UNIVERSITÀ CATTOLICA DEL SACRO CUORE

Facoltà di Scienze Matematiche, Fisiche e Naturali

LOGICA E TEORIA DEGLI INSIEMI

Prof. Marco Degiovanni

Anno Accademico 2013/2014

Indice

Capitolo 1

La teoria degli insiemi di Zermelo-Fraenkel

1 Primi assiomi

In questo capitolo esponiamo gli assiomi e le nozioni fondamentali della teoria degli insiemi secondo Zermelo-Fraenkel.

I primi concetti di teoria degli insiemi dovrebbero essere, in forma intuitiva, familiari a tutti. Ricordiamo che la nozione di base è la frase aperta in due variabili $x \in X$ (x *appartiene a* X). Va solo precisato che, a livello intuitivo, x e X sembrano avere due nature diverse (x l'*elemento* e X l'*insieme*). Al contrario, nella teoria formale che consideriamo esiste un solo tipo di ente: l'*insieme*. Questo punto di vista è economico e conveniente perché, ad esempio, un quadrato nel piano può essere concepito come insieme dei suoi punti, ma anche come elemento dell'insieme di tutti i quadrati. A questo proposito è bene chiarire che, per ragioni di eleganza e rispondenza con l'intuizione, si preferisce dire "*famiglia di insiemi*" o "*collezione di insiemi*", intendendo "*insieme di insiemi*". Per lo stesso motivo gli insiemi vengono denotati, a seconda dei casi, con lettere di dimensione e tipo diverso, quali x, Y, $\mathfrak{F}$, anche se dal punto di vista logico si tratta di *variabili* tutte con la stessa dignità.

Riassumendo, gli oggetti della teoria sono di un unico tipo e si chiamano *insiemi*. La teoria contiene due frasi aperte (in due variabili) primitive. Esse sono *la frase aperta di identità*, proveniente dalla logica,

$$x = y \qquad (x \text{ è uguale ad } y)$$

e *la frase aperta di appartenenza*, tipica della teoria degli insiemi,

$$x \in y \qquad (x \textit{ appartiene ad } y)\,.$$

Ogni frase aperta della matematica (e quindi, in particolare, della teoria degli insiemi) è costruita, secondo le regole della logica, a partire da queste due frasi aperte.

Per evitare di dover maneggiare frasi aperte di volta in volta sempre più lunghe, introdurremo all'occorrenza delle abbreviazioni. Le prime due, $x \neq y$ (x *è diverso da* y) e $x \notin X$ (x *non appartiene ad* y), sono ovvie:

$$\begin{array}{ccc} x \neq y & \text{significa} & non(x = y)\,; \\ x \notin X & \text{significa} & non(x \in X)\,. \end{array}$$

Introduciamo anche delle abbreviazioni nella scrittura delle frasi aperte:

$$\begin{array}{ccc} \forall x \in X : \mathcal{P}(x) & \text{significa} & \forall x : (x \in X) \Longrightarrow \mathcal{P}(x)\,; \\ \exists x \in X : \mathcal{P}(x) & \text{significa} & \exists x : (x \in X)\, e\, \mathcal{P}(x)\,. \end{array}$$

Un'ulteriore notazione è collegata con la nozione fondamentale di *sottoinsieme*. Se X ed Y sono due insiemi, diciamo che X è *sottoinsieme* di Y e scriviamo $X \subseteq Y$ (X *è incluso in* Y o X *è una parte di* Y), se ogni elemento di X è anche elemento di Y. Più formalmente,

$$X \subseteq Y \qquad \text{significa} \qquad \forall x : x \in X \Longrightarrow x \in Y\,.$$ [1]

Le due proprietà seguenti sono di immediata verifica.

(1.1) Teorema *Per ogni* X, Y *e* Z *si ha*

$$X \subseteq X\,; \tag{1.2}$$

$$(X \subseteq Y\, e\, Y \subseteq Z) \Longrightarrow X \subseteq Z\,. \tag{1.3}$$

Il primo assioma, che ora introduciamo, stabilisce una terza naturale proprietà dell'inclusione.

[1] Nella letteratura si incontra anche la notazione $X \subset Y$, che può però avere due significati diversi a seconda degli autori. Per alcuni vuol dire $(X \subseteq Y)\, e\, (X \neq Y)$, mentre per altri è sinonimo di $X \subseteq Y$.

(1.4) Assioma (di estensionalità) *Per ogni X ed Y si ha*

$$(X \subseteq Y \, e \, Y \subseteq X) \implies X = Y \,.$$[2]

L'assioma di estensionalità fornisce lo strumento principale per dimostrare che due insiemi sono uguali. Se X ed Y sono due insiemi, per dimostrare che $X = Y$, molto spesso si prova che ogni elemento di X è un elemento di Y e viceversa.

Il secondo assioma postula l'esistenza di un insieme con una particolare proprietà.

(1.5) Assioma (dell'insieme vuoto) *Esiste X tale che*

$$\forall x : \, x \notin X \,. \tag{1.6}$$

Se X ed Y sono due insiemi verificanti entrambi la (1.6), si ha $X \subseteq Y$, ossia

$$\forall x : \, x \in X \implies x \in Y \,.$$

Infatti, quale che sia x, è sicuramente falso che $x \in X$ e quindi vero che

$$(x \in X) \implies (x \in Y) \,.$$

In modo simile si verifica che $Y \subseteq X$, per cui $X = Y$ per l'assioma di estensionalità. Pertanto l'insieme di cui all'assioma precedente è unico. Da ora in poi verrà denotato col simbolo $\emptyset$ (*insieme vuoto*).

Osserviamo incidentalmente che qualunque affermazione della forma

$$\forall x \in X : \, \mathcal{P}(x)$$

è vera, se $X = \emptyset$.

Il terzo, il quarto ed il quinto assioma garantiscono la possibilità di costruire insiemi con particolari proprietà a partire da un dato insieme.

Il primo dei tre consente, dato un qualunque insieme X, di costruire un insieme che abbia per elementi esattamente i sottoinsiemi di X.

(1.7) Assioma (dell'insieme delle parti) *Per ogni X esiste $\mathfrak{F}$ tale che*

$$\forall Y : \, Y \in \mathfrak{F} \iff Y \subseteq X \,. \tag{1.8}$$

[2] L'implicazione contraria "$X = Y \implies (X \subseteq Y \, e \, Y \subseteq X)$" è invece facilmente deducibile dal Teorema (1.1).

Assegnato X, siano $\mathfrak{F}$ e $\mathfrak{G}$ due insiemi verificanti la (1.8). Per ogni $Y \in \mathfrak{F}$ si ha $Y \subseteq X$, quindi $Y \in \mathfrak{G}$. Pertanto risulta $\mathfrak{F} \subseteq \mathfrak{G}$. In modo simile si prova che $\mathfrak{G} \subseteq \mathfrak{F}$, da cui $\mathfrak{F} = \mathfrak{G}$ per l'assioma di estensionalità. Pertanto, fissato X, l'insieme di cui all'assioma precedente è unico. Da ora in poi verrà denotato col simbolo $\mathfrak{P}(X)$ (*insieme delle parti* di X o *insieme potenza* di X).

Naturalmente per ogni insieme X si ha $\emptyset \subseteq X$ e $X \subseteq X$, per cui risulta sempre $\emptyset \in \mathfrak{P}(X)$ e $X \in \mathfrak{P}(X)$.

(1.9) Esempio

(*a*) *Si ha* $\emptyset \in \mathfrak{P}(\emptyset)$, *per cui* $\mathfrak{P}(\emptyset) \neq \emptyset$.

(*b*) *Si ha* $\emptyset \in \mathfrak{P}(\mathfrak{P}(\emptyset))$ *ed anche* $\mathfrak{P}(\emptyset) \in \mathfrak{P}(\mathfrak{P}(\emptyset))$, *per cui* $\emptyset$ *e* $\mathfrak{P}(\emptyset)$ *sono due elementi distinti di* $\mathfrak{P}(\mathfrak{P}(\emptyset))$.

L'assioma successivo garantisce la possibilità di costruire un insieme come unione di più insiemi. In effetti, per le esigenze della matematica moderna è necessario poter fare l'unione di *molti* insiemi. Per non scontrarsi con le difficoltà connesse con la nozione di infinito, è opportuno affrontare la questione da un punto di vista appropriato. Per poter fare l'unione di certi insiemi, si richiede che esista un insieme $\mathfrak{F}$ che abbia per *elementi* esattamente gli insiemi che si vogliono unire (intuitivamente $\mathfrak{F}$ sarà quindi una famiglia di insiemi). L'unione sarà allora qualcosa che dipenderà da $\mathfrak{F}$ (che è *un solo* oggetto), piuttosto che dagli insiemi che si vogliono unire, ossia gli elementi di $\mathfrak{F}$ (che possono essere *tanti*).

(1.10) Assioma (dell'insieme-unione) *Per ogni* $\mathfrak{F}$ *esiste* X *tale che*

$$\forall x : x \in X \iff (\exists F : F \in \mathfrak{F} \, e \, x \in F) .$$

In termini meno formali, X è l'insieme che ha per elementi tutti e soli gli x che appartengono ad almeno un $F \in \mathfrak{F}$.

Anche in questo caso, fissato $\mathfrak{F}$, l'insieme X di cui all'assioma precedente è unico per l'assioma di estensionalità. Da ora in poi verrà denotato col simbolo $\bigcup \mathfrak{F}$ oppure $\bigcup\limits_{F \in \mathfrak{F}} F$ (*insieme-unione* di $\mathfrak{F}$).

(1.11) Osservazione *Per ogni $\mathfrak{F}$, valgono i seguenti fatti:*

$$\forall F: \; F \in \mathfrak{F} \Longrightarrow F \subseteq \bigcup \mathfrak{F}\,,$$

$$\mathfrak{F} \subseteq \mathfrak{P}\left(\bigcup \mathfrak{F}\right).$$

L'ultimo degli assiomi che introduciamo ora è importante quando si affrontano alcune questioni avanzate di teoria degli insiemi. A noi servirà solo per dedurre i principi di accoppiamento e specificazione, dopodiché non avremo più occasione di menzionarlo.

(1.12) Assioma (di rimpiazzamento) *Sia $\mathcal{R}(x, y)$ una frase aperta in due variabili tale che*

$$\forall x,\, \forall y_1,\, \forall y_2: \; (\mathcal{R}(x, y_1) \text{ e } \mathcal{R}(x, y_2)) \Longrightarrow y_1 = y_2\,.$$

Allora per ogni X esiste Y tale che

$$\forall y: \; y \in Y \Longleftrightarrow (\exists x: \; x \in X \text{ e } \mathcal{R}(x, y))\,.$$

Vediamo le due conseguenze dell'assioma di rimpiazzamento che ci interessano.

(1.13) Teorema (Principio di accoppiamento) *Per ogni a e per ogni b esiste uno ed un solo Y tale che*

$$\forall y: \; y \in Y \Longleftrightarrow (y = a \text{ o } y = b)\,.$$

Dimostrazione. Assegnati a e b, sia $\mathcal{R}(x, y)$ la frase aperta

$$(x = \emptyset \text{ e } y = a) \text{ o } (x = \mathfrak{P}(\emptyset) \text{ e } y = b)\,.$$

Poiché $\emptyset \neq \mathfrak{P}(\emptyset)$, si tratta di una frase aperta a cui si può applicare l'assioma di rimpiazzamento. Sia $X = \mathfrak{P}(\mathfrak{P}(\emptyset))$. Se Y è tale che

$$\forall y: \; y \in Y \Longleftrightarrow (\exists x: \; x \in X \text{ e } \mathcal{R}(x, y))\,,$$

risulta che Y ha la proprietà richiesta dalla tesi. L'unicità di Y segue dall'assioma di estensionalità. ■

L'insieme definito dal teorema precedente verrà denotato col simbolo $\{a, b\}$. Poniamo anche per definizione $\{a\} := \{a, a\}$ (la notazione := significa "uguale per definizione" ed è comoda, anche se il solo = è logicamente sufficiente).

(1.14) Teorema (Principio di specificazione) *Siano $\mathcal{P}(x)$ una frase aperta in una variabile e X un insieme. Allora esiste uno ed un solo insieme Y tale che*

$$\forall x : x \in Y \iff (x \in X \text{ e } \mathcal{P}(x))\,.$$

Dimostrazione. Sia $\mathcal{R}(x, y)$ la frase aperta

$$(x = y) \text{ e } \mathcal{P}(y)\,.$$

Ovviamente si può applicare a $\mathcal{R}$ l'assioma di rimpiazzamento. Sia Y tale che

$$\forall y : y \in Y \iff (\exists x : x \in X \text{ e } \mathcal{R}(x, y))\,.$$

L'insieme Y verifica la proprietà richiesta dalla tesi. Per l'assioma di estensionalità Y è unico. ■

L'insieme definito dal teorema precedente verrà denotato nel seguito con la scrittura

$$\{x : x \in X \text{ e } \mathcal{P}(x)\}$$

o, più brevemente,

$$\{x \in X : \mathcal{P}(x)\}\,.$$[3]

Il principio di specificazione è forse la proprietà della teoria degli insiemi di uso più frequente. Se si vuole costruire un insieme Y costituito esattamente da certi elementi, è sufficiente costruire un insieme X contenente tali elementi. Il principio di specificazione consente poi di "ritagliare" la parte di X che interessa.

Osserviamo che il principio di specificazione consente di rispondere (negativamente) alla questione circa l'esistenza di un insieme universale.

(1.15) Teorema *Per ogni X esiste x tale che $x \notin X$.*

Dimostrazione. Dato un qualunque insieme X, sia

$$x = \{y \in X : y \notin y\}\,.$$

Ragioniamo per assurdo, supponendo che $x \in X$. Se $x \notin x$, si ha $x \in x$, che è assurdo. Se invece $x \in x$, si ha $x \notin x$, che è pure assurdo. ■

[3]Molti autori utilizzano la barra verticale | al posto dei due punti.

Quando la teoria degli insiemi era ancora in una fase iniziale, si riteneva che dovesse esistere *l'insieme di tutti gli insiemi.* Questa convinzione, combinata col teorema precedente, portava ad una contraddizione, nota nella letteratura come *paradosso di Russell.*

Come dicevamo, il principio di specificazione consente di costruire un gran numero di insiemi, purché siano sottoinsiemi di qualche insieme a sua volta già costruito. Ad esempio, l'intersezione può essere costruita come opportuno sottoinsieme dell'unione.

(1.16) Teorema *Per ogni* $\mathfrak{F} \neq \emptyset$ *esiste uno ed un solo* X *tale che*

$$\forall x : x \in X \iff (\forall F : F \in \mathfrak{F} \Longrightarrow x \in F) .$$

Dimostrazione. Poniamo

$$X = \left\{x \in \bigcup \mathfrak{F} : (\forall F : F \in \mathfrak{F} \Longrightarrow x \in F)\right\} .$$

Se $x \in X$, è ovvio che

$$\forall F : F \in \mathfrak{F} \Longrightarrow x \in F .$$

Viceversa, sia x tale che

$$\forall F : F \in \mathfrak{F} \Longrightarrow x \in F .$$

Poiché $\mathfrak{F} \neq \emptyset$, esiste $F_0 \in \mathfrak{F}$. Ne segue $x \in F_0$, quindi $x \in \bigcup \mathfrak{F}$, per cui $x \in X$. Pertanto l'insieme X ha la proprietà richiesta.

Per l'assioma di estensionalità, X è unico. ■

Nel seguito l'insieme definito dal teorema precedente verrà denotato col simbolo $\bigcap \mathfrak{F}$ oppure $\bigcap\limits_{F \in \mathfrak{F}} F$ (*insieme-intersezione* di $\mathfrak{F}$).

Osserviamo che la condizione $\mathfrak{F} \neq \emptyset$ è necessaria. Se $\mathfrak{F} = \emptyset$, la proprietà

$$\forall F : F \in \mathfrak{F} \Longrightarrow x \in F$$

è vera per ogni x. Pertanto $\bigcap \mathfrak{F}$ dovrebbe essere un insieme che contiene tutti gli insiemi come elementi. Il Teorema (1.15) asserisce che un tale insieme non esiste.

Introduciamo le seguenti notazioni:

$$X \cup Y := \bigcup \{X, Y\} ,$$

$$X \cap Y := \bigcap \{X, Y\}\,,$$

$$X \setminus Y := \{x \in X : x \notin Y\}\,,$$

$$\{x, y, z\} := \{x, y\} \cup \{z\}\,.$$

Si verifica facilmente che

$$\forall x : x \in X \cup Y \iff (x \in X \; o \; x \in Y)\,,$$

$$\forall x : x \in X \cap Y \iff (x \in X \; e \; x \in Y)\,,$$

$$\forall x : x \in X \setminus Y \iff (x \in X \; e \; x \notin Y)\,.$$

Esercizi

1. Siano X un insieme e $\mathfrak{F} \subseteq \mathfrak{P}(X)$ con $\mathfrak{F} \neq \emptyset$. Si dimostri che

$$X \setminus \left(\bigcup_{F \in \mathfrak{F}} F\right) = \bigcap_{F \in \mathfrak{F}} (X \setminus F)\,,$$

$$X \setminus \left(\bigcap_{F \in \mathfrak{F}} F\right) = \bigcup_{F \in \mathfrak{F}} (X \setminus F)\,.$$

2. Si dimostri che non esiste nessun insieme X tale che

$$\forall x : x \neq X \Longrightarrow x \in X\,.$$

2 Relazioni ed applicazioni

(2.1) Definizione *Per ogni x ed y poniamo*

$$(x, y) := \big\{\{x\}, \{x, y\}\big\}\,.$$

L'insieme (x, y) si chiama coppia ordinata*.*

Per ogni $\mathfrak{F}$, con $\mathfrak{F} \neq \emptyset$ e $\mathfrak{F} \neq \{\emptyset\}$, poniamo anche

$$\pi_1\mathfrak{F} := \bigcup\bigcap\mathfrak{F}\,,$$
$$\pi_2\mathfrak{F} := \left(\left(\bigcup\bigcup\mathfrak{F}\right) \setminus \left(\bigcup\bigcap\mathfrak{F}\right)\right) \cup \left(\bigcap\bigcup\mathfrak{F}\right)\,.$$

La nozione di coppia ordinata è importante a causa della seguente proprietà fondamentale.

(2.2) Teorema *Per ogni x, y si ha*

$$\pi_1(x,y) = x\,, \qquad \pi_2(x,y) = y\,.$$

In particolare, per ogni a, b, x, y si ha

$$(a,b) = (x,y) \iff (a = x \text{ e } b = y)\,.$$

Dimostrazione. Risulta

$$\bigcap(x,y) = \bigcap\big\{\{x\},\{x,y\}\big\} = \{x\} \cap \{x,y\} = \{x\}\,,$$

da cui

$$\pi_1(x,y) = \bigcup\{x\} = \bigcup\{x,x\} = x \cup x = x\,.$$

D'altronde si ha

$$\bigcup(x,y) = \bigcup\big\{\{x\},\{x,y\}\big\} = \{x\} \cup \{x,y\} = \{x,y\}\,,$$

da cui

$$\bigcup\bigcup(x,y) = \bigcup\{x,y\} = x \cup y\,,$$
$$\bigcap\bigcup(x,y) = \bigcap\{x,y\} = x \cap y\,.$$

Ne segue

$$\pi_2(x,y) = ((x \cup y) \setminus x) \cup (x \cap y) = y\,,$$

da cui la tesi. ■

Dati due insiemi X ed Y, vogliamo costruire un insieme che abbia per elementi tutte e sole le coppie ordinate (x,y) con $x \in X$ ed $y \in Y$. In virtù del principio di specificazione, è sufficiente costruire un insieme che contenga tali coppie ordinate.

