Paolo Vitolo

Appunti di Teoria degli Insiemi

Versione del 10 maggio 2015

CAPITOLO 1

Insiemi

In questo capitolo illustreremo la teoria assiomatica degli insiemi. Alla fine daremo le definizioni di filtro e di ultrafiltro.

Per una trattazione più dettagliata della teoria degli insiemi, si rimanda ai testi specializzati, come [**1**] o [**3**].

I. Formule ben formate

Fin dall'inizio della teoria degli insiemi è indispensabile usare formule. Ne daremo quindi una definizione il più precisa possibile, evitando però eccessive pedanterie.

Una formula sarà una sequenza di simboli del nostro linguaggio formale. I simboli sono dei seguenti tipi:

Variabili: lettere come v_0, v_1, v_2, ecc., ma ci permetteremo di usare qualunque lettera, quandi anche a, b, c, ... o A, B, C, ... o $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, ... o α, β, γ, ... o altre ancora.
Simboli relazionali: $=$ e $\in$, più altri che potremmo aggiungere in seguito.
Parentesi: (e). Useremo, se necessario, parentesi di diverse grandezze per migliorare la leggibilità.
Connettivi logici: $\wedge$, $\vee$, $\neg$, $\Rightarrow$, $\Leftrightarrow$.
Quantificatori: $\forall$ e $\exists$.

Una *formula ben formata*, o più brevemente una *formula*, è costruita rispettando le seguenti regole:

(1) Se x e y sono variabili, allora $x = y$ e $x \in y$ sono formule.
(2) Se φ e ψ sono formule, lo sono anche le seguenti:

$$(\varphi) \wedge (\psi), \quad (\varphi) \vee (\psi), \quad \neg(\varphi), \quad (\varphi) \Rightarrow (\psi), \quad (\varphi) \Leftrightarrow (\psi).$$

(3) Se φ è una formula e z è una variabile, anche $\forall z(\varphi)$ e $\exists z(\varphi)$ sono formule.

Indicheremo una forumla con Φ, o anche $\Phi(v_0, v_1, \dots)$ nel caso si vogliano evidenziare una o più variabili che eventualmente vi compaiano. È bene sottolineare, comunque, che la notazione $\Phi(v)$ non significa necessariamente che la variabile v compaia effettivamente nella formula. Queste notazioni sono utili anche nel caso in cui, data una formula $\Psi(x)$, si voglia considerare la formula ottenuta sostituendo y a x in tutte le (eventuali) occorrenze di x in $\Psi(x)$: indicheremo con $\Psi(y)$ la formula così ottenuta.

Una *sottoformula* di una formula Φ è una sequenza di simboli consecutivi di Φ che costituisca ancora una formula. Ad esempio, se Φ è la formula

$$(a = b) \vee (a = c),$$

le sottoformule di Φ, oltre a Φ stessa, sono $a = b$ e $b = c$. Il *campo di azione* di un quantificatore in una formula Φ è la sottoformula di Φ che inizia con quel quantificatore. Una variabile si dice *vincolata* se è immediatamente preceduta da un quantificatore; in caso contrario si dice *libera*.

Le formule saranno da interpretarsi quali *predicati* della nostra teoria, esprimenti proprietà degli enti rappresentati dalle variabili libere. Le formule senza variabili libere saranno da intendersi come proposizioni, che possono semplicemente essere vere o false nella teoria. Pertanto può accadere che due formule si equivalgano in quanto hanno la stessa interpretazione. È possibile formalizzare questi concetti, ma ci asterremo dal farlo, considerando l'interpretazione di una formula come intuitivamente evidente.

Un caso tipico di formule che si equivalgono nel senso su esposto è il seguente. Sia Φ una formula in cui la variabile x compare subito dopo un quantificatore; indichiamo con $\Psi(x)$ il campo di azione di quel quantificatore. Se Φ' è la formula ottenuta da Φ sostituendo la sottoformula $\Psi(x)$ con $\Psi(y)$, le formule Φ e Φ' si equivalgono.

Rararmente scriveremo una formula per esteso, e comunque di solito ometteremo quante più coppie di parentesi sia possibile, eventualmente sostituendole con una maggiore spaziatura, purché la comprensione della formula sia garantita. Inoltre ci riserveremo di estendere, anche tacitamente, la regola (1) vista sopra, ampliando la quantità di simboli relazionali a nostra disposizione. (In effetti è possibile estendere anche le altre regole in modo simile). Possiamo fin da ora definire $\neq$ e $\notin$ come segue: per qualunque scelta delle variabili x e y,

$$
\begin{aligned}
x \neq y \quad &\text{equivale a} \quad \neg(x = y);\\
x \notin y \quad &\text{equivale a} \quad \neg(x \in y).
\end{aligned}
$$

II. Gli assiomi di Zermelo–Fraenkel

Presentiamo la teoria degli insiemi che fu introdotta da Ernst Zermelo e successivamente rielaborata da Abraham Fraenkel[1]. Per indicare questi assiomi e la teoria sviluppata a partire da essi, si usa comunemente l'acronimo ZF.

Il concetto primitivo è l'*appartenenza*, che sarà indicata, come è d'uso, dal simbolo $\in$. La scrittura $x \in Y$ si leggerà "*x appartiene a Y*" o, equivalentemente, "*x è elemento di Y*"; scriveremo anche, a volte, $Y \ni x$ e diremo che Y *possiede* x.

Gli oggetti della teoria sono—è bene tenerlo presente—solo *insiemi*. Ciò significa, in particolare, che un oggetto che appartiene a un insieme sarà sempre esso stesso un insieme.

Tuttavia seguiremo quanto più è possibile la convenzione di usare lettere latine minuscole a sinistra del simbolo di appartenenza, e maiuscole a destra. A volte poi, se oltre che agli elementi di un insieme A siamo interessati anche a un oggetto di cui A stesso è elemento, useremo per tale oggetto il termine *collezione* (che è comunque sinonimo di insieme) e lo denoteremo con una lettera callgrafica maiuscola, come $\mathcal{A}$.

Gli assiomi che seguono ci dicono, intuitivamente, quali tipi di insiemi è possibile formare a partire da quelli che già abbiamo. Ad esempio ci sarà l'insieme di tutti i sottoinsiemi di un insieme dato, mentre, come vedremo, l'insieme di tutti i possibili insiemi non esiste.

Enunceremo gli assiomi in linguaggio naturale; naturalmente è sempre possibile usare una formulazione rigorosa, ma ce ne asterremo per migliorare la leggibilità.

ASSIOMA 0 (di esistenza). *Esiste almeno un insieme.*

In altre parole, c'è qualche oggetto della teoria. Senza questo assioma, si correrebbe il rischio di ragionare sul nulla.

[1] Vi sono anche altre assiomatizzazioni della teoria degli insiemi: una di esse, dovuta Bernays e Gödel, è schematizzata in [**1**, pag. 76]; un'altra è riportata in appendice a [**2**].

Assioma 1 (di estensionalità). *Siano A e B insiemi. Se per ogni x si ha che $x \in A$ se e solo se $x \in B$, allora $A = B$.*

Dunque un insieme è individuato dai suoi elementi, e solo da essi.

Diciamo che A è *sottoinsieme* di B, o che A è *contenuto* o *incluso* in B, e scriviamo $A \subseteq B$, se ogni elemento di A appartiene anche a B; a volte scriveremo anche $B \supseteq A$, e diremo che B è *soprainsieme* di A (o che B *contiene* o *include* A).

A volte, quando useremo il la parola "collezione" come sinonimo di insieme, useremo anche il termine "*sottocollezione*" come sinonimo di sottoinsieme.

Dall'assioma di estensionalità discende immediatamente che l'insieme A coincide con l'insieme B se e solo se si ha simultaneamente $A \subseteq B$ e $B \subseteq A$.

Assioma 2 (di fondazione). *Se A è un insieme con almeno un elemento, allora esiste $x \in A$ tale che x e A non hanno elementi in comune.*

Questo assioma non è strettamente indispensabile. Il suo scopo è di evitare comportamenti troppo strani (e comunque inutili) della relazione di appartenenza.

Il prossimo assioma necessita del concetto di formula, che abbiamo introdotto nel paragrafo precedente.

Assioma 3 (di comprensione). *Sia $\Phi = \Phi(x_1, \dots, x_n)$ una formula. Per ogni A e per ogni scelta di $x_1, \dots, x_n$, esiste un insieme B i cui elementi sono tutti e soli gli $y \in A$ tali che $\Phi(x_1, \dots, x_n)$ è vera.*

Questo, a rigor di termini, è uno *schema di assiomi* perché si ha un assioma diverso per ogni possibile formula.

L'insieme B (unico per l'assioma di estensionalità) la cui esistenza è postulata dall'assioma di comprensione si indicherà con la scrittura

$$\{\, x \in A \mid \Phi(x_1, \dots, x_n) \,\}.$$

Possiamo allora definire l'*insieme vuoto* nel modo seguente:

$$\{\, x \in A \mid x \neq x \,\},$$

dove A è un insieme qualunque (la cui esistenza è assicurata dall'assioma 0). L'insieme vuoto verrà indicato con $\varnothing$.

1.1. Esercizio. Dati due insiemi A e B, definire l'*intersezione* $A \cap B$ e la *differenza* $A \smallsetminus B$.

Inoltre, dati gli insiemi A, B e C, verificare che

(1) $A \cap B = A \iff A \subseteq B$;
(2) $A \cap A = A$;
(3) $A \cap B = B \cap A$;
(4) $(A \cap B) \cap C = A \cap (B \cap C)$.

Infine, mostrare che, se A e B sono sottoinsiemi di C, si ha $A \smallsetminus B = A \cap (C \smallsetminus B)$.

Due insiemi A e B tali che $A \cap B = \varnothing$ vengono detti *disgiunti*.

Ora siamo in grado di verificare che non è possibile costruire ogni insieme immaginabile. In particolare, l'insieme di tutti gli insiemi non esiste.

Ragioniamo per assurdo. Supponiamo che esista un insieme V tale che ogni insieme è elemento di V. Mediante l'Assioma 3, costruiamo l'insieme

$$T = \{\, x \in V \mid x \notin x \,\}.$$

È immediato controllare che $T \in T$ se e solo se $T \notin T$, il che è ovviamente assurdo.

Questo fenomeno è noto come *Paradosso di Russell*.

L'assioma di comprensione è detto anche assioma di *isolamento* perché permette di isolare determinati elementi in un insieme che li possiede già. Ciò consente di semplificare i successivi assiomi, postulando l'esistenza di insiemi che potrebbero avere altri elementi oltre a quelli voluti, da cui poi eventualmente isolare questi ultimi usando l'Assioma 3.

Assioma 4 (della coppia). *Comunque siano scelti a e b, esiste un insieme di cui entrambi sono elementi.*

Come abbiamo osservato, poiché questo assioma asserisce l'esistenza di un insieme C tale che $a \in C$ e $b \in C$, occorre poi applicare l'assioma di comprensione per ottenere

$$\{\, x \in C \mid x = a \ \vee \ x = b \,\}.$$

Tale insieme si chiama *coppia (non ordinata)* di elementi a e b, e si indica con $\{a, b\}$; se $a = b$, si indica con $\{a\}$ e si chiama *singoletto* di a.

1.2. Esercizio. Provare che non può aversi contemporaneamente $x \in y$ e $y \in x$.

Suggerimento. Applicare l'assioma di fondazione a $\{x, y\}$.

La *coppia ordinata* di primo elemento a e secondo elemento b è, per definizione,

$$(a, b) = \big\{\{a, b\}, \{a\}\big\}.$$

1.3. Esercizio. Verificare (a', b') coincide con (a'', b'') se e solo se $a' = a''$ e $b' = b''$.

Assioma 5 (dell'unione). *Per ogni insieme $\mathcal{F}$, esiste un insieme U cui appartengono tutti gli x tali che si abbia $x \in Y$ per qualche $Y \in \mathcal{F}$.*

Analogamente a quanto visto per la coppia, e con riferimento alle notazioni usate nell'Assioma 5, possiamo definire l'*unione di $\mathcal{F}$* come l'insieme

$$\bigcup \mathcal{F} = \{\, x \in U \mid \exists Y \in \mathcal{F} \ \ x \in Y \,\}.$$

Se $\mathcal{F}$ è la coppia $\{A, B\}$, la sua unione sarà indicata con $A \cup B$ e chiamata *unione (binaria) di A e B*.

