandare x in un $f_{i+1}(x)$ con $f_i(a_2) < f_{i+1}(x) < f_i(a_3)$, e questo esiste per la densità di $\mathbb{Q}$.

Ragionando simmetricamente, possiamo anche estendere f_i, dato un $y \in \mathbb{Q}$ con $y \notin Q_i$, in modo tale che $y \in \mathrm{Im}(f_{i+1})$.



In definitiva, ci basta quindi fissare un'enumerazione di A e una di $\mathbb{R}$, e fare questi passi di estensione in maniera alternata, assicurandoci così di aggiungere al dominio della f, uno per uno, tutti gli elementi di A, e di aggiungere all'immagine, uno per uno, tutti gli elementi di $\mathbb{R}$.
Ci sarà comodo la seguente osservazione.

Oss. Sia $F \subseteq \mathcal{P}(A \times B)$ un insieme di funzioni. Se

$$\forall f_1, f_2 \in F \quad f_1|_{Dom(f_1) \cap Dom(f_2)} = f_2|_{Dom(f_1) \cap Dom(f_2)}$$

ossia $\forall x \in Dom(f_1) \cap Dom(f_2) \quad f_1(x) = f_2(x)$

Allora $\bigcup F$ è una funzione: $\bigcup \{Dom\, f \mid f \in F\} \to B$.

Dim Bisogna verificare che, se $(x, y_1) \in \bigcup F$ e $(x, y_2) \in \bigcup F$, allora $y_1 = y_2$. Dalla prima abbiamo che esiste $f_1 \in F$ con $y_1 = f_1(x)$ e dalla seconda abbiamo che esiste $f_2 \in F$ con $y_2 = f_2(x)$, ma quindi $x \in Dom(f_1) \cap Dom(f_2)$ e, per ipotesi, $y_1 = f_1(x) = f_2(x) = y_2$. ∎

Dim (Teorema)
Fissiamo due enumerazioni di A e $\mathbb{R}$ rispettivamente

$$A = \{a_i \mid i \in \omega\} \qquad \mathbb{R} = \{q_i \mid i \in \omega\}$$

Intendiamo costruire una successione di funzioni $\{f_i\}_{i \in \omega}$ tali che, per ogni $i \in \omega$

1. $f_i : A_i \to \mathbb{R}_i$ con $|A_i| = |\mathbb{R}_i| < \aleph_0$
2. f_i è un isomorfismo di ordini fra A_i e $\mathbb{R}_i$

3. $f_i \subseteq f_{s(i)}$ ossia f_{i+1} estende f_i

4. $\forall j < i \quad a_j \in A_i \wedge q_j \in Q_i$ ossia $\{a_0 \dots a_{i-1}\} \subseteq Dom(f_i)$

$\{q_0 \dots q_{i-1}\} \subseteq Im(f_i)$

Verifichiamo, per cominciare, che da 1...4 segue che $f \overset{def}{=} \bigcup_{i \in \omega} f_i$ è un isomorfismo di ordini fra A e Q. Da 3. segue, con una facile induzione, che $\forall i,j \in \omega \; i \leq j \to f_i \subseteq f_j$. Quindi siamo nella situazione dell'osservazione, e, di conseguenza, f è una funzione. Inoltre 4. implica che $Dom(f) = A$ e $Im(f) = Q$.

Ci resta quindi da verificare che, date $x, y \in A$,

$$x < y \iff f(x) < f(y)$$

Siccome $\{a_i\}_{i \in \omega}$ enumera A, esistono $m, n \in \omega$ tali che $x = a_m$ $y = a_n$. Preso $t \in \omega$ con $m, n < t$, per la 4., $a_m, a_n \in Dom(f_t)$, e, siccome f_t è un isomorfismo di ordini per la 2., abbiamo

$$x = a_m < a_n = y \iff f(x) = f_t(a_m) < f_t(a_n) = f(y).$$

Descriviamo ora la costruzione per ricorsione numerabile della successione di funzioni f_i. Intanto poniamo $f_0 = \emptyset$.