(2.3) Lemma *Per ogni X, Y, x, y si ha*

$$(x \in X \text{ e } y \in Y) \implies (x,y) \in \mathfrak{P}\left(\mathfrak{P}\left(X \cup Y\right)\right) .$$

Dimostrazione. Se $x \in X$ ed $y \in Y$, si ha evidentemente $\{x,y\} \subseteq X \cup Y$. A maggior ragione risulta $\{x\} \subseteq X \cup Y$, per cui $\{x\}$ e $\{x,y\}$ sono entrambi elementi di $\mathfrak{P}\left(X \cup Y\right)$. Ne segue che $(x,y) = \big\{\{x\},\{x,y\}\big\}$ è un sottoinsieme di $\mathfrak{P}\left(X \cup Y\right)$ e quindi un elemento di $\mathfrak{P}\left(\mathfrak{P}\left(X \cup Y\right)\right)$. ■

(2.4) Teorema *Se X ed Y sono due insiemi, esiste uno ed un solo insieme Z tale che*

$$\forall z : z \in Z \iff (\exists x \in X, \exists y \in Y : z = (x,y)) .$$

Dimostrazione. Poniamo

$$Z := \left\{z \in \mathfrak{P}\left(\mathfrak{P}\left(X \cup Y\right)\right) : \Big(\exists x \in X, \exists y \in Y : z = (x,y)\Big)\right\} .$$

Se $z \in Z$, è ovvio che

$$\exists x \in X, \exists y \in Y : z = (x,y) .$$

Viceversa, se z soddisfa

$$\exists x \in X, \exists y \in Y : z = (x,y) ,$$

segue dal Lemma (2.3) che $z \in \mathfrak{P}\left(\mathfrak{P}\left(X \cup Y\right)\right)$, per cui $z \in Z$. Pertanto l'insieme Z ha la proprietà richiesta.

L'unicità segue dall'assioma di estensionalità. ■

Nel seguito l'insieme definito dal teorema precedente verrà denotato col simbolo $X \times Y$ (*insieme-prodotto* di X ed Y).

(2.5) Definizione *Un insieme R si dice* relazione, *se tutti i suoi elementi sono coppie ordinate. Formalmente, R si dice* relazione, *se*

$$\forall z : z \in R \implies \big(\exists x, \exists y : z = (x,y)\big) .$$

Se R è una relazione, la notazione xRy (x è nella relazione *R* con *y) significa $(x,y) \in R$.*

Osserviamo che non si richiede a x ed y di appartenere a qualche prefissato insieme.

Evidentemente, se X ed Y sono due insiemi, ogni sottoinsieme R di $X \times Y$ è una relazione. Per motivi tecnici è utile sapere che ogni relazione può essere ottenuta in questo modo, attraverso un'opportuna scelta di X ed Y.

(2.6) Lemma *Per ogni relazione R si ha*

$$R \subseteq \left(\bigcup\left(\bigcup R\right)\right) \times \left(\bigcup\left(\bigcup R\right)\right).$$

Dimostrazione. Se $z \in R$, si ha $z \subseteq \bigcup R$. D'altronde risulta $z = (x,y) = \big\{\{x\},\{x,y\}\big\}$ per qualche x e per qualche y. Poiché $\{x,y\} \in z$, ne segue che $\{x,y\} \in \bigcup R$, quindi che $\{x,y\} \subseteq \bigcup(\bigcup R)$. D'altronde $x \in \{x,y\}$ ed $y \in \{x,y\}$, per cui $x \in \bigcup(\bigcup R)$ ed $y \in \bigcup(\bigcup R)$. Pertanto $z = (x,y) \in \left(\bigcup(\bigcup R)\right) \times \left(\bigcup(\bigcup R)\right)$. ■

(2.7) Teorema *Sia R una relazione. Allora esiste uno ed un solo insieme X tale che*

$$\forall x : \ x \in X \iff (\exists y : \ xRy)$$

ed esiste uno ed un solo insieme Y tale che

$$\forall y : \ y \in Y \iff (\exists x : \ xRy)\,.$$

Dimostrazione. Poniamo

$$X = \left\{x \in \bigcup\left(\bigcup R\right) : \ (\exists y : \ xRy)\right\}.$$

Se $x \in X$, è ovvio che

$$\exists y : xRy\,.$$

Viceversa, se x verifica

$$\exists y : \ xRy\,,$$

tenuto conto del Lemma (2.6) risulta

$$(x,y) \in R \subseteq \left(\bigcup\left(\bigcup R\right)\right) \times \left(\bigcup\left(\bigcup R\right)\right),$$

da cui $x \in \bigcup(\bigcup R)$, quindi $x \in X$. Pertanto l'insieme X ha la proprietà richiesta. Per l'assioma di estensionalità X è unico.

Un ragionamento simile può essere fatto per Y, dopo aver posto

$$Y = \left\{y \in \bigcup\left(\bigcup R\right) : \left(\exists x : xRy\right)\right\} .$$

Ne segue la tesi. ■

Nel seguito i due insiemi definiti dal teorema precedente verranno denotati rispettivamente col simbolo $\mathrm{dom}\,(R)$ (*dominio di* R) e col simbolo $\mathrm{img}\,(R)$ (*immagine di* R).

(2.8) Proposizione *Se R e S sono due relazioni e X è un insieme, gli insiemi*

$$S \circ R := \left\{(x,z) \in (\mathrm{dom}\,(R)) \times (\mathrm{img}\,(S)) : \left(\exists y : xRy \text{ e } ySz\right)\right\} ,$$

$$R^{-1} := \{(x,y) \in (\mathrm{img}\,(R)) \times (\mathrm{dom}\,(R)) : yRx\} ,$$

$$R_{|X} := \{(x,y) \in R : x \in X\}$$

sono delle relazioni.

Dimostrazione. Gli insiemi $S \circ R$ e R^{-1} sono per definizione dei sottoinsiemi di prodotti cartesiani, quindi ovviamente delle relazioni. Poiché $R_{|X} \subseteq R$, è evidente che anche $R_{|X}$ è una relazione. ■

(2.9) Definizione *La relazione $S \circ R$ si chiama* composizione *di R e S. La relazione R^{-1} si chiama* relazione inversa *di R. La relazione $R_{|X}$ si chiama* restrizione *di R all'insieme X.*

Consideriamo ora alcuni tipi particolari di relazione.

(2.10) Definizione *Sia R un insieme. Diciamo che R è* una relazione di equivalenza, *se R è una relazione,* $\mathrm{dom}\,(R) = \mathrm{img}\,(R)$ *e, posto* $X = \mathrm{dom}\,(R)$, *valgono le seguenti proprietà:*

(*a*) $\forall x : x \in X \Longrightarrow xRx$ (*proprietà* riflessiva*);*

(*b*) $\forall x, \forall y : xRy \Longrightarrow yRx$ (*proprietà* simmetrica*);*

(*c*) $\forall x, \forall y, \forall z : \left(xRy \text{ e } yRz\right) \Longrightarrow xRz$ (*proprietà* transitiva*).*

Se R è una relazione di equivalenza e $X = \mathrm{dom}\,(R)$, diciamo che R è una relazione di equivalenza nell'insieme X. *Se xRy, diciamo che x ed y sono* equivalenti *(secondo la relazione di equivalenza R).*

(2.11) Definizione *Sia R una relazione di equivalenza in un insieme X e sia $A \subseteq X$. Diciamo che A è* una classe di equivalenza*, se valgono le seguenti proprietà:*

(*a*) $A \neq \emptyset$;

(*b*) $\forall x, \forall y : (x \in A \text{ e } y \in A) \implies xRy$;

(*c*) $\forall x, \forall y : (x \in A \text{ e } xRy) \implies y \in A$.

(2.12) Definizione *Sia R una relazione di equivalenza in un insieme X. Poniamo*

$$X/R := \{A \in \mathfrak{P}\,(X) : \, A \text{ è una classe di equivalenza}\} \, .$$

L'insieme X/R si chiama insieme quoziente di X rispetto alla relazione di equivalenza R.

(2.13) Definizione *Sia R un insieme. Diciamo che R è* una relazione d'ordine*, se R è una relazione,* $\mathrm{dom}\,(R) = \mathrm{img}\,(R)$ *e, posto $X = \mathrm{dom}\,(R)$, valgono le seguenti proprietà:*

(*a*) $\forall x : x \in X \implies xRx$ *(proprietà* riflessiva*);*

(*b*) $\forall x, \forall y : (xRy \text{ e } yRx) \implies x = y$ *(proprietà* antisimmetrica*);*

(*c*) $\forall x, \forall y, \forall z : \big(xRy \text{ e } yRz\big) \implies xRz$ *(proprietà* transitiva*).*

Se poi vale l'ulteriore proprietà

(*d*) $\forall x, \forall y : (x \in X \text{ e } y \in X) \implies (xRy \text{ o } yRx)$,

diciamo che R è una relazione d'ordine totale.

Se R è una relazione d'ordine e $X = \mathrm{dom}\,(R)$, diciamo che R è una relazione d'ordine nell'insieme X. *Invece della notazione xRy, si usa scrivere $x \leq y$.*

(2.14) Definizione Un'applicazione *(o* funzione*) è una relazione f tale che*

$$\forall x, \forall y_1, \forall y_2 : \, (xfy_1 \text{ e } xfy_2) \implies y_1 = y_2 \, .$$

Se f è un'applicazione e $x \in \mathrm{dom}\,(f)$, si denota con $f(x)$ oppure f_x l'unico y tale che xfy.

Intuitivamente, f può essere concepita come una "legge" che ad ogni elemento di $\mathrm{dom}\,(f)$ associa uno ed un solo valore $f(x)$. In omaggio a questo punto di vista, si usa spesso la notazione

$$\{x \mapsto f(x)\}$$

per denotare l'applicazione f, mentre l'insieme f viene chiamato *grafico* dell'applicazione. Nella teoria formale degli insiemi l'applicazione viene identificata col suo grafico. Questo consente di trattare l'applicazione come un qualunque insieme, senza introdurre un'entità di natura diversa.

(2.15) Teorema *Se f e g sono due applicazioni e X è un insieme, le relazioni $g \circ f$ e $f_{|X}$ sono delle applicazioni.*

Dimostrazione. Siano x, z_1 e z_2 tali che $x(g \circ f)z_1$ e $x(g \circ f)z_2$. Per definizione di composizione esistono y_1 ed y_2 tali che xfy_1, y_1gz_1, xfy_2 ed y_2gz_2. Poiché f è un'applicazione, si ha $y_1 = y_2$. Poiché g è un'applicazione, ne segue che $z_1 = z_2$. Pertanto $g \circ f$ è un'applicazione.

Il fatto che $f_{|X}$ sia un'applicazione è evidente. ■

(2.16) Definizione *Un'applicazione f si dice* iniettiva*, se*

$$\forall x_1,\, \forall x_2,\, \forall y:\, (x_1 f y \text{ e } x_2 f y) \implies x_1 = x_2\,.$$

(2.17) Teorema *Un'applicazione f è iniettiva se e solo se la relazione f^{-1} è un'applicazione.*

Dimostrazione. Il fatto che f sia iniettiva equivale a dire che

$$\forall x_1,\, \forall x_2,\, \forall y:\, \left(y f^{-1} x_1 \text{ e } y f^{-1} x_2\right) \implies x_1 = x_2\,,$$

che esprime il fatto che f^{-1} sia un'applicazione. ■

(2.18) Definizione *Siano X ed Y due insiemi e sia f un'applicazione. Diciamo che f è* un'applicazione da X in Y *(e scriviamo $f : X \to Y$), se* $\mathrm{dom}\,(f) = X$ *ed* $\mathrm{img}\,(f) \subseteq Y$*. In tal caso diciamo che Y è* il codominio *di $f : X \to Y$.*

Per ogni $A \subseteq X$ e $B \subseteq Y$ poniamo

$$f(A) = \{f(x) : x \in A\} := \big\{y \in Y : \big(\exists x : x \in A \, e \, f(x) = y\big)\big\} ,$$

$$f^{-1}(B) := \{x \in X : f(x) \in B\} .$$

Se $y \in Y$, si usa anche la notazione abbreviata $f^{-1}(y)$ invece di $f^{-1}(\{y\})$.[4]

(2.19) Definizione *Un'applicazione $f : X \to Y$ si dice* suriettiva*, se* $\mathrm{img}\,(f) = Y$*. Si dice* biiettiva*, se f è iniettiva e suriettiva.*

(2.20) Proposizione *Siano $f : X \to Y$ e $g : Y \to Z$ due applicazioni. Valgono allora i seguenti fatti:*

(a) *se $g \circ f$ è iniettiva, allora f è iniettiva;*

(b) *se $g \circ f$ è suriettiva, allora g è suriettiva.*

Dimostrazione.
(a) Se $f(x_1) = f(x_2)$, ne segue $g(f(x_1)) = g(f(x_2))$, quindi $x_1 = x_2$ per l'iniettività di $g \circ f$.
(b) Dato $z \in Z$, sia $x \in X$ tale che $g(f(x)) = z$. Allora $f(x) \in Y$ e $g(f(x)) = z$, per cui g è suriettiva. ■

Vediamo ora alcuni esempi notevoli di applicazioni.

(2.21) Teorema *Se X ed Y sono due insiemi,*

$$\pi_1 = \{(z, x) \in (X \times Y) \times X : x = \pi_1 z\} ,$$

$$\pi_2 = \{(z, y) \in (X \times Y) \times Y : y = \pi_2 z\}$$

[4] Queste notazioni lasciano a desiderare quanto a consistenza, ma sono ormai diventate tradizionali. Ad esempio, può capitare benissimo che si abbia contemporaneamente $A \in X$ ed $A \subseteq X$. In tal caso la notazione $f(A)$ è ambigua. Tuttavia, nelle situazioni concrete che si incontrano nello studio dell'analisi, si capisce usualmente dal contesto se A viene considerato come elemento o come sottoinsieme di X.

sono due applicazioni rispettivamente da $X \times Y$ *in* X *e da* $X \times Y$ *in* Y *che si chiamano* proiezioni canoniche *sul primo e sul secondo fattore e soddisfano*

$$\forall x \in X,\, \forall y \in Y : \pi_1(x, y) = x\,, \qquad \pi_2(x, y) = y\,.$$

Dimostrazione. Si tratta di una conseguenza del Teorema (2.2). ■

(2.22) Teorema *Sia* R *una relazione di equivalenza in un insieme* X*. Allora l'insieme*

$$\pi = \{(x, A) \in X \times (X/R) : x \in A\}$$

è un'applicazione suriettiva da X *in* X/R *e si chiama* proiezione canonica sul quoziente.

Dimostrazione. L'insieme π è una relazione, perché sottoinsieme di un prodotto cartesiano, e risulta $\mathrm{dom}\,(\pi) \subseteq X$ ed $\mathrm{img}\,(\pi) \subseteq (X/R)$. Siano $x\pi A_1$ e $x\pi A_2$. Per ogni $y \in A_1$ si ha xRy, quindi $y \in A_2$. Pertanto $A_1 \subseteq A_2$. Similmente si prova che $A_2 \subseteq A_1$, da cui $A_1 = A_2$. Ne segue che π è un'applicazione.

Per ogni $x \in X$ sia

$$A = \{y \in X : xRy\}\,.$$

Si verifica facilmente che A è una classe di equivalenza e $x \in A$, per cui $x\pi A$. Pertanto il dominio di π è tutto X. Infine, se $A \in X/R$, sia $x \in A$. Allora $\pi(x) = A$, per cui π è suriettiva. ■

In sostanza, per ogni $x \in X$ esiste una ed una sola classe di equivalenza che contenga x. La proiezione sul quoziente associa a x tale classe di equivalenza. Si usa spesso il simbolo $[x]$ per denotare la classe di equivalenza che contiene x.

Se f è un'applicazione da X in Y, si ha evidentemente $f \subseteq X \times Y$. Si può quindi definire l'insieme delle applicazioni da X in Y come un opportuno sottoinsieme di $\mathfrak{P}\,(X \times Y)$.

(2.23) Teorema *Se* X *ed* Y *sono due insiemi, esiste uno ed un solo insieme* F *tale che*

$$\forall f : f \in F \iff \big(f \text{ è un'applicazione da } X \text{ in } Y\big)\,.$$

Dimostrazione. Poniamo

$$F = \{f \in \mathfrak{P}\,(X \times Y) : f \text{ è un'applicazione e } \mathrm{dom}\,(f) = X\}\,.$$

Si verifica facilmente che F ha la proprietà richiesta. Per l'assioma di estensionalità F è unico. ■

Nel seguito denoteremo con Y^X l'insieme definito dal teorema precedente (*insieme delle applicazioni da X in Y*).

Quando occorre fare l'unione (o l'intersezione) di una famiglia $\mathfrak{F}$ di insiemi, si usa spesso interpretare $\mathfrak{F}$ come l'immagine di un'opportuna applicazione X. In questo caso gli insiemi da unire sono i valori X_j dell'applicazione X. Inoltre si usa denotare con $\{X_j : j \in J\}$ l'immagine di X, ossia la famiglia di insiemi in questione. Questo approccio comporta l'introduzione di due nuove notazioni.

(2.24) Definizione *Se X è un'applicazione e $J = \mathrm{dom}\,(X)$, poniamo*

$$\bigcup_{j \in J} X_j := \bigcup (\mathrm{img}\,(X)) \,.$$

Se poi $J \neq \emptyset$, poniamo anche

$$\bigcap_{j \in J} X_j := \bigcap (\mathrm{img}\,(X)) \,.$$

(2.25) Definizione *Se X è un'applicazione e $J = \mathrm{dom}\,(X)$, poniamo*

$$\prod_{j \in J} X_j := \left\{ x \in \left(\bigcup_{j \in J} X_j \right)^J : (\forall j \in J : x_j \in X_j) \right\} .$$

(2.26) Teorema *Se X è un'applicazione e $J = \mathrm{dom}\,(X)$, per ogni $j \in J$*

$$\pi_j = \left\{ (x, c) \in \left(\prod_{j \in J} X_j \right) \times X_j : c = x_j \right\}$$

è un'applicazione da $\prod_{j \in J} X_j$ in X_j che si chiama proiezione canonica *sul fattore j-esimo e soddisfa*

$$\forall j \in J, \forall x \in \prod_{j \in J} X_j : \pi_j(x) = x_j \,.$$

Dimostrazione. Evidente. ■

Esercizi

1. Siano R, S e T tre relazioni. Si dimostri che

$$T \circ (S \circ R) = (T \circ S) \circ R\,,$$

$$\left(R^{-1}\right)^{-1} = R\,.$$

2. Siano R e S due relazioni. Si dimostri che

$$\mathrm{dom}\,(S \circ R) \subseteq \mathrm{dom}\,(R)\ , \qquad \mathrm{img}\,(S \circ R) \subseteq \mathrm{img}\,(S)\ .$$

3. Si dimostri che $\emptyset$ è un'applicazione.

3 L'assioma di infinità

Gli assiomi finora introdotti garantiscono l'esistenza dell'insieme vuoto e ci forniscono la possibilità di costruire certi insiemi a partire dall'insieme vuoto. Per poter tuttavia costruire i primi insiemi numerici, come ad esempio l'insieme dei numeri naturali, è necessario un ulteriore assioma che garantisca l'esistenza di un insieme *sufficientemente grande*.

(3.1) Assioma (di infinità) *Esiste un insieme X tale che*

$$\emptyset \in X\,; \tag{3.2}$$

$$\forall x : \, x \in X \implies x \cup \{x\} \in X\,. \tag{3.3}$$

(3.4) Teorema *Esiste uno ed un solo insieme ω con le seguenti proprietà:*

(a) ω soddisfa la (3.2) e la (3.3);

(b) *se Y è un insieme che soddisfa la* (3.2) *e la* (3.3), *si ha $\omega \subseteq Y$.*

Dimostrazione. Sia X un insieme conforme all'assioma di infinità. Poniamo

$$\mathfrak{F} = \{F \in \mathfrak{P}(X) : F \text{ soddisfa la (3.2) e la (3.3)}\} .$$

Risulta $\mathfrak{F} \neq \emptyset$, perché $X \in \mathfrak{F}$. Si può quindi porre $\omega = \bigcap \mathfrak{F}$. Poiché $\emptyset \in F$ per ogni $F \in \mathfrak{F}$, si ha $\emptyset \in \omega$. Se poi $x \in \omega$, si ha $x \in F$ per ogni $F \in \mathfrak{F}$. Ne segue $x \cup \{x\} \in F$ per ogni $F \in \mathfrak{F}$, quindi $x \cup \{x\} \in \omega$. Pertanto ω soddisfa la (3.2) e la (3.3).

Sia ora Y un qualunque insieme verificante la (3.2) e la (3.3). Allora anche $X \cap Y$ soddisfa queste due proprietà. Ne segue che $X \cap Y \in \mathfrak{F}$, quindi $\omega \subseteq X \cap Y \subseteq Y$. Pertanto ω è il più piccolo insieme verificante la (3.2) e la (3.3).

