

INSIEMI

1. INTRODUZIONE

In modo piuttosto informale si introducono nozioni e notazioni insiemistiche che vengono correntemente usate per sviluppare le teorie matematiche tra cui quelle che sono argomento del corso.

La notazione fondamentale è

$$a \in A$$

che si legge “*a è un elemento dell’insieme A*” oppure, equivalentemente, “*a appartiene ad A*”. I concetti di “elemento” e di “insieme” sono concetti *primitivi*, cioè *non* vengono definiti in termini di altri concetti più elementari. Per dare sostanza al discorso *postuleremo* che certi enti sono insiemi. Per esempio gli insiemi di numeri $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ (naturali, interi, razionali) che assumiamo familiari al lettore sono, appunto, insiemi. Inoltre fisseremo in modo preciso certe maniere di manipolare gli insiemi.

La notazione

$$A \subset B$$

si legge dicendo che “*l’insieme A è un sottoinsieme dell’insieme B*” oppure, equivalentemente, che *A è contenuto in B*; significa che ogni elemento di *A* è anche un elemento di *B*. Per ogni insieme *A*, si ha che $A \subset A$. Poniamo

$$A = B$$

se valgono entrambe le inclusioni

$$A \subset B \text{ e } B \subset A.$$

Quindi $A \neq B$ se esiste $a \in A$ che non appartiene a *B* o esiste $b \in B$ che non appartiene ad *A* (dove questo “o” non è esclusivo, ma significa che *almeno una* delle due circostanze si verifica).

Si noti che se *A* e *B* sono insiemi, $A \in B$ non ha senso. Se $a \in A$, allora $a \subset A$ non ha senso. Invece ha senso $\{a\} \subset A$, dove $\{a\}$ è l’insieme costituito dal solo elemento *a* (in particolare ha senso $a \in \{a\}$). Postuliamo che esiste l’*insieme vuoto*, indicato con il simbolo $\emptyset$ e che per ogni insieme *A*, $\emptyset \subset A$.

1.1. Unione, intersezione, complementare. Dati due insiemi *A* e *B*, l’insieme *unione* $A \cup B$ è caratterizzato dalla proprietà che $x \in A \cup B$ se $x \in A$ o $x \in B$ (qui, come sopra, questo “o” non è esclusivo).

L’insieme *intersezione* $A \cap B$ è tale che $x \in A \cap B$ se e solo se $x \in A$ e $x \in B$, cioè *x* è un elemento di *entrambi* gli insiemi.

Se $A \subset B$, allora

$$C_B(A) = \{x \in B \mid x \notin A\}$$

è l’insieme *complementare di A in X*. E’ chiaro che $C_B(C_B(A)) = A$. Dati due insiemi *A*, *B*

$$A \setminus B := C_A(A \cap B)$$

è per definizione l’insieme *differenza*.

1.2. Prodotto. Dati insiemi non vuoti $A_1, \dots, A_n$, l’insieme prodotto $A_1 \times \dots \times A_n$ ha per elementi le *n*-uple ordinate $(a_1, \dots, a_n)$ tali che, per ogni $j = 1, \dots, n$, $a_j \in A_j$.

1.3. L’insieme delle parti. Dato un insieme *A*, $\mathcal{P}(A)$ è l’insieme che ha per elementi i sottoinsiemi di *A*. L’insieme delle parti $\mathcal{P}(A)$ è sempre non vuoto perché $\emptyset \in \mathcal{P}(A)$. Se *A* è non vuoto e $a \in A$, allora $a \in \{a\} \in \mathcal{P}(A)$, ma $a \notin \mathcal{P}(A)$ (mentre se $a \in A$ e $A \subset B$, allora $a \in B$). Questo mette in evidenza il fatto (sottile e importante) che lo stato di un ente in quanto “elemento” o “insieme” non è dato una volta per tutte ma dipende dalla relazione con altri enti. Si noti che si può iterare la costruzione in modo induttivo ponendo $\mathcal{P}^{(n)}(A) = \mathcal{P}(\mathcal{P}^{(n-1)}(A))$. La possibilità di creare insiemi i cui elementi sono insiemi è un punto molto delicato del discorso, su cui torneremo in seguito.