Per costruire $f_{s(i)}$ definiamo prima un passo intermedio $f_{i+0.5}$:

Se $a_i \in Dom(f_i)$ allora $f_{i+0.5} = f_i$ (ossia è strettamente crescente)

Altrimenti sia $\bar{j} = \min \{ j \in \omega \mid f_i \cup \{(a_i, q_j)\} \text{ è un iso.} \}$, poniamo $f_{i+0.5} = f_i \cup \{(a_i, q_{\bar{j}})\}$

Ora definiamo $f_{s(i)}$

Se $q_i \in Im(f_{i+0.5})$ allora $f_{s(i)} = f_{i+0.5}$

Altrimenti: sia $\bar{l} = \min\{l \in \omega \mid f_{i+0.5} \cup \{(a_l, q_i)\} \text{ è un iso}\}$

poniamo $f_{s(i)} = f_{i+0.5} \cup \{(a_{\bar{l}}, q_i)\}$

Le proprietà 1..4 seguono in maniera immediata per induzione, a patto che la costruzione sia ben posta, ossia i minimi esistano. Ad essere precisi, occorre quindi dimostrare, per induzione su i, la proposizione

$\forall i \in \omega$ "la costruzione di f_i è ben posta e valgono 1...4"

Vediamo che esiste il minimo nel primo passaggio:

$$\bar{j} = \min\{j \in \omega \mid f_i \cup \{(a_i, q_j)\} \text{ è un iso.}\}$$

ossia che l'insieme di cui si prende il minimo non è vuoto. Il secondo caso è analogo. Per ipotesi induttiva A_i è finito. Se $A_i = \emptyset$ non c'è niente da dimostrare, altrimenti, detto $n = |A_i|$, e sfruttando il fatto che un ordine totale finito è isomorfo ad un numero naturale

$$A_i = \{a_0, \dots, a_{n-1}\} \qquad \text{con} \qquad a_0 < \dots < a_{n-1}$$

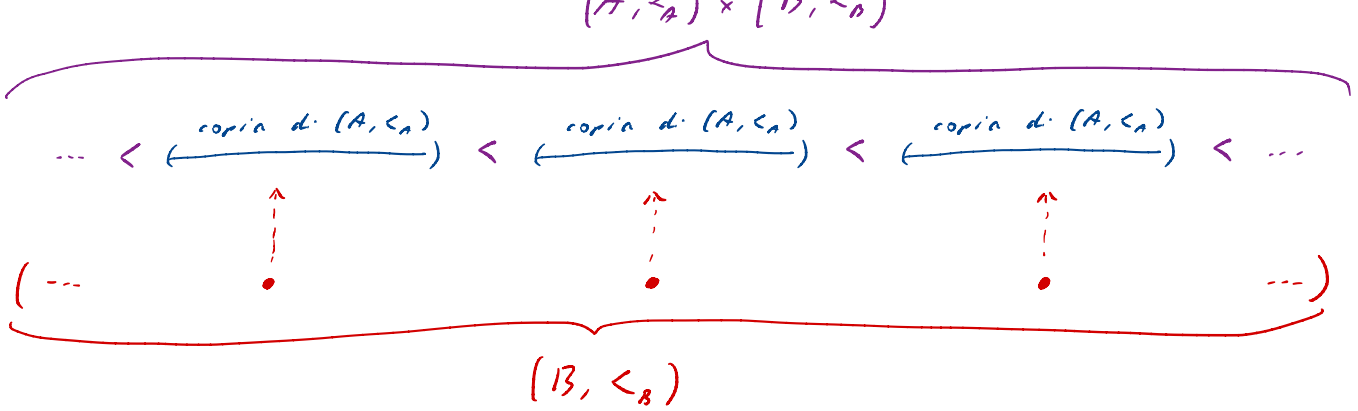
Ora, l'ipotesi è che $a_i \notin A_i$ quindi o $a_i < a_0$, o $a_k < a_i < a_{k+1}$ per qualche k, o $a_{n-1} < a_i$. Nel primo e nel terzo caso, rispettivamente, siccome $\mathbb{Q}$ non ha estremi, c'è un $q_j < f_i(a_0)$, o $q_j > f_i(a_n)$ rispettivamente. Nel secondo caso, per la densità di $\mathbb{Q}$, esiste q_j con $f_i(a_k) < q_j < f_i(a_{k+1})$. ∎

Cor Sia $(A, <)$ un ordine totale con $|A| \leq \aleph_0$.
Allora esiste $B \subseteq \mathbb{Q}$ tale che $(A, <) \sim (B, <)$ con l'ordinamento indotto su B da $\mathbb{Q}$.