Se poi ω' fosse un altro insieme con le stesse proprietà di ω, si avrebbe $\omega \subseteq \omega'$ ed $\omega' \subseteq \omega$, da cui $\omega' = \omega$. ∎

(3.5) Definizione *L'insieme ω introdotto nel teorema precedente si chiama* insieme dei cardinali finiti *e gli elementi di ω si chiamano* cardinali finiti.

Definiamo un'applicazione $\sigma : \omega \to \omega$ ponendo

$$\sigma := \{(n, m) \in \omega \times \omega : m = n \cup \{n\}\} .$$

L'elemento $\sigma(n) = n \cup \{n\}$ si chiama *successivo* di n.

Vogliamo dimostrare che l'insieme ω e l'applicazione σ soddisfano alcune proprietà notevoli. Per questo premettiamo un lemma.

(3.6) Lemma *Siano $m, n \in \omega$ tali che $m \in n$. Allora si ha $m \subseteq n$.*

Dimostrazione. Sia Y l'insieme degli $n \in \omega$ tali che

$$\forall m : m \in n \implies m \subseteq n .$$

Evidentemente basta dimostrare che $Y = \omega$. Poiché per costruzione $Y \subseteq \omega$, è sufficiente provare che Y soddisfa la (3.2) e la (3.3).

Osserviamo che si ha $\emptyset \in Y$, perché la condizione $m \in \emptyset$ è sempre falsa. Sia ora $n \in Y$. Evidentemente $n \cup \{n\} \in \omega$. Se $m \in n \cup \{n\}$, si ha $m \in n$ oppure $m = n$. In ogni caso, tenendo conto che $n \in Y$, ne segue $m \subseteq n$. A maggior ragione si ha $m \subseteq n \cup \{n\}$. Pertanto $n \cup \{n\} \in Y$. ■

Possiamo adesso dimostrare le proprietà fondamentali dell'insieme ω e dell'applicazione σ.

(3.7) Teorema *L'insieme ω e l'applicazione σ soddisfano le seguenti proprietà:*

(a) *$\emptyset \in \omega$;*

(b) *σ è un'applicazione da ω in ω;*

(c) *per ogni $n \in \omega$ si ha $\sigma(n) \neq \emptyset$;*

(d) *l'applicazione σ è iniettiva;*

(e) *se $A \subseteq \omega$, $\emptyset \in A$ e per ogni $n \in A$ risulta $\sigma(n) \in A$, si ha $A = \omega$.*

Dimostrazione. Le proprietà (a) e (b) sono evidenti. La (e) segue dal fatto che ω è il più piccolo insieme che soddisfi la (3.2) e la (3.3). La proprietà (c) è pure evidente, perché $n \in \sigma(n) = n \cup \{n\}$.

Dimostriamo la (d). Siano $m, n \in \omega$ tali che $m \cup \{m\} = n \cup \{n\}$. Poiché $m \in m \cup \{m\}$, risulta $m \in n \cup \{n\}$, ossia $m \in n$ o $m = n$. Per il Lemma (3.6) si ha in ogni caso $m \subseteq n$. In maniera analoga si prova che $n \subseteq m$, da cui $m = n$ per l'assioma di estensionalità. ■

Agli inizi del XX secolo, in seguito agli studi del matematico Giuseppe Peano, era stato riconosciuto che la Matematica poteva essere fondata sulla teoria degli insiemi e sull'esistenza di un insieme e di un'applicazione (l'insieme dei numeri naturali e l'applicazione successivo) verificanti la tesi del Teorema (3.7). In quell'approccio le (a), (b), (c), (d) ed (e) del teorema diventavano cinque assiomi, noti come *assiomi di Peano*.

Successivamente si è visto che gli assiomi di Peano potevano essere dedotti dai principi generali della teoria degli insiemi. La nostra esposizione si è attenuta a questa seconda linea.

La proprietà (e) sta alla base di una particolare tecnica di dimostrazione. Data una frase aperta $\mathcal{P}(x)$, supponiamo di sapere che le due affermazioni seguenti sono vere:

$$\mathcal{P}(\emptyset),$$

$$\forall n \in \omega : \mathcal{P}(n) \implies \mathcal{P}(\sigma(n)) .$$

Allora si ha

$$\forall n \in \omega : \mathcal{P}(n) .$$

Infatti

$$A = \{n \in \omega : \mathcal{P}(n)\}$$

è un sottoinsieme di ω conforme alla (e). Ne segue $A = \omega$, che corrisponde all'affermazione desiderata.

Questo particolare tipo di argomentazione si chiama *dimostrazione per induzione*.

Dal Teorema (3.7) segue la seguente ulteriore proprietà legata all'insieme ω.

(3.8) Teorema (di ricorsione) *Siano X un insieme, $f : \omega \times X \to X$ un'applicazione e $x_0 \in X$.*

Allora esiste una ed una sola applicazione $\varphi : \omega \to X$ tale che

$$\varphi(\emptyset) = x_0 ,$$

$$\forall n \in \omega : \varphi(\sigma(n)) = f(n, \varphi(n)) .$$

Dimostrazione. Sia Φ l'insieme delle applicazioni $\psi \subseteq \omega \times X$ tali che

$$\emptyset \in \mathrm{dom}\,(\psi) \ \text{e}\ \psi(\emptyset) = x_0 ,$$

$$\forall n \in \omega : \sigma(n) \in \mathrm{dom}\,(\psi) \implies \big(n \in \mathrm{dom}\,(\psi) \ \text{e}\ \psi(\sigma(n)) = f(n, \psi(n))\big) .$$

Poniamo

$$\varphi = \bigcup \Phi .$$

Evidentemente φ è una relazione con $\varphi \subseteq \omega \times X$.

Proviamo anzitutto che φ è un'applicazione. Se $\psi_1, \psi_2 \in \Phi$, si tratta di dimostrare che

$$\forall n \in \omega : n \in \mathrm{dom}\,(\psi_1) \cap \mathrm{dom}\,(\psi_2) \implies \psi_1(n) = \psi_2(n) .$$

Per questo ragioniamo per induzione su n. Evidentemente $\psi_1(\emptyset) = x_0 = \psi_2(\emptyset)$. Assumiamo ora che l'affermazione sia vera per un certo $n \in \omega$ e dimostriamo che è vera per $\sigma(n)$.

Se $\sigma(n) \notin \mathrm{dom}\,(\psi_1) \cap \mathrm{dom}\,(\psi_2)$, il fatto è certo. Se $\sigma(n) \in \mathrm{dom}\,(\psi_1) \cap \mathrm{dom}\,(\psi_2)$, risulta $n \in \mathrm{dom}\,(\psi_1) \cap \mathrm{dom}\,(\psi_2)$, da cui $\psi_1(n) = \psi_2(n)$, e

$$\psi_1(\sigma(n)) = f(n, \psi_1(n)) = f(n, \psi_2(n)) = \psi_2(\sigma(n)) \,.$$

Pertanto φ è un'applicazione.

Poiché $\{(\emptyset, x_0)\} \in \Phi$, si ha $\emptyset \in \mathrm{dom}\,(\varphi)$ e $\varphi(\emptyset) = x_0$. Se $n \in \mathrm{dom}\,(\varphi)$, esiste $\psi \in \Phi$ tale che $n \in \mathrm{dom}\,(\psi)$ e $\psi(n) = \varphi(n)$. Sia

$$\tilde{\psi} = \psi \cup \{(\sigma(n), f(n, \psi(n)))\} \;.$$

Evidentemente $\tilde{\psi} \in \Phi$, per cui $\sigma(n) \in \mathrm{dom}\,(\varphi)$ e

$$\varphi(\sigma(n)) = \tilde{\psi}(\sigma(n)) = f(n, \psi(n)) = f(n, \varphi(n)) \,.$$

Ne segue che $\mathrm{dom}\,(\varphi) = \omega$ e l'applicazione φ soddisfa le condizioni richieste.

Per dimostrare l'unicità di φ, supponiamo di avere un'altra applicazione $\tilde{\varphi} : \omega \to X$ con le stesse proprietà. Dobbiamo dimostrare che

$$\forall n \in \omega : \; \tilde{\varphi}(n) = \varphi(n) \,.$$

Per questo ragioniamo ancora per induzione su n. Evidentemente $\tilde{\varphi}(\emptyset) = x_0 = \varphi(\emptyset)$. Supponiamo ora che l'affermazione sia vera per un certo n. Allora

$$\tilde{\varphi}(\sigma(n)) = f(n, \tilde{\varphi}(n)) = f(n, \varphi(n)) = \varphi(\sigma(n)) \,,$$

da cui la tesi. ■

Le applicazioni definite utilizzando il teorema precedente si dicono *definite per ricorrenza* o *in modo ricorsivo.*

4 L'assioma della scelta

(4.1) Proposizione *Sia $f : X \to Y$ un'applicazione con $X \neq \emptyset$. Allora sono fatti equivalenti:*

(*a*) *f è iniettiva;*

(*b*) *esiste un'applicazione $g : Y \to X$ tale che $(g \circ f)(x) = x$ per ogni $x \in X$.*

Dimostrazione.
(*a*) $\Longrightarrow$ (*b*) Sia $x_0 \in X$. Poniamo

$$g = f^{-1} \cup ((Y \setminus \operatorname{img}(f)) \times \{x_0\})$$

ossia definiamo

$$g(y) = \begin{cases} f^{-1}(y) & \text{se } y \in \operatorname{img}(f)\,, \\ x_0 & \text{se } y \in Y \setminus \operatorname{img}(f)\,. \end{cases}$$

Allora $g : Y \to X$ soddisfa $(g \circ f)(x) = x$ per ogni $x \in X$.
(*b*) $\Longrightarrow$ (*a*) Evidentemente $g \circ f : X \to X$ è biiettiva, in particolare iniettiva. Dalla Proposizione (2.20) segue che f è iniettiva. ■

(4.2) Proposizione *Sia $f : X \to Y$ un'applicazione. Supponiamo che esista un'applicazione $g : Y \to X$ tale che $(f \circ g)(y) = y$ per ogni $y \in Y$.*

Allora f è suriettiva.

Dimostrazione. Evidentemente $f \circ g : Y \to Y$ è biiettiva, in particolare suriettiva. Dalla Proposizione (2.20) segue che f è suriettiva. ■

Il prossimo assioma asserisce l'implicazione mancante per poter allineare la Proposizione (4.2) con la Proposizione (4.1).

(4.3) Assioma (della scelta) *Sia $f : X \to Y$ un'applicazione suriettiva. Allora esiste un'applicazione $g : Y \to X$ tale che $(f \circ g)(y) = y$ per ogni $y \in Y$.*

Vediamo subito una prima conseguenza.

(4.4) Teorema (di selezione) *Sia Φ un'applicazione tale che*

$$\forall x \in \operatorname{dom}(\Phi) : \ \Phi(x) \neq \emptyset\,.$$

Allora esiste un'applicazione φ tale che $\operatorname{dom}(\varphi) = \operatorname{dom}(\Phi)$ *e*

$$\forall x \in \operatorname{dom}(\varphi) : \ \varphi(x) \in \Phi(x)\,.$$

Dimostrazione. Se $\Phi = \emptyset$, scegliamo $\varphi = \emptyset$. Altrimenti poniamo $X = \mathrm{dom}\,(\Phi)$ ed $Y = \bigcup_{x \in X} \Phi(x)$, per cui si ha $\Phi : X \to \mathfrak{P}\,(Y)$.

Poniamo ora

$$Z = \{(y, A) \in Y \times \mathfrak{P}\,(Y) : \; y \in A\}$$

e denotiamo con $f : Z \to \mathfrak{P}\,(Y) \setminus \{\emptyset\}$ la restrizione a Z di π_2. Per ogni $A \in \mathfrak{P}\,(Y) \setminus \{\emptyset\}$ esiste $y \in A$, da cui $(y, A) \in Z$ e $f(y, A) = A$. Pertanto f è suriettiva. Sia $g : \mathfrak{P}\,(Y) \setminus \{\emptyset\} \to Z$ conforme all'assioma della scelta e sia $\gamma = \pi_1 \circ g$. Allora $\gamma : \mathfrak{P}\,(Y) \setminus \{\emptyset\} \to Y$ e $\gamma(A) \in A$ per ogni $A \in \mathfrak{P}\,(Y) \setminus \{\emptyset\}$.

Se poniamo $\varphi = \gamma \circ \Phi$, risulta allora $\mathrm{dom}\,(\varphi) = \mathrm{dom}\,(\Phi)$ e $\varphi(x) = \gamma(\Phi(x)) \in \Phi(x)$ per ogni $x \in \mathrm{dom}\,(\varphi)$. ■

(4.5) Definizione *Siano $(X, \leq)$ un insieme ordinato, $A \subseteq X$ e $m, M \in X$. Diciamo che*

- m *è* un minorante *per A, se risulta $m \leq x$ per ogni $x \in A$;*
- M *è* un maggiorante *per A, se risulta $x \leq M$ per ogni $x \in A$.*

Se $(X, \leq)$ è un insieme ordinato, conveniamo che

$$x < y \qquad \text{significhi} \qquad (x \leq y)\; e\; (x \neq y)\,.$$

(4.6) Definizione *Siano $(X, \leq)$ un insieme ordinato, $A \subseteq X$ e $m, M \in A$. Diciamo che*

- m *è* minimo *per A, se risulta $m \leq x$ per ogni $x \in A$;*
- M *è* massimo *per A, se risulta $x \leq M$ per ogni $x \in A$;*
- m *è* un elemento minimale *per A, se non esiste nessun $x \in A$ con $x < m$;*
- M *è* un elemento massimale *per A, se non esiste nessun $x \in A$ con $M < x$.*

(4.7) Proposizione *Siano $(X, \leq)$ un insieme ordinato ed $A \subseteq X$. Se $m', m'' \in A$ sono due minimi per A, allora risulta $m' = m''$. Se $M', M'' \in A$ sono due massimi per A, allora risulta $M' = M''$.*

Dimostrazione. Evidentemente si ha sia $m' \leq m''$ che $m'' \leq m'$, da cui $m' = m''$. La dimostrazione per i massimi è simile. ■

(4.8) Definizione *Siano $(X, \leq)$ un insieme ordinato ed $A \subseteq X$. Diciamo che A è* una catena *in X, se A è totalmente ordinato rispetto all'ordinamento indotto da X.*

(4.9) Lemma *Sia $(X, \leq)$ un insieme ordinato. Si supponga che*

(a) *per ogni $x \in X$, che non sia massimale per X, esista $y \in X \setminus \{x\}$ tale che*

$$\{\xi \in X : x \leq \xi \leq y\} = \{x, y\};$$

(b) *ogni catena in X ammetta un maggiorante e l'insieme di tali maggioranti ammetta minimo.*

Allora X ammette un elemento massimale.

Dimostrazione. Per ogni catena C in X, denotiamo con $\sup C$ il minimo dei maggioranti per C. In particolare, poiché $\emptyset$ è una catena in X, si ha che X ammette minimo, che denotiamo con x_0.

Definiamo un'applicazione $G : X \to (\mathfrak{P}(X) \setminus \{\emptyset\})$ ponendo $G(x) = \{x\}$, se x è massimale in X, e denotando con $G(x)$ l'insieme degli $y \in X \setminus \{x\}$ tali che

$$\{\xi \in X : x \leq \xi \leq y\} = \{x, y\},$$

se x non è massimale in X. Per il Teorema di selezione, esiste un'applicazione $g : X \to X$ tale che $g(x) \in G(x)$ per ogni $x \in X$. Evidentemente si ha $g(x) = x$ se e solo se x è massimale e, in ogni caso, $x \leq g(x)$.

Denotiamo con $\mathfrak{T}$ l'insieme dei $T \in \mathfrak{P}(X)$ tali che

$$x_0 \in T,$$

$$\forall x \in T : g(x) \in T,$$

$$\text{se } C \text{ è una catena in } X \text{ con } C \subseteq T, \text{ allora } \sup C \in T.$$

Poiché $X \in \mathfrak{T}$, si ha $\mathfrak{T} \neq \emptyset$. Poniamo $X_0 = \bigcap \mathfrak{T}$. Si verifica facilmente che $X_0 \in \mathfrak{T}$.

Diciamo che $x \in X_0$ è confrontabile, se per ogni $y \in X_0$ si ha $y \leq x$ oppure $x \leq y$.

I) *Se $x \in X_0$ è confrontabile, per ogni $y \in X_0$ si ha $y \leq x$ oppure $g(x) \leq y$.*

Dato $x \in X_0$ confrontabile, poniamo

$$T = \{y \in X_0 : y \leq x \text{ oppure } g(x) \leq y\} .$$

Dimostriamo che $T \in \mathfrak{T}$.

Poiché $x_0 \leq x$, si ha $x_0 \in T$. Sia ora $y \in T$. Anzitutto risulta $g(y) \in X_0$, perché $X_0 \in \mathfrak{T}$. Tenuto conto che x è confrontabile, una almeno delle seguenti affermazioni è vera:

$$g(x) \leq y \leq g(y) ; \tag{4.10}$$

$$y \leq g(y) \leq x ; \tag{4.11}$$

$$y \leq x \leq g(y) . \tag{4.12}$$

Se valgono la (4.10) o la (4.11), è ovvio che $g(y) \in T$. Se vale la (4.12), si ha $x = g(y)$, che rimanda alla (4.11), oppure $y = x$, che implica $g(y) = g(x)$, per cui $g(y) \in T$. In ogni caso $y \in T$ implica $g(y) \in T$. Sia infine C una catena in X con $C \subseteq T$. Se $y \leq x$ per ogni $y \in C$, si ha $\sup C \leq x$. Se esiste $y \in C$ con $g(x) \leq y$, risulta $g(x) \leq \sup C$. In ogni caso $\sup C \in T$.

Poiché $T \in \mathfrak{T}$, risulta $T = X_0$, da cui la tesi.

II) *X_0 è una catena in X.*

Poniamo

$$T = \{x \in X_0 : x \text{ è confrontabile}\} .$$

È ovvio che $x_0 \in T$. Se $x \in T$, per ogni $y \in X_0$ si ha $y \leq x$, da cui $y \leq g(x)$, oppure $g(x) \leq y$. In ogni caso risulta $g(x) \in T$. Sia infine C una catena in X con $C \subseteq T$ e sia $y \in X_0$. Se $x \leq y$ per ogni $x \in C$, si ha $\sup C \leq y$. Se esiste $x \in C$ con $y \leq x$, risulta $y \leq \sup C$. In ogni caso $\sup C \in T$.

Poiché $T \in \mathfrak{T}$, risulta $T = X_0$, ossia X_0 è una catena in X.

III) $\sup X_0$ *è un elemento massimale in X.*

Poiché $X_0 \in \mathfrak{T}$, posto $M = \sup X_0$, risulta $M \in X_0$. Ne segue $g(M) \in X_0$, quindi $g(M) \leq M$. Deve quindi essere $g(M) = M$, ossia M è un elemento massimale di X. ■

(4.13) Teorema (Principio di massimalità di Hausdorff) *Sia* $(X, \leq)$ *un insieme ordinato. Allora esiste una catena in* X *massimale rispetto all'inclusione.*

Dimostrazione. Poniamo

$$\mathcal{C} = \{C \in \mathfrak{P}(X) : C \text{ è una catena in } X\} .$$

Dati $C_1, C_2 \in \mathcal{C}$, diciamo che $C_1 \leq C_2$ se $C_1 \subseteq C_2$.

I) $(\mathcal{C}, \leq)$ *è un insieme ordinato, ogni catena in* $\mathcal{C}$ *ammette maggiorante e l'insieme di tali maggioranti ammette minimo.*

È evidente che $\leq$ è una relazione d'ordine in $\mathcal{C}$. Se $\{C_j : j \in J\}$ è una catena in $\mathcal{C}$, si verifica facilmente che

$$C = \bigcup_{j \in J} C_j \in \mathcal{C} ,$$

per cui C è un maggiorante per $\{C_j : j \in J\}$ ed è chiaramente il minimo dei maggioranti.

II) *Per ogni* $C \in \mathcal{C}$, *che non sia massimale, esiste* $C' \in \mathcal{C} \setminus \{C\}$ *tale che*

$$\{C'' \in \mathcal{C} : C \subseteq C'' \subseteq C'\} = \{C, C'\} .$$

Se $C \in \mathcal{C}$ non è massimale, esiste $x \in X \setminus C$ tale che $C \cup \{x\} \in \mathcal{C}$. È allora sufficiente porre $C' = C \cup \{x\}$.

