2.6 (♡). Definire $3^{\sqrt{2}}$ utilizzando solamente le potenze ad esponente intero, il principio del minimo intero ed il principio di completezza dei numeri reali.

2.7 (♡). Usare il principio di definizione ricorsiva per dimostrare che per ogni numero reale x esiste un'applicazione bigettiva $g\colon \mathbb{N} \to \mathbb{N}$ tale che

$$\lim_{n\to\infty} \sum_{i=1}^{n} \frac{(-1)^{g(i)}}{g(i)} = x.$$

2.3 Cardinalità

Definizione 2.4. *Diremo che due insiemi X, Y hanno la stessa* ***cardinalità****, e scriveremo $|X| = |Y|$, se esiste un'applicazione bigettiva $X \to Y$.*

È chiaro che se $|X| = |Y|$ e $|Y| = |Z|$, allora anche $|X| = |Z|$. Talvolta la notazione $|X|$ potrebbe essere ambigua (ad esempio se siamo in un contesto nel quale intervengono anche dei valori assoluti); in tal caso è possibile utilizzare una delle due notazioni alternative $\mathrm{Card}(X)$ e $\#X$. Si usa anche dire che due insiemi sono **equipotenti** se hanno la stessa cardinalità.

Definizione 2.5. *Un insieme si dice* ***infinito numerabile*** *se ha la stessa cardinalità dell'insieme $\mathbb{N} = \{1, 2, 3, \ldots\}$ dei numeri naturali. Un insieme si dice* ***numerabile*** *se è finito oppure se è infinito numerabile.*

Per il Lemma 2.3 un insieme è numerabile se e soltanto se ha la stessa cardinalità di un sottoinsieme di $\mathbb{N}$. Vediamo adesso alcuni esempi.

Esempio 2.6. Gli insiemi $\mathbb{Z}$ e $\mathbb{N}_0$ sono numerabili. Infatti le applicazioni $f\colon \mathbb{Z} \to \mathbb{N}$,

$$f(n) = \begin{cases} 2n & \text{se } n > 0, \\ 1 - 2n & \text{se } n \leq 0, \end{cases}$$

e $g\colon \mathbb{N}_0 \to \mathbb{N}$, $g(n) = n + 1$, sono bigettive.

Esempio 2.7. L'insieme $\mathbb{N} \times \mathbb{N}$ delle coppie di numeri naturali è numerabile. Per dimostrarlo, osserviamo che l'insieme $C = \{(x, y) \in \mathbb{Z}^2 \mid 0 \leq x \leq y\}$ è numerabile poiché per ogni intero $n \geq 0$ esiste un unico elemento $(x, y) \in C$ tale che $n = x + \sum_{i=0}^{y} i$. Inoltre l'applicazione

$$\mathbb{N}_0 \times \mathbb{N}_0 \to C, \qquad (a, b) \mapsto (a, a + b)$$

è bigettiva. In conclusione, una bigezione esplicita tra $\mathbb{N} \times \mathbb{N}$ ed $\mathbb{N}$ è data da

$$\mathbb{N} \times \mathbb{N} \to \mathbb{N}, \qquad (a, b) \mapsto a + \sum_{i=0}^{a+b-2} i = \frac{1}{2}(a + b - 2)(a + b - 1) + a\,.$$

Per ogni insieme X denotiamo con $\mathcal{P}(X)$ la famiglia dei sottoinsiemi di X e con $\mathcal{P}_0(X) \subset \mathcal{P}(X)$ la famiglia dei sottoinsiemi finiti di X.

Esempio 2.8. La famiglia $\mathcal{P}_0(X)$ dei sottoinsiemi finiti di un sottoinsieme numerabile X è ancora numerabile. Infatti possiamo identificare X con $\mathbb{N}_0$ e osservare che ogni sottoinsieme finito di $\mathbb{N}_0$ può essere interpretato come l'insieme delle cifre uguali ad 1 di un opportuno numero binario: questo fatto è equivalente a dire che l'applicazione

$$\mathcal{P}_0(\mathbb{N}_0) \to \mathbb{N}_0, \qquad \{\emptyset\} \mapsto 0, \quad \{n_1, \dots, n_k\} \mapsto \sum_{i=1}^{k} 2^{n_i},$$

è bigettiva.

Dimostreremo più avanti (Corollario 2.31) che per ogni insieme infinito X vale $|\mathcal{P}_0(X)| = |X|$.