2. FUNZIONI

Una *funzione*

$$f : A \rightarrow B$$

(a volte detta anche, equivalentemente, una *applicazione*) definita sull'insieme A a valori nell'insieme B , associa ad ogni $a \in A$ un unico elemento $b = f(a) \in B$. A volte A è detto il *dominio* di definizione di f , B il *codominio*.

Data una funzione $f : A \rightarrow B$, il sottoinsieme di B :

$$f(A) = \text{Im}(f) = \{b \in B \mid \exists a \in A, f(a) = b\}$$

è detto *l'immagine* di f .

Per ogni $C \subset B$, il sottoinsieme di A :

$$f^{-1}(C) = \{a \in A \mid f(a) \in C\}$$

è detto *l'immagine inversa* di C .

Il sottoinsieme di $A \times B$:

$$G(f) = \{(a, b) \in A \times B \mid b = f(a)\}$$

è detto il *grafico* di f .

Una funzione $f : A \rightarrow B$ è *surgettiva* se $B = f(A)$. E' *iniettiva* se per ogni $b \in f(A)$, esiste un unico $a \in A$ tale che $f(a) = b$ (in altre parole $f^{-1}(\{b\}) = \{a\}$). Attenzione a non confondere (come agli studenti capita spesso) la definizione di "funzione iniettiva" con la definizione stessa di "funzione".

Una funzione $f : A \rightarrow B$ è *bigettiva* se è contemporaneamente iniettiva e surgettiva.

Per ogni $A \neq \emptyset$,

$$\text{id}_A : A \rightarrow A, \text{id}_A(x) = x$$

è la funzione *identità* di A che è evidentemente bigettiva. Se $C \subset A$,

$$i : C \rightarrow A, i(x) = x$$

è la funzione di *inclusione* di C in A che è evidentemente iniettiva.

Dati due insiemi non vuoti A e B indicheremo con

$$B^A = \{f : A \rightarrow B\}$$

cioè l'insieme di tutte le applicazioni definite su A a valori in B .

2.1. Funzioni di scelta. Dato $X \subset \mathcal{P}(A)$ tale che ogni $C \in X$, $C \neq \emptyset$, postuliamo l'esistenza di *funzioni di scelta*

$$s : X \rightarrow A$$

che hanno, per definizione, la proprietà che per ogni $C \in X$, $s(C) \in C$. In altre parole la funzione s "sceglie" un elemento $s(C)$ in ogni insieme C appartenente alla famiglia X di sottoinsiemi non vuoti di A .

2.2. Composizione di funzioni. Date due funzioni $f : A \rightarrow B$ e $g : B \rightarrow C$, definiamo la *funzione composta*

$$g \circ f : A \rightarrow C, (g \circ f)(x) = g(f(x)) .$$

Se f è bigettiva, possiamo definire la funzione *inversa*

$$f^{-1} : B \rightarrow A$$

dove per ogni $b \in B$, $a = f^{-1}(b)$ è l'unico $a \in A$ tale che $f(a) = b$; si ha che $(f^{-1} \circ f) = \text{id}_A$, $(f \circ f^{-1}) = \text{id}_B$.

3. INSIEMI FINITI, NUMERO DI ELEMENTI

Per ogni $n \geq 1$, il sottoinsieme di $\mathbb{N}$

$$I_n = \{0, 1, 2, \dots, n-1\} \subset \mathbb{N}$$

è l'insieme finito campione con $n \geq 1$ elementi.

Un insieme A è finito se è vuoto, oppure esistono $n \geq 1$ e un'applicazione bigettiva $f : I_n \rightarrow A$. I seguenti fatti non sono difficili da dimostrare.

- Esiste un'applicazione bigettiva $f : I_n \rightarrow I_m$ se e solo se $m = n$.
- Se A è finito e non vuoto, allora esiste un unico n per il quale esiste $f : I_n \rightarrow A$ bigettiva. $|A| = n$ è per definizione il *numero di elementi* di A .
- Se A è finito, $C \subset A$, $|A| = n$, allora: C è finito; $|C| \leq |A|$; $|C| = |A|$ se e solo se $C = A$.
- A e B finiti, allora:
 - (i) $|A| \geq |B|$ se e solo se esiste $f : B \rightarrow A$ iniettiva.
 - (ii) $|A| = |B|$ se e solo se esiste $f : B \rightarrow A$ bigettiva.
 - (iii) $|A| = |B|$ se e solo se $|A| \geq |B|$ e $|A| \leq |B|$.