III) X *ammette una catena massimale.*

Per il Lemma (4.9), esiste C massimale in $\mathcal{C}$. Questo significa che C è una catena in X massimale rispetto all'inclusione. ■

(4.14) Corollario (Lemma di Zorn) *Sia* $(X, \leq)$ *un insieme ordinato. Si supponga che ogni catena in* X *ammetta un maggiorante.*

Allora X *ammette un elemento massimale.*

Dimostrazione. Per il Principio di massimalità di Hausdorff, esiste una catena C in X massimale rispetto all'inclusione.

Sia $M \in X$ un maggiorante per C. Ne segue $C \cup \{M\} \in \mathcal{C}$, quindi $M \in C$ per la massimalità di C. Osserviamo che M è un elemento massimale in X. Infatti, se $x \in X$ e $M \leq x$, anche x è un maggiorante per C, da cui $x \in C$. Ne segue $x \leq M$, quindi $M = x$, per cui M è un elemento massimale. ∎

Concludiamo la sezione con qualche tipica applicazione del Lemma di Zorn.

(4.15) Teorema *Sia $\mathbb{A}$ un anello commutativo e sia X un modulo su $\mathbb{A}$. Allora X ammette un sottoinsieme indipendente massimale rispetto all'inclusione.*

Dimostrazione. Poniamo

$$\mathfrak{I} = \{I \in \mathfrak{P}(X) : I \text{ è indipendente}\} .$$

Se $I_1, I_2 \in \mathfrak{I}$, diciamo che $I_1 \leq I_2$ se $I_1 \subseteq I_2$. Si verifica facilmente che $\leq$ è una relazione d'ordine in $\mathfrak{I}$.

Sia ora $\{I_j : j \in J\}$ una catena in $\mathfrak{I}$. Osserviamo che $\bigcup\limits_{j\in J} I_j$ è indipendente. Siano infatti $x_1, \ldots, x_n \in \bigcup\limits_{j\in J} I_j$ e siano $\lambda_1, \ldots, \lambda_n \in \mathbb{A}$ tali che

$$\sum_{k=1}^{n} \lambda_k x_k = 0 .$$

Sarà $x_1 \in I_{j_1}, \ldots, x_n \in I_{j_n}$ con $j_1, \ldots, j_n \in J$. Essendo $\{I_j : j \in J\}$ una catena rispetto all'inclusione, esiste $m = 1, \ldots, n$ tale che $I_{j_k} \subseteq I_{j_m}$ per ogni $k = 1, \ldots, n$. Ne segue $x_1, \ldots, x_n \in I_{j_m}$, quindi $\lambda_1 = \cdots = \lambda_n = 0$, tenuto conto che I_{j_m} è indipendente.

Nel momento in cui $\bigcup\limits_{j\in J} I_j \in \mathfrak{I}$, è ovvio che $\bigcup\limits_{j\in J} I_j$ è un maggiorante per $\{I_j : j \in J\}$. Risulta quindi che ogni catena in $\mathfrak{I}$ ammette maggiorante.

Dal Lemma di Zorn si deduce che esiste un massimale in $\mathfrak{I}$, ossia un sottoinsieme indipendente di X massimale rispetto all'inclusione. ∎

(4.16) Corollario *Sia $\mathbb{K}$ un campo e sia X uno spazio vettoriale su $\mathbb{K}$. Allora X ammette un sottoinsieme indipendente che genera l'intero spazio, ossia una base.*

Dimostrazione. Per il teorema precedente, esiste $B \subseteq X$ con B indipendente e massimale rispetto all'inclusione. Si tratta di dimostrare che B genera tutto X.

Per assurdo, sia $x \in X$ non generato da B. In particolare, risulta $x \notin B$, per cui $B \subseteq B \cup \{x\}$ e $B \neq B \cup \{x\}$. Osserviamo che $B \cup \{x\}$ è indipendente. Siano infatti $x_1, \dots, x_n \in B$ e siano $\lambda_0, \lambda_1, \dots, \lambda_n \in \mathbb{K}$ tali che

$$\lambda_0 x + \sum_{k=1}^{n} \lambda_k x_k = 0\,.$$

Deve essere $\lambda_0 = 0$, altrimenti ne seguirebbe

$$x = -\sum_{k=1}^{n} (\lambda_0^{-1} \lambda_k) x_k = 0$$

contro l'ipotesi che x non sia generato da B. Ma allora risulta $\lambda_1 = \cdots = \lambda_n = 0$, perché B è indipendente.

Pertanto $B \cup \{x\}$ è indipendente e questo viola la massimalità di B. ■

(4.17) Definizione *Sia X un insieme non vuoto e sia $\mathfrak{F} \subseteq \mathfrak{P}(X)$. Diciamo che $\mathfrak{F}$ è* un filtro *in X, se*

(a) $\emptyset \notin \mathfrak{F}$ e $X \in \mathfrak{F}$;

(b) se $F_1, F_2 \in \mathfrak{F}$, risulta $F_1 \cap F_2 \in \mathfrak{F}$;

(c) se $F \subseteq G \subseteq X$ e $F \in \mathfrak{F}$, risulta $G \in \mathfrak{F}$.

(4.18) Definizione *Sia X un insieme non vuoto e sia $\mathfrak{F} \subseteq \mathfrak{P}(X)$. Diciamo che $\mathfrak{F}$ è* un ultrafiltro *in X, se $\mathfrak{F}$ è un filtro in X e $\mathfrak{F}$ è massimale rispetto all'inclusione.*

(4.19) Teorema *Sia X un insieme non vuoto e sia $\mathfrak{F}$ un filtro in X. Allora esiste un ultrafiltro $\mathfrak{G}$ in X con $\mathfrak{F} \subseteq \mathfrak{G}$.*

Dimostrazione. Sia

$$\mathcal{G} = \{\mathfrak{G} \in \mathfrak{P}(\mathfrak{P}(X)) : \mathfrak{G} \text{ è un filtro in } X \text{ con } \mathfrak{F} \subseteq \mathfrak{G}\}\,.$$

Se $\mathfrak{G}_1, \mathfrak{G}_2 \in \mathcal{G}$, diciamo che $\mathfrak{G}_1 \leq \mathfrak{G}_2$ se $\mathfrak{G}_1 \subseteq \mathfrak{G}_2$. Al solito, $\leq$ è una relazione d'ordine in $\mathcal{G}$.

Sia $\{\mathfrak{G}_j : j \in J\}$ una catena in $\mathcal{G}$. Osserviamo che $\bigcup_{j\in J} \mathfrak{G}_j$ è un filtro in X. Infatti, se $G_1, G_2 \in \bigcup_{j\in J} \mathfrak{G}_j$, si ha $G_1 \in \mathfrak{G}_{j_1}$ e $G_2 \in \mathfrak{G}_{j_2}$ con $j_1, j_2 \in J$. Essendo $\{\mathfrak{G}_j : j \in J\}$ una catena rispetto all'inclusione, deve essere $\mathfrak{G}_{j_1} \subseteq \mathfrak{G}_{j_2}$ oppure $\mathfrak{G}_{j_2} \subseteq \mathfrak{G}_{j_1}$. Nel primo caso si ha $G_1, G_2 \in \mathfrak{G}_{j_2}$, da cui

$$G_1 \cap G_2 \in \mathfrak{G}_{j_2} \subseteq \bigcup_{j\in J} \mathfrak{G}_j \,.$$

Nel secondo caso si deduce in modo simile che $G_1 \cap G_2 \in \bigcup_{j\in J} \mathfrak{G}_j$. Le altre proprietà di filtro sono evidenti, per cui $\bigcup_{j\in J} \mathfrak{G}_j$ è un filtro in X contenente ovviamente $\mathfrak{F}$. Poiché $\bigcup_{j\in J} \mathfrak{G}_j \in \mathcal{G}$, è ovvio che $\bigcup_{j\in J} \mathfrak{G}_j$ è un maggiorante per $\{\mathfrak{G}_j : j \in J\}$.

Dal Lemma di Zorn segue che esiste un massimale $\mathfrak{G}$ in $\mathcal{G}$, quindi un ultrafiltro in X contenente $\mathfrak{F}$. ■

(4.20) Teorema *Sia X un insieme non vuoto e sia $\mathfrak{F}$ un ultrafiltro in X. Allora, per ogni $E \subseteq X$, si ha $E \in \mathfrak{F}$ oppure $(X \setminus E) \in \mathfrak{F}$.*

Dimostrazione. Dato $E \subseteq X$, osserviamo che si ha

$$\forall F \in \mathfrak{F} : \ F \cap E \neq \emptyset$$

oppure

$$\forall F \in \mathfrak{F} : \ F \cap (X \setminus E) \neq \emptyset \,.$$

Se infatti così non fosse, esisterebbero $F_1, F_2 \in \mathfrak{F}$ con $F_1 \cap E = \emptyset$ e $F_2 \cap (X \setminus E) = \emptyset$, da cui $F_1 \cap F_2 = \emptyset$, il che è assurdo.

Nel primo caso, poniamo

$$\mathfrak{G} = \{G \in \mathfrak{P}(X) : \text{ esiste } F \in \mathfrak{F} \text{ tale che } F \cap E \subseteq G\} \,.$$

Si verifica facilmente che $\mathfrak{G}$ è un filtro in X. Poiché $F \cap E \subseteq F$, risulta $\mathfrak{F} \subseteq \mathfrak{G}$. Essendo $\mathfrak{F}$ un ultrafiltro, ne segue $\mathfrak{F} = \mathfrak{G}$. D'altra parte, da $X \cap E = E$ con $X \in \mathfrak{F}$ segue che $E \in \mathfrak{G} = \mathfrak{F}$.

Nel secondo caso si deduce in modo simile che $(X \setminus E) \in \mathfrak{F}$. ■

(4.21) Definizione *Sia X uno spazio topologico e sia $\mathfrak{F}$ un filtro in X. Diciamo che $\mathfrak{F}$* è convergente *se esiste $\ell \in X$ tale che si abbia $V \in \mathfrak{F}$ per ogni intorno V di ℓ. In tal caso diciamo che $\mathfrak{F}$ è convergente a ℓ.*

(4.22) Teorema *Sia X uno spazio topologico. Allora sono fatti equivalenti:*

(*a*) *X è compatto;*

(*b*) *ogni filtro in X è contenuto in un filtro convergente.*

Dimostrazione. Supponiamo che X sia compatto e consideriamo un filtro $\mathfrak{F}$ in X. Allora $\left\{\overline{F} :\, F \in \mathfrak{F}\right\}$ è una famiglia non vuota di chiusi in X con la proprietà che

$$\overline{F_1} \cap \cdots \cap \overline{F_n} \neq \emptyset$$

per ogni $F_1, \ldots, F_n \in \mathfrak{F}$. Essendo X compatto, esiste

$$\ell \in \bigcap_{F \in \mathfrak{F}} \overline{F}\,.$$

Si ha quindi $V \cap F \neq \emptyset$ per ogni $F \in \mathfrak{F}$ ed ogni intorno V di ℓ. Poniamo

$$\mathfrak{G} = \{G \in \mathfrak{P}(X) :\, \text{esistono un intorno } V \text{ di } \ell \text{ e } F \in \mathfrak{F} \text{ tali che } V \cap F \subseteq G\}\,.$$

Si verifica facilmente che $\mathfrak{G}$ è un filtro in X. Essendo X un intorno di ℓ, da $X \cap F = F$ segue $\mathfrak{F} \subseteq \mathfrak{G}$. D'altra parte, poiché $X \in \mathfrak{F}$, da $V \cap X = V$ segue che $V \in \mathfrak{G}$ per ogni intorno V di ℓ. Pertanto $\mathfrak{G}$ è convergente a ℓ.

Supponiamo ora che ogni filtro in X sia contenuto in un filtro convergente. Sia $\mathfrak{C}$ una famiglia non vuota di chiusi in X tale che

$$C_1 \cap \cdots \cap C_n \neq \emptyset$$

per ogni $C_1, \ldots, C_n \in \mathfrak{C}$.

Poniamo

$$\mathfrak{F} = \{F \in \mathfrak{P}(X) :\, \text{esistono } C_1, \ldots, C_n \in \mathfrak{C} \text{ tali che } C_1 \cap \cdots \cap C_n \subseteq F\}\,.$$

Si verifica facilmente che $\mathfrak{F}$ è un filtro in X. Sia $\mathfrak{G}$ un filtro in X contenente $\mathfrak{F}$ e convergente a qualche ℓ in X.

Sia $C \in \mathfrak{C}$ e sia V un intorno di ℓ. Evidentemente si ha $C \in \mathfrak{F} \subseteq \mathfrak{G}$. D'altra parte $V \in \mathfrak{G}$, perché $\mathfrak{G}$ è convergente a ℓ. Ne segue $V \cap C \neq \emptyset$. Per l'arbitrarietà di V, si deduce che ℓ è aderente a C, quindi che $\ell \in C$, essendo C chiuso. Ne segue che $\ell \in \bigcap \mathfrak{C}$. Pertanto X è conpatto. ■

(4.23) Corollario *Sia X uno spazio topologico. Allora sono fatti equivalenti:*

(a) *X è compatto;*

(b) *ogni ultrafiltro in X è convergente.*

Dimostrazione. Supponiamo che X sia compatto e consideriamo un ultrafiltro $\mathfrak{F}$ in X. Allora $\mathfrak{F}$ è contenuto in un filtro $\mathfrak{G}$ convergente in X. Essendo $\mathfrak{F}$ un ultrafiltro, deve essere $\mathfrak{F} = \mathfrak{G}$, per cui $\mathfrak{F}$ stesso è convergente.

Supponiamo ora che ogni ultrafiltro in X sia convergente. Se $\mathfrak{F}$ è un filtro in X, per il Teorema (4.19) $\mathfrak{F}$ è contenuto in qualche ultrafiltro $\mathfrak{G}$. Essendo $\mathfrak{G}$ convergente, si ha che $\mathfrak{F}$ è contenuto in un filtro convergente. Pertanto X è compatto. ■

(4.24) Teorema (di Tychonoff) *Sia X un'applicazione e sia $J = \mathrm{dom}\,(X)$. Supponiamo che X_j sia uno spazio topologico compatto per ogni $j \in J$.*

Allora $\prod_{j\in J} X_j$ è compatto.

Dimostrazione. Sia $\mathfrak{F}$ un ultrafiltro in $\prod_{j\in J} X_j$. Per ogni $j \in J$, poniamo

$$\mathfrak{E}_j = \left\{E \in \mathfrak{P}\,(X_j) : \pi_j^{-1}(E) \in \mathfrak{F}\right\} ,$$

dove π_j denota la proiezione canonica sul fattore X_j. Si verifica facilmente che $\mathfrak{E}_j$ è un filtro in X_j. Essendo X_j compatto, si ha che $\mathfrak{E}_j$ è contenuto in un filtro convergente in X_j. Dal Teorema di selezione segue che esiste $\ell \in \prod_{j\in J} X_j$ tale che, per ogni $j \in J$, esiste un filtro in X_j contenente $\mathfrak{E}_j$ e convergente a ℓ_j.

Sia V un intorno di ℓ in $\prod\limits_{j\in J} X_j$. Questo significa che esistono $j_1, \ldots, j_n \in J$ e $U_1, \ldots, U_n$, con U_k intorno di ℓ_{j_k} in X_{j_k} per ogni $k = 1, \ldots, n$, tali che

$$\pi_{j_1}^{-1}(U_1) \cap \cdots \cap \pi_{j_n}^{-1}(U_n) \subseteq V\,.$$

Se $\mathfrak{G}_1$ è un filtro in X_{j_1} contenente $\mathfrak{E}_{j_1}$ e convergente a ℓ_{j_1}, si ha che $U_1 \in \mathfrak{G}_1$. Poiché $(X_{j_1} \setminus U_1) \cap U_1 = \emptyset$, ne segue che $(X_{j_1} \setminus U_1) \notin \mathfrak{G}_1$, quindi $(X_{j_1} \setminus U_1) \notin \mathfrak{E}_{j_1}$. Questo significa che

$$\left(\prod_{j\in J} X_j\right) \setminus \pi_{j_1}^{-1}(U_1) = \pi_{j_1}^{-1}(X_{j_1} \setminus U_1) \notin \mathfrak{F}\,.$$

Essendo $\mathfrak{F}$ un ultrafiltro, ne segue che $\pi_{j_1}^{-1}(U_1) \in \mathfrak{F}$. In modo simile si verifica che $\pi_{j_2}^{-1}(U_2), \ldots, \pi_{j_n}^{-1}(U_n) \in \mathfrak{F}$, per cui

$$\pi_{j_1}^{-1}(U_1) \cap \cdots \cap \pi_{j_n}^{-1}(U_n) \in \mathfrak{F}\,.$$

Ne segue $V \in \mathfrak{F}$, per cui $\mathfrak{F}$ è convergente a ℓ. Pertanto $\prod\limits_{j\in J} X_j$ è compatto. ■

5 L'assioma di regolarità

L'ultimo assioma, che ora introduciamo, è significativo solo in vista di alcune delicate questioni di teoria degli insiemi.

(5.1) Assioma **(di regolarità)** *Per ogni insieme non vuoto X esiste $x \in X$ tale che $x \cap X = \emptyset$.*

Vediamo una sua tipica conseguenza.

(5.2) Teorema *Per ogni x, y si ha*

$$x \notin x\,,$$

$$x \in y \implies y \notin x\,.$$

Dimostrazione. Applichiamo anzitutto l'assioma di regolarità a $X = \{x\}$. Ne segue $x \cap \{x\} = \emptyset$, da cui $x \notin x$.

Applichiamo poi l'assioma di regolarità a $X = \{x, y\}$. Poiché $x \in y \cap \{x, y\}$, deve essere $x \cap \{x, y\} = \emptyset$. Ne segue $y \notin x$. ■

Ricapitolando, la teoria degli insiemi di Zermelo - Fraenkel si basa sui seguenti otto assiomi:

1. Assioma di estensionalità
2. Assioma dell'insieme vuoto
3. Assioma dell'insieme delle parti
4. Assioma dell'unione
5. Assioma di rimpiazzamento
6. Assioma di infinità
7. Assioma della scelta
8. Assioma di regolarità.

Esercizi

1. Si dimostri che per ogni x, y, z non si può avere contemporaneamente $x \in y$, $y \in z$ e $z \in x$.

6 Insiemi bene ordinati

(6.1) Definizione *Siano $(X, \leq)$ e $(Y, \leq)$ due insiemi ordinati. Un'applicazione $f : X \to Y$ si dice* strettamente crescente *se, per ogni $x_1, x_2 \in X$ con $x_1 < x_2$, risulta $f(x_1) < f(x_2)$.*

(6.2) Definizione *Due insiemi ordinati $(X, \leq)$ e $(Y, \leq)$ si dicono* simili *se esiste $f : X \to Y$ biiettiva con f e f^{-1} entrambe strettamente crescenti.*

(6.3) Proposizione *Siano* $(X, \leq)$ *e* $(Y, \leq)$ *due insiemi ordinati e sia* $f : X \to Y$ *strettamente crescente e biiettiva. Se* $(X, \leq)$ *è totalmente ordinato, allora* f^{-1} *è strettamente crescente.*

Dimostrazione. Siano $x_1, x_2 \in X$ con $f(x_1) < f(x_2)$. Se, per assurdo, non si ha $x_1 < x_2$, deve essere $x_2 \leq x_1$, da cui $f(x_2) \leq f(x_1)$: assurdo. ■

(6.4) Definizione *Siano* $(X, \leq)$ *un insieme ordinato e* $S \subseteq X$. *Diciamo che* S *è un* segmento inizale *in* X *se, per ogni* $s \in S$ *ed ogni* $x \in X$ *con* $x \leq s$, *risulta* $x \in S$.

(6.5) Definizione *Sia* $(X, \leq)$ *un insieme ordinato. Diciamo che* $(X, \leq)$ *è* bene ordinato*, se ogni sottoinsieme non vuoto di* X *ammette minimo.*

(6.6) Proposizione *Sia* $(X, \leq)$ *bene ordinato. Allora* $(X, \leq)$ *è totalmente ordinato.*

Dimostrazione. Siano $x, y \in X$. Se $x = \min\{x, y\}$, risulta $x \leq y$. Se $y = \min\{x, y\}$, risulta $y \leq x$. ■

(6.7) Proposizione *Sia* $(X, \leq)$ *bene ordinato e sia* $S \subseteq X$. *Allora* S *è un segmento iniziale in* X *con* $S \neq X$ *se e solo se esiste* $x \in X$ *tale che*

$$S = \{\xi \in X : \ \xi < x\} .$$

Dimostrazione. Se S è della forma

$$S = \{\xi \in X : \ \xi < x\}$$

con $x \in X$, si verifica facilmente che S è un segmento iniziale in X con $S \neq X$.