Nota Volendo, si potrebbe dimostrare questo corollario ripetendo, con qualche variazione, la dimostrazione del teorema. Ora daremo, però, un argomento che, invece, applica il teorema.
È comodo definire, prima, il prodotto di ordini.

Def (prodotto lessicografico di ordini)
Dati $(A, <_A)$ e $(B, <_B)$ definiamo $(A, <_A) \times (B, <_B) \overset{\text{def.}}{\equiv} (A \times B, <_{A\times B})$
dove $(a, b) <_{A\times B} (a', b') \overset{\text{def}}{\equiv} b <_B b' \vee [b = b' \wedge a <_A a']$.

Ossia: $(A, <_A) \times (B, <_B)$ è il prodotto cartesiano $A \times B$ munito dell'ordine che CONFRONTA PRIMA LA SECONDA COMPONENTE.
Visualmente, si può immaginare $(A, <_A) \times (B, <_B)$ come "$(A, <_A)$ ripetuto $(B, <_B)$ volte"



Oss. Il prodotto è un ordine. Inoltre se $(A, <_A)$ e $(B, <_B)$ sono ordini totali, allora anche $(A, <_A) \times (B, <_B)$ lo è.

Esercizio Dati $(A, <_A)$, $(B, <_B)$ e $(C, <_C)$ dimostrare che

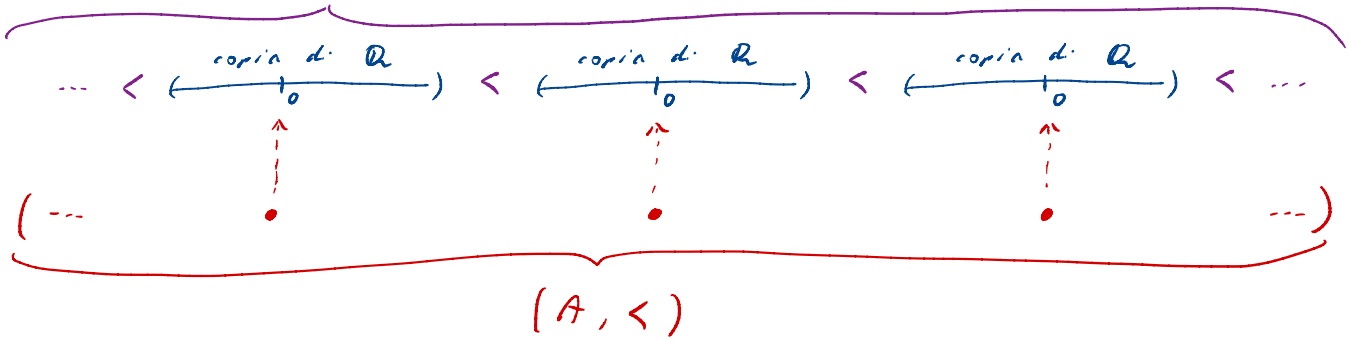
$$\big((A, <_A) \times (B, <_B)\big) \times (C, <_C) \sim (A, <_A) \times \big((B, <_B) \times (C, <_C)\big)$$

ossia che il prodotto di ordini è associativo a meno di isomorfismi.