3.1. Un po' di calcolo combinatorio. In una certa misura il “calcolo combinatorio” consiste nel determinare il numero di elementi di un certo insieme finito A in funzione del numero di elementi di altri insiemi finiti che intervengono nella definizione di A . Vedremo alcuni esempi.

- (1) Siano $|A| = m$, $|B| = n$, $n, m \geq 1$. Allora $|B^A| = n^m$. Dimostriamolo per induzione su $m \geq 1$.
Se $m = 1$, $A = \{a\}$, e ci sono n modi di definire $f(a)$. Se $|A| = s + 1$, fissiamo $a \in A$ e sia $A' = A \setminus \{a\}$. $|A'| = s$. Ci sono n modi di definire $b = f(a)$. Per ogni scelta di $b = f(a)$ questa si completa ad una $f : A \rightarrow B$, per mezzo di una qualsiasi $g : A' \rightarrow B$. Per induzione ci sono n^s possibilità per g e quindi in totale $n \cdot n^s = n^{s+1}$ possibilità per f .
- (2) Se $|A| = n$, allora $|\mathcal{P}(A)| = 2^n$. Diamo una dimostrazione costruendo un'applicazione bigettiva

$$f : \mathcal{P}(A) \rightarrow \{0, 1\}^A.$$

In tal caso si avrà che $|\mathcal{P}(A)| = |\{0, 1\}^A| = 2^n$. Per ogni $C \in \mathcal{P}(A)$, sia $1_C : A \rightarrow \{0, 1\}$ tale che $1_C(x) = 1$ se e solo se $x \in C$. Questa è detta la *funzione indicatrice del sottoinsieme* C . Poniamo allora $f(C) = 1_C$. Dimostriamo che f è iniettiva: infatti se $C \neq C'$ (a meno di invertire l'ordine dei due insiemi) esiste $x \in C$ tale che $x \notin C'$. Ma allora $1 = 1_C(x) \neq 1_{C'}(x) = 0$, cioè $f(C) \neq f(C')$. Dimostriamo che f è surgettiva. Infatti data $g : A \rightarrow \{0, 1\}$, sia $C = g^{-1}(1)$. Allora $f(C) = 1_C = g$. Diamo un'altra dimostrazione per induzione su $n \geq 0$. Se $n = 0$, $A = \emptyset$, $\mathcal{P}(A) = \{\emptyset\}$, $1 = 2^0$. Supponiamo ora che $|A| = n + 1$. Fissiamo $a \in A$. Definiamo $X = \{C \in \mathcal{P}(A) \mid a \in C\}$, $Y = \{C \in \mathcal{P}(A) \mid a \notin C\}$. Allora $\mathcal{P}(A) = X \cup Y$ e $X \cap Y = \emptyset$. Ne segue che $|\mathcal{P}(A)| = |X| + |Y|$. Sia $A' = A \setminus \{a\}$. $|A'| = n$. Definiamo

$$\phi : \mathcal{P}(A') \rightarrow X, \quad \phi(C) = C \cup \{a\}$$

$$\psi : \mathcal{P}(A') \rightarrow Y, \quad \psi(C) = C.$$

Si verifica facilmente che sono entrambe bigettive. Allora, per induzione $|X| = |Y| = |\mathcal{P}(A')| = 2^n$, $|\mathcal{P}(A)| = 2^n + 2^n = 2^{n+1}$.

- (3) Se $|A| = n$, $|B| = m$, $m \geq n \geq 1$, poniamo $i(A, B)$ l'insieme delle applicazioni iniettive definite su A a valori in B . Allora $|i(A, B)| = m(m-1) \dots (m-n+1) = \frac{m!}{(m-n)!}$. Operiamo per induzione su $n \geq 1$. Per $n = 1$, $A = \{a\}$, e ci sono m modi di definire $b = f(a) \in B$. Se $|A| = s + 1$, $s + 1 \leq m$, fissiamo $a \in A$, poniamo $A' = A \setminus \{a\}$, $|A'| = s$. Ci sono m modi di assegnare $b = f(a) \in B$. Fissato uno di questi modi ci sono $|i(A', B \setminus \{b\})|$ modi di completare il dato $b = f(a)$ ad un'applicazione iniettiva definita su tutto A . Dunque, per induzione, $|i(A, B)| = m[(m-1) \dots (m-1 - (s-1) + 1)]$ come voluto. Se $n = m$, $i(A, B)$ è l'insieme delle applicazioni bigettive definite su A a valori in B e risulta $|i(A, B)| = n!$.
- (4) Sia $|A| = n$, $0 \leq m \leq n$. Poniamo