Dati gli insiemi A, B e C, in modo analogo a quanto visto nell'Esercizio 1.1, si può verificare che

(1) $A \cup B = A \iff A \supseteq B$;
(2) $A \cup A = A$;
(3) $A \cup B = B \cup A$;
(4) $(A \cup B) \cup C = A \cup (B \cup C)$.

1.4. Esercizio. Costruire l'intersezione una collezione $\mathcal{F}$. Verificare poi che, nel caso particolare in cui $\mathcal{F}$ è una coppia $\{A, B\}$, si ritrova $A \cap B$ quale risulta dall'Esericizio 1.1.

Enunciare e dimostrare le proprietà distributive dell'intersezione rispetto all'unione e dell'unione rispetto all'intersezione.

Mostrare infine che, se X è un soprainsieme di $\bigcup \mathcal{F}$, si ha

$$X \smallsetminus \bigcup \mathcal{F} = \bigcap \{\, X \smallsetminus A \mid A \in \mathcal{F} \,\}, \tag{1.1}$$

$$X \smallsetminus \bigcap \mathcal{F} = \bigcup \{\, X \smallsetminus A \mid A \in \mathcal{F} \,\}. \tag{1.2}$$

Suggerimento. Occore anzitutto escludere il caso in cui $\mathcal{F}$ è vuoto.

Anche il prossimo è in realtà uno schema di assiomi, cioè dà luogo a una quantità potenzialmente infinita di assiomi, uno per ogni possibile formula.

Assioma 6 (di rimpiazzamento). *Sia $\Phi = \Phi(x, y, x_1, \dots, x_n)$ una formula. Dati A e $x_1, \dots, x_n$, supponiamo che, per ogni $x \in A$, esista uno e un solo y per cui Φ è vera. Allora esiste un insieme B tale che, per ogni $x \in A$, esiste $y \in B$ per cui Φ è vera.*

In termini intuitivi, se abbiamo una funzione il cui dominio è un insieme A, possiamo costruire un insieme B che abbia come elementi le immagini di tutti gli elementi di A.

Non è però ancora possibile usare le funzioni all'interno della teoria: esse saranno definite più avanti (si veda la Definizione 2.26 a pagina 13).

Con gli assiomi introdotti finora si può già sviluppare una teoria piuttosto ricca, sufficiente a comprendere in sé l'Aritmetica. In particolare è possibile costruire infiniti insiemi, ma non un insieme con infiniti elementi: per questo serve un ulteriore assioma.

Prima dell'enunciato di tale ulteriore assioma dobbiamo definire, per ogni insieme x, il *successore ordinale* di x:

$$S(x) = x \cup \{x\}.$$

Assioma 7 (dell'infinito). *Esiste un insieme A, con $\varnothing \in A$, e tale che, se $x \in A$, anche $S(x) \in A$.*

Questo assioma, in effetti, ci assicura l'esistenza di insiemi che possiedono infiniti elementi (si veda l'Esercizio 2.37 a pagina 14).

L'ultimo assioma risulta indispensabile per alcune costruzioni, in particolare per definire i numeri reali.

Assioma 8 (dell'insieme potenza). *Per ogni insieme A esiste un insieme $\mathcal{B}$ tale che tutti i sottoinsiemi di A appertengono a $\mathcal{B}$.*

Sia dunque A un insieme, e sia $\mathcal{B}$ dato dal precedente assioma. Possiamo definire l'*insieme delle parti*, (o *insieme potenza*) di A, al seguente modo:

$$\mathcal{P}(A) = \{\, X \in \mathcal{B} \mid X \subseteq A \,\}.$$

Abbiamo così completato la lista degli assiomi di ZF: con essi è possibile costruire la consueta teoria degli insiemi. In particolare, si possono dare tutte le usuali definizioni riguardanti le relazioni, le funzioni e le operazioni.

Più avanti (si veda la Definizione 3.5) introdurremo anche i numeri naturali, mentre i numeri reali verranno dati per scontati.

In definitiva, basandosi su ZF, si costruisce l'intero edificio della matematica.

Come esempio definiamo il prodotto cartesiano[2].

1.5. Definizione. Il *prodotto cartesiano* di due insiemi A e B è

$$A \times B = \big\{\, (x, y) \in \mathcal{P}\big(\mathcal{P}(A \cup B)\big) \;\big|\; x \in A \;\wedge\; y \in B \,\big\}.$$

III. Classi e insiemi

Consideremo come *classe* un aggregato di oggetti, cioè di insiemi, del tipo $\{\, x \mid \Phi \,\}$, dove Φ è una formula. Nella teoria degli insiemi ZF, ciò viene fatto in modo informale, mentre in altre assiomatizzazioni le classi sono oggetti della teoria.

Bisogna tenere presente che ogni insieme è una classe, ma non tutte le classi sono insiemi. Una classe che non è un insieme verrà detta *propria*.

Ad esempio, l'insieme vuoto è la classe $\{\, x \mid x \neq x \,\}$. Invece $\mathbf{V} = \{\, x \mid x = x \,\}$ è una classe propria: la classe di tutti gli insiemi, detta anche *classe universale* o *universo*.

Come abbiamo fatto per gli insiemi, parleremo di elementi di una classe e di sottoclassi. Gli elementi di una classe però non possono mai essere classi proprie, ma solo insiemi.

[2]Applicando opportunamente l'assioma di rimpiazzamento è possibile definire il prodotto cartesiano anche senza fare uso dell'Assioma 8 (si veda ad esempio [**3**, pag. 13]).

Ogni classe è dunque una sottoclasse della classe universale, mentre ogni sottoclasse di un insieme è anch'essa un insieme: quest'ultimo fatto può essere visto come una riformulazione dell'assioma di comprensione.

Usando le classi in luogo degli insiemi si possono costruire enti analoghi alle relazioni e alle funzioni. Non ci sono termini specifici per questi enti, che saranno quindi anch'essi chiamati relazioni o funzioni, rispettivamente. Il fatto che si tratti di insiemi o di classi proprie, sarà comunque chiaro dal contesto.

Si noti che in tal modo l'assioma di rimpiazzamento può essere espresso semplicemente dall'affermazione che l'immagine di un insieme mediante una funzione è ancora un insieme.

Ci limitiamo ai precedenti cenni sulle classi, rimandando per una trattazione più dettagliata ai testi specializzati.

IV. Filtri e basi di filtro

1.6. Definizione. Sia X un insieme. Un *filtro su X* è una collezione non vuota $\mathcal{F}$ di sottoinsiemi non vuoti di X tali che:

- Se $A, B \in \mathcal{F}$, anche $A \cap B \in \mathcal{F}$;
- Se $A \in \mathcal{F}$ e $C \subseteq X$ è soprainsieme di A, anche $C \in \mathcal{F}$.

Una *base* del filtro $\mathcal{F}$ è una $\mathcal{B} \subseteq \mathcal{F}$ tale che ogni $A \in \mathcal{F}$ è soprainsieme di qualche $B \in \mathcal{B}$.

Dati i filtri $\mathcal{F}$ e $\mathcal{G}$ su X, diciamo che $\mathcal{G}$ è *più fine* di $\mathcal{F}$ se $\mathcal{F} \subseteq \mathcal{G}$. Un *ultrafiltro* su X è un filtro $\mathcal{U}$ tale che, se $\mathcal{F}$ è un filtro più fine di $\mathcal{U}$, si ha necessariamente $\mathcal{F} = \mathcal{U}$.

Ad esempio $\{X\}$ è un filtro su X, se X non è vuoto; invece $\mathcal{P}(X)$ non è un filtro[3] perché $\varnothing \in \mathcal{P}(X)$.

1.7. Esercizio. Sia $p \in X$. Verificare che la collezione $\mathcal{U}$ di tutti i sottoinsiemi di X che possiedono p è un ultrafiltro, di cui $\big\{\{p\}\big\}$ è una base.

1.8. Definizione. Diremo che $\mathcal{B}$ è una *base di filtro* (o un *prefiltro*) se esiste un filtro $\mathcal{F}$ su $\bigcup \mathcal{B}$ di cui $\mathcal{B}$ è base.

Se $\mathcal{B}$ è una base di filtro e $X \supseteq \bigcup \mathcal{B}$ diremo che $\mathcal{B}$ è una base di filtro *su* X.

Dato un insieme non vuoto X, per ogni base di filtro $\mathcal{B}$ su X esiste uno e un solo filtro su X di cui $\mathcal{B}$ è base: esso si dirà *filtro generato da $\mathcal{B}$ (su X)*.

1.9. Esercizio. Mostrare che una collezione non vuota $\mathcal{B}$ di insiemi non vuoti è una base di filtro se e solo se

$$\forall F, G \in \mathcal{B} \quad \exists H \in \mathcal{B} \quad H \subseteq F \cap G.$$

1.10. Definizione. Date le basi di filtro $\mathcal{B}$ e $\mathcal{C}$ diremo che $\mathcal{C}$ è *più fine* di $\mathcal{B}$ se per ogni $B \in \mathcal{B}$ esiste un $C \in \mathcal{C}$ contenuto in B.

1.11. Esercizio. Dato un insieme non vuoto X, siano $\mathcal{B}$ e $\mathcal{C}$ basi di filtro su X. Mostrare che $\mathcal{C}$ è più fine di $\mathcal{B}$ se e solo se il filtro generato da $\mathcal{C}$ su X è più fine di quello generato da $\mathcal{B}$.

[3] A volte $\mathcal{P}(X)$ viene chiamato *filtro improprio* su X.

CAPITOLO 2

Relazioni e Funzioni

Daremo la definizione di relazione e ne passeremo in rassegna le principali proprietà. Ci soffermeremo inoltre sulle relazioni d'ordine e sulle funzioni. Al termine del capitolo daremo una definizione generale di prodotto cartesiano.

I. Relazioni

2.1. Definizione. Chiamiamo *relazione* un insieme $\mathcal{R}$ i cui elementi sono coppie ordinate.

Il *campo di una relazione* $\mathcal{R}$ è l'insieme

$$F(\mathcal{R}) = \bigcup \{ \bigcup X \mid X \in \mathcal{R} \}.$$

Il *dominio* di $\mathcal{R}$ è

$$\mathrm{dom}(\mathcal{R}) = \{ x \in F(\mathcal{R}) \mid \exists y \in F(\mathcal{R}) \ \ (x,y) \in \mathcal{R} \}$$

e l'*immagine* è

$$\mathrm{ran}(\mathcal{R}) = \{ y \in F(\mathcal{R}) \mid \exists x \in F(\mathcal{R}) \ \ (x,y) \in \mathcal{R} \}.$$

Se $\mathcal{R}$ è una relazione e $(a,b) \in \mathcal{R}$, scriveremo anche $a \,\mathcal{R}\, b$.

2.2. Esercizio. Dimostrare che:

(1) Se $\mathcal{R}$ è una relazione, allora $\mathrm{dom}(\mathcal{R}) \cup \mathrm{ran}(\mathcal{R}) = F(\mathcal{R})$.
(2) Si ha $\mathcal{R} \subseteq A \times B$ se e solo se $\mathcal{R}$ è una relazione con $\mathrm{dom}(\mathcal{R}) \subseteq A$ e $\mathrm{ran}(\mathcal{R}) \subseteq B$.

2.3. Definizione. Diremo che una relazione $\mathcal{R}$ è *transitiva* se

$$\forall x,y,z \in F(\mathcal{R}) \ \ \big[x \,\mathcal{R}\, y \ \wedge \ y \,\mathcal{R}\, z \implies x \,\mathcal{R}\, z \big].$$

Se $\mathcal{R}$ è una relazione e $F(\mathcal{R}) \subseteq E$, diremo anche $\mathcal{R}$ è una relazione *su* E. Se $\mathrm{dom}(\mathcal{R}) \subseteq A$ e $\mathrm{ran}(\mathcal{R}) \subseteq B$ diremo che che $\mathcal{R}$ è una relazione *da* A *a* B; in virtù dell'Esercizio 2.2(2), ciò equivale a dire che $\mathcal{R}$ è un sottoinsieme del prodotto cartesiano $A \times B$.

2.4. Definizione. Sia $\mathcal{R}$ una relazione. Diremo che $\mathcal{R}$ è *riflessiva* se per ogni $x \in F(\mathcal{R})$, si ha $(x,x) \in \mathcal{R}$. Diremo che $\mathcal{R}$ è *antiriflessiva* se, per ogni $x \in F(\mathcal{R})$, si ha $(x,x) \notin \mathcal{R}$.