Viceversa, sia S un segmento iniziale in X con $S \neq X$ e sia $x = \min(X \setminus S)$. Se $\xi \in S$, non può essere $x \leq \xi$, perché ne seguirebbe $x \in S$. Risulta quindi $\xi < x$, da cui

$$S \subseteq \{\xi \in X : \ \xi < x\} .$$

Se $\xi \in X$ con $\xi < x$, non può essere $\xi \in (X \setminus S)$, perché si violerebbe la minimalità di x. Risulta quindi $\xi \in S$, da cui

$$\{\xi \in X : \ \xi < x\} \subseteq S .$$

In conclusione si ha

$$S = \{\xi \in X : \ \xi < x\} \ .$$

■

(6.8) Teorema *Ogni insieme X ammette una relazione d'ordine che lo rende bene ordinato.*

Dimostrazione. Sia

$$\mathfrak{R} = \Big\{ R \in \mathfrak{P}(X \times X) : \ R \text{ è una relazione d'ordine su } \mathrm{dom}\,(R) \text{ che rende } \mathrm{dom}\,(R) \text{ bene ordinato} \Big\} .$$

Poniamo, per definizione, $R_1 \leq R_2$ se e solo se

$$R_1 \subseteq R_2 \text{ e } \mathrm{dom}\,(R_1) \text{ è un segmento iniziale in } \mathrm{dom}\,(R_2) \text{ rispetto a } R_2 \,.$$

Si verifica facilmente che questa è una relazione d'ordine su $\mathfrak{R}$. Inoltre, per ogni $x \in X$, si ha $\{(x,x)\} \in \mathfrak{R}$, per cui $\mathfrak{R} \neq \emptyset$.

Sia

$$\{R_j : \ j \in J\}$$

una catena in $\mathfrak{R}$. Poniamo

$$S = \bigcup_{j \in J} R_j \,.$$

Allora $S \in \mathfrak{R}$ ed è un maggiorante per

$$\{R_j : \ j \in J\} \ .$$

Per il Lemma di Zorn, esiste un massimale R in $\mathfrak{R}$.

Se, per assurdo, $\mathrm{dom}\,(R) \neq X$, esiste $x \in X \setminus \mathrm{dom}\,(R)$. Allora

$$S = R \cup ((\mathrm{dom}\,(R) \cup \{x\}) \times \{x\})$$

è una relazione d'ordine su $\mathrm{dom}\,(S) = \mathrm{dom}\,(R) \cup \{x\}$ che rende $\mathrm{dom}\,(S)$ bene ordinato. Poiché $R \subseteq S$ e $R \neq S$, viene violata la massimalità di R.

Deve quindi risultare $\mathrm{dom}\,(R) = X$, per cui R è una relazione d'ordine su X che rende X bene ordinato. ■

(6.9) Teorema *Sia $(X, \leq)$ bene ordinato e sia $A \subseteq X$ tale che*

$$\forall x \in X : \left(\forall \xi \in X : \ \xi < x \quad \Longrightarrow \quad \xi \in A\right) \qquad \Longrightarrow \quad x \in A\,.$$

Allora $A = X$.

Dimostrazione. Per assurdo, sia $A \neq X$ e sia $x = \min(X \setminus A)$. Per ogni $\xi \in X$ con $\xi < x$, non può essere $\xi \in (X \setminus A)$, per cui $\xi \in A$. Dall'ipotesi segue che $x \in A$, il che è assurdo. ■

Il teorema appena dimostrato sta alla base di una particolare tecnica di dimostrazione. Data una frase aperta $\mathcal{P}(x)$, supponiamo di sapere che

$$\forall x \in X : \left(\forall \xi \in X : \ \xi < x \quad \Longrightarrow \quad \mathcal{P}(\xi)\right) \qquad \Longrightarrow \quad \mathcal{P}(x)\,.$$

Allora si ha

$$\forall x \in X : \ \mathcal{P}(x)\,.$$

Infatti

$$A = \{x \in X : \ \mathcal{P}(x)\}$$

è un sottoinsieme di X conforme al teorema. Ne segue $A = X$, che corrisponde all'affermazione desiderata.

Questo particolare tipo di argomentazione si chiama *dimostrazione per induzione transfinita.*

(6.10) Teorema (di ricorsione transfinita) *Siano $(X, \leq)$ un insieme bene ordinato, Y un insieme e $f : \mathfrak{P}\,(Y) \to Y$ un'applicazione.*

Allora esiste una ed una sola applicazione $\varphi : X \to Y$ tale che

$$\forall x \in X : \ \varphi(x) = f(\varphi(\{\xi \in X : \ \xi < x\}))\,.$$

Dimostrazione. Sia Φ l'insieme delle applicazioni $\psi \subseteq X \times Y$ tali che $\mathrm{dom}\,(\psi)$ è un segmento iniziale in X e

$$\forall x \in \mathrm{dom}\,(\psi) : \ \psi(x) = f(\psi(\{\xi \in X : \ \xi < x\}))\,.$$

Poniamo

$$\varphi = \bigcup \Phi \,.$$

Evidentemente φ è una relazione con $\varphi \subseteq X \times Y$.

Proviamo anzitutto che φ è un'applicazione. Se $\psi_1, \psi_2 \in \Phi$, si tratta di dimostrare che

$$\forall x \in X : \, x \in \mathrm{dom}\,(\psi_1) \cap \mathrm{dom}\,(\psi_2) \implies \psi_1(x) = \psi_2(x) \,.$$

Per questo ragioniamo per induzione transfinita su x. Sia quindi $x \in X$ tale che

$$\xi \in \mathrm{dom}\,(\psi_1) \cap \mathrm{dom}\,(\psi_2) \implies \psi_1(\xi) = \psi_2(\xi)$$

per ogni $\xi \in X$ con $\xi < x$. Dovendo dimostrare che

$$x \in \mathrm{dom}\,(\psi_1) \cap \mathrm{dom}\,(\psi_2) \implies \psi_1(x) = \psi_2(x) \,,$$

possiamo supporre che $x \in \mathrm{dom}\,(\psi_1) \cap \mathrm{dom}\,(\psi_2)$. Allora, per ogni $\xi \in X$ con $\xi < x$, si ha $\xi \in \mathrm{dom}\,(\psi_1) \cap \mathrm{dom}\,(\psi_2)$, perché $\mathrm{dom}\,(\psi_1)$ e $\mathrm{dom}\,(\psi_2)$ sono segmenti iniziali in X. Ne segue $\psi_1(\xi) = \psi_2(\xi)$ per ogni $\xi \in X$ con $\xi < x$, quindi

$$\psi_1(\{\xi \in X : \; \xi < x\}) = \psi_2(\{\xi \in X : \; \xi < x\}) \,,$$

da cui $\psi_1(x) = \psi_2(x)$. Pertanto φ è un'applicazione.

Si verifica facilmente che $\mathrm{dom}\,(\varphi)$ è un segmento iniziale in X e che

$$\forall x \in \mathrm{dom}\,(\varphi) : \; \varphi(x) = f(\varphi(\{\xi \in X : \; \xi < x\})) \,,$$

per cui $\varphi \in \Phi$.

Se, per assurdo, $\mathrm{dom}\,(\varphi) \neq X$, allora esiste $x \in X$ tale che

$$\mathrm{dom}\,(\varphi) = \{\xi \in X : \; \xi < x\} \,.$$

Allora

$$\psi = \varphi \cup \big\{(x, f(\varphi(\{\xi \in X : \; \xi < x\}))\big\}$$

soddisfa $\psi \in \Phi$, per cui $x \in \mathrm{dom}\,(\psi) \subseteq \mathrm{dom}\,(\varphi)$, il che è assurdo. Dal momento che $\mathrm{dom}\,(\varphi) = X$, l'applicazione φ ha i requisiti richiesti.

Per dimostrare l'unicità di φ, supponiamo di avere un'altra applicazione $\tilde{\varphi} : X \to Y$ con le stesse proprietà. Dobbiamo dimostrare che

$$\forall x \in X : \tilde{\varphi}(x) = \varphi(x) .$$

Per questo ragioniamo ancora per induzione transfinita su x. Sia quindi $x \in X$ tale che $\tilde{\varphi}(\xi) = \varphi(\xi)$ per ogni $\xi \in X$ con $\xi < x$. Ne segue

$$\tilde{\varphi}(\{\xi \in X : \ \xi < x\}) = \varphi(\{\xi \in X : \ \xi < x\}) ,$$

da cui $\tilde{\varphi}(x) = \varphi(x)$. Pertanto $\tilde{\varphi} = \varphi$. ■

(6.11) Teorema *Sia $(X, \leq)$ bene ordinato e sia $f : X \to X$ strettamente crescente. Allora si ha*

$$\forall x \in X : \ x \leq f(x) .$$

Dimostrazione. Procediamo per induzione transfinita su x. Sia $x \in X$ tale che

$$\forall \xi \in X : \ \xi < x \quad \Longrightarrow \quad \xi \leq f(\xi)$$

e supponiamo per assurdo che non si abbia $x \leq f(x)$. Essendo l'ordine totale, deve essere $f(x) < x$. Ne segue anzitutto $f(f(x)) < f(x)$, perché f è strettamente crescente. D'altronde risulta anche $f(x) \leq f(f(x))$, perché $\xi = f(x) < x$. Ne segue un assurdo, per cui $x \leq f(x)$. ■

(6.12) Corollario *Sia $(X, \leq)$ bene ordinato, sia S un segmento iniziale in X e sia $f : X \to S$ strettamente crescente.*

Allora risulta $S = X$.

Dimostrazione. Considerando $f : X \to X$, si deduce che $x \leq f(x)$ per ogni $x \in X$. Essendo S un segmento iniziale e $f(x) \in S$, ne segue $x \in S$ per ogni $x \in X$, da cui $S = X$. ■

(6.13) Corollario *Sia* $(X, \leq)$ *bene ordinato e sia* $f : X \to X$ *strettamente crescente e biiettiva.*

Allora $f(x) = x$ *per ogni* $x \in X$*.*

Dimostrazione. Per il Teorema (6.11) risulta $x \leq f(x)$ per ogni $x \in X$. Essendo $\leq$ un ordinamento totale, ne segue che anche f^{-1} è strettamente crescente, per cui $y \leq f^{-1}(y)$ per ogni $y \in X$, che equivale a $f(x) \leq x$ per ogni $x \in X$. Risulta quindi $f(x) = x$ per ogni $x \in X$. ■

(6.14) Corollario *Siano* $(X, \leq)$ *e* $(Y, \leq)$ *bene ordinati e siano* $f, g : X \to Y$ *strettamente crescenti e biiettive.*

Allora $f = g$*.*

Dimostrazione. Si verifica facilmente che $g^{-1} \circ f$ è strettamente crescente e biiettiva da X in X. Ne segue $g^{-1}(f(x)) = x$ per ogni $x \in X$, quindi $f(x) = g(x)$ per ogni $x \in X$. ■

(6.15) Teorema *Siano* $(X, \leq)$ *e* $(Y, \leq)$ *due insiemi bene ordinati. Allora si verifica uno ed uno solo dei seguenti fatti:*

(a) $(X, \leq)$ *e* $(Y, \leq)$ *sono simili;*

(b) *esiste un segmento iniziale* S *in* X*, con* $S \neq X$*, tale che* $(Y, \leq)$ *e* $(S, \leq)$ *sono simili;*

(c) *esiste un segmento iniziale* S *in* Y*, con* $S \neq Y$*, tale che* $(X, \leq)$ *e* $(S, \leq)$ *sono simili.*

Dimostrazione. Il caso in cui $X = \emptyset$ oppure $Y = \emptyset$ è immediato. Supponiamo quindi $X \neq \emptyset$ e $Y \neq \emptyset$. Sia $y_0 = \min Y$ e sia $f : \mathfrak{P}(Y) \to Y$ definita da

$$f(E) = \begin{cases} \min(Y \setminus E) & \text{se } E \neq Y\,, \\ y_0 & \text{se } E = Y\,. \end{cases}$$

Sia $\varphi : X \to Y$ conforme al Teorema di ricorsione transfinita. Di fatto risulta

$$\varphi(x) = \begin{cases} \min(Y \setminus \varphi(\{\xi \in X : \ \xi < x\})) & \text{se } \varphi(\{\xi \in X : \ \xi < x\} \neq Y\,, \\ y_0 & \text{se } \varphi(\{\xi \in X : \ \xi < x\} = Y\,. \end{cases}$$

Osserviamo che, se S è un segmento iniziale in X, allora $\varphi(S)$ è un segmento iniziale in Y. Siano infatti $x \in S$ ed $y \in Y$ con $y \leq \varphi(x)$. Se $y = \varphi(x)$, è ovvio che $y \in \varphi(S)$. Sia quindi $y < \varphi(x)$. Non può essere $\varphi(\{\xi \in X : \ \xi < x\}) = Y$, perché ne seguirebbe $\varphi(x) = y_0 \leq y$. Allora si ha $\varphi(\{\xi \in X : \ \xi < x\}) \neq Y$, per cui

$$\varphi(x) \leq z \qquad \text{per ogni } z \in Y \setminus \varphi(\{\xi \in X : \ \xi < x\})\,.$$

Ne segue

$$y \in \varphi(\{\xi \in X : \ \xi < x\}) \subseteq \varphi(S)\,.$$

In particolare, se $\varphi(\{\xi \in X : \ \xi < x\}) \neq Y$, risulta $\varphi(\xi) < \varphi(x)$ per ogni $\xi < x$.

Se esiste $x \in X$ tale che $\varphi(\{\xi \in X : \ \xi < x\}) = Y$, sia x_0 il minimo elemento di X con tale proprietà. Allora $S = \{\xi \in X : \ \xi < x_0\}$ è un segmento iniziale in X con $S \neq X$. Inoltre $\varphi_{|_S} : S \to Y$ è strettamente crescente e biiettiva, per cui vale l'affermazione (b).

Altrimenti risulta $\varphi(\{\xi \in X : \ \xi < x\}) \neq Y$ per ogni $x \in X$. Ne segue che $\varphi : X \to Y$ è strettamente crescente. Allora $\varphi : X \to \varphi(X)$ è strettamente crescente e biiettiva. Inoltre $\varphi(X)$ è un segmento iniziale in Y. Se $\varphi(X) = Y$, vale l'affermazione (a), altrimenti vale la (c).

Se, per assurdo, valgono sia la (b) che la (c), esistono $f : Y \to S_1$ e $g : X \to S_2$ strettamente crescenti e biiettive con S_1 segmento iniziale in X con $S_1 \neq X$ e S_2 segmento iniziale in Y con $S_2 \neq Y$. Allora $f \circ g : X \to S_1$ è strettamente crescente, per cui $S_1 = X$: assurdo.

In modo simile si verifica che non possono essere vere (a) e (b) contemporaneamente e nemmeno (a) e (c) contemporaneamente. ∎

7 Ordinali

(7.1) Definizione *Un insieme X si dice* ordinale *se*

(a)

$$R = \{(x, y) \in X \times X : \ x \in y \ o \ x = y\}$$

è una relazione d'ordine su X che rende X bene ordinato;

(b) *rispetto a tale relazione d'ordine, risulta*

$$\forall x \in X: \; x = \{\xi \in X: \; \xi < x\} \; .$$

(7.2) Proposizione *Sia X un ordinale. Valgono allora i seguenti fatti:*

(a) *risulta*

$$\forall x: \; x \in X \qquad \Longleftrightarrow \qquad (x \text{ è un segmento iniziale in } X \text{ con } x \neq X) \; ;$$

(b) *per ogni $x \in X$ risulta $x \subseteq X$;*

(c) *ogni $x \in X$ è un ordinale.*

Dimostrazione.
(a) Sia x un segmento iniziale in X con $x \neq X$. Essendo X bene ordinato, risulta

$$x = \{\xi \in X: \; \xi < y\}$$

con $y \in X$. Essendo X un ordinale, ne segue $x = y$, da cui la tesi. Il viceversa è la (b) della definizione di ordinale.

(b) Sia $x \in X$ e sia $\xi \in x$. Allora risulta $\xi \in X$, da cui la tesi.

(c) Sia $x \in X$. Anzitutto risulta $x \subseteq X$ e R ristretta a x è ancora una relazione d'ordine che rende x bene ordinato.

Sia ora $\xi \in x$. Poiché $\xi \in X$, risulta

$$\xi = \{\eta \in X: \; \eta < \xi\} \; .$$

D'altronde da $\eta \in X$ con $\eta < \xi$ e $\xi \in x$ segue $\eta < x$, quindi $\eta \in x$. Allora

$$\{\eta \in X: \; \eta < \xi\} = \{\eta \in x: \; \eta < \xi\} \; ,$$

da cui la tesi. ■

(7.3) Proposizione *Se X è un ordinale, allora*

$$\sigma(X) := X \cup \{X\}$$

è un ordinale con $\sigma(X) \neq X$ *e* $\sigma(X) \notin X$.

Dimostrazione. Per ogni $x \in X$ risulta

$$x \notin \{\xi \in X : \ \xi < x\} = x$$

(anche a prescindere dall'Assioma di regolarità). Non può quindi essere $X \in X$, perché ne seguirebbe $X \notin X$.

Dal momento che $X \notin X$, mentre $X \in \sigma(X)$, risulta $\sigma(X) \neq X$. Inoltre non può essere $\sigma(X) \in X$, perché ne seguirebbe $X \in X$ per transitività.

Si verifica facilmente che $\sigma(X)$ è un ordinale. ■

(7.4) Teorema *Siano* X *e* Y *due ordinali simili. Allora* $X = Y$.

Dimostrazione. Sia $f : X \to Y$ biiettiva e strettamente crescente. Dimostriamo che

$$\forall x \in X : \ f(x) = x\,,$$

ragionando per induzione trasfinita su x.

Sia quindi $x \in X$ tale che $f(\xi) = \xi$ per ogni $\xi \in X$ con $\xi < x$. Se $\xi \in x$, ne segue $\xi \in X$ con $\xi < x$, quindi $\xi = f(\xi) \in Y$ con $\xi = f(\xi) < f(x)$, da cui $\xi \in f(x)$. Risulta quindi

$$x \subseteq f(x)\,.$$

In modo simile si prova l'inclusione opposta, da cui $f(x) = x$. Risulta quindi $Y = \mathrm{img}\,(f) = X$. ■

(7.5) Teorema *Siano* X *e* Y *due ordinali. Allora si verifica uno ed uno solo dei seguenti fatti:*

(a) $X = Y$;

(b) $X \in Y$;

(c) $Y \in X$.

Dimostrazione. Per il Teorema (7.4) si ha $X = Y$ se e solo X e Y sono simili. D'altra parte per la Proposizione (7.2) $S \in X$ se e se solo se S è un segmento iniziale in X con $S \neq X$, nel qual caso anche S è un ordinale. La tesi discende allora dal Teorema (6.15). ■

(7.6) Teorema *Sia $\mathfrak{F}$ un insieme di ordinali. Allora $\bigcup \mathfrak{F}$ è un ordinale e*

$$\mathfrak{F} \subseteq \sigma \left(\bigcup \mathfrak{F}\right) .$$

Dimostrazione. Se $x, y, z \in \bigcup \mathfrak{F}$, si ha $x \in X$, $y \in Y$ e $z \in Z$ con $X, Y, Z \in \mathfrak{F}$. Essendo X, Y, Z ordinali, si avrà ad esempio $X \in Y \in Z$. Ne segue $x, y, z \in Z$, per cui è chiaro che

$$\left\{(u, v) \in \bigcup \mathfrak{F} \times \bigcup \mathfrak{F} : \; u \in v \text{ o } u = v\right\}$$

è una relazione d'ordine su $\bigcup \mathfrak{F}$.

Se E è un sottoinsieme non vuoto di $\bigcup \mathfrak{F}$, sia $x \in E$. Allora $x \in X$ con $X \in \mathfrak{F}$. Sia m il minimo di $E \cap X$. Dal momento che $\xi \in x$ implica $\xi \in X$, risulta che m è anche il minimo di E. Pertanto $\bigcup \mathfrak{F}$ è bene ordinato.