$$\mathcal{P}_m(A) := \{C \in \mathcal{P}(A) \mid |C| = m\}$$

$$\binom{n}{m} := |\mathcal{P}_m(A)| .$$

Ricaviamo un metodo induttivo per calcolare questi numeri, noto anche come *triangolo di Tartaglia*.

- Il “triangolo” in questione è dato dal sottoinsieme di $\mathbb{N}^2$, $T = \{(n, m) \in \mathbb{N}^2 \mid n \geq m\}$. lungo il “bordo” di T abbiamo $\binom{n}{n} = \binom{n}{0} = 1$. Infatti A è l’unico sottoinsieme di A con n elementi, $\emptyset$ è l’unico con 0 elementi.
- Consideriamo ora $0 < m < n$. Fissiamo $a \in A$. $A' = A \setminus \{a\}$. $|A'| = n - 1$. Analogamente a quanto fatto prima

$$|\mathcal{P}_m(A)| = |\mathcal{P}_{m-1}(A')| + |\mathcal{P}_m(A')|$$

da cui equivalentemente:

$$\binom{n}{m} = \binom{n-1}{m-1} + \binom{n-1}{m} .$$

Questo schema induttivo determina completamente $\binom{n}{m}$ per ogni $(n, m) \in T$. Per ricondursi ad una induzione formalmente più ordinaria, definiamo per ogni $(n, m) \in T$ la *distanza* $d(n, m)$ di (n, m) dal bordo di T come il numero minimo di segmenti orizzontali o verticali nel piano $\mathbb{R}^2$ con estremi in $\mathbb{N}^2$ che è necessario percorrere per andare da (n, m) ad un punto di coordinate (p, p) o $(p, 0)$. Chiaramente $d(p, p) = d(p, 0) = 0$. Allora lo schema induttivo stabilito sopra può essere riconvertito in una definizione di $\binom{n}{m}$ per induzione su $d = d(n, m) \geq 0$.

Nelle stesse ipotesi, poniamo adesso

$$F(n, m) = \frac{n!}{m!(n-m)!} .$$

Affermiamo che

$$F(n, m) = \binom{n}{m} .$$

Ci sono almeno due modi per dimostrarlo; il primo consiste nel verificare *algebricamente* che $F(n, m)$ verifica lo stesso schema induttivo che definisce $\binom{n}{m}$. Il secondo metodo considera l’applicazione surgettiva

$$g : i(I_m, A) \rightarrow \mathcal{P}_m(A), \quad g(h) = h(I_m) .$$

Si osserva poi che per ogni $C \in \mathcal{P}_m(A)$ ci sono $m!$ funzioni h tali che $g(h) = h(I_m) = C$. Si conclude che

$$\binom{n}{m} = \frac{|i(I_m, A)|}{m!} = F(n, m) .$$

Segue inoltre dalle considerazioni precedenti che:

$$\sum_{j=0}^n \binom{n}{j} = \sum_{j=0}^n |\mathcal{P}_j(A)| = |\mathcal{P}(A)| = 2^n .$$

- (5) I numeri $\binom{n}{m}$ si chiamano anche *coefficienti binomiali* perché intervengono nello sviluppo delle potenze di un binomio secondo la *formula di Newton*:

$$(a + b)^n = \sum_{j=0}^n \binom{n}{j} a^j b^{n-j}$$

che si può dimostrare sia per induzione su $n \geq 0$, sia identificando esplicitamente il coefficiente del monomio $a^j b^{n-j}$ con il numero $\binom{n}{j}$, usando la prima definizione che ne abbiamo dato.

4. INSIEMI INFINITI, CARDINALITÀ

Un insieme A è *infinito* se non è finito. Vogliamo estendere la nozione di “numero degli elementi” al caso di insiemi arbitrari (finiti o infiniti). Prendiamo alcune delle proprietà del numero di elementi di un insieme finito come modello della definizione generale.