2.5. Esercizio. La *relazione di appartenenza su un insieme* A è l'iniseme delle coppie $(x,y) \in A \times A$ tali che $x \in y$.

Mostrare che tale relazione è antiriflessiva.

Suggerimento. Si veda l'Esercizio 1.2.

2.6. Definizione. Sia $\mathcal{R}$ una relazione. Diremo che $\mathcal{R}$ è *simmetrica* se per ogni $(x,y) \in \mathcal{R}$, si ha $(y,x) \in \mathcal{R}$. Diremo che $\mathcal{R}$ è *antisimmetrica* se, per ogni $x,y \in F(\mathcal{R})$, con $x \neq y$ non si può avere contemporaneamente $(x,y) \in \mathcal{R}$ e $(y,x) \in \mathcal{R}$.

2.7. Esercizio. Sia $\mathfrak{B}(X)$ la collezione delle basi di filtro su un insieme non vuoto X. Si consideri la relazione σ su $\mathfrak{B}(X)$ così definita:

$$\mathcal{A} \,\sigma\, \mathcal{B} \iff \mathcal{A} \text{ è più fine di } \mathcal{B}.$$

Mostrare che σ è riflessiva e transitiva. Verificare inoltre che, se X ha almeno due elementi distinti, σ non è né simmetrica né antisimmetrica.

II. Relazioni di equivalenza

2.8. Definizione. Una *relazione di equivalenza*, o semplicemente una *equivalenza*, è una relazione riflessiva, simmetrica e transitiva.

Dato un insieme A, l'*identità su A* è la relazione

$$\iota_A = \{\, (x,x) \mid x \in A \,\}.$$

Si tratta evidentemente di una relazione di equivalenza su A. Un'altro esempio di equivalenza su A è $A \times A$, detta anche *relazione universale* (su A).

2.9. Esercizio. Sia $\mathfrak{B}(X)$ la collezione delle basi di filtro su un insieme non vuoto X. Si consideri la relazione ξ su $\mathfrak{B}(X)$ così definita:

$$\mathcal{A} \,\xi\, \mathcal{B} \iff (\mathcal{A} \text{ è più fine di } \mathcal{B}) \wedge (\mathcal{B} \text{ è più fine di } \mathcal{A}).$$

Mostrare che ξ è una relazione di equivalenza.

Una relazione di equivalenza sarà solitamente indicata con un simbolo come $\equiv$ o altri simili.

2.10. Definizione. Sia $\equiv$ una relazione di equivalenza su A, e sia $x \in A$. La *classe di equivalenza* di x è l'insieme

$$[x] = \{\, a \in A \mid a \equiv x \,\}.$$

La collezione $\{\, [x] \mid x \in A \,\}$ verrà chiamata *insieme quoziente*, o semplicemente *quoziente*, e indicata con la notazione $A/{\equiv}$, che si legge A *modulo* $\equiv$.

Ad esempio, le classi di equivalenza dell'identità su A sono i singoletti degli elementi di A; la relazione universale ha invece un'unica classe di equivalenza, costituita da tutto A.

2.11. Esercizio. Sia $\mathcal{F}$ un filtro su X. Mostrare che la classe di equivalenza di $\mathcal{F}$ rispetto alla relazione introdotta nell'Esercizio 2.9 è l'insieme delle basi di $\mathcal{F}$.

L'insieme quoziente rispetto a una relazione di equivalenza è una collezione di insiemi caratterizzata da particolari proprietà. Diamo un nome a questo genere di collezioni.

2.12. Definizione. Sia A un insieme. Una *partizione* di A è una collezione $\mathcal{C} \subseteq \mathcal{P}(A)$ tale che:

- $\forall C \in \mathcal{C} \quad C \neq \varnothing$;
- $\forall C', C'' \in \mathcal{C} \quad (C' \neq C'' \implies C' \cap C'' = \varnothing)$;
- $\bigcup \mathcal{C} = A$.

Da ogni relazione di equivalenza si può ricavare una partizione e viceversa. Il procedimento è indicato in dettaglio nell'esercizio che segue.

2.13. Esercizio. Sia A un insieme. Data una partizione $\mathcal{C}$ di A, definiamo la relazione $\mathcal{R}(\mathcal{C})$ su A come segue: per ogni $a, b \in A$

$$(a,b) \in \mathcal{R}(\mathcal{C}) \iff \exists C \in \mathcal{C}\ (a \in C \ \wedge \ b \in C). \tag{2.1}$$

Mostrare che $\mathcal{R}(\mathcal{C})$ è una relazione di equivalenza e che l'insieme quoziente coincide con $\mathcal{C}$.

Dimostrare inoltre che, per ogni equivalenza $\equiv$ su A, l'insieme quoziente $A/{\equiv}$ è una partizione di A, e la relazione $\mathcal{R}(A/{\equiv})$, definita come in (2.1), coincide con $\equiv$.

III. Relazioni di ordine

2.14. Definizione. Diremo che $\mathcal{R}$ è una *relazione di ordine (stretto)* su A, o anche che l'insieme è *parzialmente ordinato (in senso stretto)* da $\mathcal{R}$, se $\mathcal{R}$ è una relazione antiriflessiva e transitiva su A.

Chiameremo *insieme parzialmente ordinato (in senso stretto)* la coppia $(A, \mathcal{R})$, o anche solo l'insieme A, quando $\mathcal{R}$ sia chiara dal contesto.

2.15. Esercizio. La *relazione di inclusione su un insieme* A è l'insieme $\mathcal{I}$ delle coppie $(x, y) \in A \times A$ tali che $x \subseteq y$.

Verificare che $\mathcal{I}$ è una relazione transitiva.

Osservare poi che $\mathcal{I}$ è anche riflessiva, e che quindi $\mathcal{I}$ non è una relazione d'ordine stretto se $A \neq \varnothing$.

Mostrare infine che è una relazione d'ordine stretto l'*inclusione propria*, definita da

$$x \subset y \iff x \subseteq y \ \wedge \ x \neq y. \tag{2.2}$$

Se $x \subset y$ come definito nella (2.2), diremo che x è un *sottoinsieme proprio* di y.

Per indicare una relazione d'ordine (stretto) useremo il simbolo $<$ o altri simili. La scrittura $x < y$ si leggerà "x precede (strettamente) y", o anche "x è minore di y".

2.16. Definizione. Un insieme ordinato $(A, <)$ si dice *totalmente ordinato*, e $<$ si dice *relazione di ordine totale*, se

$$\forall x, y \in A \ \ [x < y \ \vee \ y < x \ \vee \ x = y].$$

Ad esempio, è noto che l'ordinamento usuale $<$ sull'insieme $\mathbb{R}$ dei numeri reali è una relazione di ordine totale.

In seguito, quando $\mathbb{R}$ sarà considerato come insieme ordinato da una relazione $<$, sarà sempre sottinteso che $<$ è l'ordinamento usuale.

2.17. Esercizio. Dimostrare che $(\mathcal{P}(A), \subset)$, dove $\subset$ indica l'inclusione propria (si veda l'Esercizio 2.15), è un insieme totalmente ordinato se e solo se A ha al più un elemento.

Nell'ambito degli insiemi ordinati, saranno impiegate le convenzioni e la terminologia usuale, che daremo per scontate. D'ora in avanti useremo dunque simboli come $\leqslant$, termini come "minimo" e "massimo", o locuzioni come "estremo superiore", senza che sia necessario spiegarne il significato.

2.18. Definizione. Sia $(A, <)$ un insieme ordinato. Un *intervallo* è un sottoinsieme I di A tale che

$$\forall x, y \in I \quad \forall z \in A \quad \big[[x < z \ \wedge \ z < y] \implies z \in I \big]. \tag{2.3}$$

Esempi di intervalli in un insieme ordinato $(A, <)$ sono l'insieme vuoto, A stesso, e tutti i sottoinsiemi delle seguenti forme[1]:

[1]Alcuni autori chiamano *insiemi convessi* quelli che verificano la (2.3) e limitano il termine "intervallo" ai soli insiemi dei tipi (2.4).

$$
\begin{aligned}
]{\leftarrow}, a[&= \{\, x \in A \mid x < a \,\}, \\
]{\leftarrow}, a] &= \{\, x \in A \mid x \leqslant a \,\}, \\
]b, {\rightarrow}[&= \{\, x \in A \mid b < x \,\}, \\
[b, {\rightarrow}[&= \{\, x \in A \mid b \leqslant x \,\}, \\
]a, b[&= \{\, x \in A \mid a < x \ \wedge \ x < b \,\}, \\
[a, b] &= \{\, x \in A \mid a \leqslant x \ \wedge \ x \leqslant b \,\}, \\
[a, b[&= \{\, x \in A \mid a \leqslant x \ \wedge \ x < b \,\}, \\
]a, b] &= \{\, x \in A \mid a < x \ \wedge \ x \leqslant b \,\}.
\end{aligned}
\tag{2.4}
$$

Se A è l'insieme $\mathbb{R}$ dei numeri reali, si usa scrivere $-\infty$ e $+\infty$ in luogo di $\leftarrow$ e $\rightarrow$, rispettivamente.

2.19. Esercizio. Sia A un insieme ordinato, e sia $\mathcal{I}$ una collezione non vuota di intervalli di A.

(1) Verificare che l'intersezione di $\mathcal{I}$ è ancora un intervallo.
(2) Dimostrare che, se A è totalmente ordinato e $\bigcap \mathcal{I} \neq \varnothing$, anche l'unione $\bigcup \mathcal{I}$ è un intervallo.
(3) Dare un esempio che mostri che, nel punto precedente, non si può eliminare l'ipotesi che A sia totalmente ordinato.

IV. Composizione di relazioni

2.20. Definizione. La *composizione* della relazione $\mathcal{R}$ con la relazione $\mathcal{S}$ è la relazione

$$\mathcal{S} \circ \mathcal{R} = \{\, (x, z) \in \operatorname{dom}(\mathcal{R}) \times \operatorname{ran}(\mathcal{S}) \mid \exists y \ [(x, y) \in \mathcal{R} \ \wedge \ (y, z) \in \mathcal{S}] \,\}.$$

2.21. Esercizio. Verificare che una relazione $\mathcal{R}$ è transitiva se e solo se $\mathcal{R} \circ \mathcal{R} \subseteq \mathcal{R}$.

2.22. Definizione. Data una relazione $\mathcal{R}$, la sua *inversa* è la relazione

$$\mathcal{R}^{-1} = \{\, (x, y) \in F(\mathcal{R}) \times F(\mathcal{R}) \mid (y, x) \in \mathcal{R} \,\}.$$

2.23. Esercizio. Siano $\mathcal{R}$ e $\mathcal{S}$ relazioni. Verificare che $(\mathcal{S} \circ \mathcal{R})^{-1} = \mathcal{R}^{-1} \circ \mathcal{S}^{-1}$.

Se $<$ indica una relazione d'ordine, la relazione inversa verrà indicata con $>$. Essa è ancora una relazione d'ordine, come immediatamente si verifica. La scrittura $x > y$ si leggerà "x segue (strettamente) y", o "x è maggiore di y".

2.24. Definizione. Sia $\mathcal{R}$ una relazione, e sia A un insieme. La *restrizione* di $\mathcal{R}$ ad A è la relazione

$$\mathcal{R}_{\restriction A} = \{\, (x, y) \in \mathcal{R} \mid x \in A \,\}.$$

Se $\mathcal{S}$ è una restrizione di $\mathcal{R}$ diremo anche che $\mathcal{R}$ è un'*estensione* di $\mathcal{S}$ a $\operatorname{dom}(\mathcal{R})$.

Se $\mathcal{R}$ è una relazione, e A è un insieme, l'*immagine di A tramite* $\mathcal{R}$ è l'insieme $\mathcal{R}[A] = \operatorname{ran}(\mathcal{R}_{\restriction A})$.

L'immagine $\mathcal{R}^{-1}[B]$ di un insieme B tramite l'inversa di una relazione $\mathcal{R}$ viene anche detta *immagine inversa* o *controimmagine* di B (tramite $\mathcal{R}$).

2.25. Esercizio. Verificare che:

(1) Una relazione $\mathcal{R}$ è riflessiva se e solo se $\iota_{\operatorname{dom}(\mathcal{R})} \subseteq \mathcal{R}$.
(2) Una relazione $\mathcal{R}$ è antiriflessiva se e solo se $\mathcal{R} \cap \iota_{\operatorname{dom}(\mathcal{R})} = \varnothing$.
(3) Per ogni relazione $\mathcal{R}$ e ogni $A \subseteq \operatorname{dom} \mathcal{R}$, si ha $\mathcal{R}_{\restriction A} = \mathcal{R} \circ \iota_A$.