Se infine $x \in \bigcup \mathfrak{F}$, risulta $x \in X$ con $X \in \mathfrak{F}$, quindi con X ordinale, per cui

$$x = \{\xi \in X : \; \xi < x\} .$$

D'altra parte, se $\xi \in \bigcup \mathfrak{F}$ con $\xi < x$, risulta $\xi \in X$, per cui

$$x = \left\{\xi \in \bigcup \mathfrak{F} : \; \xi < x\right\} .$$

Gli altri casi si trattano in modo simile, per cui $\bigcup \mathfrak{F}$ è un ordinale.

Se $\mathfrak{F}$ non ammette massimo, per ogni $X \in \mathfrak{F}$ esiste $Y \in \mathfrak{F}$ con $X \in Y$. Ne segue $X \in \bigcup \mathfrak{F}$, per cui

$$\mathfrak{F} \subseteq \bigcup \mathfrak{F} \subseteq \sigma \left(\bigcup \mathfrak{F}\right) .$$

Se invece $\mathfrak{F}$ ammette M per massimo, per ogni $X \in M$ si ha $X \in \bigcup \mathfrak{F}$, per cui

$$M \subseteq \bigcup \mathfrak{F} .$$

D'altra parte, se $X \in \bigcup \mathfrak{F}$, si ha $X \in Y$ con $Y \in \bigcup \mathfrak{F}$. Ne segue $X \in M$, per cui

$$\bigcup \mathfrak{F} \subseteq M .$$

Risulta quindi

$$M = \bigcup \mathfrak{F}\,.$$

Come in precedenza si ha

$$\{X \in \mathfrak{F} : \; X \neq M\} \subseteq \bigcup \mathfrak{F} \subseteq \sigma\left(\bigcup \mathfrak{F}\right)\,.$$

D'altra parte

$$M \in \left\{\bigcup \mathfrak{F}\right\} \subseteq \sigma\left(\bigcup \mathfrak{F}\right)\,,$$

per cui

$$\mathfrak{F} \subseteq \sigma\left(\bigcup \mathfrak{F}\right)\,.$$

■

(7.7) Teorema *Ogni insieme bene ordinato è simile ad uno ed un solo ordinale.*

Dimostrazione. Sia X bene ordinato. L'unicità segue subito dal Teorema 7.4. Sia ora $\mathcal{R}(S, y)$ la frase aperta

$$S \text{ è un segmento iniziale in } X \text{ ed } y \text{ è un ordinale simile a } S\,.$$

Per il Teorema 7.4, se $\mathcal{R}(S, y_1)$ e $\mathcal{R}(S, y_2)$, risulta $y_1 = y_2$. Per l'assioma di rimpiazzamento, esiste un insieme $\mathfrak{F}$ che ha per elementi esattamente gli ordinali simili a qualche segmento iniziale S in X. Sia

$$Y = \sigma\left(\bigcup \mathfrak{F}\right)\,.$$

Allora Y è un ordinale con $\mathfrak{F} \subseteq Y$.

Dimostriamo che Y non può essere simile ad un segmento iniziale S in X con $S \neq X$. Ragionando per assurdo, sia $f : S \to Y$ biiettiva e strettamente crescente e sia

$$x = \min(X \setminus S)\,.$$

Allora $T = S \cup \{x\}$ è un segmento iniziale in X e $g : T \to \sigma(Y)$, definita da

$$g(\xi) = \begin{cases} f(\xi) & \text{se } \xi \in S\,, \\ Y & \text{se } \xi = x\,, \end{cases}$$

è biiettiva e strettamente crescente. Ne segue $\sigma(Y) \in \mathfrak{F}$, quindi $\sigma(Y) \in Y$, il che è assurdo.

Dal Teorema (6.15) segue allora che X è simile all'ordinale Y oppure ad un segmento iniziale U in Y con $U \neq Y$. Poiché $U \in Y$, anche U è un ordinale. ■

(7.8) Definizione *Due insiemi X e Y si dicono* equipotenti *se esiste $f : X \to Y$ biiettiva.*

(7.9) Teorema *Per ogni insieme X, non esiste nessuna $f : \mathfrak{P}(X) \to X$ iniettiva.*

Dimostrazione. Sia, per assurdo, $f : \mathfrak{P}(X) \to X$ iniettiva. Poniamo

$$Y = \left\{ x \in \mathrm{img}\,(f) : \; x \notin f^{-1}(x) \right\} .$$

Poiché $Y \in \mathfrak{P}(X)$, è chiaro che $f(Y) \in \mathrm{img}\,(f)$. Se $f(Y) \in Y$, allora $f(Y) \notin f^{-1}(f(Y)) = Y$, il che è assurdo. Se invece $f(Y) \notin Y = f^{-1}(f(Y))$, ne segue $f(Y) \in Y$, che è di nuovo assurdo. ■

(7.10) Teorema *Ogni insieme è equipotente ad un ordinale.*

Dimostrazione. Dato un qualunque insieme X, per il Teorema (6.8) esiste un ordinamento che rende X bene ordinato. Per il Teorema (7.7) $(X, \leq)$ è simile ad un ordinale, in particolare equipotente. ■

(7.11) Teorema *Sia X un ordinale. Allora esiste un ordinale $\mathfrak{F}$ tale che, per ogni ordinale Y equipotente a X, risulta $Y \in \mathfrak{F}$.*

Dimostrazione. Sia $\mathfrak{F}$ un ordinale equipotente a $\mathfrak{P}(X)$. Se Y è un ordinale equipotente a X, per il Teorema (7.9) non può essere $Y = \mathfrak{F}$ e nemmeno $\mathfrak{F} \in Y$, che implicherebbe $\mathfrak{F} \subseteq Y$. Deve quindi essere $Y \in \mathfrak{F}$. ■

8 Cardinali

(8.1) Definizione *Un insieme X si dice* cardinale *se:*

(a) *X è un ordinale;*

(b) *per ogni ordinale Y equipotente a X si ha $X \in Y$ oppure $X = Y$.*

(8.2) Teorema *Siano X e Y due cardinali equipotenti. Allora $X = Y$.*

Dimostrazione. Sia $\mathfrak{F} = \{X, Y\}$ e sia $Z = \sigma(\bigcup \mathfrak{F})$. Allora Z è un ordinale con $X \in Z$ e $Y \in Z$. Essendo X e Y cardinali, si ha $X \leq Y$ e $Y \leq X$, da cui $X = Y$. ∎

(8.3) Teorema *Ogni insieme è equipotente ad uno ed un solo cardinale.*

Dimostrazione. L'unicità segue dal teorema precedente. Sia X un insieme. Per il Teorema (7.10) X è equipotente ad un ordinale Y. Inoltre esiste un ordinale $\mathfrak{F}$ per cui si ha $Z \in \mathfrak{F}$ per ogni ordinale Z equipotente a Y. In particolare, $Y \in \mathfrak{F}$. Sia

$$Y_0 = \min \{Z \in \mathfrak{F} : \ Z \text{ è equipotente a } Y\} \ .$$

Allora Y_0 è equipotente a Y, quindi a X, ed è chiaramente un cardinale. ∎

Capitolo 2

Insiemi numerici

1 Numeri naturali

Come vedremo in questa sezione, l'insieme ω dei cardinali finiti fornisce un modello per l'insieme dei numeri naturali.

Poniamo anzitutto

$$0 := \emptyset\,, \qquad 1 := \sigma(\emptyset) = \{\emptyset\}\,.$$

Il teorema di ricorsione consente di definire somma e prodotto in ω in modo che, per ogni $m, n \in \omega$, siano soddisfatte le seguenti proprietà:

$$m + 0 = m\,, \qquad m + (n+1) = (m+n) + 1\,;$$

$$m \cdot 0 = 0\,, \qquad m \cdot (n+1) = m \cdot n + m\,.$$

Più precisamente, fissato $m \in \omega$, si considera l'applicazione $\varphi_m : \omega \to \omega$ tale che

$$\varphi_m(\emptyset) = m\,,$$

$$\forall n \in \omega : \ \varphi_m(\sigma(n)) = \sigma(\varphi_m(n))\,.$$

In altre parole, φ_m si ottiene applicando il Teorema (1.3.8) con $X = \omega$, $f : \omega \times \omega \to \omega$ definita da $f(n,k) = \sigma(k)$ e $x_0 = m$. Si pone poi per definizione

$$m + n := \varphi_m(n)\,.$$

In particolare risulta $m + 1 = \sigma(m)$.

Fissato di nuovo $m \in \omega$, sia $\psi_m : \omega \to \omega$ l'applicazione tale che

$$\psi_m(\emptyset) = \emptyset\,,$$

$$\forall n \in \omega : \psi_m(\sigma(n)) = \psi_m(n) + m\,.$$

In questo caso si tratta di applicare il Teorema (1.3.8) con $X = \omega$, $f : \omega \times \omega \to \omega$ definita da $f(n, k) = k + m$ e $x_0 = \emptyset$. Si pone poi per definizione

$$m \cdot n := \psi_m(n)\,.$$ [1]

(1.1) Teorema *Per ogni $k, m, n \in \omega$ si ha*

$$(k + m) + n = k + (m + n)\,,$$

$$m + n = n + m\,,$$

$$0 + n = n\,,$$

$$k + n = m + n \implies k = m\,,$$

$$(km)n = k(mn)\,,$$

$$mn = nm\,,$$

$$k(m + n) = km + kn\,,$$

$$1 \cdot n = n\,.$$

Dimostrazione. Fissati $k, m \in \omega$, dimostriamo per induzione su n che

$$(k + m) + n = k + (m + n)\,.$$

Per definizione si ha

$$(k + m) + 0 = k + m = k + (m + 0)\,.$$

Supponiamo ora che l'affermazione sia vera per n. Risulta

$$\begin{aligned}(k + m) + (n + 1) &= ((k + m) + n) + 1 = (k + (m + n)) + 1 = \\ &= k + ((m + n) + 1) = k + (m + (n + 1))\,,\end{aligned}$$

da cui la tesi.

Dimostriamo per induzione su n che

$$0 + n = n\,.$$

[1] Quando non vi sia rischio di ambiguità, si usa omettere il punto e scrivere semplicemente mn.

Evidentemente $0+0=0$. Supponiamo che l'affermazione sia vera per n. Risulta

$$0+(n+1)=(0+n)+1=n+1\,,$$

da cui la tesi.

Dimostriamo ora per induzione su n che

$$1+n=n+1\,.$$

Tenuto conto del passo precedente, si ha $1+0=1=0+1$. Supponiamo che l'affermazione sia vera per n. Risulta

$$1+(n+1)=(1+n)+1=(n+1)+1\,,$$

da cui la tesi.

Fissato $m\in\omega$, dimostriamo per induzione su n che

$$m+n=n+m\,.$$

Sappiamo già che $m+0=m=0+m$. Supponiamo che l'affermazione sia vera per n. Tenuto conto del passo precedente, risulta

$$m+(n+1)=(m+n)+1=(n+m)+1=1+(n+m)=(1+n)+m=(n+1)+m\,,$$

da cui la tesi.

Fissati $k,m\in\omega$, dimostriamo per induzione su n che

$$k+n=m+n\implies k=m\,.$$

È evidente che $k+0=m+0$ implica $k=m$. Supponiamo che l'affermazione sia vera per n. Se $k+(n+1)=m+(n+1)$, risulta $(k+n)+1=(m+n)+1$, quindi $k+n=m+n$ perché l'applicazione successivo è iniettiva. Per l'ipotesi induttiva si conclude che $k=m$.

Fissati $k,m\in\omega$, dimostriamo per induzione su n che

$$k(m+n)=km+kn\,.$$

Anzitutto si ha $k(m+0)=km=km+0=km+k\cdot 0$. Supponiamo che l'affermazione sia vera per n. Risulta

$$\begin{aligned}k(m+(n+1))&=k((m+n)+1)=k(m+n)+k=\\&=(km+kn)+k=km+(kn+k)=km+k(n+1)\,,\end{aligned}$$

da cui la tesi.

Fissati $k, m \in \omega$, dimostriamo ora per induzione su n che

$$(k+m)n = kn + mn\,.$$

Anzitutto si ha $(k+m)\cdot 0 = 0 = 0+0 = k\cdot 0 + m\cdot 0$. Supponiamo che l'affermazione sia vera per n. Risulta

$$\begin{aligned}(k+m)(n+1) &= (k+m)n + (k+m) = (kn+mn) + (k+m) = \\ &= (kn+k) + (mn+m) = k(n+1) + m(n+1)\,,\end{aligned}$$

da cui la tesi.

Fissati $k, m \in \omega$, dimostriamo per induzione su n che

$$(km)n = k(mn)\,.$$

Anzitutto si ha $(km)\cdot 0 = 0 = k\cdot 0 = k(m\cdot 0)$. Supponiamo che l'affermazione sia vera per n. Risulta

$$(km)(n+1) = (km)n + km = k(mn) + km = k((mn)+m) = k(m(n+1))\,,$$

da cui la tesi.

Dimostriamo per induzione su n che

$$0\cdot n = 0\,.$$

Evidentemente $0\cdot 0 = 0$. Supponiamo che l'affermazione sia vera per n. Risulta

$$0\cdot(n+1) = (0\cdot n) + 0 = 0 + 0 = 0\,,$$

da cui la tesi.

Dimostriamo ora per induzione su n che

$$1\cdot n = n\,.$$

Anzitutto si ha $1\cdot 0 = 0$. Supponiamo che l'affermazione sia vera per n. Risulta

$$1\cdot(n+1) = (1\cdot n) + 1 = n + 1\,,$$

da cui la tesi.

Fissato $m \in \omega$, dimostriamo per induzione su n che

$$mn = nm\,.$$

Anzitutto si ha $m \cdot 0 = 0 = 0 \cdot m$. Supponiamo che l'affermazione sia vera per n. Risulta

$$m(n+1) = mn + m = nm + 1 \cdot m = (n+1)m\,,$$

da cui la tesi. ■

(1.2) Teorema *Per ogni $m, n \in \omega$, si ha*

$$n = 0 \quad o \quad (\exists k \in \omega : \, n = k+1)\,,$$

$$m + n = 0 \implies m = n = 0\,,$$

$$mn = 0 \implies (m = 0 \ o \ n = 0)\,.$$

Dimostrazione. Poniamo

$$A = \{0\} \cup \sigma(\omega)\,.$$

Evidentemente $0 \in A$ e, per ogni $n \in A$, risulta $\sigma(n) \in A$. Ne segue $A = \omega$, da cui la prima affermazione.

Sia ora $m + n = 0$. Se $n = 0$, risulta anche $m = 0$, da cui la tesi. Se $n \neq 0$, si ha $n = k + 1$ con $k \in \omega$, quindi

$$m + n = m + (k+1) = (m+k) + 1 = 0\,.$$

Ma questo è assurdo, perché 0 non è successivo di alcun numero. La seconda affermazione è quindi dimostrata.

Sia $mn = 0$. Se $n \neq 0$, risulta $n = k + 1$ con $k \in \omega$. Ne segue

$$mn = m(k+1) = mk + m = 0\,.$$

Dall'affermazione precedente si deduce che $m = 0$, da cui la tesi. ■

(1.3) Definizione *Introduciamo una relazione R in ω ponendo*

$$R = \{(m,n) \in \omega \times \omega : \, (\exists k \in \omega : \, n = m + k)\} \, .$$

Scriviamo $m \leq n$ invece di mRn.

(1.4) Teorema *Si ha che $\leq$ è una relazione d'ordine totale in ω e, per ogni $k, m, n \in \omega$, risulta*

$$0 \leq n \, ,$$

$$m \leq n \quad o \quad n+1 \leq m \, ,$$

$$k \leq m \Longrightarrow k+n \leq m+n \, ,$$

$$k \leq m \Longrightarrow kn \leq mn \, .$$

Dimostrazione. È facile verificare che la relazione $\leq$ è riflessiva e transitiva e che

$$0 \leq n \, ,$$

$$k \leq m \Longrightarrow k+n \leq m+n \, ,$$

$$k \leq m \Longrightarrow kn \leq mn \, .$$

Sia $m \leq n$ e $n \leq m$. Siano $h, k \in \omega$ tali che $n = m + h$ e $m = n + k$. Ne segue $n = (n+k) + h = n + (k+h)$, quindi $k + h = 0$, da cui $k = h = 0$. Risulta pertanto $m = n$, ossia vale la proprietà antisimmetrica.

Dimostriamo ora che

$$m \leq n \quad o \quad n+1 \leq m \, .$$

Per questo ragioniamo per induzione su n, considerando la frase aperta

$$\forall m \in \omega : \, m \leq n \quad o \quad n+1 \leq m \, .$$

Per $n = 0$ si ha $m = 0$ oppure $m = 1 + k$ con $k \in \omega$, nel qual caso $1 \leq m$. Supponiamo ora che l'affermazione sia vera per n. Se $m = 0$, è ovvio che $m \leq n+1$. Altrimenti risulta $m = k + 1$ con $k \in \omega$. Per l'ipotesi induttiva, si ha $k \leq n$ oppure $n + 1 \leq k$. Nel primo caso ne segue $m = k + 1 \leq n + 1$, nel secondo $(n+1) + 1 \leq k + 1 = m$. L'affermazione è quindi vera per $n + 1$.

Poiché $n \leq n+1$, si ha in particolare che $\leq$ è una relazione d'ordine totale. ■

(1.5) Teorema *Per ogni $k, m, n \in \omega$ si ha*

$$(kn = mn,\ n \neq 0) \implies k = m\,.$$

Dimostrazione. A meno di scambiare k con m, possiamo supporre che $k \leq m$. Sia $m = k + h$ con $h \in \omega$. Allora risulta $kn = (k+h)n = kn + hn$, da cui $hn = 0$. Poiché $n \neq 0$, deve essere $h = 0$, ossia $k = m$. ■

(1.6) Teorema *Ogni sottoinsieme non vuoto di ω ammette minimo.*

Dimostrazione. Sia B un sottoinsieme non vuoto di ω e sia A l'insieme dei minoranti per B. Se $n \in B$, si ha $n+1 \notin A$, per cui $A \neq \omega$. D'altronde $0 \in A$. Esiste allora $m \in A$ con $m+1 \notin A$. Sia $k \in B$ con $k \leq m$. Risulta allora $m = k \in B$, per cui m è il minimo di B. ■

L'ordinamento introdotto su ω consente di formulare una variante più forte del principio di induzione.

Data una frase aperta $\mathcal{P}(x)$, supponiamo di sapere che le due affermazioni seguenti sono vere:

$$\mathcal{P}(0)\,,$$

$$\forall n \in \omega :\ \Big(\forall k \in \omega :\ k \leq n \implies \mathcal{P}(k)\Big) \implies \mathcal{P}(n+1)\,.$$

Allora si ha

$$\forall n \in \omega :\ \mathcal{P}(n)\,.$$

Denotiamo infatti con $\mathcal{Q}(n)$ la frase aperta

$$n \in \omega \text{ e } \Big(\forall k \in \omega :\ k \leq n \implies \mathcal{P}(k)\Big)\,.$$

Evidentemente si ha

$$\forall n \in \omega :\ \mathcal{Q}(n) \implies \mathcal{P}(n)\,.$$

D'altra parte si può applicare a $\mathcal{Q}$ l'usuale principio di induzione. Ne segue

$$\forall n \in \omega : \mathcal{Q}(n) ,$$

quindi in particolare

$$\forall n \in \omega : \mathcal{P}(n) .$$

(1.7) Definizione *Per ogni $n \in \omega$ poniamo*

$$I_n := \{m \in \omega : m < n\} .$$

(1.8) Teorema *Sia $n \in \omega$ e sia $f : I_n \to I_n$ un'applicazione iniettiva. Allora f è suriettiva.*

Dimostrazione. Ragioniamo per induzione su n. Per $n = 0$ l'affermazione è evidente. Supponiamo ora che sia vera per n e consideriamo $f : I_{n+1} \to I_{n+1}$ iniettiva.

Se $f(n+1) = n+1$, consideriamo $f_{|I_n} : I_n \to I_n$ che è iniettiva, quindi suriettiva. Allora è ovvio che $f : I_{n+1} \to I_{n+1}$ è suriettiva.