Definizione 4.1. Dati due insiemi A e B diciamo che A ha *cardinalità* (a volte si dice anche *potenza*) maggiore o uguale a quella di B (e scriveremo $|A| \geq |B|$) se esiste $f : B \rightarrow A$ iniettiva. Diremo che $|A| = |B|$ se esiste $g : B \rightarrow A$ bigettiva. Diremo che $|A| > |B|$ se $|A| \geq |B|$ ma $|A| \neq |B|$ (cioè esiste $f : B \rightarrow A$ iniettiva ma non esiste $g : B \rightarrow A$ bigettiva).

Nel caso degli insiemi finiti ritroviamo l'usuale *numero di elementi* $|A| \in \mathbb{N}$. In generale la cardinalità *non* è un “numero” ma una specie di qualità condivisa da due insiemi correlati da una applicazione bigettiva. Se $|A| = |\mathbb{N}|$, allora diciamo che A è *numerabile*. Bisogna stare attenti perché diverse proprietà che sono “intuitivamente evidenti” nel caso degli insiemi finiti, invece *non sono più vere* per gli insiemi infiniti, come mostra il punto (2) nel seguente teorema.

Teorema 4.1. (1) Sia A un insieme infinito. Allora $|A| \geq |\mathbb{N}|$.

(2) L'insieme A è infinito se e solo se esiste $B \subset A$, $B \neq A$, tale che $|A| = |B|$.

Dim. (1) Sia X il sottoinsieme di $\mathcal{P}(A)$ formato dai sottoinsiemi non vuoti di A . Definiamo per induzione $f : \mathbb{N} \rightarrow A$ iniettiva, partendo da una funzione di scelta $s : X \rightarrow A$. Poniamo allora $f(0) = s(A)$, $f(n+1) = s(A \setminus \{f(0), \dots, f(n)\})$. Si osservi che f è ben definita perché, essendo A infinito, per ogni n , $A \setminus \{f(0), \dots, f(n)\}$ è non vuoto. E' immediato che f così definita è iniettiva.

(2) Se A è finito sappiamo già che un tale B non esiste. Resta da dimostrare che invece esiste se A è infinito. Dimostriamo intanto la tesi quando $A = \mathbb{N}$. Poniamo $B = 2\mathbb{N}$, cioè l'insieme dei numeri pari. $g : \mathbb{N} \rightarrow 2\mathbb{N}$, $g(n) = 2n$ è bigettiva, quindi $|\mathbb{N}| = |2\mathbb{N}|$. In generale sia $f : \mathbb{N} \rightarrow A$ iniettiva come in (1). $A = f(\mathbb{N}) \cup C_A(f(\mathbb{N}))$ e poniamo: $B = f(2\mathbb{N}) \cup C_A(f(\mathbb{N}))$; $G : A \rightarrow B$, $G(x) = f(g(f^{-1}(x)))$ se $x \in f(\mathbb{N})$, $G(x) = x$ altrimenti. G è bigettiva. $\square$

Altre proprietà del numero degli elementi invece si generalizzano. Indichiamone alcune.

- Vale in generale il seguente *Teorema di Bernstein* la cui dimostrazione, abbastanza complicata, viene omessa.

Teorema 4.2. Dati due insiemi A e B , se $|A| \geq |B|$ e $|B| \geq |A|$, allora $|A| = |B|$.

Si ricordi che le cardinalità *non* sono numeri ordinari. Si tratterebbe di dimostrare che se esistono $f : B \rightarrow A$ e $h : A \rightarrow B$ entrambe iniettive (e del tutto indipendenti tra loro), allora esiste $g : A \rightarrow B$ bigettiva. Se ci si pensa un attimo si capisce che la cosa non è affatto evidente.

- Abbiamo visto prima che se A è finito, $|A| = n$, allora $|\mathcal{P}(A)| = 2^n$ e quindi $|\mathcal{P}(A)| > |A|$. Anche questa proprietà si generalizza.

Teorema 4.3. Per ogni insieme A , $|\mathcal{P}(A)| > |A|$.