V. Funzioni

2.26. Definizione. Una *funzione*, o *applicazione*, è una relazione f tale che

$$\forall x \in \mathrm{dom}(f) \quad \exists! y \in \mathrm{ran}(f) \quad (x,y) \in f. \tag{2.5}$$

Dove il simbolo $\exists!$, che si legge "esiste uno e un solo" o "esiste ed è unico", indica appunto esistenza e unicità. In realtà, l'esitenza di y tale che $(x,y) \in f$ è assicurata dal fatto che $x \in \mathrm{dom}(f)$. Pertanto la (2.5) si può scrivere equivalentemente come segue:

$$\forall x \in \mathrm{dom}(f) \;\; \forall y', y'' \in \mathrm{ran}(f) \quad \Big(\big((x,y') \in f \wedge (x,y'') \in f \big) \implies y' = y'' \Big).$$

Diremo che f è *costante* se $\mathrm{ran}(f)$ è un singoletto.

Diremo che f è *iniettiva*, o *invertibile*, se f^{-1} è anch'essa una funzione.

Diremo che f è una *funzione da A a (valori in) B*, e scriveremo $f\colon A \to B$, se f è una funzione con $\mathrm{dom}(f) = A$ e $\mathrm{ran}(f) \subseteq B$: l'insieme B si dice *codominio* di f; se $\mathrm{ran}(f) = B$ si parlerà di funzione *suriettiva*.

Una *biiezione*, o funzione *biiettiva*, da A a B è una $f\colon A \to B$ che sia contemporaneamente iniettiva e suriettiva.

2.27. Esercizio. Sia $f\colon X \to Y$; siano $A \subseteq X$, $\mathcal{A} \subseteq \mathcal{P}(X)$, $B \subseteq Y$ e $\mathcal{B} \subseteq \mathcal{P}(X)$. Verificare che:

(1) $f\big[f^{-1}[B]\big] \subseteq B$, e vale l'uguaglianza se f è suriettiva.
(2) $f^{-1}\big[f[A]\big] \supseteq A$, e vale l'uguaglianza se f è iniettiva.
(3) $f[X \setminus A] \supseteq f[X] \setminus f[A]$, e vale l'uguaglianza se f è iniettiva.
(4) $f^{-1}[Y \setminus B] = f^{-1}[Y] \setminus f^{-1}[B] = X \setminus f^{-1}[B]$.
(5) $f[\bigcup \mathcal{A}] = \bigcup\{\, f[A] \mid A \in \mathcal{A} \,\}$.
(6) $f[\bigcap \mathcal{A}] \subseteq \bigcap\{\, f[A] \mid A \in \mathcal{A} \,\}$, e vale l'uguaglianza se f è iniettiva.
(7) $f^{-1}[\bigcup \mathcal{B}] = \bigcup\{\, f^{-1}[B] \mid B \in \mathcal{B} \,\}$.
(8) $f^{-1}[\bigcap \mathcal{B}] = \bigcap\{\, f^{-1}[B] \mid B \in \mathcal{B} \,\}$.

Se f è una funzione e $x \in \mathrm{dom}(f)$, l'immagine di $\{x\}$ ha un unico elemento y, che verrà chiamato *immagine dell'elemento x (tramite f)*: scriveremo, come è consuetudine, $f(x) = y$, (anziché $f[\{x\}] = \{y\}$). Scriveremo anche $f\colon x \mapsto f(x)$.

L'insieme delle funzioni da A a B verrà indicato con B^A.

2.28. Esercizio. Sia $f\colon A \to B$ e $g\colon B \to C$. Verificare che:

(1) $g \circ f\colon A \to C$, e per ogni $E \subseteq A$ si ha $(g \circ f)[E] = g\big[f[E]\big]$.
(2) Se f e g sono entrambe iniettive, anche $g \circ f$ è iniettiva.
(3) Se f e g sono entrambe suriettive, anche $g \circ f$ è suriettiva.
(4) Se $g \circ f$ è iniettiva, anche f è iniettiva.
(5) Se $g \circ f$ è suriettiva, anche g è suriettiva.

2.29. Definizione. Una *operazione binaria interna*, o semplicemente una *operazione*, su un insieme A è una funzione da $A \times A$ ad A.

Una operazione si indica spesso con un simbolo come $*$, $\cdot$, $+$ o altri dello stesso tipo. L'immagine della coppia (a,b) tramite l'operazione $*$ sarà sempre indicata con $a * b$.

2.30. Esempio. Qualunque sia l'insieme E, l'unione, l'intersezione e la differenza definiscono operazioni binarie su $\mathcal{P}(E)$.

2.31. Definizione. Sia $*$ una operazione su A. Si dice che $*$ è *associativa* se per ogni scelta di a, b, c in A si ha $(a * b) * c = a * (b * c)$. Si dice che $*$ è *commutativa* se per ogni coppia di elementi $a, b \in A$ si ha $a * b = b * a$.

2.32. Esercizio. Sia A l'insieme delle relazioni su un insieme X. Mostrare che la composizione è un'operazione associativa su A. Verificare inoltre che, in generale, tale operazione non è commutativa.

VI. Insiemi equipotenti

2.33. Definizione. Diremo che A è *equipotente* a B se esiste una biiezione $f\colon A \to B$.

2.34. Esercizio. Mostrare che:

(1) Ogni insieme è equipotente a sé stesso.
(2) Se A è equipotente a B, anche B è equipotente ad A.
(3) Se A è equipotente a B e B è equipotente ad C, allora A è equipotente a C.

2.35. Teorema (Cantor). *Nessun insieme è equipotente al proprio insieme dell parti.*

Dimostrazione. Supponiamo di avere $f\colon A \to \mathcal{P}(A)$ e mostriamo che f non può essere suriettiva.

Sia $B = \{\, x \in A \mid x \notin f(x) \,\}$. Se f fosse suriettiva, esisterebbe un elemento e di A tale che $B = f(e)$. Ora, se e appartenesse a $B = f(e)$, per la definizione di B avremmo $e \notin B$; d'altra parte se $e \notin f(e) = B$ allora $e \in B$: questa contraddizione ci dice che f non può essere suriettiva. □

È possibile dare un significato al concetto intuitivo di "insieme con infiniti elementi".

2.36. Definizione. Se A è equipotente a un suo sottoinsieme proprio, diremo che A è un *insieme infinito*; in caso contrario diremo che A è un *insieme finito*.

2.37. Esercizio. Sia A un insieme verificante l'Assioma 7. Mostrare che l'applicazione $x \mapsto S(x)$ è iniettiva.

Dedurre che A è effettivamente infinito.

Suggerimento. Si applichi l'Esercizio 1.2.

L'insieme vuoto, i singoletti e le coppie sono insiemi finiti, come è facile verificare.

2.38. Proposizione. *Ogni sottoinsieme di un insieme finito è anch'esso finito.*

Dimostrazione. Sia A un insieme. Mostriamo che se almeno un sottoinsieme di A è infinito, allora A stesso è infinito.

Supponiamo dunque che $B \subseteq A$ sia infinito. Ciò significa che possiamo trovare un sottonisieme proprio C di B e una biiezione $f\colon B \to C$. Posto $D = (A \setminus B) \cup C$, definiamo $g\colon A \to D$, come segue:

$$x \mapsto \begin{cases} x, & \text{se } x \in A \setminus B; \\ f(x), & \text{se } x \in B. \end{cases}$$

Si vede subito che abbiamo una biiezione, e che D è sottoinsieme proprio di A. Pertanto A è infinito, come volevamo. □

2.39. Esercizio. Se A e B sono insiemi finiti, anche $A \cup B$ è finito.

Suggerimento. Se C è un sottoinsieme proprio di $A \cup B$ allora almeno una tra le due inclusioni $A \cap C \subseteq A$ e $B \cap C \subseteq B$ è propria.

2.40. Definizione. Siano $(A, <)$ e $(B, \prec)$ insiemi ordinati. Una biiezione $f\colon A \to B$ è detta *isomorfismo (di insiemi ordinati)* se per ogni coppia di elementi $x, y \in A$ si ha $x < y \iff f(x) \prec f(y)$.

In tal caso diremo che $(A, <)$ è *isomorfo* a $(B, \prec)$ e scriveremo $(A, <) \simeq (B, \prec)$, o semplicemente $A \simeq B$.

Segue immediatemente dalla definizione che due insiemi ordinati isomorfi sono anche equipotenti.

2.41. Esercizio. Verificare che un insieme ordinato è sempre isomorfo a sé stesso, che $A \simeq B$ equivale a $B \simeq A$, e che due insiemi ordinati isomorfi a un altro insieme ordinato sono anche isomorfi tra loro.

VII. Famiglie di insiemi

Nel caso in cui $\mathcal{E}$ sia una collezione di insiemi di cui ci interessa considerare gli elementi, per indicare una funzione F da un insieme J a $\mathcal{E}$ useremo il termine *famiglia (di insiemi)*; diremo che tale famiglia è *indicizzata in* J, chiameremo *indice* un elemento $j \in J$, e denoteremo la sua immagine con F_j anziché $F(j)$; inoltre scriveremo $(F_j)_{j\in J}$ in luogo di F.

2.42. Definizione. L'*unione di una famiglia di insiemi* F (indicizzata in J) è l'unione di $\operatorname{ran}(F) = \{ F_j \mid j \in J \}$. Anziché $\bigcup\{ F_j \mid j \in J \}$ scriveremo, più concisamente, $\bigcup_{j\in J} F_j$.
Analogamente si definisce l'*intersezione di una famiglia di insiemi* F; in questo caso occore però accertarsi che sia $F \neq \varnothing$ (cosicché anche $\operatorname{ran}(F) \neq \varnothing$).

Si badi a non far confusione tra famiglia $(F_j)_{j\in J}$ e collezione (cioè insieme) $\{ F_j \mid j \in J \}$, anche quando F è iniettiva[2].

2.43. Definizione. Il *prodotto cartesiano di una famiglia di insiemi* $(F_j)_{j\in J}$ è

$$\prod_{j\in J} F_j = \Big\{ f \colon J \to \bigcup_{j\in J} F_j \;\Big|\; \forall j \in J \;\; f(j) \in F_j \Big\}.$$

L'applicazione $\pi_j \colon \prod_{j\in J} F_j \to F_j$ definita da $f \mapsto f(j)$ viene chiamata *proiezione* su F_j.

Se x è un elemento del prodotto $\prod_{j\in J} F_j$ (e $j \in J$), scriveremo spesso x_j anziché $x(j)$: in altre parole x sarà visto come la famiglia $(x_j)_{j\in J}$.
Notiamo che nel caso di una famiglia costante, con $\{ F_j \mid j \in J \} = \{E\}$, il prodotto $\prod_{j\in J} F_j$ si riduce a E^J.

Se $h \colon I \to J$ è una biiezione, possiamo costruire un'applicazione H, definita da $H \colon f \mapsto f \circ h$, dal prodotto cartesiano della famiglia $(F_j)_{j\in J}$ a quello della famiglia $G = F \circ h$. Si verifica facilmente che H è una biiezione, che verrà detta *biiezione naturale*, poiché è indipendente dagli elementi degli insiemi F_j. Una tale biiezione permette di identificare i prodotti $\prod_{j\in J} F_j$ e $\prod_{i\in I} G_i$.

2.44. Esercizio.
(1) Dati $\mathcal{E} = \{A\}$ e $J = \{\alpha\}$, si consideri la famiglia F definita da $F_\alpha = A$. Costruire una biiezione naturale $H \colon \prod_{j\in J} F_j \to A$.
(2) Dati $\mathcal{E} = \{A, B\}$ e $J = \{\alpha, \beta\}$, con $\alpha \neq \beta$, si consideri la famiglia F definita da $F_\alpha = A$ e $F_\beta = B$. Costruire una biiezione naturale $H \colon \prod_{j\in J} F_j \to A \times B$.