Se invece $f(n+1) = k \leq n$, definiamo $g : I_{n+1} \to I_{n+1}$ ponendo

$$g(h) = \begin{cases} n+1 & \text{se } h = k \,, \\ k & \text{se } h = n+1 \,, \\ h & \text{altrimenti} \,. \end{cases}$$

Si verifica facilmente che g è biiettiva e che $(g \circ f) : I_{n+1} \to I_{n+1}$ è iniettiva con $(g \circ f)(n+1) = n+1$. Dal caso precedente segue che $g \circ f$ è suriettiva, per cui anche f è suriettiva. ■

(1.9) Corollario *Siano $m, n \in \omega$ e sia $f : I_m \to I_n$ biiettiva. Allora $m = n$.*

Dimostrazione. A meno si scambiare m con n, possiamo supporre $n \leq m$. Se $m = 0$, la tesi è evidente. Sia quindi $m = k+1$ con $k \in \omega$. Poiché $I_n \subseteq I_m$, risulta che $f : I_m \to I_m$ è iniettiva, quindi suriettiva per il teorema precedente. In particolare $k \in I_n$, ossia $k < n$, da cui $m \leq n$. Ne segue $m = n$. ■

(1.10) Definizione *Un insieme X si dice* finito, *se esistono $n \in \omega$ e $f : I_n \to X$ biiettiva.*

(1.11) Proposizione *Sia X un insieme finito, siamo $m, n \in \omega$ e siano $f : I_m \to X$ e $g : I_n \to X$ due applicazioni biiettive.*

Allora $m = n$.

Dimostrazione. Evidentemente $g^{-1} \circ f : I_m \to I_n$ è biiettiva, per cui $m = n$. ■

(1.12) Definizione *Sia X un insieme finito e siano $n \in \omega$ e $f : I_n \to X$ biiettiva. Diciamo che n è* il numero di elementi *di X.*

(1.13) Teorema *L'insieme ω è un cardinale*

Dimostrazione. Dimostriamo che, per ogni $n \in \omega$, si ha

$$n = I_n = \{m \in \omega : \; m < n\} \,.$$

Ragioniamo per induzione su n. Per $n = 0 = \emptyset$ l'affermazione è vera. Supponiamo che sia vera per un certo $n \in \omega$. Se $m \in \omega$ e $m < n + 1$, allora $m < n$ oppure $m = n$. Ne segue $m \in n \cup \{n\} = n + 1$. Se viceversa $m \in n + 1 = n \cup \{n\}$, allora $m \in n$ oppure $m = n$. Ne segue $m \in \omega$ e $m \leq n < n + 1$.

In particolare, $m \leq n$ se e solo se $m \in n$ oppure $m = n$. Ne segue che ω è un ordinale. Sia ora X un ordinale equipotente ad ω. Non può essere $X = n \in \omega$, altrimenti esisterebbe un'applicazione biiettiva $\omega \to I_n$, quindi un'applicazione $I_n \to I_n$ iniettiva e non suriettiva, in contraddizione con il Teorema (1.8). Deve quindi essere $\omega = X$ oppure $\omega \in X$, per cui ω è un cardinale. ■

(1.14) Teorema *Per ogni X si ha che $X \in \omega$ se e solo se X è un cardinale finito.*

Dimostrazione. Se $X \in \omega$, si ha che X è un ordinale ed è un insieme finito. Se Y è un ordinale equipotente a X, per il Teorema (1.8) non può essere $Y \in X$. Ne segue che X è un cardinale.

Sia viceversa X un cardinale finito. Allora esiste $n \in \omega$ e $f : n \to X$ biiettiva. Essendo anche n un cardinale, deve essere $X = n$. ■

(1.15) Definizione *Un insieme X si dice* al più numerabile, *se esiste un'applicazione suriettiva $f : \omega \to X$.*

(1.16) Teorema *Siano X ed Y due insiemi al più numerabili. Allora $X \times Y$ è al più numerabile.*

Dimostrazione. Sia $g : \omega \times \omega \to \omega \times \omega$ definita da

$$g(m,n) = \begin{cases} (m+1,k) & \text{se } n = k+1\,, \\ (0,m+1) & \text{se } n = 0\,. \end{cases}$$

Sia $f : \omega \to \omega \times \omega$ definita ricorsivamente da

$$f(0) = (0,0)\,,$$

$$\forall h \in \omega : \ f(h+1) = g(f(h))\,.$$

Verifichiamo che f è suriettiva. Anzitutto è chiaro che da $(m,n) = f(h)$ si deduce che $g(m,n) = f(h+1)$. Posto

$$A_j = \{(m,n) \in \omega \times \omega : \ m+n = j\}\,,$$

risulta evidentemente

$$\omega \times \omega = \bigcup_{j \in \omega} A_j\,.$$

Basta quindi dimostrare che $A_j \subseteq f(\omega)$ per ogni $j \in \omega$. Per questo ragioniamo per induzione su j. Ovviamente si ha $A_0 = \{(0,0)\} = \{f(0)\} \subseteq f(\omega)$. Supponiamo ora $A_j \subseteq f(\omega)$ per un certo j e proviamo che $A_{j+1} \subseteq f(\omega)$. Per questo dimostriamo per induzione su m che

$$\forall m \in \omega : \ \left(\forall n \in \omega : \ m+n = j+1 \implies (m,n) \in f(\omega)\right).$$

Risulta anzitutto

$$(0,j+1) = g(j,0) \in g(A_j) \subseteq g(f(\omega)) \subseteq f(\omega)\,,$$

per cui la proprietà è vera per $m = 0$. Supponiamo ora che sia vera per un certo $m \in \omega$ e consideriamo $m+1$. Se $m+1 \geq j+2$, l'implicazione è banalmente vera. Se $m+1 \leq j+1$, ossia $m \leq j$, risulta

$$(m+1, n) = g(m, n+1) \in g(f(\omega)) \subseteq f(\omega)\,,$$

per cui la proprietà è vera per $m+1$. Pertanto $A_{j+1} \subseteq f(\omega)$. Risulta quindi che f è suriettiva.

Per ipotesi esistono due applicazioni suriettive $\varphi : \omega \to X$ e $\psi : \omega \to Y$. Evidentemente è suriettiva anche l'applicazione $\Phi : \omega \times \omega \to X \times Y$ definita da

$$\Phi(m, n) = (\varphi(m), \psi(n))\,.$$

Allora $\Phi \circ f$ è un'applicazione suriettiva da ω su $X \times Y$. ■

(1.17) Teorema *Sia X un'applicazione con* dom $(X) = \omega$. *Supponiamo che per ogni $n \in \omega$ l'insieme X_n sia al più numerabile.*

Allora

$$\bigcup_{n\in\omega} X_n$$

è al più numerabile.

Dimostrazione. Per ogni $n \in \omega$ sia $g_n : \omega \to X_n$ un'applicazione suriettiva. Si verifica facilmente che l'applicazione $G : \omega\times\omega \to \bigcup\limits_{n\in\omega} X_n$ definita da $G(m, n) = g_n(m)$ è suriettiva.

Per il teorema precedente esiste un'applicazione suriettiva $f : \omega \to \omega \times \omega$. Allora $G \circ f$ è un'applicazione suriettiva da ω su $\bigcup\limits_{n\in\omega} X_n$. ■

2 Frazioni

A questo punto introduciamo l'insieme delle frazioni. Definiamo una relazione in

$$\omega \times (\omega \setminus \{0\})$$

ponendo

$$(m_1, m_2)R(n_1, n_2) \iff m_1 n_2 = n_1 m_2 \,.$$

(2.1) Proposizione *Si ha che R è una relazione di equivalenza sull'insieme*

$$\omega \times (\omega \setminus \{0\}) \,.$$

Dimostrazione. È evidente che R è riflessiva e simmetrica. Siano ora

$$(k_1, k_2), (m_1, m_2), (n_1, n_2) \in \omega \times (\omega \setminus \{0\})$$

con $(k_1, k_2)R(m_1, m_2)$ e $(m_1, m_2)R(n_1, n_2)$. Risulta $k_1 m_2 = m_1 k_2$ e $m_1 n_2 = n_1 m_2$, da cui $k_1 n_2 m_2 = m_1 k_2 n_2 = n_1 k_2 m_2$. Poiché $m_2 \neq 0$, dal Teorema (1.5) segue che $k_1 n_2 = n_1 k_2$, ossia $(k_1, k_2)R(n_1, n_2)$. ■

Poniamo

$$\mathbb{F} := \Big(\omega \times (\omega \setminus \{0\})\Big)/R \,.$$

La classe di equivalenza di (m, n) viene usualmente denotata con $\frac{m}{n}$. In particolare, si denota con 0 la classe di equivalenza di $(0, 1)$ e con 1 la classe di equivalenza di $(1, 1)$. Evidentemente risulta $0 \neq 1$.

(2.2) Proposizione *Se $\alpha, \beta \in \mathbb{F}$ ed $\alpha = \frac{m_1}{m_2}$, $\beta = \frac{n_1}{n_2}$, poniamo*

$$\alpha + \beta := \frac{m_1 n_2 + n_1 m_2}{m_2 n_2} \,,$$

$$\alpha \cdot \beta := \frac{m_1 n_1}{m_2 n_2} \,, \text{[2]}$$

$$\textit{se } \alpha \neq 0 \,, \qquad \alpha^{-1} := \frac{m_2}{m_1} \,,$$

Dimostrazione. Siano $\frac{m_1}{m_2} = \frac{m_1'}{m_2'}$ e $\frac{n_1}{n_2} = \frac{n_1'}{n_2'}$. Risulta $m_1 m_2' = m_1' m_2$ e $n_1 n_2' = n_1' n_2$, da cui $m_1 m_2' n_2 n_2' = m_1' m_2 n_2 n_2'$ e $n_1 n_2' m_2 m_2' = n_1' n_2 m_2 m_2'$. Ne segue

$$m_1 m_2' n_2 n_2' + n_1 n_2' m_2 m_2' = m_1' m_2 n_2 n_2' + n_1' n_2 m_2 m_2' \,,$$

ossia

$$\frac{m_1 n_2 + n_1 m_2}{m_2 n_2} = \frac{m_1' n_2' + n_1' m_2'}{m_2' n_2'} \,.$$

Pertanto la definizione di $\alpha + \beta$ è ben posta.

Risulta anche

$$m_1 m_2' n_1 n_2' = m_1' m_2 n_1' n_2 \,,$$

ossia

$$\frac{m_1 n_1}{m_2 n_2} = \frac{m_1' n_1'}{m_2' n_2'} \,,$$

per cui anche $\alpha\beta$ è ben definito.

Infine, se $m_2 \neq 0$ e $m_2' \neq 0$, si ha

$$\frac{m_2}{m_1} = \frac{m_2'}{m_1'} \,,$$

per cui anche α^{-1} è ben definito. ■

Le proprietà fondamentali di $\mathbb{F}$ si possono compendiare nel seguente risultato.

(2.3) Teorema *Valgono i seguenti fatti:*

(a) *per ogni $\alpha, \beta, \gamma \in \mathbb{F}$ si ha*

$$(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma) \,,$$

$$\alpha + \beta = \beta + \alpha \,,$$

$$\alpha + 0 = \alpha \,,$$

$$(\alpha\beta)\gamma = \alpha(\beta\gamma) \,,$$

$$\alpha\beta = \beta\alpha \,,$$

$$(\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma \,,$$

$$\alpha \cdot 1 = \alpha \,,$$

$$\alpha \neq 0 \implies \alpha\alpha^{-1} = 1 \,;$$

(b) *per ogni $\alpha, \beta \in \mathbb{F}$ si verifica una ed una sola delle seguenti eventualità:*

- $\exists \gamma \in \mathbb{F} \setminus \{0\} : \alpha + \gamma = \beta$,
- $\alpha = \beta$,
- $\exists \gamma \in \mathbb{F} \setminus \{0\} : \alpha = \beta + \gamma$;

(*c*) *per ogni* $\alpha, \beta, \gamma \in \mathbb{F}$ *si ha*

$$\alpha + \gamma = \beta + \gamma \implies \alpha = \beta\,.$$

Dimostrazione. Le affermazioni (a) e (b) possono essere dimostrate per esercizio, tenendo conto dei Teoremi (1.1) e (1.4).

Per provare la (c), supponiamo per assurdo che esista $\delta \in \mathbb{F} \setminus \{0\}$ con $\alpha + \delta = \beta$. Ne segue $(\alpha + \gamma) + \delta = \beta + \gamma$, il che è assurdo. Nello stesso modo si esclude che $\alpha = \beta + \delta$. ∎

3 Numeri reali positivi

Descriviamo ora dettagliatamente il passo successivo, che porta all'introduzione dei "numeri reali positivi".

Per ogni $A, B \subseteq \mathbb{F}$ poniamo

$$A + B := \{\alpha + \beta : \alpha \in A,\ \beta \in B\}\ ,$$

$$A \cdot B := \{\alpha\beta : \alpha \in A,\ \beta \in B\}\ .$$ [3]

Poniamo anche

$$\mathbf{0} := \{0\}\,, \qquad \mathbf{1} := \left\{(\gamma + \delta)^{-1}\gamma :\ \gamma \in \mathbb{F}\,,\ \delta \in \mathbb{F} \setminus \{0\}\right\}\ , \qquad \boldsymbol{\infty} := \mathbb{F}\,.$$

Evidentemente risulta $\mathbf{0} \neq \mathbf{1}$, $\mathbf{0} \neq \boldsymbol{\infty}$ e $\mathbf{1} \neq \boldsymbol{\infty}$.

(3.1) Definizione *Poniamo*

$$\overline{\mathbb{P}} = \{A \in \mathfrak{P}(\mathbb{F}) :\ 0 \in A \ \text{ e } \ A \cdot \mathbf{1} = A\}\ .$$

Per ogni $A \in \overline{\mathbb{P}}$ poniamo infine

$$A^{-1} := \left\{\gamma \in \mathbb{F} :\ A \cdot \{\gamma\} \subseteq \mathbf{1}\right\} \cdot \mathbf{1}\,.$$

[3] Anche in questo caso si usa omettere il punto, se non v'è rischio di ambiguità.

(3.2) Lemma *Sia $A \in \overline{\mathbb{P}}$ con $A \neq \mathbf{0}$ e $A \neq \infty$. Allora, per ogni $\varphi \in \mathbf{1}$, esiste $\beta \in \mathbb{F} \setminus A$ tale che $\varphi\beta \in A$.*

Dimostrazione. Sia $\varphi \in \mathbf{1}$ e sia $\beta_0 \in \mathbb{F} \setminus A$. Se $\varphi = 0$, si ha immediatamente $\varphi\beta_0 \in A$. Se invece $\varphi \neq 0$, sarà

$$\varphi = (\gamma + \delta)^{-1}\gamma$$

con $\gamma, \delta \in \mathbb{F} \setminus \{0\}$. Ne segue

$$\varphi^{-1} = 1 + \varepsilon$$

con $\varepsilon = \gamma^{-1}\delta$.

Sia $\alpha \in A \setminus \{0\}$. Osserviamo che esiste $n \in \omega$ tale che $\alpha(1 + \frac{n}{1}\,\varepsilon) \notin A$. Siano infatti $\alpha = \frac{m_1}{m_2}$, $\varepsilon = \frac{k_1}{k_2}$ e $\beta_0 = \frac{h_1}{h_2}$. Risulta

$$\alpha\left(1 + \frac{n}{1}\,\varepsilon\right) = \frac{m_1}{m_2}\left(1 + \frac{nk_1}{k_2}\right) = \frac{m_1}{m_2} + \frac{nm_1k_1}{m_2k_2} = \frac{m_1}{m_2} + \frac{nm_1k_1h_2}{m_2k_2h_2}\,.$$

Se scegliamo $n = m_2k_2h_1$, si ha

$$\alpha\left(1 + \frac{n}{1}\,\varepsilon\right) = \frac{m_1}{m_2} + \frac{m_1k_1h_2h_1}{h_2} = \frac{h_1}{h_2}(1 + \sigma)$$

per un'opportuna $\sigma \in \mathbb{F} \setminus \{0\}$. Risulta allora $\alpha(1 + \frac{n}{1}\,\varepsilon) \notin A$, altrimenti si avrebbe

$$\beta_0 = \frac{h_1}{h_2} = \left[\alpha\left(1 + \frac{n}{1}\,\varepsilon\right)\right](1 + \sigma)^{-1} \in A \cdot \mathbf{1} = A\,.$$

Sia ora

$$m = \min\left\{n \in \omega :\, \alpha\left(1 + \frac{n}{1}\,\varepsilon\right) \notin A\right\}\,.$$

Poiché $m \neq 0$, sarà $m = k + 1$ con $k \in \omega$. Risulta quindi

$$\alpha\left(1 + \frac{k}{1}\,\varepsilon\right) \in A\,,$$
$$\alpha\left(1 + \frac{k+1}{1}\,\varepsilon\right) \notin A\,.$$

Ne segue

$$\alpha\left(1 + \frac{k}{1}\,\varepsilon\right)(1 + \varepsilon) = \alpha\left(1 + \frac{k+1}{1}\,\varepsilon\right) + \alpha\frac{k}{1}\,\varepsilon \cdot \varepsilon \notin A\,,$$

da cui la tesi con $\beta = \alpha\left(1 + \frac{k}{1}\,\varepsilon\right)(1 + \varepsilon)$. ■

(3.3) Teorema *Risulta*

$$\mathbf{0} \in \overline{\mathbb{P}}\,, \qquad \mathbf{1} \in \overline{\mathbb{P}}\,, \qquad \infty \in \overline{\mathbb{P}}\,.$$

Inoltre per ogni $A, B, C \in \overline{\mathbb{P}}$ *si ha*

$$A + B \in \overline{\mathbb{P}}\,, \qquad AB \in \overline{\mathbb{P}}\,, \qquad A^{-1} \in \overline{\mathbb{P}}\,,$$

$$(A + B) + C = A + (B + C)\,,$$

$$A + B = B + A\,,$$

$$A + \mathbf{0} = A\,,$$

$$A + \infty = \infty\,,$$

$$(AB)C = A(BC)\,,$$

$$AB = BA\,,$$

$$(A + B)C = AC + BC\,,$$

$$A \cdot \mathbf{0} = \mathbf{0}\,,$$

$$A \cdot \mathbf{1} = A\,,$$

$$A \neq \mathbf{0} \implies A \cdot \infty = \infty\,,$$

$$A \notin \{\mathbf{0}, \infty\} \implies AA^{-1} = \mathbf{1}\,,$$

$$\mathbf{0}^{-1} = \infty\,, \qquad \infty^{-1} = \mathbf{0}\,.$$

Dimostrazione. Si verifica facilmente che, per ogni $A, B, C \subseteq \mathbb{F}$ con $0 \in A$, risulta

$$(A + B) + C = A + (B + C)\,,$$

$$A + B = B + A\,,$$

$$A + \mathbf{0} = A\,,$$

$$A + \infty = \infty\,,$$

$$(AB)C = A(BC)\,,$$

$$AB = BA\,,$$

$$A \cdot \mathbf{0} = \mathbf{0}\,,$$

$$A \neq \mathbf{0} \implies A \cdot \boldsymbol{\infty} = \boldsymbol{\infty}\,,$$

$$\mathbf{0}^{-1} = \boldsymbol{\infty}\,, \qquad \boldsymbol{\infty}^{-1} = \mathbf{0}\,.$$

In particolare, si ha $\mathbf{0}, \boldsymbol{\infty} \in \overline{\mathbb{P}}$.

Se $\beta, \gamma \in \mathbb{F}$ e $\delta, \varepsilon \in \mathbb{F} \setminus \{0\}$, si ha

$$(\beta + \delta)^{-1}\beta(\gamma + \varepsilon)^{-1}\gamma = [\beta\gamma + (\gamma\delta + \beta\varepsilon + \delta\varepsilon)]^{-1}\,\beta\gamma$$

con $\gamma\delta + \beta\varepsilon + \delta\varepsilon \neq 0$, da cui $\mathbf{1} \cdot \mathbf{1} \subseteq \mathbf{1}$. D'altronde risulta anche

$$(\gamma + \delta)^{-1}\gamma = \left[\left(\gamma + \frac{\delta}{2}\right)^{-1}\gamma\right]\left(1 + \frac{\delta}{2\gamma + \delta}\right)^{-1}\,,$$

per cui $\mathbf{1} \subseteq \mathbf{1} \cdot \mathbf{1}$. Pertanto risulta $\mathbf{1} \in \overline{\mathbb{P}}$. Inoltre, per definizione, si ha $A \cdot \mathbf{1} = A$ per ogni $A \in \overline{\mathbb{P}}$.