Dim. Dimostriamo intanto che $|\mathcal{P}(A)| \geq |A|$ cioè che esiste $f : A \rightarrow \mathcal{P}(A)$ iniettiva. Infatti basta porre $f(a) = \{a\}$. Per concludere basta dimostrare che qualsiasi $g : A \rightarrow \mathcal{P}(A)$ non può essere surgettiva. Infatti, data g , poniamo $C = \{x \in A \mid x \notin g(x)\}$. Affermiamo che C non appartiene all'immagine $g(A)$. Infatti se fosse $C = g(y)$, $y \in C$ se e solo se $y \notin g(y) = C$ e questo è assurdo. $\square$

- Se A e B sono finiti ed esiste $g : A \rightarrow B$ surgettiva, allora è facile vedere che $|A| \geq |B|$. Anche questa proprietà si generalizza:

Teorema 4.4. Sia $g : A \rightarrow B$ un'applicazione surgettiva. Allora $|A| \geq |B|$.

Dim. Vogliamo mostrare che esiste $f : B \rightarrow A$ iniettiva. Per ogni $b \in B$, $X_b = g^{-1}(b) \in \mathcal{P}(A)$ è non vuoto perché g è surgettiva. Poniamo $X = \{X_b \mid b \in B\}$. Sia $s : X \rightarrow A$ una funzione di scelta. Definiamo $f(b) = s(X_b)$. Resta da verificare che f è iniettiva. Infatti se $b \neq b'$, $X_b \cap X_{b'} = \emptyset$, da cui $f(b) \neq f(b')$ perchè appartengono a sottoinsiemi disgiunti di A . $\square$

Osservazioni 4.2. (*Rivolta soprattutto ad un lettore particolarmente interessato.*) Abbiamo detto all'inizio che la possibilità di formare insiemi i cui elementi sono insiemi è un punto delicato che può portare a delle serie difficoltà. Per esempio, ispirati anche dalla penultima dimostrazione, aggiungiamo agli assiomi della nostra “teoria degli insiemi” la proprietà che *ogni insieme non può essere un elemento di se stesso*. Indichiamo con U l'insieme di tutti gli insiemi. Nella nostra teoria c'è allora un *paradosso*. Infatti l'insieme U dovrebbe essere necessariamente un elemento di se stesso, cosa che non ammettiamo. Proviamo allora ad abbandonare quella richiesta. Adesso un paradosso si ottiene considerando come U l'insieme di tutti gli insiemi che non sono un elemento di se stessi. Un modo di aggirare il paradosso è quello di “decretare” che U non è un insieme, accettando così che la nostra “teoria degli insiemi” non è “chiusa in se stessa” e si immerge in una qualche “sovra-teoria”, in cui magari si annidano altri paradossi Ma anche ammettendo questo, noi nella pratica lavoriamo “tranquillamente” con molti “insiemi di insiemi” che, appunto, abbiamo decretato essere insiemi. E se ci fosse annidato da qualche parte un paradosso meno evidente ma altrettanto fatale ?

4.1. Alcuni confronti di cardinalità. Dimostriamo per esempio che $|\mathbb{N}| = |\mathbb{N}^2|$. Costruiamo cioè $f : \mathbb{N} \rightarrow \mathbb{N}^2$ bigettiva. Consideriamo $\mathbb{N}^2$ come un sottoinsieme del piano $\mathbb{R}^2$. Consideriamo la famiglia di rette parallele r_n , $n \geq 0$, di equazione $x + y = n$. Sia $U_n = r_n \cap \mathbb{N}^2$. Allora: per ogni $n \in \mathbb{N}$, $|U_n| = n + 1$; $U_n \cap U_m = \emptyset$ se $n \neq m$; $\mathbb{N}^2 = \cup_{n \in \mathbb{N}} U_n$. Ordiniamo totalmente gli elementi di $\mathbb{N}^2$ nel modo seguente:

- Se $(a, b) \in r_m$, $(c, d) \in r_n$, $n > m$, allora $(c, d) > (a, b)$.
- Se $(a, b), (c, d) \in r_m$, $a > c$, allora $(a, b) > (c, d)$.

Si verifica che è un *buon ordinamento* (l'insieme degli U_n è bene ordinato come lo è $\mathbb{N}$, ogni U_n è finito e quindi ben ordinato). Si può allora definire f per induzione, ponendo $f(0) = (0, 0)$ cioè uguale al minimo elemento di $\mathbb{N}^2$, $f(n+1)$ uguale al minimo elemento di $\mathbb{N}^2 \setminus \{f(0), \dots, f(n)\}$.

