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 $\mathcal{B} \subseteq \mathcal{S}(M)$. $\mathcal{B}$ sarebbe dunque finito, contro l'ipotesi. ∎

Esercizio Dimostra che se $|A| \leq \aleph_0$ e $f: A \to B$ è una funzione surgettiva allora $|B| \leq \aleph_0$.

Insiemi numerabili in pratica

Sapere che, se $|A| \leq \aleph_0$, allora o A è finito o è numerabile, ci fornisce lo strumento essenziale per dimostrare la numerabilità di molti insiemi concreti. Spesso, infatti, è facile dimostrare che un insieme infinito è tale. Rimane poi da gestire un discorso di disuguaglianze per dire che esso è al più numerabile.
Cominciamo quindi con qualche considerazione generale a proposito delle disuguaglianze fra cardinalità

Oss. Dati A, B, C con $|B| \leq |C|$

$$|A| + |B| \leq |A| + |C| \qquad |A|^{|B|} \leq |A|^{|C|}$$
$$|A| \cdot |B| \leq |A| \cdot |C| \qquad |B|^{|A|} \leq |C|^{|A|}$$

Vale a dire che le operazioni sulle cardinalità sono monotone, nel senso delle disuguaglianze larghe. Attenzione però che, in generale, NON sono strettamente monotone!

Dim Detta $f : B \to C$ la funzione iniettiva che testimonia che $|B| \leq |C|$ e detto $B' = f[B]$ abbiamo $|B| = |B'|$, quindi basta dimostrare la disuguaglianza associata con B' al posto di B. Ora, giocando sul fatto che $B' \subseteq C$, si vede che queste disuguaglianze rappresentano, in realtà, relazioni di contenimento fra il membro di sinistra e il membro di destra. Per esempio:

$$B' \subseteq C \implies A \times \{0\} \cup B' \times \{1\} \subseteq A \times \{0\} \cup C \times \{1\}$$

$$|A \times \{0\} \cup B' \times \{1\}| \leq |A \times \{0\} \cup C \times \{1\}|$$

$$\| \qquad\qquad \| \qquad\qquad \|$$

$$|A| + |B'| \qquad\qquad |A| + |C|$$

Le altre si ottengono allo stesso modo. ∎

Oss $|A \cup B| \leq |A| + |B|$

Dim La funzione seguente è iniettiva

$$f : A \cup B \to A \times \{0\} \cup B \times \{1\} \qquad f(x) = \begin{cases} (x,0) & \text{se } x \in A \\ (x,1) & \text{altrimenti} \end{cases}$$

∎

Veniamo ora a calcolare le operazioni aritmetiche. Già sappiamo, per il teorema di Cantor, che $2^{\aleph_0} > \aleph_0$, per cui mettere un $\aleph_0$ a esponente di qualunque cosa non sia uno 0 o un 1 conduce fuori dal numerabile. Tutto il resto invece no.

Prop $\aleph_0 + \aleph_0 = \aleph_0 \cdot \aleph_0 = \aleph_0^n = \aleph_0$ con $n \in \omega \setminus \{0\}$.

Dim Supponiamo di sapere già che $\aleph_0 \cdot \aleph_0 = \aleph_0$, allora possiamo formare la catena di disuguaglianze

$$\aleph_0 = \aleph_0 + 0 \leq \aleph_0 + \aleph_0 = \aleph_0 \cdot 2 \leq \aleph_0 \cdot \aleph_0 = \aleph_0$$

Da cui, per il teorema di Cantor – Bernstein,

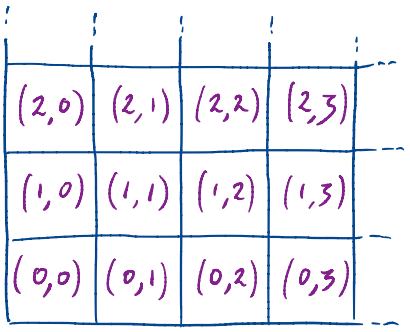
$$\aleph_0 + \aleph_0 = \aleph_0 \cdot \aleph_0 = \aleph_0$$

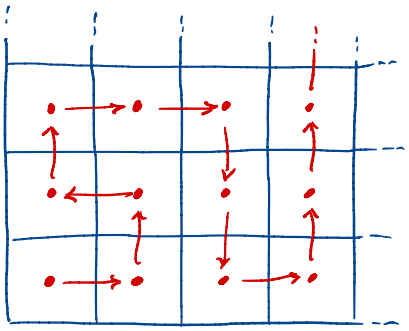
Ora è facile vedere per induzione che $n \in \{0,1,2,\dots\} \to \aleph_0^n = \aleph_0$ infatti $\aleph_0^1 = \aleph_0$ e $\aleph_0^{n+1} = \aleph_0^n \cdot \aleph_0 = \aleph_0 \cdot \aleph_0 = \aleph_0$.