Teorema 2.9 (Cantor). *Sia X un insieme non vuoto, allora non esistono applicazioni surgettive $f\colon X \to \mathcal{P}(X)$. In particolare X e $\mathcal{P}(X)$ non hanno la stessa cardinalità.*

Dimostrazione. Sia $f\colon X \to \mathcal{P}(X)$ un'applicazione e proviamo che il sottoinsieme

$$S = \{x \in X \mid x \notin f(x)\} \in \mathcal{P}(X)$$

non appartiene all'immagine di f. Supponiamo per assurdo che esista un elemento $s \in X$ tale che $f(s) = S$. Se $s \in S$, allora dalla definizione di S segue che $s \notin f(s) = S$; se invece $s \notin S = f(s)$, allora dalla definizione di S segue che $s \in f(s) = S$. In ogni caso si arriva ad una contraddizione. □

Esempio 2.10. Ogni intervallo aperto $]a, b[\ \subset \mathbb{R}$, con $a < b$, ha la stessa cardinalità di $\mathbb{R}$. Infatti, fissato un numero reale $c \in\ ]a, b[$, l'applicazione $f\colon]a, b[\ \to \mathbb{R}$,

$$f(x) = \begin{cases} \dfrac{x-c}{b-x} & \text{se } c \leq x < b \\[2ex] \dfrac{x-c}{x-a} & \text{se } a < x \leq c \end{cases}$$

è bigettiva.

Lemma 2.11. *Siano X, Y insiemi e siano $f\colon X \to Y$, $g\colon Y \to X$ applicazioni. Allora esiste un sottoinsieme $A \subset X$ tale che*

$$A \cap g(Y - f(A)) = \emptyset, \qquad A \cup g(Y - f(A)) = X.$$

Dimostrazione. Consideriamo la famiglia $\mathcal{A}$ dei sottoinsiemi $B \subset X$ tali che $B \cap g(Y - f(B)) = \emptyset$. Sicuramente $\mathcal{A}$ non è vuota poiché contiene il sottoinsieme vuoto. Verifichiamo che $A = \cup\{B \mid B \in \mathcal{A}\}$ ha le proprietà richieste.

Se $x \in A$, allora esiste $B \in \mathcal{A}$ tale che $x \in B$, quindi $x \notin g(Y - f(B))$ ed a maggior ragione $x \notin g(Y - f(A))$. Se esistesse $x \notin A \cup g(Y - f(A))$ allora, ponendo $C = A \cup \{x\}$ si avrebbe $g(Y - f(C)) \subset g(Y - f(A))$ e quindi $C \cap g(Y - f(C)) = \emptyset$ in contraddizione con la definizione di A. $\square$

Dal Lemma 2.11 segue facilmente il seguente utile criterio per determinare se due insiemi hanno la stessa cardinalità.

Teorema 2.12 (di Cantor–Schröder–Bernstein). *Siano X, Y due insiemi. Se esistono due applicazioni iniettive $f\colon X \to Y$ e $g\colon Y \to X$, allora X e Y hanno la stessa cardinalità.*

Dimostrazione. Per il Lemma 2.11 esiste un sottoinsieme $A \subset X$ tale che, ponendo $B = Y - f(A)$ vale

$$A \cap g(B) = \emptyset \quad \text{e} \quad A \cup g(B) = X.$$

Per come abbiamo definito B si ha inoltre che $B \cap f(A) = \emptyset$ e $B \cup f(A) = Y$, mentre dall'iniettività di f e g segue che le due applicazioni $f\colon A \to f(A)$ e $g\colon B \to g(B)$ sono bigettive. Basta adesso osservare che l'applicazione

$$h\colon X \to Y, \qquad h(x) = \begin{cases} f(x) & \text{se } x \in A \\ g^{-1}(x) & \text{se } x \in g(B) \end{cases}$$

è bigettiva. $\square$

Se X e Y sono insiemi scriveremo $|X| \leq |Y|$ se esiste un'applicazione iniettiva $X \to Y$. Abbiamo appena dimostrato che valgono le proprietà:

Riflessiva: *$|X| \leq |X|$ per ogni insieme X.*
Antisimmetrica: *se $|X| \leq |Y|$ e $|Y| \leq |X|$, allora $|X| = |Y|$.*
Transitiva: *se $|X| \leq |Y|$ e $|Y| \leq |Z|$, allora $|X| \leq |Z|$.*

Scriveremo $|X| \geq |Y|$ se e solo se $|Y| \leq |X|$.

Osservazione 2.13. È possibile dimostrare, e lo faremo più avanti (Proposizione 2.25), che le cardinalità di due insiemi sono sempre confrontabili, cioè che per ogni coppia di insiemi X, Y vale $|X| \leq |Y|$ oppure $|Y| \leq |X|$.