Dim (corollario)

Il caso $A = \emptyset$ è banale. Supponiamo $A \neq \emptyset$ e consideriamo

$$(S, <) \overset{\text{def.}}{=} (\mathbb{Q}, <) \times (A, <)$$



$S = \mathbb{Q} \times A$ è numerabile. Inoltre, dato $(q, a) \in \mathbb{Q} \times A$ abbiamo $(q-1, a) < (q, a) < (q+1, a)$, quindi $\mathbb{Q} \times A$ non ha estremi. Per verificare che è denso, consideriamo $(q_1, a_1) < (q_2, a_2)$

Se $a_1 < a_2$, allora $(q_1, a_1) < (q_1 + 1, a_1) < (q_2, a_2)$

Se $a_1 = a_2$, allora $(q_1, a_1) < \left(\frac{q_1 + q_2}{2}, a_1\right) < (q_2, a_1) = (q_2, a_2)$. ∎

Esercizio Dimostra che se $(A, <)$ è denso e $2 \leq |A| \leq \aleph_0$, allora $(A, <)$ è isomorfo a uno dei seguenti intervalli di $\mathbb{Q}$.

$$[0, 1]_{\mathbb{Q}} \qquad]0, 1]_{\mathbb{Q}} \qquad [0, 1[_{\mathbb{Q}} \qquad]0, 1[_{\mathbb{Q}}$$

La tecnica di estendere indefinitamente isomorfismi parziali che ci ha permesso di dimostrare il teorema di isomorfismo

di Cantor si chiama back-and-forth, ed è un metodo fondamentale per trovare isomorfismi fra strutture.
Colgo questa occasione per suggerirne un esercizio di applicazione della medesima tecnica che è un po' complicato. Si tratta di definire il grafo random o grafo di Rado.

Def (grafo)
Un grafo (V, e) sull'insieme di vertici V è dato da una relazione e simmetrica e irriflessiva.

$$\forall x,y \in V \ (x,y) \in e \leftrightarrow (y,x) \in e \qquad \forall x \in V \ (x,x) \notin e$$

L'idea è che V può essere immaginato come un insieme di punti che possono essere connessi da archi. C'è un arco fra x e y se $(x,y) \in e$.

Partiamo da un'idea intuitiva — chi ha già seguito un corso di probabilità saprà formalizzare questa cosa in termini precisi. Data una probabilità $p \in]0,1[$ costruiamo un grafo G_p con insieme di vertici ω come segue. Per ogni coppia $(i,j) \in \omega \times \omega$ con $i<j$ lanciamo una moneta che fa testa con probabilità p — tutte queste monete indipendenti — e, se viene testa, mettiamo un arco fra i e j.

Potremmo pensare che i grafi $G_{0.01}$ e $G_{0.99}$ debbano venire molto diversi: uno ha l'1% degli archi possibili, l'altro

ha il 99%, insomma uno è quasi vuoto, l'altro quasi completo. Avviene, tuttavia, che, con probabilità 1, questi grafi sono isomorfi, dove, per essere precisi:

Def I grafi (V_1, e_1) e (V_2, e_2) sono *isomorfi* se esiste una biiezione $f: V_1 \to V_2$ tale che

$$\forall v, w \in V_1 \quad (v,w) \in e_1 \longleftrightarrow (f(v), f(w)) \in e_2$$

Vediamo perché: Dati due sottoinsiemi finiti X e Y di ω, e dato un vertice $v \notin X \cup Y$ la probabilità che v sia connesso da un arco a tutti i vertici di X e a nessuno di quelli di Y è $p^{|X|} \cdot (1-p)^{|Y|}$ — come che sia, è un certo numero >0 — e ci sono infiniti $v \notin X \cup Y$. Si capisce, quindi, che con probabilità 1 — ossia certamente — almeno uno di questi vincerà questa lotteria, ossia sarà connesso a tutti gli X e a nessuno degli Y. Usiamo l'esistenza di questo v per definire un grafo random.

Def Il grafo (ω, e) è un grafo random se

$$\forall X \subseteq \omega \; \forall Y \subseteq \omega \setminus X \; \exists v \in \omega \setminus (X \cup Y) \; \underbrace{X \times \{v\} \subseteq e}_{\forall x \in X \; (x,v) \in e} \wedge \underbrace{(Y \times \{v\}) \cap e = \emptyset}_{\neg \exists y \in Y \; (y,v) \in e}$$

Esercizio Dimostra che esiste un grafo random, ed è unico a meno di isomorfismi.