2.45. Definizione. Dato un insieme X, sia $(Y_j)_{j\in J}$ una famiglia di insiemi e, per ogni $j \in J$, sia $f_j \colon X \to Y_j$. La *valutazione*, o *funzione diagonale*, della famiglia $(f_j)_{j\in J}$ è la funzione $\triangle_{j\in J} f_j \colon X \to \prod_{j\in J} Y_j$ definita da $x \mapsto \big(f_j(x)\big)_{j\in J}$.
La valutazione $\triangle_{j\in J} \iota_X$ verrà indicata con $\triangle_{X^J}$, o più semplicemente con $\triangle_J$, e la sua immagine verrà chiamata *diagonale del prodotto* X^J.

Dunque la diagonale $\triangle_J[X]$ del prodotto X^J coincide con l'insieme delle funzioni costanti da J a X.

[2]È bene però sapere che, nel caso in cui F è l'identità su $\mathcal{E}$, è invalso l'uso di identificare la famiglia F con la collezione $\mathcal{E}$, finendo con l'usare i termini “famiglia” e “collezione” come fossero sinonimi.

2.46. Esercizio. Sia F una funzione da un insieme X al prodotto $\prod_{j\in J} Y_j$. Mostrare che $\triangle_{j\in J}(\pi_j \circ F) = F$.

CAPITOLO 3

Numeri ordinali e pricipio di induzione

In questo capitolo costruiamo gli ordinali seguendo l'approccio usuale, dovuto a Von Neumann. I numeri naturali saranno gli ordinali finiti.

Inoltre introduciamo il principio di induzione (transfinita) e le definizioni per ricorrenza.

I. Numeri ordinali

Sia $(A, <)$ un insieme ordinato, e sia $B \subseteq A$. Diremo che B *ha minimo* in $(A, <)$ se esiste $m \in B$ tale che per ogni $x \in B \setminus \{m\}$ si abbia $m < x$; tale m è unico, come immediatamente si verifica, e verrà detto *il minimo di* B (rispetto a $<$).

3.1. Definizione. Diciamo che A *è bene ordinato dalla relazione* $<$, o che $(A, <)$ è un *insieme bene ordinato*, se $<$ è una relazione di ordine su A tale che ogni sottoinsieme non vuoto di A ha minimo.

A volte sottintenderemo la relazione $<$, quando non ci sia rischio di equivoci; in tal caso il minimo di un sottoinsieme B di A potrà essere indicato semplicemente con $\min B$.

3.2. Esercizio. Verificare che un insieme bene ordinato è totalmente ordinato.

3.3. Definizione. Un *(numero) ordinale* è un insieme α tale che:

- $\forall x, y\ [x \in y \wedge y \in \alpha \implies x \in \alpha]$ (α è un *insieme transitivo*).
- α è bene ordinato da $\in$ (cioè dalla relazione $\{ (x, y) \mid x \in y \}$).

3.4. Esercizio. Verificare che $\varnothing$ e $\{\varnothing\}$ sono ordinali, ma $\big\{\{\varnothing\}\big\}$ non lo è.

3.5. Definizione. Diciamo che n è un *numero naturale* se è un ordinale finito.

In base all'Esercizio 3.4, gli insiemi $\varnothing$ e $\{\varnothing\}$ sono numeri naturali. Nel seguito, quando essi saranno considerati come ordinali, $\varnothing$ verrà sempre indicato con 0 ("*zero*"), e $\{\varnothing\}$ con 1 ("*uno*").

3.6. Esercizio. Mostrare che il successore ordinale di un numero naturale è anch'esso un numero naturale.

Suggerimento. Usare l'Esercizio 2.39.

In particolare, il successore di 0 è 1. Il successore di 1, come c'è da aspettarsi, verrà indicato con 2 ("*due*"); il successore di 2, poi, sarà 3 ("*tre*"), e così via. In tal modo, i numeri naturali, come intuitivamente li conosciamo, sono effettivamente rappresentati da oggetti della teoria degli insiemi[1].

Useremo spesso la convenzione di indicare un numero naturale con una lettera come n, m o anche k. Gli altri ordinali si indicano di solito con lettere greche minuscole.

3.7. Teorema. *Sia* $(A, <)$ *un insieme bene ordinato. Esiste uno e un solo ordinale* α *tale che* $(A, <) \simeq \alpha$.

[1]In effetti i numeri naturali nel senso della Definizione 3.5 soddisfano i postulati dell'Aritmetica di Peano: si veda, ad esempio, [**3**, Theor. 7.16, pag. 19].

Omettiamo la dimostrazione[2]. Osserviamo invece che, in particolare, due ordinali isomorfi devono coincidere.

L'ordinale isomorfo a un insieme bene ordinato $(A, <)$ si dice *tipo di ordine di* $(A, <)$.

Anche del prossimo fondamentale teorema non diamo la dimostrazione. Il lettore interessato può consultare i testi specializzati[3].

3.8. TEOREMA. *Dati due ordinali* α *e* β *si ha sempre una e una sola delle seguenti alternative:* $\alpha \in \beta$*, oppure* $\beta \in \alpha$*, oppure* $\alpha = \beta$.

D'ora in avanti ci adegueremo alla pratica comune di scrivere $\alpha < \beta$ (o $\beta > \alpha$) quando α e β sono ordinali con $\alpha \in \beta$.

3.9. ESERCIZIO. Mostrare che, se α e β sono ordinali, si ha $\alpha \leqslant \beta$ se e solo se $\alpha \subseteq \beta$.

3.10. TEOREMA. *Ogni insieme non vuoto di ordinali ha minimo.*

DIMOSTRAZIONE. Sia Θ un insieme non vuoto di ordinali. Per l'Assioma 2, possiamo trovare $\nu \in \Theta$ tale che $\nu \cap \Theta = \varnothing$. Mostriamo che ν è il minimo di Θ.

Sia infatti $\alpha \in \Theta$: allora $\alpha \notin \nu$, poiché ν e Θ non hanno elementi in comune; quindi $\alpha \leqslant \nu$ per il Teorema 3.8. □

3.11. ESERCIZIO. Verificare che ogni ordinale coincide con l'insieme degli ordinali che lo precedono.

3.12. TEOREMA.

(1) *Se* ξ *è un ordinale, allora* $S(\xi) = \xi \cup \{\xi\}$ *è il minimo ordinale maggiore di* ξ.
(2) *Se* Ξ *è un insieme di ordinali, allora* $\bigcup \Xi$ *è l'estremo superiore di* Ξ *(cioè il minimo ordinale* λ *tale che* $\kappa \leqslant \lambda$ *per ogni* $\kappa \in \Xi$*).*

DIMOSTRAZIONE.

(1) Poniamo $\eta = S(\xi)$, e cominciamo col mostrare che η è un ordinale.

Sia $\beta \in \eta$, e fissiamo un qualunque $\alpha \in \beta$. Se $\beta = \xi$ si ha ovviamente $\alpha \in \xi$; altrimenti $\beta \in \xi$, e allora α appartiene a ξ perché ξ è un ordinale. In ogni caso $\alpha \in \eta$.

Sia ora Σ un sottoinsieme non vuoto di η. Se $\Sigma = \{\xi\}$, ovviamente ξ è il minimo di Σ; altrimenti $\Sigma \setminus \{\xi\}$ è un sottoinsieme non vuoto di ξ e quindi ha il minimo, che indichiamo con μ: poiché $\mu \neq \xi$, deve essere $\mu \in \xi$, quindi μ è il minimo anche di Σ. Ciò conclude la dimostrazione che η è un ordinale.

Naturalmente $\xi \in \eta$, cioè η è maggiore di ξ. Sia infine γ un ordinale maggiore di ξ. Essendo $\xi \in \gamma$, si ha $\xi \subseteq \gamma$ poiché γ è un ordinale, quindi anche $\eta \subseteq \gamma$. Pertanto $\eta \leqslant \gamma$ in virtù dell'Esercizio 3.9.

(2) Poniamo $\sigma = \bigcup \Xi$, e cominciamo col mostrare che σ è un ordinale: se $\sigma = \varnothing$ questo è già stato visto nell'Esercizio 3.4, per cui possiamo supporre che Ξ possieda almeno un elmento non vuoto.

Sia $\beta \in \sigma$, e fissiamo un qualunque $\alpha \in \beta$. Preso $\gamma \in \Xi$ con $\beta \in \gamma$, si ha $\alpha \in \gamma$ perché γ è un ordinale, quindi $\alpha \in \sigma$ essendo $\gamma \subseteq \sigma$. Sia ora Λ un sottoinsieme non vuoto di σ; indichiamo con Θ l'insieme dei $\beta \in \Xi$ che hanno almeno un elemento in comune con Λ. Poiché $\Lambda \neq \varnothing$ e Ξ possiede almeno un elemento non vuoto, si ha $\Theta \neq \varnothing$ e quindi, per il Teorema 3.10, Θ ha il minimo, che indichiamo con ν. A sua volta $\nu \cap \Lambda$, essendo un sottoinsieme non vuoto dell'ordinale ν, avrà il minimo, che indichiamo con μ. Proveremo che μ è in effetti il minimo di Λ.

---

[2] Rimandiamo i lettori interessati a [**1**, Theor. 2, pag. 15] o [**3**, Theor. 7.6, pag. 17].

[3] Si veda, ad esempio, [**1**, Lemma 2.3, pag. 15], oppure [**3**, Theor. 7.3(3), pag. 16].

Ovviamente $\mu \in \Lambda$, perché $\mu \in \Lambda \cap \nu$. Sia poi $\alpha \in \Lambda$, con $\alpha \neq \mu$: deve necessariamente essere $\mu \in \alpha$ perché, in caso contrario, $\alpha \in \mu$ per il Teorema 3.8, quindi $\alpha \in \nu$, essendo ν un ordinale, e allora avremmo che α è un elemento di $\Lambda \cap \nu$ che precede μ, il che è impossibile in quanto il minimo è μ. Ciò conclude la dimostrazione che σ è un ordinale.

Osserviamo che, per ogni $\kappa \in \Xi$, si ha $\kappa \leqslant \sigma$ per l'Esercizio 3.9. Sia infine λ un ordinale tale che per ogni $\kappa \in \Xi$ si abbia $\kappa \leqslant \lambda$: ciò significa, in virtù dell'Esercizio 3.9, che si ha $\kappa \subseteq \lambda$ per tutti i $\kappa \in \Xi$ e, di conseguenza, $\sigma \subseteq \lambda$. Applicando ancora l'Esercizio 3.9 si conclude che $\sigma \leqslant \lambda$. □

II. Somma e prodotto ordinale

3.13. Esercizio. Siano α, β ordinali.

(1) Sull'insieme $\alpha \times \{0\} \cup \beta \times \{1\}$, che indicheremo con $\alpha \sqcup \beta$, definiamo la relazione $\sqsubset$ come segue:

$$\begin{aligned}&\forall (m,h),(n,k) \in \alpha \sqcup \beta\\ &\quad (m,h) \sqsubset (n,k) \iff [h < k \quad \vee \quad h = k \ \wedge \ m < n].\end{aligned}$$

Verificare che $\alpha \sqcup \beta$ è bene ordinato da $\sqsubset$.

(2) Sul prodotto $\alpha \times \beta$, definiamo la relazione $\prec$ come segue:

$$\begin{aligned}&\forall (m,h),(n,k) \in \alpha \times \beta\\ &\quad (m,h) \prec (n,k) \iff [h < k \quad \vee \quad h = k \ \wedge \ m < n].\end{aligned}$$

Verificare che $\alpha \times \beta$ è bene ordinato da $\prec$.

(3) Verificare che, se $\alpha = \beta$, si ha $\alpha \sqcup \alpha = \alpha \times 2$ e, in tal caso, $\sqsubset$ coincide con $\prec$.

3.14. Definizione. Siano α, β ordinali. La *somma ordinale* di α e β è il tipo di ordine dell'insieme bene ordinato $(\alpha \sqcup \beta, \sqsubset)$ introdotto nell'Esercizio 3.13(1). Essa sarà indicata con $\alpha + \beta$.

Il *prodotto ordinale* di α e β è il tipo di ordine dell'insieme bene ordinato $(\alpha \times \beta, \prec)$ introdotto nell'Esercizio 3.13(2). Esso sarà indicato con $\alpha \cdot \beta$.

3.15. Esercizio. Verificare che per ogni ordinale α, il successore $S(\alpha) = \alpha \cup \{\alpha\}$ coincide con $\alpha + 1$.

3.16. Definizione. Sia β un ordinale diverso da 0. Diremo che β è un *ordinale successore* se esiste un ordinale α tale che $\beta = \alpha + 1$. In caso contrario diremo che β è un *ordinale limite*.