Per ogni coppia di insiemi X, Y denotiamo con X^Y l'insieme di tutte le applicazioni $f\colon Y \to X$. Ad esempio $\mathbb{R}^{\mathbb{N}}$ indica l'insieme di tutte le successioni $a_1, a_2, \ldots$ di numeri reali. Esiste una bigezione naturale

$$\alpha\colon (X^Y)^Z \to X^{Y \times Z}, \qquad \alpha(g)(y, z) = g(z)(y).$$

Proposizione 2.14. *Gli insiemi $\mathbb{R}$, $\mathbb{N}^{\mathbb{N}}$, $\mathbb{R}^{\mathbb{N}}$, $2^{\mathbb{N}}$ e $\mathcal{P}(\mathbb{N})$ hanno tutti la stessa cardinalità. In particolare l'insieme $\mathbb{R}$ dei numeri reali non è numerabile.*

Dimostrazione. Prima di iniziare la dimostrazione, ricordiamo che per ogni insieme X esiste una bigezione naturale tra $\mathcal{P}(X)$ e l'insieme di tutte le applicazioni da X nell'insieme $\{0,1\}$. Tale bigezione associa ad ogni funzione $f\colon X \to \{0,1\}$ il sottoinsieme $A = \{x \in X \mid f(x) = 1\}$. Quindi $\mathcal{P}(X)$ e 2^X hanno la stessa cardinalità.

Sia C l'insieme delle successioni $\{f_n\}$ strettamente crescenti di numeri naturali. L'applicazione bigettiva

$$\alpha\colon \mathbb{N}^{\mathbb{N}} \to C, \qquad \alpha(f)_n = \sum_{i=1}^{n} f(i)\,,$$

mostra che C ha la stessa cardinalità di $\mathbb{N}^{\mathbb{N}}$. L'applicazione

$$\beta\colon]1,+\infty[\to C, \qquad \beta(x)_n = \text{ parte intera di } 10^n x,$$

è iniettiva e quindi $|\mathbb{R}| \le |C|$. Viceversa l'applicazione $\gamma\colon C \to \mathbb{R}$ definita da

$$\gamma(f) = \sum_{n=1}^{+\infty} \frac{1}{10^{f_n}} = \sup\left\{\sum_{n=1}^{N} \frac{1}{10^{f_n}} \mid N \in \mathbb{N}\right\}$$

è anch'essa iniettiva e quindi $|\mathbb{R}| \ge |C|$. Per il Teorema di Cantor–Schröder–Bernstein si ha $|\mathbb{R}| = |C| = |\mathbb{N}^{\mathbb{N}}|$.

Poiché esiste una bigezione tra $\mathbb{N}$ e $\mathbb{N} \times \mathbb{N}$, gli insiemi $\mathbb{N}^{\mathbb{N}}$ e $\mathbb{N}^{\mathbb{N}\times\mathbb{N}}$ hanno la stessa cardinalità e quindi $|\mathbb{N}^{\mathbb{N}\times\mathbb{N}}| = |(\mathbb{N}^{\mathbb{N}})^{\mathbb{N}}| = |\mathbb{R}^{\mathbb{N}}|$. Similmente si ha $|\mathcal{P}(\mathbb{N})| = |2^{\mathbb{N}}| = |2^{\mathbb{N}\times\mathbb{N}}| = |(2^{\mathbb{N}})^{\mathbb{N}}| = |\mathcal{P}(\mathbb{N})^{\mathbb{N}}|$ e poiché esistono delle naturali applicazioni iniettive $2^{\mathbb{N}} \to \mathbb{N}^{\mathbb{N}}$ e $\mathbb{N} \to \mathcal{P}(\mathbb{N})$ ne segue che

$$|\mathbb{N}^{\mathbb{N}}| \le |\mathcal{P}(\mathbb{N})^{\mathbb{N}}| = |2^{\mathbb{N}}| \le |\mathbb{N}^{\mathbb{N}}|. \qquad \square$$

Esercizi

2.8. Descrivere una bigezione tra gli intervalli $[0,1[$ e $[0,+\infty[$.

2.9. Mostrare che se $A \subset \mathbb{R}$ contiene un intervallo aperto non vuoto, allora $|A| = |\mathbb{R}|$.

2.10. Provare che l'insieme dei numeri razionali è numerabile.

2.11 (♡). Sia X l'insieme delle successioni finite di numeri naturali. Dimostrare che X è numerabile.