$\mathbb{R}$ e la cardinalità del continuo

In questa sezione daremo una definizione di $\mathbb{R}$ come insieme ordinato. Estenderemo, poi, la definizione ad includere le operazioni di campo, ma senza svolgere verifiche.

Definizioni

Sia $(A, <)$ un ordine totale.

- $m \in A$ è un *maggiorante* di $B \subseteq A$ se $\forall x \in B \; x \leq m$
- $B \subseteq A$ è *superiormente limitato* se ha un maggiorante
- $s \in A$ è l'*estremo superiore* di B — denotato $\sup B$ — se s è il minimo dei maggioranti di B.

Nota Non sempre gli estremi superiori esistono, e, se B ha un estremo superiore, questo è unico.

Def. Un ordine totale $(A, <)$ è *completo* se ogni $B \subseteq A$ superiormente limitato ha un estremo superiore $\sup B \in A$.

Esercizio Dimostra, usando solo le proprietà di $\mathbb{Q}$, che l'insieme $\{x \in \mathbb{Q} \mid x^2 < 2\}$ NON ha un estremo superiore in $\mathbb{Q}$.

In conseguenza dell'esercizio, possiamo dire che $\mathbb{Q}$ non è completo. Costruiamo ora un ordine completo $(\mathbb{R}, <)$ che contiene una copia isomorfa di $\mathbb{Q}$ come sottoinsieme denso.

Def. Sia $(A, <)$ un ordine totale. $B \subseteq A$ è un *segmento iniziale* di A se $\forall x \in B \; \forall y \in A \; y < x \to y \in B$.

Ossia B è un segmento iniziale di A se, ogniqualvolta B contiene un elemento, B contiene altresì tutti gli elementi minori di questo.

Un segmento iniziale B di A si dice *proprio* se $B \neq A$.

Esempi Dato $(A, <)$ ordine totale, A stesso e $\emptyset$ sono segmenti iniziali di A. Dato $x \in A$, l'insieme

$$A_x \overset{\text{def.}}{=} \{y \in A \mid y < x\}$$

è un segmento iniziale proprio di A — detto segmento iniziale *principale* determinato da x.

L'insieme $\{x \in \mathbb{Q} \mid x < 0 \vee x^2 < 2\}$ è un segmento iniziale di $\mathbb{Q}$ che non è principale.

Nota: Useremo nuovamente il concetto di segmento iniziale studiando gli ordinali. Il prossimo concetto, quello di sezione di Dedekind, invece, ci serve unicamente per definire $\mathbb{R}$.

Def (Sezioni di Dedekind)

Una *sezione* sull'insieme totalmente ordinato $(A, <)$ è un segmento iniziale *proprio* e *non vuoto* di A che *non ha un maggiore* elemento. Ossia B segmento iniziale di A è una sezione se $B \neq A$, $B \neq \emptyset$ e $\forall x \in B \; \exists y \in B \; x < y$.

Def (di $\mathbb{R}$ come insieme ordinato)

$$\mathbb{R} \overset{\text{def.}}{=} \{x \in \mathcal{P}(\mathbb{Q}) \mid x \text{ è una sezione su } \mathbb{Q}\}$$

Dati $x, y \in \mathbb{R}$

$$x \leq y \overset{\text{def.}}{=} x \subseteq y$$

Prop. $(\mathbb{R}, <)$ è un ordine totale completo.

Prima della dimostrazione, isoliamo un semplice lemma.

Lemma Sia $(A, <)$ un ordine totale e X un insieme di segmenti iniziali di A. Allora $\bigcup X$ è un segmento iniziale di A.