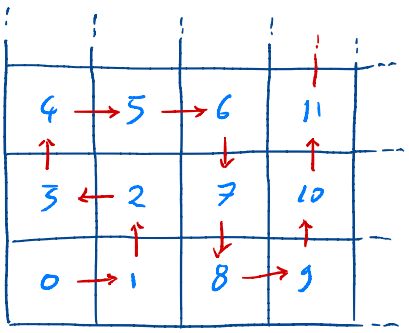
Resta quindi da dimostrare il lemma seguente

Lemma $\aleph_0 \cdot \aleph_0 = \aleph_0$ ossia esiste una bigezione fra $\omega \times \omega$ e ω

Ci sono diverse vie per illustrare questo risultato. Per esempio, possiamo rappresentare le coppie $(x,y) \in \omega \times \omega$ sotto la specie di una griglia a maglie quadrate. Poi disegnamo un percorso che pare visitare tutte le maglie della griglia, con sufficiente apparenza di regolarità, possibilmente, da convincere il lettore che vi debba essere un metodo. Infine numeriamo le maglie secondo l'ordine in cui sono visitate dal percorso. Avremo così numerato tutte le coppie di numeri naturali dal disegno.







Altrimenti, è possibile ossibire delle bigezioni esplicite, per esempio $f(x,y) = 2^x \cdot (2y+1) - 1$ $\quad g(x,y) = \dfrac{(x+y)^2 + 3x + y}{2}$

È possibile scrivere i due numeri della coppia in base 10 a cifre alternate, tipo: $(64, 4096) \mapsto 40009664$

E saranno possibili mille altre scelte, ma noi useremo, invece il tipo d'ordine di ω.

Dim (lemma)

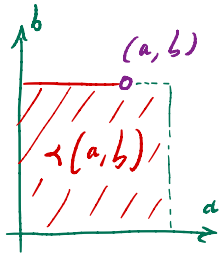
Consideriamo l'ordinamento seguente su $\omega \times \omega$

$(a,b) \prec (a',b') \overset{\text{def.}}{\equiv}$ $\max(a,b) < \max(a',b')$

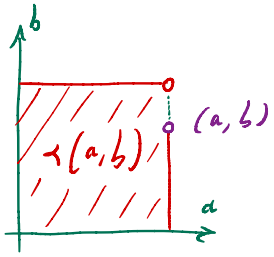
$\vee \left(\max(a,b) = \max(a',b') \wedge a < a' \right)$

$\vee \left(\max(a,b) = \max(a',b') \wedge a = a' \wedge b < b' \right)$

Ossia, per confrontare (a,b) con (a',b'), si confrontano prima



$\max(a,b)$ e $\max(a',b')$; a parità si confrontano a ed a'; se anche queste coincidono, si confrontano b e b'.



L'idea è che, in questo modo, le coppie $\prec$ di una certa (a,b) fissata sono tutte contenute nel quadrato $\{0 \dots \max(a,b)\} \times \{0 \dots \max(a,b)\}$, quindi sono in numero finito, e questo implica che $(\omega \times \omega, \prec)$ è isomorfo a $(\omega, <)$.

Formalmente, iniziamo col verificare che $\prec$ sia effettivamente un ordine stretto. La proprietà irriflessiva è immediata. Per verificare la proprietà transitiva, prendiamo $(a,b) \prec (a',b') \prec (a'',b'')$. Allora $\max(a,b) \leq \max(a',b') \leq \max(a'',b'')$. Se una di queste disuguaglianze è stretta allora $(a,b) \prec (a'',b'')$, altrimenti $\max(a,b) = \max(a',b') = \max(a'',b'')$ e segue dalla definizione che $a \leq a' \leq a''$. Nuovamente, se una disuguaglianza è stretta abbiamo concluso, altrimenti $a = a' = a''$, quindi $b < b' < b''$, da cui $(a,b) \prec (a'',b'')$. Per dire che l'ordine è totale osserviamo che se (a,b) e (a',b') non sono né $\prec$ né $\succ$ allora dobbiamo avere $\max(a,b) = \max(a',b')$, $a = a'$, $b = b'$, quindi $(a,b) = (a',b')$.