3.17. Esercizio. Mostrare che ogni ordinale limite è infinito.

Suggerimento. Se γ è un ordinale limite, $S\colon \alpha \mapsto \alpha + 1$ è una biiezione da γ a $\gamma \setminus \{0\}$.

III. L'insieme dei numeri naturali

3.18. Proposizione. *Sia A un insieme che verifichi l'assioma dell'infinito. Per ogni numero naturale n si ha $n \in A$.*

Dimostrazione. Procediamo per assurdo, supponendo che ci sia un numero naturale $n \notin A$. Allora $\Theta = \{\, \alpha < n + 1 \mid \alpha \notin A \,\}$ è un insieme non vuoto di ordinali, e quindi ha un minimo che indichiamo con m.

Ora, non può essere $m = 0$, perché $0 \in A$; né m può essere un ordinale limite, in quanto un ordinale limite è infinito come si è visto nell'Esercizio 3.17, mentre $m \leqslant n$ e dunque m è finito. Pertanto c'è un ordinale k, in effetti un numero naturale, tale che $m = k + 1$. Poiché $k < m$, si ha $k \in A$. Ma allora anche $m = k + 1 \in A$: assurdo. □

3.19. Teorema. *Esiste un insieme ω i cui elementi sono (tutti e soli) i numeri naturali.*

Dimostrazione. Sia A un insieme che verifichi l'assioma dell'infinito. Come abbiamo visto nella Proposizione 3.18, ogni numero naturale è un elemento di A. Possiamo quindi definire

$$\omega = \{\, \nu \in A \mid \nu \text{ è un numero naturale} \,\}$$

ed è evidente che tale definizione non dipende dalla scelta di A. □

L'insieme dei numeri naturali verrà sempre indicato con ω. Useremo il simbolo $\mathbb{N}$ per indicare $\omega \smallsetminus \{0\}$.

3.20. Esercizio. Verificare che:

(1) ω è il minimo ordinale limite e il minimo ordinale infinito;
(2) $1 + \omega = \omega$;
(3) $2 \cdot \omega = \omega$.

Dedurre che le operazioni di somma e prodotto ordinale non sono commutative.

Terminiamo questo paragrafo con i postulati dell'Aritmentica di Peano.

3.21. Teorema (Postulati di Peano). *L'insieme ω soddisfa le seguenti proprietà:*

(1) $0 \in \omega$.
(2) $\forall n \in \omega \;\; S(n) \in \omega$.
(3) $\forall n, m \in \omega \;\; \big(n \neq m \implies S(n) \neq S(m)\big)$.
(4) $\forall x \subseteq \omega \; \Big(\big(0 \in x \;\wedge\; \forall n \in x \; (S(n) \in x)\big) \implies x = \omega\Big)$.

Dimostrazione. Le proprietà (1) e (2) sono immediate. seguono immediatamente dalla definizione di ω. La (3) segue dall'Esercizio 2.37.

Infine osserviamo che un insieme x che soddisfi la (4) verifica l'Assioma dell'infinito, quindi $\omega \subseteq x$ per la Proposizione 3.18. Poiché è $x \subseteq \omega$, si conclude che $x = \omega$. □

Per mezzo delle proprietà elencate nel teorema precendente è possibile formalizzare tutta l'artmetica, a cominciare dalle operazioni di somma e prodotto di numeri naturali. In effetti si verifica che tali operazioni coincidono con le restrizioni a ω della somma e del prodotto ordinale definiti in precedenza. Tuttavia, nel caso dei numeri naturali, la somma e il prodotto si rivelano entrambe commutative e associative.

IV. Principio di induzione e definizioni per ricorrenza

3.22. Teorema (Principio di induzione). *Sia γ un ordinale. Data una formula Φ, supponiamo che, per ogni $\beta \in \gamma$ si abbia l'implicazione:*

$$[\forall \alpha < \beta \;\; \Phi(\alpha)] \implies \Phi(\beta).$$

Allora, per ogni $\beta \in \gamma$, vale $\Phi(\beta)$.

Dimostrazione. Infatti, se l'insieme $\Theta = \{\, \beta \in \gamma \mid \neg\Phi(\beta) \,\}$ fosse non vuoto, esso avrebbe il minimo, che indichiamo con ν. Dunque, per ogni $\alpha < \nu$, si avrebbe $\Phi(\alpha)$; ma applicando la (3.22) con $\beta = \nu$ otterremmo $\Phi(\nu)$: assurdo. □

Non è difficile rendersi conto che il precendente teorema varrebbe anche se γ fosse un arbitrario insieme bene ordinato. Con l'aiuto di questo teorema si dimostrano le principali proprietà degli insiemi bene ordinati e degli ordinali.

Diamo ora una variante del principio di induzione.

3.23. Teorema (Seconda forma del principio di induzione).
Sia γ un ordinale non nullo. Data una formula Φ, supponiamo che:

(1) *valga* $\Phi(0)$*;*
(2) *se* $\beta \in \gamma$ *con* $\beta = \alpha + 1$*, si abbia l'implicazione*
$\Phi(\alpha) \implies \Phi(\beta)$*;*
(3) *se* $\beta \in \gamma$ *è un ordinale limite, si abbia l'implicazione*
$[\forall \alpha < \beta \;\; \Phi(\alpha)] \implies \Phi(\beta)$.

Allora, per ogni $\beta \in \gamma$*, vale* $\Phi(\beta)$*.*

Dimostrazione. La dimostrazione è analoga a quella del Teorema 3.22. Supponiamo che l'insieme

$$\Theta = \{\, \beta \in \gamma \mid \neg\Phi(\beta) \,\}$$

sia non vuoto; allora ha il minimo, che indichiamo con ν.

Per la (1), non può essere $\nu = 0$; se fosse $\nu = \mu + 1$ allora varrebbe $\Phi(\mu)$ e quindi, per la (2), anche $\Phi(\nu)$, il che è assurdo; se infine μ fosse un ordinale limite, poiché abbiamo $\Phi(\alpha)$ per ogni $\alpha < \nu$, deduciamo, in virtù della (3), che si ha $\Phi(\nu)$, ancora un assurdo.

Pertanto $\Theta = \varnothing$, cioè $\Phi(\beta)$ vale per ogni $\beta \in \gamma$. □

Con riferimento a questa forma del principio di induzione, notiamo che l'ipotesi (3) è necessaria solo quando $\gamma > \omega$. Si parla in tal caso di *induzione transfinita*.

Il principio di induzione serve anche per dare definizioni ricorsive.

3.24. Definizione. Chiamiamo *successione* una famiglia indicizzata in un ordinale γ. Si parlerà di *successione finita* se $\gamma < \omega$, di *successione semplice* se $\gamma = \omega$, o di *successione transfinita* se $\gamma > \omega$.

Diremo che la successione $(x_\beta)_{\beta\in\gamma}$ di elementi di un insieme X è *ricorsiva* (o *definita per ricorrenza*) se esiste una funzione

$$F\colon \bigcup_{\beta\in\gamma} X^\beta \to X \tag{3.1}$$

tale che, per ogni $\beta \in \gamma$ si abbia

$$x_\beta = F\big((x_\alpha)_{\alpha\in\beta}\big). \tag{3.2}$$

Se vogliamo definire per ricorrenza una successione $(x_\beta)_{\beta\in\gamma}$ di elementi di un insieme X, ci basta una funzione F come in (3.1). Infatti si dimostra per induzione (usando il Teorema 3.22) che, per ogni $\beta \in \gamma$ esiste uno e un solo x_β tale che sia verificata la (3.2).

Una variante consiste nell'assegnare un elemento $x_0 \in X$, una funzione

$$F\colon \bigcup\{\, X^\beta \mid \beta \in \gamma,\ \beta \text{ ordinale limite} \,\} \to X$$

e una funzione

$$f\colon \{\, \alpha \in \gamma \mid \alpha + 1 < \gamma \,\} \times X \to X$$

Tali che, per ogni $\beta \in \gamma$ non nullo, valga la (3.2) se β è un ordinale limite, mentre, se $\beta = \alpha + 1$, si abbia

$$x_\beta = f(\alpha, x_\alpha).$$

In questo caso si usa la seconda forma del principio di induzione per dimostrare che la successione è ben definita (ed evidentemente $F \neq \varnothing$ se e solo se la successione è transfinita).

CAPITOLO 4

Numeri cardinali e assioma della scelta

I cardinali saranno definiti come particolari ordinali. Allo scopo di assegnare ad ogni insieme A un cardinale (da riguardarsi come numerosità di A), è necessario introdurre un ulteriore assioma: l'assioma della scelta.

I. Numeri cardinali

4.1. Definizione. Un *(numero) cardinale* è un ordinale κ tale che nessun $\alpha \in \kappa$ sia equipotente a κ.

Segue immediatamente dalla definizione che due cardinali equipotenti devono coincidere.

4.2. Esercizio. Mostrare che ω e tutti i numeri naturali sono cardinali, mentre $\omega + 1$ non lo è.

Suggerimento. La successione (semplice) $(\gamma_n)_{n\in\omega}$, definita per ricorrenza da $\gamma_0 = \omega$ e $\gamma_{n+1} = n$, è una biiezione da ω a $\omega + 1$.

Ragionando in maniera simile a quanto suggerito per il precedente esercizio si vede che, se α è un qualunque ordinale infinito, il suo successore non è un cardinale. In altre parole, ogni cardinale infinito è un ordinale limite.

4.3. Esercizio. Verificare che $\omega + \omega$ (è un ordinale limite ma) non è un cardinale.

Suggerimento. Ponendo $f(2n) = n$ e $f(2n+1) = \omega + n$, si definisce una biiezione da ω a $\omega + \omega$.

Adotteremo nel seguito la convenzione di indicare un cardinale con una lettera come κ, λ, μ o ν.

4.4. Definizione. Dato un insieme A, se κ è un cardinale equipotente ad A allora κ (è unico e) verrà detto *cardinalità* di A, e si indicherà con $|A|$.

Diremo che A è un insieme *numerabile* se $|A| \leqslant \omega$; se invece $|A| > \omega$ diremo che A *più che numerabile*.

Dunque dire che A è un insieme infinito numerabile equivale a dire che A è equipotente a ω.

4.5. Esercizio. Mostare che ogni ordinale γ ha una cardinalità, e si ha $|\gamma| \leqslant \gamma$.

Suggerimento. Verificare che $|\gamma|$ è il minimo dell'insieme degli $\alpha \in \gamma + 1$ equipotenti a γ.

II. L'assioma della scelta

Per avere una teoria significativa della cardinalità, o anche soltanto per assegnare una cardinalità a ogni insieme, è necessario introdurre un altro assioma.

Assioma 9 (della scelta). *Se $\mathcal{C}$ è una collezione di insiemi non vuoti, a due a due disgiunti, esiste un insieme E che ha esattamente un elemento in comune con ogni $A \in \mathcal{C}$.*

Questo assioma, a causa di alcune sue conseguenze, non fu subito accettato volentieri dalla comunità matematica, ma ebbe all'inizio una sorte simile a quella del postulato delle parallele nella geometria euclidea.

D'altra parte, si è visto che molti importanti teoremi di diverse aree della matematica necessitano dell'assioma della scelta: quindi è esso è ora ormai (quasi) universalmente accettato.

Nel seguito dunque adotteremo l'assioma della scelta, aggiungendolo agli altri assiomi di ZF. La teoria che ne risulta è solitamente indicata con l'acronimo ZFC, dove "C" sta appunto per "scelta" (in inglese "*choice*").

Presentiamo ora, senza dimostrazione[1], un utile teorema che deriva dall'assioma della scelta, anzi è equivalente a esso[2]. Per comprenderne l'enunciato è necessario conoscere un po' di terminologia sugli insiemi ordinati.

Sia $(A, <)$ un insieme ordinato: un *elemento massimale* è un $m \in A$ tale che non esiste nessun $x \in A$ per il quale si abbia $m < x$; se poi $B \subseteq A$, diciamo che B è una *catena* se la restrizione di $<$ a B è una relazione di ordine totale; diciamo infine che B è *limitato superiormente* se esiste $s \in A$ tale che $x \leqslant s$ per tutti gli $x \in B$.

4.6. Teorema (Lemma di Zorn). *Un insieme ordinato in cui ogni catena è limitata superiormente ha almeno un elemento massimale.*

4.7. Esercizio. Sia $\mathcal{F}$ un filtro su un insieme X. Provare che esiste un ultrafiltro più fine di $\mathcal{F}$.