Dimostriamo che $|\mathbb{N}| = |\mathbb{Q}^+|$. Usando la rappresentazione di ogni numero razionale per mezzo di un'unica *frazione ridotta ai minimi termini* abbiamo che

$$\mathbb{Q}^+ = \left\{ \frac{n}{d} \mid (n, d) \in \mathbb{N}^2, d > 0, \text{MCD}(n, d) = 1 \right\}.$$

L'applicazione

$$j : \mathbb{Q}^+ \rightarrow \mathbb{N}^2, j\left(\frac{n}{d}\right) = (n, d)$$

è evidentemente iniettiva. Consideriamo $j^{-1} : j(\mathbb{Q}^+) \rightarrow \mathbb{Q}^+$ che è bigettiva. Consideriamo su $\mathbb{N}^2$ il buon ordinamento totale già usato prima. Il sottoinsieme $j(\mathbb{Q}^+) \subset \mathbb{N}^2$ eredita un buon ordinamento totale. Possiamo allora definire per induzione $g : \mathbb{N} \rightarrow j(\mathbb{Q}^+)$ bigettiva usando la stessa procedura usata prima per definire $f : \mathbb{N} \rightarrow \mathbb{N}^2$. Infine $j^{-1} \circ g : \mathbb{N} \rightarrow \mathbb{Q}^+$ è l'applicazione bigettiva cercata. Questo risultato può apparire *anti-intuitivo* se consideriamo $\mathbb{N}$ e $\mathbb{Q}^+$ come sottoinsiemi di $\mathbb{R}^+$ e ricordiamo che $\mathbb{N}$ è discreto mentre $\mathbb{Q}^+$ è *denso* in $\mathbb{R}$ (vedi [REALI]). Il punto è che quando trattiamo la cardinalità, gli insiemi sono “nudi” cioè privi di qualsiasi altra struttura ulteriore (quale quella, per esempio, che è necessaria per potere definire cosa vuol dire che $\mathbb{Q}$ è denso in $\mathbb{R}$).

Poiché l'inclusione $i : \mathbb{N} \rightarrow \mathbb{R}$ è iniettiva, ne segue che $|\mathbb{R}| \geq |\mathbb{N}|$. In effetti si può mostrare che $|\mathbb{R}| > |\mathbb{N}|$ (vedi [AD]).

5. PROPOSIZIONI E TEOREMI

All'interno di una teoria matematica (per esempio “analisi I” di questo corso) si trattano “proposizioni sensate” (cioè che, in particolare, sono formulate rispettando le regole di una certa sintassi - includendo le regole della sintassi dell'italiano) che possono essere *vere* o *false*, ma non contemporaneamente vere e false. Il corpo della teoria in un dato momento del suo sviluppo è dato dall'insieme delle proposizioni che sono state riconosciute come vere (e magari anche “significative”). La dimostrazione di un nuovo *teorema* della teoria accresce il numero di proposizioni riconosciute come vere. Di solito la teoria non è completa nel senso che restano sul campo proposizioni sensate e “significative” che però sono ancora *indeterminate*, cioè non è ancora noto se sono vere o false.

Di solito una proposizione dichiara che certi elementi di un insieme verificano una determinata proprietà; nella sua formulazione è cruciale l'uso corretto dei “quantificatori” *esiste* ($\exists$) e *per ogni* ($\forall$). Esempi “minimali” di proposizioni sono della forma

“ $\exists a \in A$ che verifica la proprietà p ” oppure “ $\forall a \in A$, a verifica la proprietà p ”.

L'espressione *senza* quantificatori “ $a \in A$, a verifica la proprietà p ”, non è sensata.

Di solito si ha però a che fare con proposizioni sensate più complicate dove frammenti elementari si combinano variamente. Per esempio in [C-INTER] incontriamo una proposizione sensata (e vera) del tipo:

$\forall f : [a, b] \rightarrow \mathbb{R}$ continua, $\forall \epsilon \in \mathbb{R}$, $\epsilon > 0$, $\exists \delta \in \mathbb{R}$, $\delta > 0$, tale che $\forall x \in [a, b]$, $\forall y \in [a, b]$, se $|y - x| < \delta$, allora $|f(y) - f(x)| < \epsilon$.

