INSIEMI INFINITI

6.4 TEOREMA I_n non può essere posto in corrispondenza biunivoca con una sua parte propria.

7.1 TEOREMA *L'insieme* N *è infinito.*

Dimostrazione. Per assurdo: supponiamo che esista un'applicazione f: $\mathsf{N} \to I_n$ biiettiva; $f|_{I_n}$ è iniettiva e ha, come subito si verifica, un'immagine che è un sottoinsieme *proprio* di I_n. In tal modo I_n viene posto in corrispondenza biunivoca con un suo sottoinsieme proprio, ciò che è escluso dal teorema 6.4. ∎

7.2 DEFINIZIONE *Un insieme viene detto* numerabile *se può essere posto in corrispondenza biunivoca con* N.

Ad esempio, sono numerabili l'insieme Z degli interi relativi, l'insieme P degli interi naturali pari; per quest'ultimo, basta considerare l'applicazione $n \mapsto 2n$, che è evidentemente biiettiva di N su P. Riflettiamo che l'insieme P ha lo stesso numero cardinale di N, pur essendo un sottoinsieme proprio di N. Così pure Z ed N hanno lo stesso numero cardinale, malgrado sia $\mathsf{N} \subsetneqq \mathsf{Z}$. Una situazione di questo tipo non può presentarsi nell'ambito degli insiemi finiti (teorema 6.4); noi dimostreremo che essa è caratteristica degli insiemi infiniti, precisamente:

7.3 TEOREMA *Ogni insieme infinito può essere messo in corrispondenza biunivoca con una sua parte propria.*

La tesi è già stata riscontrata per l'insieme N, e quindi per un qualunque insieme numerabile. Per passare a un insieme infinito arbitrario cominciamo col dimostrare che:

7.4 TEOREMA *Ogni insieme infinito contiene un sottoinsieme numerabile.*

Dimostrazione. Sia X un insieme infinito e sia φ: $\mathcal{P}(X) \to X$ una funzione di scelta per X (si ricordi l'osservazione 4.5). Definiamo per induzione una successione di elementi di X, tutti distinti fra loro, in questo modo:

$$a_0 = \varphi(X), \qquad a_n = \varphi(X - \{a_0, a_1, \ldots, a_{n-1}\}).$$

La definizione si regge perché l'insieme $X - \{a_0, a_1, \ldots, a_{n-1}\}$ non è vuoto per alcuna n: se lo fosse, X sarebbe un insieme finito. L'insieme $A = \{a_n \colon n \in \mathsf{N}\}$ è l'insieme cercato. ∎

INSIEMI INFINITI

L'enunciato 7.4 ha carattere intuitivo, e tuttavia la sua dimostrazione richiede in modo essenziale l'uso dell'assioma della scelta. Rinunciando a questo assioma dovremmo dunque rinunciare a una proposizione di notevole importanza.

Possiamo ora facilmente completare la dimostrazione del teorema 7.3. Sia X un insieme infinito qualunque; possiamo scrivere $X = A \cup A'$ dove A è numerabile, A' è il complementare di A. Un'applicazione iniettiva $f\colon X \to X$ che mandi A in una sua parte propria e tale che $f_{|A'} = I_{A'}$ pone una corrispondenza biunivoca tra X e una sua parte propria. ∎

Dai teoremi 6.4 e 7.3 risulta dunque chiaramente che la proprietà di possedere sottoinsiemi propri con lo stesso numero cardinale è caratteristica degli insiemi infiniti. Si potrebbe assumere questa proprietà per definire gli insiemi infiniti: così non sarebbe necessario svolgere preventivamente la teoria degli interi naturali.

Enunciamo ora alcune proposizioni sugli insiemi numerabili, lasciando allo studioso il compito di scrivere per disteso le semplici dimostrazioni.

7.5 Teorema *L'unione di una famiglia finita non vuota di insiemi numerabili è un insieme numerabile.*

7.6 Teorema *L'unione di una famiglia numerabile di insiemi finiti, non vuoti, a due a due disgiunti, è un insieme numerabile.*

7.7 Teorema *Un sottoinsieme di un insieme numerabile è finito o numerabile.*

7.8 Teorema *Una partizione di un insieme numerabile è finita o numerabile.*

Il teorema 7.6 ha un'interessante conseguenza.