Ora vogliamo dire che $(\omega \times \omega, \prec) \sim (\omega, <)$. Partiamo dall'osservazione che se $(a,b) \in \omega \times \omega$ allora

$$(\omega \times \omega)_{(a,b)} \overset{\text{def.}}{\equiv} \{(x,y) \in \omega \times \omega \mid (x,y) \prec (a,b)\}$$

detto "il segmento iniziale determinato da (a,b) su $(\omega \times \omega, \prec)$" è finito. Infatti $(\omega \times \omega)_{(a,b)} \subseteq S(\max(a,b)) \times S(\max(a,b))$. Ci serve dire 1. $(\omega \times \omega, \prec)$ è ben ordinato. 2. $(\omega \times \omega, \prec)$ è illimitato 3. ogni sottoinsieme non vuoto e superiormente limitato di $\omega \times \omega$ ha un massimo.

1. Dato $A \subseteq \omega \times \omega$ con $A \neq \emptyset$, consideriamo $a \in A$. Se $(\omega \times \omega)_a \cap A = \emptyset$ allora a è il minimo di A. Altrimenti $A' = (\omega \times \omega)_a \cap A$

è non vuoto e finito, quindi ha minimo m. Questo deve essere anche il minimo di A, perché se $x \in A \setminus A'$ allora $m \prec a \preceq x$.

2. Dato $(a,b) \in \omega \times \omega$, $(a,b) \prec (s(a), s(b))$.

3. Dato $A \subseteq \omega \times \omega$ non vuoto e superiormente limitato da $(a,b) \in \omega \times \omega$, abbiamo che $A \subseteq (\omega \times \omega)_{(a+1,b+1)}$ è finito, quindi ammette massimo perché l'ordine $\prec$ è totale. ∎

Usando la proposizione appena dimostrata, potremmo dimostrare, per esempio, che $\mathbb{Z}$ e $\mathbb{Q}$ sono numerabili, se non fosse che non abbiamo ancora definito questi oggetti. Allo scopo, ricordiamo che — cfr. a pag. 38 delle note — una relazione di equivalenza induce un insieme di classi di equivalenza.

Def. ($\mathbb{Z}$) Definiamo $\mathbb{Z}$ come l'insieme delle classi di equivalenza su $\omega \times \omega$ indotte dalla relazione

$$(a,b) \sim_{\mathbb{Z}} (a',b') \overset{def}{\iff} a + b' = b + a' \qquad \text{morale: } "(a,b) = a - b"$$

Esercizio Dimostra che $\sim_{\mathbb{Z}}$ è una relazione di equivalenza

Esercizio Definiamo $+$, $-$ e $\cdot$ su $\mathbb{Z}$ mediante

$$[(a,b)]_{\mathbb{Z}} + [(a',b')]_{\mathbb{Z}} \overset{def.}{=} [(a+a', b+b')]_{\mathbb{Z}}$$

$$-[(a,b)]_{\mathbb{Z}} \overset{def.}{=} [(b,a)]_{\mathbb{Z}}$$

$$[(a,b)]_{\mathbb{Z}} \cdot [(a',b')]_{\mathbb{Z}} \overset{def.}{=} [(a \cdot a' + b \cdot b', \; a \cdot b' + b \cdot a')]_{\mathbb{Z}}$$

dimostra che $\mathbb{Z}$, con queste operazioni, è un anello commutativo con identità $1 \overset{\text{def.}}{=} [(1,0)]_{\mathbb{Z}}$

Def. ($\mathbb{Q}$) Definiamo $\mathbb{Q}$ come l'insieme delle classi di equivalenza su $\mathbb{Z} \times (\omega \setminus \{0\})$ indotte dalla relazione

$$(n,d) \sim_{\mathbb{Q}} (n',d') \overset{\text{def.}}{\equiv} n \cdot d' = d \cdot n' \quad \text{morale: } "(n,d) = \frac{n}{d}"$$

Esercizio Dimostra che $\sim_{\mathbb{Q}}$ è una relazione di equivalenza

Esercizio Definisci $+, -, \cdot$ e $\square^{-1}$ su $\mathbb{Q}$ nella maniera ragionevole e dimostra che $\mathbb{Q}$ è un campo.