2.12 (☕, ♡). Si dimostri l'esistenza, sull'insieme $\mathbb{N}$ dei numeri naturali, di una famiglia infinita non numerabile di sottoinsiemi C_i tali che $C_i \cap C_j$ abbia cardinalità finita per ogni $i \neq j$.

2.4 L'assioma della scelta

Supponiamo di avere un'applicazione surgettiva di insiemi $g\colon Y \to X$ e cerchiamo di costruire un'applicazione $f\colon X \to Y$ tale che $g(f(x)) = x$ per ogni x. Possiamo procedere nel modo seguente: si prende un elemento $x_1 \in X$ e si *sceglie* un elemento $f(x_1)$ nell'insieme non vuoto $g^{-1}(\{x_1\})$, poi si prende un elemento $x_2 \in X - \{x_1\}$ e si *sceglie* un elemento $f(x_2)$ nell'insieme non vuoto $g^{-1}(\{x_2\})$ eccetera. Se X è un insieme finito, allora tale procedura ha termine e ci fornisce l'applicazione f cercata. Se invece X è infinito, in assenza di altre informazioni non c'è alcuna ragione elementare che ci assicuri la possibilità di fare le *infinite scelte* necessarie per poter definire f. Per questo motivo, se vogliamo fare qualche progresso matematico, dobbiamo aggiungere al nostro arsenale il celeberrimo assioma della scelta, che enunceremo in due versioni equivalenti.

Assioma della scelta (prima versione): *Se $g\colon Y \to X$ è un'applicazione surgettiva di insiemi, allora esiste un'applicazione $f\colon X \to Y$ tale che $g(f(x)) = x$ per ogni $x \in X$.*

C'è da dire che, in un certo senso, l'assioma della scelta non è né vero né falso ed ognuno può crederci o meno (con le relative conseguenze). Per maggiori informazioni e delucidazioni su questo argomento rimandiamo a [24]. Tuttavia l'assioma della scelta è accettato dalla quasi totalità dei matematici ed anche noi accetteremo la sua validità senza riserva alcuna.

Proposizione 2.15. *Dati due insiemi non vuoti X e Y, vale $|X| \le |Y|$ se e solo se esiste un'applicazione surgettiva $Y \twoheadrightarrow X$.*

Dimostrazione. È chiaro che se esiste un'applicazione iniettiva $f\colon X \to Y$ di insiemi non vuoti, allora esiste anche un'applicazione surgettiva $g\colon Y \to X$. Infatti basta fissare un elemento $x_0 \in X$ e porre $g(y) = f^{-1}(y)$ se $y \in f(X)$ e $g(y) = x_0$ altrimenti.

Viceversa se esiste $g\colon Y \to X$ surgettiva, allora per l'assioma della scelta esiste $f\colon X \to Y$ tale che $g(f(x)) = x$ per ogni $x \in X$. Una tale applicazione f è iniettiva, infatti se $f(x_1) = f(x_2)$ allora $x_1 = g(f(x_1)) = g(f(x_2)) = x_2$. □

Una **relazione** in un insieme X è un qualsiasi sottoinsieme $\mathfrak{R} \subset X \times X$. È consuetudine scrivere $x\mathfrak{R}y$ se e solo se $(x, y) \in \mathfrak{R}$.

Una **relazione di equivalenza** su di un insieme X è una relazione $\sim$ che soddisfa le proprietà:

Riflessiva:	*$x \sim x$ per ogni $x \in X$.*
Simmetrica:	*se $x \sim y$, allora $y \sim x$.*
Transitiva:	*se $x \sim y$ e $y \sim z$, allora $x \sim z$.*

Definizione 2.16. *Sia $\sim$ una relazione di equivalenza su un insieme X. La* ***classe di equivalenza*** *di un elemento $x \in X$ è il sottoinsieme*

$$[x] \subset X, \qquad [x] = \{y \in X \mid y \sim x\}.$$

Le classi di equivalenza determinano univocamente la relazione di equivalenza e le tre proprietà precedenti diventano:

Riflessiva: *$x \in [x]$ per ogni $x \in X$.*
Simmetrica: *se $x \in [y]$, allora $y \in [x]$.*
Transitiva: *se $x \in [y]$ e $y \in [z]$, allora $x \in [z]$.*

Si dimostra facilmente che se $[x] \cap [y] \neq \emptyset$ allora $x \sim y$ e $[x] = [y]$. L'insieme delle classi di equivalenza $X/\sim = \{[x] \mid x \in X\}$ viene detto **quoziente** di X per la relazione $\sim$. È ben definita un'applicazione

$$\pi \colon X \to X/\sim, \qquad \pi(x) = [x],$$

detta **proiezione al quoziente**. Per l'assioma della scelta esiste un'applicazione $f \colon X/\sim \to X$ tale che $f([x]) \in [x]$ per ogni classe di equivalenza. L'immagine di f è quello che viene detto **insieme di rappresentanti**, ossia un sottoinsieme $S \subset X$ che interseca ogni classe di equivalenza in uno ed un solo punto.