7.9 Teorema *Il prodotto* $\mathsf{N} \times \mathsf{N}$ *è numerabile.*

Dimostrazione. Per gli elementi (m, n) di $\mathsf{N} \times \mathsf{N}$ possiamo introdurre un "peso" $m+n=r$. Fissato un $r \in \mathsf{N}$ vi è solo un numero finito (esattamente $r+1$) di elementi di peso r. La tesi allora discende subito dal teorema 7.6. ∎

INSIEMI INFINITI

7.10 TEOREMA *L'insieme* $\mathbb{Q}$ *dei numeri razionali è numerabile.*

Dimostrazione. Ogni numero razionale si può identificare con una classe di equivalenza dell'insieme $\mathbb{Z}\times\mathbb{Z}^*$ (vedi § 4, esempio *e*)). Ma l'insieme $\mathbb{Z}\times\mathbb{Z}^*$, che è prodotto di due insiemi numerabili, è numerabile. In base al teorema 7.8 l'insieme $\mathbb{Q}$, che non è certo finito, è numerabile.

7.11 TEOREMA *L'unione di una famiglia numerabile di insiemi numerabili è numerabile.*

Dimostrazione. Sia $A=\bigcup_0^\infty{}_k B_k$; essendo ogni insieme B_k numerabile, per ipotesi, si può porre $B_k=\{x_{k,n}\colon n\in\mathbb{N}\}$. Dunque: $A=\{x_{k,n}\colon k\in\mathbb{N}, n\in\mathbb{N}\}$. L'applicazione $(k, n)\mapsto x_{k,n}$ è un'applicazione surgettiva di $\mathbb{N}\times\mathbb{N}\to A$. Allora, essendo $\mathbb{N}\times\mathbb{N}$ numerabile, l'insieme A, che è in corrispondenza biunivoca con una partizione di $\mathbb{N}\times\mathbb{N}$, è finito o numerabile (vedi teorema 7.8). Ma non può essere, evidentemente, finito. ▪

Concludiamo con qualche ulteriore osservazione sui numeri cardinali.

7.12 DEFINIZIONE *Dati due insiemi X, Y, diciamo che Y ha numero cardinale maggiore o uguale di quello di X, e scriviamo $c(Y)\geqslant c(X)$, se esiste un'applicazione iniettiva di X in Y.*

La relazione così definita tra X e Y gode della proprietà riflessiva (come è evidente) e transitiva. Infatti, sia $f\colon X\to Y$ e $g\colon Y\to Z$, essendo f e g iniettive: evidentemente $g\circ f\colon X\to Z$ è iniettiva. È interessante notare che questa relazione gode anche della proprietà antisimmetrica. Precisamente:

7.13 TEOREMA (DI BERNSTEIN) *Se è $c(X)\leqslant c(Y)$ e $c(Y)\leqslant c(X)$, allora è $c(X)=c(Y)$.*

Premettiamo un lemma, molto interessante.

7.14 LEMMA *Se un insieme X si può porre in corrispondenza biunivoca con un suo sottoinsieme Z, allora esso può essere posto in corrispondenza biunivoca con un qualunque sottoinsieme V tale che $Z\subset V\subset X$.*

INSIEMI INFINITI

Dimostrazione. Per ipotesi, esiste un'applicazione biiettiva $h: X \to Z$. Poniamo $E = V - Z$, $F = X - V$. Avremo:

$$X = Z \cup E \cup F, \qquad V = Z \cup E,$$

dove gli insiemi Z, E, F sono a due a due disgiunti.

Poniamo:

$$h(Z) = Z_1, \qquad h(E) = E_1, \qquad h(F) = F_1.$$

Avremo

$$Z = h(X) = Z_1 \cup E_1 \cup F_1,$$

dove, per il carattere biiettivo di h, Z_1, E_1, F_1 sono disgiunti.

Analogamente, posto, per ogni n intero > 0,

$$h^n(Z) = Z_n, \qquad h^n(E) = E_n, \qquad h^n(F) = F_n,$$

avremo:

$$h^n(X) = h^{n-1}(Z) = Z_{n-1} = Z_n \cup E_n \cup F_n.$$

Può essere utile il seguente schema (fig. 7.1):