Esercizio Definisci la relazione $<$ su $\mathbb{Q} \times \mathbb{Q}$ dicendo che $q \in \mathbb{Q}$ è positivo se $q = [(n,d)]_{\mathbb{Q}}$, con $n, d \in \omega \setminus \{0\}$, e dicendo che $a < b$ se e solo se $b - a$ è positivo. Dimostra che questo è un ordine totale e denso, cioè

$$\forall a, b \in \mathbb{Q} \quad a < b \to \exists c \in \mathbb{Q} \quad a < b < c.$$

Nota Gli esercizi precedenti sono tediosi, ma non sono difficili. Nel resto del corso daremo per scontate le proprietà aritmetiche elementari di $\mathbb{Z}$ e di $\mathbb{Q}$. D'ora innanzi scriveremo $a - b \overset{\text{def.}}{\equiv} [(a,b)]_{\mathbb{Z}}$ $\quad \frac{n}{d} \overset{\text{def.}}{\equiv} [(n,d)]_{\mathbb{Q}}$.

Per dimostrare la numerabilità di $\mathbb{Z}$ e $\mathbb{Q}$, è comodo richiamare ancora un esercizio, però, questa volta, lo risolviamo.

Esercizio Dimostra che se $|A| \leq \aleph_0$ e $f: A \to B$ è una funzione surgettiva allora $|B| \leq \aleph_0$.

Sol Per ipotesi esiste $g: A \to \omega$ iniettiva, e dobbiamo trovare una $h: B \to \omega$ iniettiva. Poniamo

$$h(b) = \min\left(g\left[\underbrace{\{a \in A \mid f(a) = b\}}_{\text{“}f^{-1}(b)\text{”}}\right]\right)$$

L'insieme fra graffe non è vuoto per la surgettività di f, quindi il minimo è ben definito. Inoltre, se $h(b) = h(b')$, allora $b = g(a)$ e $b' = g(a')$ con a e a' tali che $f(a) = b$ e $f(a') = b'$. Per l'iniettività di g, $a = a'$, quindi $b = f(a) = f(a') = b'$. ∎

Con Un insieme $A \neq \emptyset$ è al più numerabile se e solo se esiste $f: \omega \to A$ surgettiva.

Dim Il se è l'esercizio. Il solo se vale perché se $|A| = \aleph_0$ allora c'è f bigettiva, se $|A| < \aleph_0$ allora c'è $g: n \to A$ bigettiva per qualche $n \in \omega \setminus \{0\}$ e definiamo

$$f(x) = \begin{cases} g(x) & \text{se } x < n \\ g(0) & \text{altrimenti} \end{cases}$$

∎

Notazione Con **successione** (numerabile) intendiamo semplicemente una funzione con dominio ω, per cui

$$a = \{a_i\}_{i \in \omega} \overset{\text{def.}}{\equiv} a: \omega \to \dots, \quad a: i \longmapsto a_i$$

una **enumerazione** di A una successione $a = \{a_i\}_{i \in \omega}$ tale che $A = \mathrm{Im}(a)$, ossia, informalmente, $A = \{a_i \mid i \in \omega\}$.

Il corollario dice che $A \neq \emptyset$ è al più numerabile se e solo se ha una enumerazione.

Esempio $\mathbb{Z}$ è numerabile.

Dim La funzione $\omega \times \omega \to \mathbb{Z}$, $(a,b) \mapsto a-b$ è surgettiva per definizione, e $\omega \times \omega$ è numerabile, quindi $|\mathbb{Z}| \leq \aleph_0$.
D'altro canto la funzione $\omega \to \mathbb{Z}$ $n \mapsto n = [(n,0)]_{\mathbb{Z}}$ è iniettiva, quindi $\mathbb{Z}$ è infinito, quindi $|\mathbb{Z}| = \aleph_0$. ∎