Dimostriamo ora altre conseguenze dell'assioma della scelta.

4.8. Teorema.
(1) *Il prodotto cartesiano di una famiglia di insiemi non vuoti è non vuoto.*
(2) *Se $f\colon A \to B$ è suriettiva, esiste $g\colon B \to A$ tale che $f \circ g = \iota_B$.*

Dimostrazione.
(1) Data una famiglia $(F_j)_{j\in J}$ di insiemi non vuoti, poniamo $\mathcal{C} = \{\, F_j \times \{j\} \mid j \in J \,\}$, e sia E dato dall'Assioma 9. Se f è la funzione che ad ogni $j \in J$ associa l'unico z tale che $(z, j) \in F_j \cap E$, allora $f \in \prod_{j\in J} F_j$.
(2) Sia $\mathcal{C} = \{\, f^{-1}[\{y\}] \mid y \in B \,\}$, e sia E dato dall'Assioma 9. Per ogni $y \in B$ sia $g(y)$ l'unico elmento di $f^{-1}[\{y\}] \cap E$: si ha allora $f\bigl(g(y)\bigr) = y$. □

4.9. Esercizio. Dimostrare (senza fare uso dell'assioma della scelta) che se $f\colon A \to B$ è iniettiva, esiste $g\colon B \to A$ tale che $g \circ f = \iota_A$.

Torniamo alla cardinalità, presentando un'altra importantissima conseguenza dell'assioma della scelta.

4.10. Teorema (Zermelo). *Ogni insieme può essere bene ordinato.*

Il teorema di Zermelo è detto anche *principio del buon ordinamento*. Per la dimostrazione rimandiamo il lettore a uno dei tanti testi specializzati[3].

4.11. Corollario. *Ogni insieme ha una cardinalità.*

Dimostrazione. Sia A un insieme. Il teorema di Zermelo ci assicura che esiste una relazione $\prec$ tale che $(A, \prec)$ è un insieme bene ordinato. Detto γ il tipo di ordine di $(A, \prec)$, il cardinale $|\gamma|$, che esiste in virtù dell'Esercizio 4.5, è equipotente ad A. □

[1] Il lettore interessato può consultare [**1**, Theor. 16, pag. 40].
[2] Si veda [**1**, Exer. 5.3, pag. 40].
[3] Si veda ad esempio [**1**, Theor. 15, pag. 39].

4.12. ESERCIZIO. Dedurre l'assioma della scelta dal principio del buon ordinamento[4].

III. Confronto di cardinalità

4.13. TEOREMA. *Siano A e B insiemi. Le seguenti condizioni sono equivalenti:*

(1) $|A| \geqslant |B|$;
(2) *se* $B \neq \varnothing$, *esiste* $f\colon A \to B$ *suriettiva;*
(3) *esiste* $g\colon B \to A$ *iniettiva;*
(4) A *ha un sottoinsieme equipotente a* B.

DIMOSTRAZIONE.

(1)⇒(2) Poniamo $|A| = \lambda$ e $|B| = \kappa$; abbiamo allora una biiezione $\varphi\colon A \to \lambda$ e una biiezione $\psi\colon \kappa \to B$.

Se $B \neq \varnothing$, si ha $\kappa > 0$ e quindi anche $\lambda > 0$. Per ogni $\alpha \in \lambda$, poniamo $\sigma(\alpha) = \alpha$ se $\alpha \in \kappa$, e $\sigma(\alpha) = 0$ se $\alpha \geqslant \kappa$: allora $\sigma\colon \lambda \to \kappa$ è suriettiva, quindi la composizione $f = \psi \circ \sigma \circ \varphi$ è una funzione suriettiva da A a B.

(2)⇒(3) Se $B = \varnothing$, allora $\varnothing\colon B \to A$ è banalmente iniettiva. Se invece $B \neq \varnothing$, sia $f\colon A \to B$ suriettiva. Per il Teorema 4.8(2), possiamo trovare $g\colon B \to A$ per la quale si ha $f \circ g = \iota_B$. Tale g è iniettiva in virtù di quanto visto nell'Esercizio 2.28(4).

(3)⇒(4) Se $g\colon B \to A$ è iniettiva, è ovvio che $g[B]$ è un sottoinsieme di A equipotente a B.

(4)⇒(1) Sia C un sottoinsieme di A equipotente a B. Poniamo $\lambda = |A|$ e $\kappa = |B| = |C|$; abbiamo allora una biiezione $\psi\colon A \to \lambda$ e una biiezione $\varphi\colon \kappa \to C$.

Poiché la composizione $h = \psi \circ \varphi$ è iniettiva, si ha che il sottoinsieme $\Theta = h[\kappa]$ di λ è equipotente a κ. Possiamo allora trovare, per il Teorema 3.7, un ordinale γ e un isomorfismo η da γ a Θ: così $|\gamma| = \kappa$, quindi $\kappa \leqslant \gamma$.

Ora, supponiamo per assurdo che $\lambda < \kappa$. Avremo allora $\lambda < \gamma$, e l'insieme $\Xi = \{\, \alpha \in \gamma \mid \eta(\alpha) < \alpha \,\}$ sarà non vuoto, in quanto $\lambda \in \Xi$.

Sia dunque ν il minimo di Ξ. Ponendo $\mu = \eta(\nu)$, si ha $\mu < \nu$; quindi, poiché η è un isomorfismo, $\eta(\mu) < \eta(\nu) = \mu$. Ciò significa che $\mu \in \Xi$, il che è impossibile perché il minimo di Ξ è ν. □

Il prossimo teorema si ottiene come conseguenza immediata del precedente. Avvertiamo il lettore che è però possibile dimostrarlo anche senza fare uso dell'assioma della scelta[5].

4.14. TEOREMA (Cantor–Schröder–Bernstein). *Siano A e B insiemi. Supponiamo che esistano $f\colon A \to B$ e $g\colon B \to A$ entrambe iniettive. Allora A e B sono equipotenti.*

DIMOSTRAZIONE. Per il teorema precedente, essendo $f\colon A \to B$ iniettiva, si ha $|A| \leqslant |B|$; essendo poi $g\colon B \to A$ iniettiva, si ha anche $|B| \leqslant |A|$: dunque $|A| = |B|$. □

IV. Somma, prodotto ed esponenziazione cardinale

4.15. DEFINIZIONE. Siano κ e λ cardinali. La *somma cardinale* di κ e λ è

$$\kappa \oplus \lambda = |\kappa + \lambda|.$$

Il *prodotto cardinale* è

$$\kappa \otimes \lambda = |\kappa \cdot \lambda| = |\kappa \times \lambda|.$$

L'*esponenziazione cardinale* è $|\kappa^\lambda|$, che si indica con κ^λ e si legge "κ elevato a λ"; in seguito sarà chiaro dal contesto se κ^λ indicherà l'insieme delle funzioni da λ a κ o la cardinalità di tale insieme.

---

[4] Oltre al principio del buon ordinamento (e al lemma di Zorn), molti altri enunciati di varie branche della matematica risultano essere equivalenti all'assioma della scelta. A questo proposito, invitiamo i lettori interessati a consultare [**4**].

[5] Si veda, ad esempio, [**1**, Theor. 7, pag. 23], oppure [**3**, Exer. (8), pag. 43].

Si vede facilmente che le operazioni di somma e prodotto cardinale sono commutative. Inoltre, se $\lambda \leqslant \mu$, si ha $\kappa \oplus \lambda \leqslant \kappa \oplus \mu$, $\kappa \otimes \lambda \leqslant \kappa \otimes \mu$, $\kappa^\lambda \leqslant \kappa^\mu$ e $\lambda^\kappa \leqslant \mu^\kappa$. Se poi κ e λ sono entrambi finiti, si ritrovano le operazioni usuali tra numeri naturali.

4.16. Esercizio. Mostrare che, per ogni insieme X, gli insiemi 2^X e $\mathcal{P}(X)$ sono equipotenti.
Dedurre che, per ogni cardinale κ, il cardinale 2^κ è maggiore di κ.

4.17. Teorema. *Se κ e λ sono cardinali, di cui almeno uno è infinito, si ha $\kappa \oplus \lambda = \kappa \otimes \lambda = \max\{\kappa, \lambda\}$.*

Omettiamo la dimostrazione[6].

4.18. Esercizio. Siano κ, λ e μ cardinali: mostrare che $\kappa^{\lambda \oplus \mu} = \kappa^\lambda \otimes \kappa^\mu$ e $\kappa^{\lambda \otimes \mu} = (\kappa^\lambda)^\mu$.
Deudurre che, se ν è un cardinale infinito, si ha $2^\nu = \nu^\nu$.

4.19. Proposizione. *Sia $\mathcal{C}$ una collezione di insiemi, con $|\mathcal{C}| = \kappa$; sia λ un cardinale tale che $|A| \leqslant \lambda$ per ogni $A \in \mathcal{C}$. Allora $|\bigcup \mathcal{C}| \leqslant \kappa \otimes \lambda$.*

Dimostrazione. Possiamo ovviamente supporre $\bigcup \mathcal{C} \neq \varnothing$. Fissiamo un biiezione $\psi \colon \mathcal{C} \to \kappa$. In virtù del Teorema 4.13, troviamo, per ogni $A \in \mathcal{C}$, una funzione iniettiva $\varphi_A \colon A \to \lambda$.
Definiamo ora $F \colon \bigcup_{A \in \mathcal{C}} A \times \{A\} \to \kappa \times \lambda$ al seguente modo

$$(x, A) \mapsto \big(\psi(A), \varphi_A(x)\big).$$

È evidente che F è iniettiva; quindi, per il Teorema 4.13, abbiamo $|\bigcup_{A \in \mathcal{C}} A \times \{A\}| \leqslant \kappa \otimes \lambda$.
Sia infine $\eta \colon \bigcup_{A \in \mathcal{C}} A \times \{A\} \to \bigcup \mathcal{C}$ data da $(x, A) \mapsto x$. Poiché η è suriettiva, applicando di nuovo il Teorema 4.13, otteniamo $|\bigcup \mathcal{C}| \leqslant |\bigcup_{A \in \mathcal{C}} A \times \{A\}| \leqslant \kappa \otimes \lambda$. $\square$

4.20. Corollario.
(1) *L'unione di una collezione finita di insiemi finiti è finita.*
(2) *L'unione di una collezione numerabile di insiemi numerabili è numerabile.*

Dimostrazione.
(1) Sia $\mathcal{C}$ una collezione finita, con $|\mathcal{C}| = m$. Possiamo supporre $\mathcal{C} \neq \varnothing$, cosicché l'insieme $\{\, |A| \mid A \in \mathcal{C} \,\}$ ha il massimo, che indichiamo con n. Per la proposizione precedente abbiamo $|\bigcup \mathcal{C}| \leqslant m \otimes n = mn$.
(2) Sia $\mathcal{C}$ numerabile, con $|\mathcal{C}| = \nu$. Applicando la proposizione precedente e il Teorema 4.17 otteniamo $|\bigcup \mathcal{C}| \leqslant \nu \otimes \omega = \max\{\nu, \omega\} = \omega$. $\square$

4.21. Esercizio. Sia A un insieme infinito, e sia $\mathcal{F}$ la collezione dei sottoinsiemi finiti di A. Mostrare che $|\mathcal{F}| = |A|$.

Suggerimento. Per ogni $n \in \omega$, sia $\mathcal{F}_n = \big\{\, E \subseteq A \bigm| |E| = n \,\big\}$. Osservare che esiste una funzione iniettiva da $\mathcal{F}_n$ a A^n.

V. L'ipotesi del continuo

4.22. Definizione. Il numero cardinale 2^ω sarà indicato con $\mathfrak{c}$. Se $|X| = \mathfrak{c}$ diremo che X è un insieme *continuo*, o anche che X ha la *cardinalità del continuo*.

Abbiamo già accennato al fatto che, a partire dall'insieme dei numeri naturali, si costruiscono gli insiemi $\mathbb{Z}$ e $\mathbb{Q}$ rispettivamente dei numeri interi e razionali relativi, e l'insieme $\mathbb{R}$ dei numeri reali. Usando il Teorema 4.17, si vede che $\mathbb{Z}$ e $\mathbb{Q}$ sono insiemi numerabili. Si dimostra inoltre che $\mathbb{R}$ ha la cardinalità del continuo.

[6]Si rimanda il lettore interessato a [**3**, Theor. 10.12 e Cor. 10.13(1), pag. 29] o [**1**, Theor. 8, pag. 25].