Le proposizioni si possono manipolare e combinare in un modo che ricorda quanto abbiamo fatto con gli insiemi. Per esempio se P e Q sono due proposizioni, abbiamo la proposizione

“ $P \circ Q$ ”

che è vera se e solo se P è vera o Q è vera (ancora una volta “o” non è esclusivo).

La proposizione

“ $P \text{ e } Q$ ”

è vera se e solo se P e Q sono entrambe vere.

La negazione

“non P ”

è vera se e solo se P è falsa; $\text{non}(\text{non } P) = P$. È importante sapere negare una proposizione. Per le proposizioni minimali, basta scambiare i quantificatori $\exists \longleftrightarrow \forall$ e negare la proprietà. Ad esempio la negazione di:

“ $\forall a \in \mathbb{N}$, a è pari”

(che è falsa) è

“ $\exists a \in \mathbb{N}$ che non è pari”

(che è vera). Per le proposizioni più complesse occorre applicare ripetutamente questa regola di base, insieme all'altra per cui “o” $\longleftrightarrow$ “e” si scambiano, facendo un po' di pratica.

Per esempio una proposizione della forma

“ P e non P ”

è sempre falsa e viene detta una *contraddizione*. La sua negazione

“non P o P ”

è sempre vera.

Tipicamente la dimostrazione di un teorema consiste nel dimostrare che una certa *implicazione* è vera. Una implicazione ha la forma

$$P \implies Q$$

e si legge “se P allora Q ”. Infatti vale la seguente *regola di deduzione*:

Se P è vera ed è vera l'implicazione $P \implies Q$, allora anche Q è vera.

Dunque se P faceva già parte del corpo della teoria che stiamo sviluppando, dimostrando che l'implicazione è vera, aggiungiamo Q al corpo della teoria. Il lettore esigente potrebbe pensare che in effetti non abbiamo ancora detto troppo precisamente cosa intendiamo per $P \implies Q$. Lo accontentiamo dicendo che è un altro modo di denotare la proposizione

“(non P) o Q ”

Si noti infatti che se quest'ultima è vera e P è vera, allora (non P) è falsa e quindi necessariamente Q è vera, in perfetto accordo con la regola di deduzione che abbiamo discusso.

Un fatto che spesso è utile è che l'implicazione

$$P \implies Q$$

è equivalente alla sua *contronominale*

$$\text{non } Q \implies \text{non } P$$

cioè la prima implicazione è vera se e solo se è vera la seconda. Per esempio in uno dei fogli di esercizi, si chiedeva di dimostrare

$$h = f \circ g \text{ iniettiva} \implies g \text{ iniettiva}$$

la contronominale è

$$g \text{ non iniettiva} \implies h = f \circ g \text{ non iniettiva}$$

e questa è facile da dimostrare: se $x \neq y$ sono tali che $g(x) = g(y)$, allora $h(x) = f(g(x)) = f(g(y)) = h(y)$. Una versione più elaborata ma sostanzialmente equivalente al passaggio alla contronominale è la cosiddetta *dimostrazione per assurdo*. Si procede così: volendo dimostrare l'implicazione

$$P \implies Q$$

si dimostra invece l'implicazione

$$P \text{ e non } Q \implies S$$

dove S è falsa. Allora, se P è vera, necessariamente non Q è falsa, perché altrimenti, grazie alla solita regola di deduzione, S sarebbe vera (ed invece sappiamo che è falsa). Dunque Q è vera. Nella pratica molto spesso la S che funziona è della forma

$$S = N \text{ e non } N$$

cioè è una contraddizione. Abbiamo visto prima un esempio di dimostrazione per assurdo.

Osservazioni 5.1. (*Rivolta soprattutto ad un lettore particolarmente interessato.*) Consideriamo la seguente proposizione “sensata”

Esiste un insieme infinito X tale che $|\mathbb{N}| < |X| < |\mathbb{R}|$.

La sua negazione è anche nota come *ipotesi del continuo*. Per lungo tempo è stata una proposizione “indeterminata” della “teoria degli insiemi”. Alla fine è stato appurato che è in effetti “indecidibile”. Quest’ultimo aggettivo ha un significato preciso e molto riposto che non siamo in grado qui di spiegare. Vogliamo solo segnalare che lo studio di questa proposizione ha portato ad alcune delle riflessioni più profonde sui fondamenti della logica e della matematica.