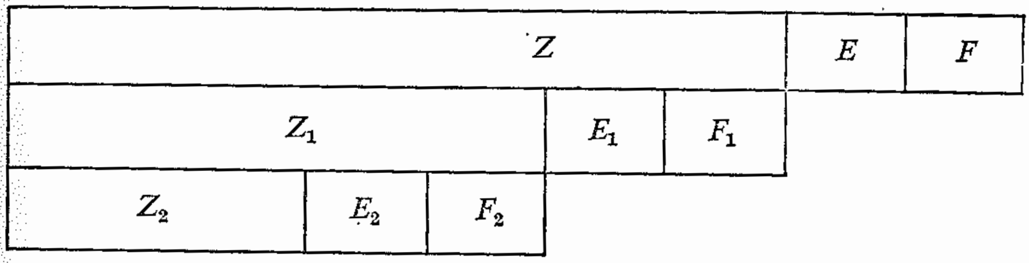

Figura 7.1

Indichiamo ora con M l'insieme $\bigcap_1^\infty{}_k Z_k$. Sia $x \in Z - M$; poiché x non appartiene a tutti gli insiemi Z_k, vi sarà un indice $\overline{k}$ tale che $x \in Z_{\overline{k}}$, $x \notin Z_{\overline{k}+1}$. Poiché è $Z_{\overline{k}} = Z_{\overline{k}+1} \cup E_{\overline{k}+1} \cup F_{\overline{k}+1}$, si deduce che x appartiene a $E_{\overline{k}+1}$, oppure a $F_{\overline{k}+1}$.

Possiamo dunque affermare che X e V risultano decomposti nel seguente modo:

$$X = M \cup E \cup F \cup E_1 \cup F_1 \cup \ldots \cup E_n \cup F_n \cup \ldots$$

$$V = M \cup E \cup F_1 \cup E_1 \cup F_2 \cup \ldots \cup E_n \cup F_{n+1} \cup \ldots$$

Questa decomposizione ci permette di costruire facilmente una applicazione biiettiva: $g: X \to V$. Definiamo infatti g in modo che su M e sugli insiemi E_k sia l'applicazione identica e che sugli insiemi F_n coincida con l'applicazione h. Tenendo presente che è $F_{n+1} = g(F_n)$, si costata che g è biiettiva. ∎

Veniamo ora alla dimostrazione del teorema 7.13. Per ipotesi, esiste un'applicazione iniettiva $f: X \to Y$ ed esiste un'applicazione iniettiva $s: Y \to X$. Si ha, evidentemente

$$s \circ f(X) \subset s(Y) \subset X .$$

Gli insiemi X ed $s \circ f(X)$ sono posti in corrispondenza biunivoca; allora, per il lemma, si può porre una corrispondenza biunivoca tra X ed $s(Y)$. Ma allora anche X e Y si possono porre in corrispondenza biunivoca. ∎

7.15 Definizione *Si dice che Y ha numero cardinale maggiore di X e si scrive* $c(X) < c(Y)$ *se è* $c(X) \leqslant c(Y)$ *ed è* $c(X) \neq c(Y)$.

È interessante notare che, dato un qualunque insieme X, ne esiste uno che ha numero cardinale maggiore.

Vale infatti il seguente teorema:

7.16 Teorema *Per ogni insieme X, si ha* $c(X) < c(\mathcal{P}(X))$.

Dimostrazione. Anzitutto, l'applicazione iniettiva $x \mapsto \{x\}$ ci dice che è $c(X) \leqslant c(\mathcal{P}(X))$. Dimostriamo che non è $c(X) = c(\mathcal{P}(X))$: basterà, a questo scopo, far vedere che non esistono applicazioni surgettive $X \to \mathcal{P}(X)$. La cosa è evidente se X è vuoto. Supponendo X non vuoto, sia ψ un'applicazione: $X \to \mathcal{P}(X)$. Consideriamo il sottoinsieme di X:

$$H = \{x \colon (x \in X) \text{ e } (x \notin \psi(x))\} .$$

Dico che H differisce da ciascuno degli insiemi $\psi(x)$; infatti, preso un qualunque $\bar{x} \in X$, le relazioni $\bar{x} \in \psi(\bar{x})$ e $\bar{x} \in H$ sono fra loro contraddittorie (cioè: se è vera l'una è falsa l'altra) dal momento che per ogni $x \in H$ è $x \notin \psi(x)$. ∎

7.17 *Osservazione.* Nelle operazioni insiemistiche considerate nei teoremi 7.5, 7.6, 7.7, 7.8, 7.9, 7.11 i dati sono insiemi finiti o numerabili e i risultati sono sempre insiemi finiti o numerabili. L'operazione $X \to \mathcal{P}(X)$ invece fa crescere il numero cardinale; in particolare $\mathcal{P}(\mathrm{N})$ *non è un insieme numerabile.*