Esempio $\mathbb{Q}$ è numerabile.
Come nell'esempio precedente $\mathbb{Z} \times (\omega \setminus \{0\}) \to \mathbb{Q}$, $(n,d) \mapsto \frac{n}{d}$ è surgettiva e $|\mathbb{Z} \times (\omega \setminus \{0\})| = \aleph_0 \cdot \aleph_0 = \aleph_0$. Inoltre $\mathbb{Q}$ è infinito perché $\omega \to \mathbb{Q}$, $n \mapsto \frac{n}{1}$ è iniettiva. ∎

Adesso, ci piacerebbe poter dire che, se abbiamo un insieme A al più numerabile, e tutti i suoi elementi sono, a loro volta, insiemi al più numerabili, allora $\bigcup A$ è al più numerabile. D'altro canto è ragionevole: se esiste una enumerazione $\{a_i\}_{i \in \omega}$ di A, e, per ogni $i \in \omega$, esiste una enumerazione $a_i = \{a_{i,j}\}_{j \in \omega}$ di a_i, allora possiamo mandare surgettivamente $\omega \times \omega$ in A: $(i,j) \mapsto a_{i,j}$, e, siccome $\omega \times \omega$ è al più numerabile, lo è anche A.

L'errore è credere di poter fissare una a_i per ogni $i \in \omega$.

Usando l'assioma della scelta potremo farlo, ma, per ora, non abbiamo modo, in generale, di procurarci la funzione $i \mapsto \alpha_i$. Possiamo però assumere di averla, così si corregge il ragionamento impreciso di prima.

Prop: Sia $A = \{a_i \mid i \in \omega\}$ e sia $\{\alpha_i\}_{i\in\omega}$ una successione di funzioni tali che, per ogni $i \in \omega$, $\alpha_i : \omega \to a_i$ è una enumerazione di a_i. Allora $|\bigcup A| \leq \aleph_0$.

Dim Basta osservare che

$$f : \omega \times \omega \longrightarrow \bigcup A \qquad f : (i, j) \longmapsto \alpha_i(j)$$

è surgettiva. ∎

Notazione Data una funzione $f : I \to S$ definiamo

$$\bigcup_{i\in I} f(i) \overset{def.}{\equiv} \bigcup f[I]$$

Così, per esempio, se $A = \{a_i \mid i \in \omega\}$

$$\bigcup_{i\in\omega} a_i = \bigcup A = \{x \mid \exists i \in \omega \; x \in a_i\}$$

Def. (parti finite)

$$\mathcal{P}^{fin}(A) \overset{def.}{\equiv} \{X \in \mathcal{P}(A) \mid |X| < \aleph_0\}$$

Prop: $|A| \leq \aleph_0 \to |\mathcal{P}^{fin}(A)| \leq \aleph_0$

Dim Il caso $A = \emptyset$ è immediato. Assumiamo $A \neq \emptyset$. Sia

$$\mathcal{P}^{\leq n}(A) \overset{def.}{\equiv} \{X \in \mathcal{P}(A) \mid |X| \leq n\}$$

siccome $\mathcal{P}^{fin}(A)$ è l'unione degli insiemi $\mathcal{P}^{\leq n}(A)$, basta

esibire una successione di enumerazioni a_n di $\mathcal{P}^{\leq n}(A)$.

Fissiamo $f : w \to w \times A$, $f : x \mapsto (f_1(x), f_2(x))$ surgettiva, che esiste perché A è al più numerabile. Costruiamo la successione $\{a_n\}_{n \in w}$ per ricorsione.

Per $n = 0$, $\mathcal{P}^{\leq 0}(A) = \{\emptyset\}$ e a_0 è la costante $\emptyset$.

Per $n = s(m)$

$$a_{s(m)}(x) = \begin{cases} \emptyset & \text{se } x = 0 \\ a_m(f_1(x-1)) \cup \{f_2(x-1)\} & \text{se } x > 0 \end{cases}$$

Dimostriamo per induzione che, per ogni $n \in w$, a_n è surgettiva $w \to \mathcal{P}^{\leq n}(A)$.

caso $n = 0$ Immediato.