4.23. Esercizio. Dimostrare che per ogni cardinale κ esiste il minimo cardinale maggiore di κ.

4.24. Definizione. Sia κ un cardinale. Il minimo cardinale maggiore di κ (che esiste in virtù dell'esercizio precedente) è chiamato *successore cardinale* di κ e indicato con κ^+.

Sia λ un cardinale non nullo. Se esiste un cardinale κ tale che $\lambda = \kappa^+$, diremo che λ è un *cardinale successore*; in caso contario diremo che λ è un *cardinale limite*.

Il cardinale ω^+, che è il minimo ordinale non numerabile, verrà indicato con ω_1, come è usuale[7].

Sappiamo che è $\omega_1 \leqslant \mathfrak{c}$. L'affermazione che $\mathfrak{c} = \omega_1$ è chiamata *ipotesi del continuo*. Essa, riguardo agli assiomi della teoria degli insiemi, si trova nella stessa posizione dell'assioma della scelta ma, a differenza di questo, non viene universalmente accettata come ulteriore assioma.

Analoghe considerazioni valgono per l'*ipotesi del continuo generalizzata*, cioè l'affermazione che $2^\kappa = \kappa^+$ per ogni cardinale infinito κ.

VI. Cofinalità

4.25. Definizione. Sia $(S, \leqslant)$ un insieme parzialmente ordinato. Un sottoinsieme T si dice *cofinale* in S se per ogni $s \in S$ esiste almeno un $t \in T$ con $s \leqslant t$. La *cofinalità* di $(S, \leqslant)$, indicata con $\operatorname{cf}(S, \leqslant)$ o semplicemente con $\operatorname{cf}(S)$, è la minima cardinalità di un sottoinsieme cofinale di S.

Dalla definizione segue subito che $\operatorname{cf}(S) \leqslant |S|$. Inoltre $\operatorname{cf}(S) = 0$ se e solo se S è vuoto, e $\operatorname{cf}(S) = 1$ se e solo se S ha massimo.

Di conseguenza, per ogni ordinale α (con l'ordinamento naturale), si ha $\operatorname{cf}(\alpha) = 1$ se e solo se α è un ordinale successore.

4.26. Esercizio. Sia κ un cardinale infinito. Mostrare che $\operatorname{cf}(\kappa)$ è un cardinale infinito non superiore a κ.

Ricordiamo che un sottoinsieme A di un insieme ordinato S si dice limitato superiormente (inferiormente) se esiste $b \in S$ tale che per ogni $a \in A$ si ha $a \leqslant b$ (risp. $a \geqslant b$). In caso contrario si dice che A è illimitato superiomente (risp. inferiormente). Un sottoinsieme A è detto limitato se è limitato superiormente e inferiormente; è detto illimitato se non è limitato.

Una funzione $f\colon E \to S$, dove S è un insieme ordinato, si dice limitata superiormente (o inferiormente, o illimitata, ecc.) se lo è il sottoinsieme $f[E]$.

4.27. Proposizione. *Sia A un sottoinsieme di un insieme ordinato S non vuoto e privo di massimo. Condizione necessaria perché A sia cofinale, è che sia illimitato superiormente. Se poi S è totalmente ordinato, la condizione è anche sufficiente.*

Dimostrazione. Infatti se A fosse limitato superiormente, potremmo trovare $b \in S$ tale che $a \leqslant b$ per ogni $a \in A$; inoltre, poiché S è privo di massimo, ci sarà almeno un $c \in S$ con $c \nleqslant b$: ne segue che $c \nleqslant a$ per ogni $a \in A$, quindi A non è cofinale.

Sia ora S totalmente ordinato, e sia $A \subseteq S$ illimitato superiormente; per ogni $s \in S$ esiste $a \in A$ tale che $a \nleqslant s$, quindi $s < a$: pertanto A è cofinale. □

4.28. Corollario. *Sia S un insieme totalmente ordinato non vuoto e privo di massimo. Dato un qualunque cardinale $\lambda \geqslant \operatorname{cf}(S)$, almeno una funzione $f\colon \lambda \to S$ è illimitata superiormente.*

[7] Alcuni testi usano il simbolo Ω invece di ω_1 per indicare il primo ordinale non numerabile. Nel caso che ω e ω_1 siano considerati come cardinali, essi vengono indicati anche con $\aleph_0$ e $\aleph_1$, rispettivamente.

Dimostrazione. Sia T un sottoinsieme cofinale di S avente cardinalità minima: poiché $T \neq \varnothing$ e $|T| = \mathrm{cf}(S) \leqslant \lambda$, esiste $f\colon \lambda \to T$ suriettiva, quindi $f\colon \lambda \to S$ è illimitata superiormente per la proposizione precedente, in quanto $f[\lambda] = T$. □

Siano $(S, \leqslant)$ e $(T, \preceq)$ insiemi ordinati. Ricordiamo che una funzione $\varphi\colon S \to T$ è detta *crescente* se per ogni $x, y \in S$ con $x \leqslant y$ si ha $\varphi(x) \preceq \varphi(y)$.

4.29. Lemma. *Se γ un ordinale limite, esiste una funzione iniettiva $g\colon \mathrm{cf}(\gamma) \to \gamma$ crescente e illimitata superiormente.*

Dimostrazione. Per il Corollario 4.28, possiamo trovare $f\colon \mathrm{cf}(\gamma) \to \gamma$ illimitata superiormente. Definiamo g per induzione. Anzitutto poniamo $g(0) = f(0)$.

Sia poi $\eta \in \mathrm{cf}(\gamma)$, con $\eta > 0$, e supponiamo di aver definito $g(\xi)$ per ogni $\xi < \eta$. Poiché γ è un ordinale limite, deve essere $g(\xi) + 1 \in \gamma$ per ogni $\xi < \eta$. Inoltre l'insieme $\{\, g(\xi) + 1 \mid \xi < \eta \,\}$, avendo cardinalità non superiore a η e quindi minore di $\mathrm{cf}(\gamma)$, è limitato superiormente grazie alla Proposizione 4.27. Possiamo dunque porre

$$g(\eta) = \max\bigl\{ f(\eta), \sup\{\, g(\xi) + 1 \mid \xi < \eta \,\}\bigr\}. \tag{4.1}$$

Ciò completa la costruzione della funzione g.

Osserviamo ora che g è iniettiva e crescente in quanto, se $\xi < \eta < \mathrm{cf}(\gamma)$, si ha $g(\eta) \geqslant g(\xi) + 1 > g(\xi)$. Inoltre la (4.1) implica che $g(\eta) \geqslant f(\eta)$ per ogni $\eta \in \mathrm{cf}(\gamma)$, e pertanto anche g è illimitata superiormente. □

4.30. Teorema. *Per ogni cardinale infinito κ, si ha $\mathrm{cf}\bigl(\mathrm{cf}(\kappa)\bigr) = \mathrm{cf}(\kappa)$.*

Dimostrazione. Sappiamo dall'Esercizio 4.26 che $\mathrm{cf}\bigl(\mathrm{cf}(\kappa)\bigr) \leqslant \mathrm{cf}(\kappa)$. Resta da dimostrare che $\mathrm{cf}\bigl(\mathrm{cf}(\kappa)\bigr) \geqslant \mathrm{cf}(\kappa)$.

Per il lemma precedente, possiamo trovare una funzione $f\colon \mathrm{cf}(\kappa) \to \kappa$ e una funzione $g\colon \mathrm{cf}\bigl(\mathrm{cf}(\kappa)\bigr) \to \mathrm{cf}(\kappa)$, entrambe iniettive, crescenti e illimitate superiormente. La composizione $h = f \circ g$ è dunque una funzione iniettiva e illimitata superiormente da $\mathrm{cf}\bigl(\mathrm{cf}(\kappa)\bigr)$ a κ. Pertanto

$$\mathrm{cf}(\kappa) \leqslant \Bigl| h\bigl[\mathrm{cf}\bigl(\mathrm{cf}(\kappa)\bigr)\bigr] \Bigr| = \mathrm{cf}\bigl(\mathrm{cf}(\kappa)\bigr).$$ □

4.31. Definizione. Un cardinale infinito si dice *regolare* se coincide con la propria cofinalità. In caso contrario si dice *singolare*.

Dall'Esercizio 4.26 segue immediatamente che ω è regolare. Inoltre, per il Teorema 4.30, $\mathrm{cf}(\kappa)$ è regolare per ogni cardinale infinito κ.

4.32. Proposizione. *Ogni cardinale successore infinito è regolare.*

Dimostrazione. Sia κ un cardinale infinito. Se κ^+ non fosse regolare, ci sarebbe $T \subseteq \kappa^+$ cofinale tale che $|T| \leqslant \kappa$, e quindi si avrebbe $\kappa^+ = \sup T = \bigcup T$. D'altra parte, poiché $|\alpha| \leqslant \kappa$ per ogni $\alpha \in T$, deve essere $|\bigcup T| \leqslant \kappa$, e abbiamo una contraddizione. □

Dato un qualunque cardinale infinito κ, è facile costruire un cardinale singolare λ maggiore di κ: sia $\kappa_0 = \kappa$ e $\kappa_{n+1} = \kappa_n^+$ per ogni $n \in \omega$; ponendo $\lambda = \sup_{n\in\omega} \kappa_n$ si ha $\mathrm{cf}(\lambda) = \omega \leqslant \kappa < \lambda$.

D'altro canto non è possibile dimostrare in ZFC l'esistenza di cardinali limite regolari non numerabili. Tali cardinali vengono detti *debolmente inaccessibili*.

4.33. Teorema (König). *Siano κ e λ cardinali infiniti, con $\lambda \geqslant \mathrm{cf}(\kappa)$. Allora $\kappa^\lambda > \kappa$.*

Dimostrazione. Fissiamo $f\colon \lambda \to \kappa$ illimitata (l'esistenza di f è assicurata dal Corollario 4.28). Presa una qualunque funzione $G\colon \kappa \to \kappa^\lambda$, mostriamo che G non può essere suriettiva.

Sia $\gamma \in \kappa$; per maggior chiarezza, indicheremo $G(\gamma)$, che è una funzione da λ a κ, con il simbolo g_γ. Per ogni $\alpha \in \lambda$, sia L_α l'insieme di tutti i $\beta \in \kappa$ della forma $g_\gamma(\alpha)$ per qualche $\gamma < f(\alpha)$; la cardinalità di L_α non supera $f(\alpha)$ e quindi è minore di κ, cosicché $\kappa \smallsetminus L_\alpha$ è non vuoto: possiamo allora porre $h(\alpha) = \min(\kappa \smallsetminus L_\alpha)$. Abbiamo così definito $h \in \kappa^\lambda$; completiamo la dimostrazione verificando che $h \neq g_\gamma$ per ogni $\gamma \in \kappa$.

Sia infatti $\gamma \in \kappa$; essendo f illimitata, possiamo trovare $\alpha \in \lambda$ tale che $f(\alpha) > \gamma$, dunque $g_\gamma(\alpha) \in L_\alpha$: poiché $h(\alpha) \notin L_\alpha$, abbiamo $h(\alpha) \neq g_\gamma(\alpha)$ e quindi $h \neq g_\gamma$. □

4.34. Corollario. *Se λ è un cardinale infinito, si ha* $\mathrm{cf}(2^\lambda) > \lambda$.

Dimostrazione. Se fosse $\lambda \geqslant \mathrm{cf}(2^\lambda)$, potremmo applicare il teorema precedente con $\kappa = 2^\lambda$, ottenendo $(2^\lambda)^\lambda > 2^\lambda$. Ciò è assurdo, perché $(2^\lambda)^\lambda = 2^{\lambda \otimes \lambda} = 2^\lambda$. □

Bibliografia

[1] Thomas Jech. *Set theory*. Seconda edizione. Springer-Verlag, Berlin, 1997.

[2] John L. Kelley. *General topology*, *Graduate Texts in Mathematics*, vol. 27. Springer-Verlag, New York, 1975.

[3] Kenneth Kunen. *Set Theory. An Introduction to Independence Proofs*, *Studies in Logic and the Foundation of Mathematics*, vol. 102. Van Nostrand, Amsterdam, 1980.

[4] Herman Rubin e Jean E. Rubin. *Equivalents of the Axiom of Choice, II*, *Studies in Logic and the Foundation of Mathematics*, vol. 116. Van Nostrand, Amsterdam, 1985.