Dim Sia $\alpha \in \bigcup X$ e $\beta \in A$ con $\beta < \alpha$. Dobbiamo dimostrare che $\beta \in \bigcup X$. Siccome $\alpha \in \bigcup X$, esiste $x \in X$ con $\alpha \in x$. Siccome x è segmento iniziale A, $\beta \in x \subseteq \bigcup X$. ∎

Dim (Prop.) Abbiamo un ordine parziale perché il contenimento, $\subseteq$, è un ordine parziale su $\mathcal{P}$(quello che sia). Supponiamo, per assurdo, che non sia totale, allora esistono $x, y \in \mathbb{R}$ con $x \not\subseteq y$ e $y \not\subseteq x$, per cui ci sono $a \in x \setminus y$ e $b \in y \setminus x$. Ora si danno due casi: se $a < b$ allora $b \in y \Rightarrow a \in y$ ~~↯~~ simmetricamente, se $b < a$ allora $a \in x \Rightarrow b \in x$ ~~↯~~

Resta da dimostrare la completezza. Sia $A \in \mathbb{R}$ non vuoto e superiormente limitato da $m \in \mathbb{R}$.

Dimostriamo che $\sup A = \bigcup A \in \mathbb{R}$.

Per il lemma, $\bigcup A$ è un segmento iniziale, siccome A non è vuoto $\bigcup A \neq \emptyset$, siccome m è un maggiorante di A, $\bigcup A \subseteq m$, quindi $\bigcup A \neq A$. In definitiva $\bigcup A$ è una sezione, e, di conseguenza, un elemento di $\mathbb{R}$.

Verifichiamo che $\bigcup A$ è un maggiorante di A. Se $x \in A$, allora $x \subseteq \bigcup A$, cioè, appunto $x \leq \bigcup A$.

Ora, se m è un maggiorante di A, allora $\forall x \in A \; x \subseteq m$, ma questo equivale a $\bigcup A \subseteq m$, quindi $\bigcup A$ è il minimo dei maggioranti di A. ∎

Oss La funzione $\iota : \mathbb{Q} \to \mathbb{R}$ $\iota(a) = \mathbb{Q}_a = \{x \in \mathbb{Q} \mid x < a\}$ immerge $\mathbb{Q}$ in $\mathbb{R}$ in maniera strettamente crescente e densa.
(Ossia $\mathrm{Im}(\iota)$ è densa in $\mathbb{R}$)

Dim Dati $a, b \in \mathbb{Q}$ con $a < b$, abbiamo $\mathbb{Q}_a \subsetneq \mathbb{Q}_b$, quindi ι è strettamente crescente. Dati $x, y \in \mathbb{R}$ con $x < y$, per definizione $x \subsetneq y$, quindi esiste $a \in y \setminus x$. Siccome y non ha massimo, c'è un $b \in y$ con $a < b$. Ora $x \subsetneq \mathbb{Q}_b \subsetneq y$.

$a \notin x$ $a \in \mathbb{Q}_b$ $b \notin \mathbb{Q}_b$ $b \in y$ ∎

Notazione (abuso di) Siccome le immersioni

$$\omega \hookrightarrow \mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{R}$$

sono tutte iniettive e crescenti, quando non c'è pericolo di confusione, possiamo abusare della notazione immaginando che

questo siano vere e proprie inclusioni

$$\omega \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R}$$

In realtà non è vero: per esempio è $\iota[\mathbb{Q}]$, non $\mathbb{Q}$, ad essere sottoinsieme di $\mathbb{R}$, ma $\iota[\mathbb{Q}]$ è in corrispondenza biunivoca, in maniera canonica, tramite appunto ι, con $\mathbb{Q}$, e questa corrispondenza preserva tutta la struttura rilevante — l'ordine, come abbiamo verificato, ma anche le operazioni di campo.

Con $\aleph_0 < |\mathbb{R}|$

Dim Per l'osservazione $\aleph_0 \leq |\mathbb{R}|$, inoltre $\mathbb{Q}$ è denso in $\mathbb{R}$, quindi $\mathbb{R}$ è denso. Si vede facilmente che $\mathbb{R}$ non ha massimo né minimo, quindi se $\mathbb{R}$ fosse numerabile sarebbe isomorfo a $\mathbb{Q}$. D'altro canto $\mathbb{R}$ è completo e $\mathbb{Q}$ no, quindi non possono essere isomorfi. ∎