caso $n = s(m)$. Per ipotesi induttiva $a_m : w \to \mathcal{P}^{\leq m}(A)$ è surgettiva. Dato $Y \in \mathcal{P}^{\leq s(m)}(A)$ si danno due casi. O $Y = \emptyset$, allora $Y = a_{s(m)}(0)$. Oppure esiste $y \in Y$. In questo caso $|Y \setminus \{y\}| \leq m$, quindi $Y \setminus \{y\} = a_m(t)$ per qualche $t \in w$. Per la surgettività di f, $(t, y) = f(x)$ per qualche $x \in w$. Quindi

$$\begin{aligned} a_{s(m)}(x+1) &= a_m(f_1(x)) \cup \{f_2(x)\} \\ &= (Y \setminus \{y\}) \cup \{y\} = Y. \end{aligned}$$

□

Applicazione Dimostriamo che l'insieme dei numeri reali algebrici $\mathbb{A}_{\mathbb{R}}$ è numerabile. Per questa applicazione, assumiamo le proprietà algebriche elementari di $\mathbb{R}$. L'insieme $\mathbb{A}_{\mathbb{R}}$ è definito come l'insieme degli $x \in \mathbb{R}$ che sono zeri di qualche polinomio non nullo a coefficienti razionali:

$$\mathbb{A}_{\mathbb{R}} \overset{d.f.}{=} \{ x \in \mathbb{R} \mid \exists p \in \mathbb{Q}[x] \setminus \{0\} \; p(x) = 0 \}$$

I numeri reali che non sono algebrici si dicono trascendenti, siccome — formalmente, vedremo questo risultato in seguito — $\mathbb{R}$ non è numerabile, deduciamo dalla numerabilità di $\mathbb{A}_{\mathbb{R}}$ che ci sono numeri reali trascendenti.

Dimostriamo, intanto, che l'insieme $\mathbb{Q}[x]$, dei polinomi a coefficienti razionali nella indeterminata x, è numerabile. Possiamo identificare un polinomio

$$p(x) = a_0 + a_1 x^1 + a_2 x^2 + \dots + a_d x^d$$

con l'insieme dei suoi monomi

$$p(x) = \{ a_0, a_1 x^1, a_2 x^2, \dots, a_d x^d \}$$

e ciascun monomio con la coppia (grado, coefficiente)

$$p(x) = \{ (0, a_0), (1, a_1), (2, a_2), \dots, (d, a_d) \}$$

Formalmente, come accade per i numeri, le coppie ordinate, le funzioni, &c., anche i polinomi non sono oggetti atomici della teoria degli insiemi: occorre, in qualche modo, fissare

una codifica. Quella appena descritta è una codifica ragionevole. Rappresentando i polinomi in questo modo

$$\mathbb{Q}[x] \subseteq \mathcal{P}^{fin}(\omega \times \mathbb{Q})$$

per cui $\mathbb{Q}[x]$ è al più numerabile, quindi numerabile perché, per esempio, è elementare immergere $\mathbb{Q}$ in $\mathbb{Q}[x]$.

Venendo ad $\mathbb{A}_{\mathbb{R}}$ abbiamo una facile surgezione

$$f : (\mathbb{Q}[x] \setminus \{0\}) \times \omega \longrightarrow \mathbb{A}_{\mathbb{R}}$$

$$(p, i) \longmapsto \text{"la } i\text{-esima radice di } p \text{ se questa esiste, altrimenti } 0\text{"}$$

Vediamo, però, in maggior dettaglio come si può rappresentare f mediante una formula insiemistica.

"α è la i-esima radice di p" $\equiv$

$$p(\alpha) = 0 \wedge \left|\{x \in \mathbb{R} \mid x \leq \alpha \wedge p(x) = 0\}\right| = |i|$$

$y = f(p,i) \equiv$ "y è la i-esima radice di p"

$$\wedge \left(y = 0 \wedge \neg \exists \alpha \in \mathbb{R} \text{ "}\alpha \text{ è la } i\text{-esima radice di } p\text{"}\right)$$

Per separazione esiste, quindi, f, e, di conseguenza $|\mathbb{A}_{\mathbb{R}}| \leq \aleph_0$.

La disuguaglianza opposta è immediata perché $\mathbb{Q} \subseteq \mathbb{A}_{\mathbb{R}}$ □

Esercizio Dato un insieme X, una funzione $f : X^2 \to X$, e un sottoinsieme $A \subseteq X$ al più numerabile, dimostra che esiste un $\bar{A} \subseteq X$ al più numerabile tale che $f[\bar{A} \times \bar{A}] \subseteq \bar{A}$. (Concludi che un gruppo finitamente generato è al più numerabile.)