Esempio 2.17. Sull'insieme $\mathbb{R}^{n+1} - \{0\}$ dei vettori non nulli a $n+1$ dimensioni definiamo $x \sim y$ se esiste $t \in]0, +\infty[$ tale che $x = ty$. È immediato osservare che $\sim$ è una relazione di equivalenza e che la sfera S^n è un insieme di rappresentanti.

Lemma 2.18. *Siano $\sim$ una relazione di equivalenza su X, $\pi \colon X \to X/\sim$ la proiezione al quoziente e $f \colon X \to Y$ un'applicazione. Sono fatti equivalenti:*

1. *L'applicazione f è costante sulle classi di equivalenza, ossia $f(x) = f(y)$ ogni volta che $x \sim y$.*
2. *Esiste un'unica applicazione $g \colon X/\sim \to Y$ tale che $f = g\pi$.*

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "\pi"] & Y \\ X/\sim \arrow[ur, dashed, "g"'] & \end{tikzcd}$$

Dimostrazione. Lasciata per esercizio. □

Per alcune applicazioni è più comoda la seguente versione dell'assioma della scelta.

Assioma della scelta (seconda versione): *Sia $X = \cup\{X_i \mid i \in I\}$ l'unione di una famiglia di insiemi non vuoti X_i indicizzati da un insieme I. Allora esiste un'applicazione $f \colon I \to X$ tale che $f(i) \in X_i$ per ogni i.*

Mostriamo che la prima e la seconda versione dell'assioma della scelta sono tra loro equivalenti. Se $X = \cup\{X_i \mid i \in I\}$, allora possiamo considerare l'insieme $Y = \{(x, i) \in X \times I \mid x \in X_i\}$ e le due proiezioni $p\colon Y \to X$, $q\colon Y \to I$. Per ipotesi p e q sono entrambe surgettive e, per la prima versione dell'assioma della scelta, esiste $h\colon I \to Y$ tale che la composizione qh è l'identità su I. Basta allora considerare la funzione $f = ph\colon I \to X$.

Viceversa, se $g\colon X \to I$ è un'applicazione surgettiva di insiemi allora l'insieme $X_i = g^{-1}(i) = \{x \in X \mid g(x) = i\}$ è non vuoto per ogni $i \in I$. Poiché $X = \cup_i X_i$, per la seconda versione dell'assioma della scelta, esiste $f\colon I \to X$ tale che $f(i) \in X_i$, ovvero tale che $gf(i) = i$ per ogni $i \in I$.

Esempio 2.19. Utilizziamo l'assioma della scelta per dimostrare che l'unione numerabile di insiemi numerabili è ancora numerabile. Sia $\{X_n \mid n \in \mathbb{N}\}$ una famiglia numerabile di insiemi numerabili; allora per ogni n l'insieme delle applicazioni iniettive $X_n \hookrightarrow \mathbb{N}$ è non vuoto e l'assioma della scelta permette di scegliere, per ogni $n \in \mathbb{N}$, un'applicazione iniettiva $f_n\colon X_n \to \mathbb{N}$. Consideriamo adesso le applicazioni:

$$\mu\colon \cup_n X_n \to \mathbb{N}, \qquad \mu(x) = \min\{n \mid x \in X_n\},$$
$$\phi\colon \cup_n X_n \to \mathbb{N} \times \mathbb{N}, \qquad \phi(x) = (\mu(x), f_{\mu(x)}(x)).$$

È immediato verificare che ϕ è iniettiva e quindi che l'insieme $\cup_n X_n$ è numerabile.

Osservazione 2.20. L'assioma della scelta permette di dimostrare alcuni teoremi che urtano con l'intuizione, e questa è una delle ragioni che creano perplessità su di esso. Gli esempi più eclatanti sono probabilmente i risultati noti come il *paradosso di Hausdorff* (Esercizio 14.9) ed il *paradosso di Banach–Tarski* [27]: diremo che due sottoinsiemi $A, B \subset \mathbb{R}^3$ sono equi-decomponibili se è possibile trovare degli insiemi $A_1, \dots, A_n$ e delle isometrie dirette (rototraslazioni) $\theta_1, \dots, \theta_n$ di $\mathbb{R}^3$ tali che A e B sono rispettivamente le unioni disgiunte di $A_1, \dots, A_n$ e $\theta_1(A_1), \dots, \theta_n(A_n)$. Il teorema di Banach–Tarski afferma che ogni palla chiusa raggio 1 in $\mathbb{R}^3$ è equidecomponibile all'unione disgiunta di due palle chiuse di raggio 1.

D'altra parte, senza l'assioma della scelta gran parte della matematica inevitabilmente collassa. Ad esempio, senza l'assioma della scelta l'unione numerabile di insiemi numerabili potrebbe non essere numerabile, vedi in proposito [24, pag. 228].

Esercizi

2.13. Dato un insieme X denotiamo con $\mathcal{P}(X)'$ la famiglia dei sottoinsiemi non vuoti di X. Una *funzione scelta* su X è per definizione un'applicazione $s\colon \mathcal{P}(X)' \to X$ tale che $s(A) \in A$ per ogni sottoinsieme non vuoto $A \subset X$. Dimostrare che l'assioma della scelta equivale all'esistenza di funzioni scelta per ogni insieme.

2.14 (♡). Siano $X = \cup\{X_i \mid i \in I\}$ e $Y = \cup\{Y_i \mid i \in I\}$ unioni disgiunte di due famiglie di insiemi indicizzate dallo stesso insieme di indici I. Dimostrare che, se per ogni $i \in I$, l'insieme X_i ha la stessa cardinalità di Y_i, allora X ha la stessa cardinalità di Y.

2.15. Dimostrare che l'assioma della scelta è equivalente al seguente **postulato di Zermelo.** *Sia $\mathcal{A}$ una famiglia di insiemi non vuoti e disgiunti. Allora esiste un insieme C tale che $C \cap A$ è formato da un solo elemento per ogni $A \in \mathcal{A}$.*

2.16 (♡). Siano dati un insieme X ed una famiglia numerabile $\mathcal{B}$ di sottoinsiemi di X. Denotiamo con $\mathcal{T}$ la collezione dei sottoinsiemi di X che si possono scrivere come unione di elementi di $\mathcal{B}$. Dimostrare che per ogni famiglia $\mathcal{A} \subset \mathcal{T}$ esiste una sottofamiglia numerabile $\mathcal{A}' \subset \mathcal{A}$ tale che

$$\bigcup_{U \in \mathcal{A}'} U = \bigcup_{V \in \mathcal{A}} V.$$

2.17. Utilizzare l'assioma della scelta per dimostrare in modo matematicamente rigoroso il seguente risultato.

Sia $f\colon X \to Y$ un'applicazione surgettiva di insiemi. Se per ogni $y \in Y$ l'insieme $f^{-1}(y)$ è infinito numerabile, allora esiste un'applicazione bigettiva $X \to Y \times \mathbb{N}$ la cui composizione con la proiezione $Y \times \mathbb{N} \to Y$ è uguale ad f.

2.18. Calcolare la cardinalità dell'insieme di tutte le applicazioni bigettive $\mathbb{N} \to \mathbb{N}$ (Sugg.: per ogni sottoinsieme $A \subset \mathbb{N}$ con almeno 2 elementi esiste un'applicazione bigettiva $f\colon \mathbb{N} \to \mathbb{N}$ tale che $f(n) = n$ se e solo se $n \notin A$.)

2.5 Il lemma di Zorn

Prima di poter essere applicato alla soluzione di molti problemi matematici, l'assioma della scelta ha bisogno di essere trasformato in enunciati ad esso equivalenti ma dal contenuto meno intuitivo. Fra le varie incarnazioni (vedi [12, p. 33]), la più celebre è senza dubbio il **lemma di Zorn**. Mentre l'assioma della scelta ha a che fare con le relazioni di equivalenza, il lemma di Zorn riguarda le relazioni d'ordine.

Un **ordinamento** in un insieme X è una relazione $\leq$ che soddisfa le tre proprietà:

Riflessiva:	*$x \leq x$ per ogni $x \in X$.*
Antisimmetrica:	*se $x \leq y$ e $y \leq x$, allora $x = y$.*
Transitiva:	*se $x \leq y$ e $y \leq z$, allora $x \leq z$.*

Un ordinamento viene anche detto una **relazione d'ordine**. Se $\leq$ è un ordinamento si definisce $x < y$ se $x \leq y$ e $x \neq y$.

Esempio 2.21. Sia Y un insieme; dati due sottoinsiemi $A, B \subset Y$ definiamo

$$A \leq B \quad \text{se} \quad A \subset B.$$

La relazione $\leq$ è un ordinamento su $\mathcal{P}(Y)$ detto di *inclusione*.

Un ordinamento su X si dice **totale** se per ogni $x, y \in X$ vale $x \leq y$ oppure $y \leq x$. Un **insieme ordinato** è un insieme dotato di un ordinamento; un **insieme totalmente ordinato** è un insieme dotato di un ordinamento totale.[2]

Ogni sottoinsieme di un insieme ordinato è a sua volta un insieme ordinato, con la relazione di ordine indotta.

Definizione 2.22. *Sia $(X, \leq)$ un insieme ordinato:*

1. *Un sottoinsieme $C \subset X$ si dice una **catena** se per ogni $x, y \in C$ vale $x \leq y$ oppure $x \geq y$. In altri termini $C \subset X$ è una catena se e solo se C è un insieme totalmente ordinato per la relazione di ordine indotta.*
2. *Sia $C \subset X$ un sottoinsieme e $x \in X$. Diremo che x è un **maggiorante** di C se $x \geq y$ per ogni $y \in C$.*
3. *Diremo che $m \in X$ è un **elemento massimale** di X se è l'unico maggiorante di se stesso, cioè se $\{x \in X \mid m \leq x\} = \{m\}$.*

Teorema 2.23 (Lemma di Zorn). *Sia $(X, \leq)$ un insieme ordinato non vuoto. Se ogni catena in X possiede almeno un maggiorante, allora X possiede elementi massimali.*

Avvertiamo il giovane studioso che le applicazioni del lemma di Zorn sono decisamente più istruttive della sua dimostrazione. Pertanto, la dimostrazione del lemma di Zorn, che richiede l'assioma della scelta e che riportiamo per completezza nella Sezione 8.2, può essere benissimo omessa ad una prima lettura.

Mostriamo che il lemma di Zorn implica l'assioma della scelta. La dimostrazione che daremo rappresenta il più classico ed utile schema di applicazione

[2] Questa definizione non è universalmente accettata: alcuni chiamano ordinamenti gli ordinamenti totali e ordinamenti parziali gli ordinamenti. Altri usano la parola **poset** (dall'inglese Partially Ordered SET) per indicare un insieme ordinato.

del lemma di Zorn e pertanto svolgeremo il nostro compito in tutti i dettagli. Consideriamo la prima versione dell'assioma della scelta: sia $g\colon Y \to X$ un'applicazione surgettiva di insiemi non vuoti e mostriamo che il lemma di Zorn implica l'esistenza di un'applicazione $f\colon X \to Y$ tale che $g(f(x)) = x$ per ogni $x \in X$. Introduciamo l'insieme $\mathcal{S}$ i cui elementi sono le coppie (E, f) tali che:

1. $E \subset X$ è un sottoinsieme.
2. $f\colon E \to Y$ è un'applicazione tale che $gf(x) = x$ per ogni $x \in E$.

L'insieme $\mathcal{S}$ non è vuoto, esso contiene infatti la coppia $(\emptyset, \emptyset \hookrightarrow Y)$. Su $\mathcal{S}$ è possibile ordinare gli elementi per *estensione*, definiamo cioè $(E, h) \le (F, k)$ se k estende h: in altri termini $(E, h) \le (F, k)$ se e solo se $E \subset F$ e $h(x) = k(x)$ per ogni $x \in E$. Mostriamo adesso che ogni catena in $\mathcal{S}$ possiede maggioranti. Sia $\mathcal{C} \subset \mathcal{S}$ una catena e consideriamo l'insieme

$$A = \bigcup_{(E,h)\in\mathcal{C}} E.$$

Definiamo poi $a\colon A \to Y$ nel modo seguente: se $x \in A$ allora esiste $(E, h) \in \mathcal{C}$ tale che $x \in E$, e si pone $a(x) = h(x)$. Si tratta di una buona definizione, infatti se $(F, k) \in \mathcal{C}$ e $x \in F$ si ha, poiché $\mathcal{C}$ è una catena $(E, h) \le (F, k)$ oppure $(E, h) \ge (F, k)$. In entrambi i casi $x \in E \cap F$ e $h(x) = k(x)$. È chiaro che $(A, a) \in \mathcal{S}$ è un maggiorante di $\mathcal{C}$.

Per il lemma di Zorn esiste un elemento massimale $(U, f) \in \mathcal{S}$ e basta dimostrare che $U = X$. Se così non fosse esisterebbe $y \in Y$ tale che $g(y) \notin U$ e la coppia $(U \cup \{g(y)\}, f')$, che estende (U, f) e tale che $f'(g(y)) = y$, appartiene a $\mathcal{S}$ e contraddice la massimalità di (U, f).

Corollario 2.24. *Sia $(X, \le)$ un insieme ordinato in cui ogni catena possiede almeno un maggiorante. Allora per ogni $a \in X$ esiste un elemento massimale m di X tale che $m \ge a$.*

Dimostrazione. Si applica il lemma di Zorn all'insieme $\{x \in X \mid x \ge a\}$. □

Proposizione 2.25. *Le cardinalità sono comparabili, e cioè se X e Y sono due insiemi, allora vale $|X| \le |Y|$ oppure $|Y| \le |X|$.*

Dimostrazione. Consideriamo la famiglia $\mathcal{A}$ dei sottoinsiemi $A \subset X \times Y$ tali che le proiezioni $p\colon A \to X$ e $q\colon A \to Y$ sono entrambe iniettive. L'insieme vuoto appartiene alla famiglia $\mathcal{A}$ che è quindi non vuota ed è ordinata per inclusione. Ogni catena $\mathcal{C} \subset \mathcal{A}$ possiede maggioranti: infatti, considerando il candidato naturale $C = \cup\{A \mid A \in \mathcal{C}\}$, si ha che $p\colon C \to X$ e $q\colon C \to Y$ sono entrambe iniettive e pertanto C è un maggiorante di $\mathcal{C}$.

Per il lemma di Zorn esiste un elemento massimale A; dimostriamo che almeno una delle due proiezioni $p\colon A \to X$ e $q\colon A \to Y$ è surgettiva. Se così non fosse esisterebbero $x \in X - p(A)$ e $y \in Y - q(A)$; quindi $A \cup \{(x, y)\} \in \mathcal{A}$ in contraddizione con la massimalità di A.

Se $p\colon A \to X$ è surgettiva allora $|X| = |A| \leq |Y|$. Viceversa, se $q\colon A \to Y$ è surgettiva, allora $|Y| = |A| \leq |X|$. □

Esercizi

2.19. Sia X un insieme ordinato con la proprietà che ogni suo sottoinsieme non vuoto possiede massimo e minimo. Mostrare che X è finito e totalmente ordinato.

2.20. Sia $\prec$ una relazione su di un insieme X tale che:

1. Per ogni $x, y \in X$, almeno una delle due relazioni $x \prec y$, $y \prec x$ è falsa.
2. Se vale $x \prec y$ e $y \prec z$, allora $x \prec z$.

Dimostrare che la relazione

$$x \leq y \quad \iff \quad x \prec y \ \text{ oppure } \ x = y$$

è una relazione di ordine.

2.21. Sia $f\colon X \to X$ un'applicazione di un insieme X in sé e denotiamo con

$$f^0 = Id_X, \quad f^1 = f, \quad f^2 = f \circ f, \quad \ldots, \quad f^n = f \circ f^{n-1}, \quad \ldots$$

le iterate di f. Consideriamo la relazione "*$x \leq y$ se esiste $n \geq 0$ tale che $x = f^n(y)$*". Dimostrare che $\leq$ è una relazione di ordine su X se e solo se ogniqualvolta $f^n(x) = x$ per qualche $n > 0$ e $x \in X$ vale $f(x) = x$.

2.22. Sia V uno spazio vettoriale (non necessariamente di dimensione finita) e consideriamo l'insieme $G(V)$ dei suoi sottospazi vettoriali, ordinato per inclusione (Esempio 2.21). Dimostrare che per ogni sottoinsieme $X \subset V$ che contiene 0 la famiglia

$$\{F \in G(V) \mid F \subset X\}$$

possiede elementi massimali.

2.23 (Lemma di Tukey, ♡). Siano X un insieme e $\mathcal{B}$ una famiglia non vuota di sottoinsiemi di X con la proprietà che $A \subset X$ appartiene a $\mathcal{B}$ se e soltanto se ogni sottoinsieme finito $B \subset A$ appartiene a $\mathcal{B}$. Dimostrare che $\mathcal{B}$ contiene elementi massimali rispetto all'inclusione.

2.24. Usare il lemma di Zorn per dimostrare che ogni insieme possiede ordinamenti totali.