Siano ora $A, B, C \in \overline{\mathbb{P}}$. Se $(\alpha + \beta) \in A + B$ con $\alpha \in A$, $\beta \in B$ e $\gamma \in C$, risulta $\alpha\gamma \in AC$ e $\beta\gamma \in BC$, per cui

$$(\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma \in AC + BC\,.$$

Pertanto $(A + B)C \subseteq AC + BC$. Viceversa, consideriamo $\alpha\gamma_1 \in AC$ e $\beta\gamma_2 \in BC$ con $\alpha \in A$, $\beta \in B$ e $\gamma_1, \gamma_2 \in C$. Se $\gamma_1 = \gamma_2$, si ha banalmente

$$\alpha\gamma_1 + \beta\gamma_2 = (\alpha + \beta)\gamma_1 \in (A + B)C\,.$$

Se invece $\gamma_1 = \gamma_2 + \delta$ con $\delta \in \mathbb{F} \setminus \{0\}$, si ha

$$\alpha\gamma_1 + \beta\gamma_2 = \left(\alpha + \beta\frac{\gamma_2}{\gamma_2 + \delta}\right)\gamma_1 \in (A + B \cdot \mathbf{1})\,C = (A + B)\,C\,.$$

Se infine $\gamma_2 = \gamma_1 + \delta$, si prova in maniera simile che $\alpha\gamma_1 + \beta\gamma_2 \in (A + B)C$. Pertanto in ogni caso $AC + BC \subseteq (A + B)C$. Dall'assioma di estensionalità si deduce che

$$(A + B)C = AC + BC\,.$$

Se $A, B \in \overline{\mathbb{P}}$, dalle formule

$$(A + B) \cdot \mathbf{1} = A \cdot \mathbf{1} + B \cdot \mathbf{1} = A + B\,,$$

$$(AB) \cdot \mathbf{1} = A(B \cdot \mathbf{1}) = AB\,,$$

$$\begin{aligned}\left(\left\{\gamma \in \mathbb{F} :\ A \cdot \{\gamma\} \subseteq \mathbf{1}\right\} \cdot \mathbf{1}\right) \cdot \mathbf{1} = \left\{\gamma \in \mathbb{F} :\ A \cdot \{\gamma\} \subseteq \mathbf{1}\right\} \cdot (\mathbf{1} \cdot \mathbf{1}) = \\ = \left\{\gamma \in \mathbb{F} :\ A \cdot \{\gamma\} \subseteq \mathbf{1}\right\} \cdot \mathbf{1}\end{aligned}$$

segue che $A + B \in \overline{\mathbb{P}}$, $AB \in \overline{\mathbb{P}}$ e $A^{-1} \in \overline{\mathbb{P}}$. È anche evidente che

$$\begin{aligned}A \cdot A^{-1} = A \cdot \left(\left\{\gamma \in \mathbb{F} :\ A \cdot \{\gamma\} \subseteq \mathbf{1}\right\} \cdot \mathbf{1}\right) = \\ = \left(A \cdot \left\{\gamma \in \mathbb{F} :\ A \cdot \{\gamma\} \subseteq \mathbf{1}\right\}\right) \cdot \mathbf{1} \subseteq \mathbf{1} \cdot \mathbf{1} = \mathbf{1}\,.\end{aligned}$$

Supponiamo ora $A \neq \mathbf{0}$ e $A \neq \infty$. Sia $\varphi \in \mathbf{1}$. Per il Lemma (3.2), esiste $\beta \in \mathbb{F} \setminus A$ tale che $\varphi\beta \in A$. Per ogni $\alpha \in A$, non può essere $\alpha = \beta + \delta$ con $\delta \in \mathbb{F} \setminus \{0\}$, perché ne seguirebbe

$$\beta = \alpha\left[(\beta + \delta)^{-1}\beta\right] \in A \cdot \mathbf{1} = A\,.$$

Risulta quindi $\beta = \alpha + \delta$ con $\delta \in \mathbb{F} \setminus \{0\}$, da cui

$$\alpha\beta^{-1} = (\alpha + \delta)^{-1}\alpha \in \mathbf{1}\,.$$

Pertanto $A \cdot \{\beta^{-1}\} \subseteq \mathbf{1}$. Ne segue

$$\varphi = (\varphi\beta)\beta^{-1} \in A \cdot \left\{\gamma \in \mathbb{F} :\ A \cdot \{\gamma\} \subseteq \mathbf{1}\right\},$$

quindi

$$\mathbf{1} \subseteq A \cdot \left\{\gamma \in \mathbb{F} :\ A \cdot \{\gamma\} \subseteq \mathbf{1}\right\}.$$

Allora si ha

$$\mathbf{1} = \mathbf{1} \cdot \mathbf{1} \subseteq A \cdot \left\{\gamma \in \mathbb{F} :\ A \cdot \{\gamma\} \subseteq \mathbf{1}\right\} \cdot \mathbf{1} = A \cdot A^{-1}\,,$$

per cui $AA^{-1} = \mathbf{1}$. ■

Definiamo una relazione in $\overline{\mathbb{P}}$, ponendo per ogni $A, B \in \overline{\mathbb{P}}$

$$A \leq B \iff A \subseteq B\,.$$

(3.4) Teorema *Valgono i seguenti fatti:*

(*a*) *$\leq$ è una relazione d'ordine totale in $\overline{\mathbb{P}}$ e per ogni $A, B, C \in \overline{\mathbb{P}}$ si ha*

$$\mathbf{0} \leq A \leq \infty\,;$$

$$A \leq B \implies A + C \leq B + C\,,$$

$$A \leq B \implies AC \leq BC\,;$$

(*b*) *per ogni $A, B, C \in \overline{\mathbb{P}}$ con $C \neq \infty$, si ha*

$$A + C \leq B + C \implies A \leq B\,;$$

(*c*) *per ogni $A, B \in \overline{\mathbb{P}}$ con $A \neq B$, si verifica una ed una sola delle seguenti eventualità:*

- *esiste uno ed un solo $C \in \overline{\mathbb{P}} \setminus \{\mathbf{0}\}$ tale che $B = A + C$,*
- *esiste uno ed un solo $C \in \overline{\mathbb{P}} \setminus \{\mathbf{0}\}$ tale che $A = B + C$;*

(*d*) *se $\mathcal{A}$ e $\mathcal{B}$ sono due sottoinsiemi non vuoti di $\overline{\mathbb{P}}$ ed $A \leq B$ per ogni $A \in \mathcal{A}$ e $B \in \mathcal{B}$, risulta che esiste $C \in \overline{\mathbb{P}}$ tale che $A \leq C \leq B$ per ogni $A \in \mathcal{A}$ e $B \in \mathcal{B}$.*

Dimostrazione.
(*a*) Dal Teorema (1.1.1) e dall'assioma di estensionalità si deduce che $\leq$ è una relazione d'ordine. È evidente che $\mathbf{0} \leq A \leq \infty$.

Supponiamo che non si abbia $A \leq B$. Sia quindi $\alpha \in A \setminus B$. Per ogni $\beta \in B$ deve essere $\alpha = \beta + \delta$ con $\delta \in \mathbb{F} \setminus \{0\}$, da cui $\beta \in A$. Pertanto $B \subseteq A$, ossia $B \leq A$. Risulta quindi che $\leq$ è una relazione d'ordine totale in $\overline{\mathbb{P}}$.

Sia ora $A \leq B$ e sia $(\alpha + \gamma) \in A + C$ con $\alpha \in A$ e $\gamma \in C$. Poiché $A \subseteq B$, risulta $\alpha \in B$, quindi $(\alpha + \gamma) \in B + C$. Pertanto $A + C \subseteq B + C$, ossia $A + C \leq B + C$. In maniera analoga si prova che $AC \leq BC$.
(*b*) Siano anzitutto $A, B \in \overline{\mathbb{P}}$ tali che $A + \mathbf{1} \leq B + \mathbf{1}$. Sia, per assurdo, $B \leq A$ con $B \neq A$. Tenuto conto che $A = A \cdot \mathbf{1}$, esistono $\alpha \in A \setminus B$ e $\delta \in \mathbb{F} \setminus \{0\}$ con $\alpha(1 + \delta) \in A$. Allora risulta

$$\alpha(1 + \delta) + (1 + \alpha\delta)^{-1} \in A + \mathbf{1} \subseteq B + \mathbf{1}\,,$$

per cui esistono $\beta \in B$ e $\varphi \in \mathbf{1}$ tali che

$$\beta + \varphi = \alpha(1 + \delta) + (1 + \alpha\delta)^{-1} = \alpha + 1 + (1 + \alpha\delta)^{-1}(\alpha\delta)^2\,.$$

Se $\varepsilon \in \mathbb{F} \setminus \{0\}$ soddisfa $\varphi + \varepsilon = 1$, ne segue

$$\beta + 1 = \beta + \varphi + \varepsilon = \alpha + 1 + (1 + \alpha\delta)^{-1}(\alpha\delta)^2 + \varepsilon\,,$$

per cui

$$\alpha + (1 + \alpha\delta)^{-1}(\alpha\delta)^2 + \varepsilon = \beta\,.$$

Poiché $B \cdot \mathbf{1} = B$, risulta $\alpha \in B$, il che è assurdo.

Sia ora $A + C \leq B + C$ con $C \neq \infty$. Se $C = 0$, l'affermazione è evidente. Altrimenti ne segue $C^{-1}A + \mathbf{1} \leq C^{-1}B + \mathbf{1}$. Dal passo precedente si deduce che $C^{-1}A \leq C^{-1}B$, da cui $A \leq B$.

(c) Sia anzitutto $B \in \overline{\mathbb{P}}$ tale che $\mathbf{1} \leq B$. Dimostriamo che esiste $C \in \overline{\mathbb{P}}$ tale che $\mathbf{1} + C = B$. Per questo poniamo

$$C = \Big\{\gamma \in \mathbb{F} :\, \mathbf{1} + \{\gamma\} \subseteq B\Big\} \cdot \mathbf{1}\,.$$

Si verifica facilmente che $C \in \overline{\mathbb{P}}$ ed è chiaro che

$$\mathbf{1} + \Big\{\gamma \in \mathbb{F} :\, \mathbf{1} + \{\gamma\} \subseteq B\Big\} \subseteq B\,.$$

Per ogni $\gamma \neq 0$ con $\mathbf{1} + \{\gamma\} \subseteq B$ e $\varphi_1, \varphi_2 \in \mathbf{1}$, risulta anzitutto $1 = \varphi_2 + \varepsilon$ con $\varepsilon \neq 0$. Ne segue

$$\varphi_1 + \gamma\varphi_2 = (\varphi_1 + \gamma)[(\varphi_1 + \gamma\varphi_2 + \gamma\varepsilon)^{-1}(\varphi_1 + \gamma\varphi_2)] \in B \cdot \mathbf{1} = B\,,$$

per cui

$$\mathbf{1} + C \subseteq B\,.$$

Viceversa, è ovvio che $B \cap \mathbf{1} \subseteq \mathbf{1} \subseteq \mathbf{1} + C$, per cui

$$(B \cap \mathbf{1}) \cdot \mathbf{1} \subseteq (\mathbf{1} + C) \cdot \mathbf{1} = \mathbf{1} + C\,.$$

Sia $\beta \in B \setminus \mathbf{1}$. Non può essere $1 = \beta + \delta$ con $\delta \in \mathbb{F} \setminus \{0\}$, perché ne seguirebbe

$$\beta = (\beta + \delta)^{-1}\beta \in \mathbf{1}\,.$$

Deve quindi essere $\beta = 1 + \delta$ con $\delta \in \mathbb{F}$. Allora, per ogni $\varphi \in \mathbf{1}$, risulta $1 = \varphi + \varepsilon$ con $\varepsilon \neq 0$, quindi

$$\varphi + \delta = \beta\left[(\varphi + \delta + \varepsilon)^{-1}(\varphi + \delta)\right] \in B \cdot \mathbf{1} = B\,,$$

per cui

$$\delta \in \left\{\gamma \in \mathbb{F} : \mathbf{1} + \{\gamma\} \subseteq B\right\}.$$

Ne segue

$$\beta = 1 + \delta \in \{1\} + \left\{\gamma \in \mathbb{F} : \mathbf{1} + \{\gamma\} \subseteq B\right\},$$

quindi

$$B \setminus \mathbf{1} \subseteq \{1\} + \left\{\gamma \in \mathbb{F} : \mathbf{1} + \{\gamma\} \subseteq B\right\},$$

da cui

$$(B \setminus \mathbf{1}) \cdot \mathbf{1} \subseteq \mathbf{1} + C\,.$$

Pertanto $B = \mathbf{1} + C$.

Consideriamo ora $A, B \in \overline{\mathbb{P}}$ con $A \neq B$. Si verifica una ed una sola delle due possibilità $A \leq B$ o $B \leq A$. Se $A \leq B$, dimostriamo che esiste $C \in \overline{\mathbb{P}}$ tale che $B = A + C$. Ovviamente risulta $A \neq \infty$ e dovrà essere automaticamente $C \neq \mathbf{0}$.

Se $A = \mathbf{0}$, si ha subito $C = B$. Altrimenti risulta $\mathbf{1} \leq A^{-1}B$. Per il passo precedente esiste $D \in \overline{\mathbb{P}}$ tale che $\mathbf{1} + D = A^{-1}B$, da cui $A + C = B$ con $C = AD$.

Il caso $B \leq A$ (ed $A \neq B$) si tratta in modo simile. Inoltre dalla (b) segue che C è unico e che le due affermazioni

$$\begin{aligned} B &= A + C \qquad \text{con } C \in \overline{\mathbb{P}} \setminus \{\mathbf{0}\}\,, \\ A &= B + C \qquad \text{con } C \in \overline{\mathbb{P}} \setminus \{\mathbf{0}\}\,, \end{aligned}$$

non possono essere vere contemporaneamente.

(d) Poniamo

$$C = \bigcup \mathcal{A}\,.$$

Si verifica facilmente che $C \in \overline{\mathbb{P}}$.

Per ogni $A \in \mathcal{A}$ si ha ovviamente $A \subseteq C$, ossia $A \leq C$. D'altronde per ogni $\gamma \in C$ esiste $A \in \mathcal{A}$ tale che $\gamma \in A$. Per ogni $B \in \mathcal{B}$ risulta $A \subseteq B$, da cui $\gamma \in B$. Pertanto $C \subseteq B$, ossia $C \leq B$. ■

4 Numeri reali

A questo punto possiamo finalmente introdurre l'insieme dei numeri reali. Poniamo

$$\overline{\mathbb{R}} := \left\{(A,B) \in \overline{\mathbb{P}} \times \overline{\mathbb{P}} :\ A = \mathbf{0} \text{ o } B = \mathbf{0}\right\} ,$$

$$0 := (\mathbf{0},\mathbf{0}) , \qquad 1 := (\mathbf{1},\mathbf{0}) , \qquad -\infty := (\mathbf{0},\infty) , \qquad +\infty := (\infty,\mathbf{0}) .$$

Evidentemente si tratta di quattro elementi tutti diversi fra loro. Definiamo un'applicazione

$$\pi : (\overline{\mathbb{P}} \times \overline{\mathbb{P}}) \setminus \{(\infty,\infty)\} \to \overline{\mathbb{R}}$$

ponendo

$$\pi(A,B) = \begin{cases} (\mathbf{0},C) & \text{se } A + C = B \text{ con } C \in \overline{\mathbb{P}} \setminus \{\mathbf{0}\} , \\ (\mathbf{0},\mathbf{0}) & \text{se } A = B , \\ (C,\mathbf{0}) & \text{se } A = B + C \text{ con } C \in \overline{\mathbb{P}} \setminus \{\mathbf{0}\} . \end{cases}$$

Se $x = (A,B) \in \overline{\mathbb{R}}$ ed $y = (C,D) \in \overline{\mathbb{R}}$ con $(x,y) \neq (-\infty,+\infty)$ e $(x,y) \neq (+\infty,-\infty)$, poniamo

$$x + y := \pi(A + C, B + D) .$$

Per ogni $x = (A,B) \in \overline{\mathbb{R}}$ ed $y = (C,D) \in \overline{\mathbb{R}}$ poniamo anche

$$x \cdot y := (AC + BD, AD + BC) ,$$ [4]

$$-x := (B,A) .$$

Se $x \neq 0$, poniamo infine

$$x^{-1} := \begin{cases} (\mathbf{0},B^{-1}) & \text{se } A = 0 , \\ (A^{-1},\mathbf{0}) & \text{se } B = 0 . \end{cases}$$

Definiamo una relazione $\leq$ in $\overline{\mathbb{R}}$ ponendo

$$x \leq y \iff A + D \leq B + C .$$

Poniamo

$$\mathbb{R} := \overline{\mathbb{R}} \setminus \{-\infty,+\infty\} .$$

Enunciamo senza dimostrazione le proprietà principali dell'insieme $\mathbb{R}$.

(4.1) Teorema *Valgono i seguenti fatti:*

[4] Anche in questo caso ometteremo il punto, scrivendo semplicemente xy, quando non vi sia ambiguità.

(a) *per ogni* $x, y, z \in \mathbb{R}$ *risulta*

$$(x + y) + z = x + (y + z)\,,$$

$$x + y = y + x\,,$$

$$x + 0 = x\,,$$

$$x + (-x) = 0\,,$$

$$(xy)z = x(yz)\,,$$

$$xy = yx\,,$$

$$(x + y)z = xz + yz\,,$$

$$x \cdot 1 = x\,,$$

$$x \neq 0 \implies xx^{-1} = 1\,;$$

(b) $\leq$ *è una relazione d'ordine totale in* $\mathbb{R}$ *e per ogni* $x, y, z \in \mathbb{R}$ *risulta*

$$x \leq y \implies x + z \leq y + z\,,$$

$$(x \leq y \text{ e } 0 \leq z) \implies xz \leq yz\,;$$

(c) **(Principio di Dedekind)** *se* X *ed* Y *sono due sottoinsiemi non vuoti di* $\mathbb{R}$ *tali che* $x \leq y$ *per ogni* $x \in X$ *ed* $y \in Y$*, esiste* $z \in \mathbb{R}$ *tale che* $x \leq z \leq y$ *per ogni* $x \in X$ *ed* $y \in Y$.

5 I numeri naturali nell'ambito dei reali

(5.1) Teorema *Esiste uno ed un solo insieme* $\mathbb{N} \subseteq [0, +\infty[$ *tale che*

$$0 \in \mathbb{N}\,, \tag{5.2}$$

$$\forall n : \; n \in \mathbb{N} \implies (n + 1) \in \mathbb{N}\,, \tag{5.3}$$

(5.4) $$\forall n : n \in \mathbb{N} \Longrightarrow]n, n+1[\cap \mathbb{N} = \emptyset \,.$$

Dimostrazione. Sia $\mathcal{P}(x)$ la frase aperta

$$\forall A : \; (A \subseteq [0, +\infty[, \; A \text{ soddisfa } (5.2) \text{ e } (5.3)) \Longrightarrow x \in A$$

e sia

$$\mathbb{N} = \{x \in \mathbb{R} : \mathcal{P}(x)\} \;.$$

Si verifica facilmente che $\mathbb{N}$ soddisfa la (5.2) e la (5.3). Per costruzione $\mathbb{N}$ è il più piccolo sottoinsieme di $[0, +\infty[$ con tali proprietà, per cui risulta anche

(5.5) $$\forall A : \; \big(A \subseteq \mathbb{N} \text{ soddisfa } (5.2) \text{ e } (5.3)\big) \Longrightarrow A = \mathbb{N} \,.$$

Sia ora $A = \mathbb{N} \setminus]0, 1[$. Evidentemente $0 \in A$ e $(n+1) \in A$ ogniqualvolta $n \in A$. Pertanto $A = \mathbb{N}$, ossia $]0, 1[\cap \mathbb{N} = \emptyset$.

Consideriamo ora un $n \in \mathbb{N}$ tale che $]n, n+1[\cap \mathbb{N} = \emptyset$. Posto $B = \mathbb{N} \setminus]n+1, n+2[$, si ha ovviamente $0 \in B$. Inoltre, se $m \in B$, si ha $m \leq n$ oppure $m \geq n+1$, da cui in ogni caso $m + 1 \in B$. Pertanto $B = \mathbb{N}$, ossia $]n+1, n+2[\cap \mathbb{N} = \emptyset$.

Se poniamo

$$C = \{n \in \mathbb{N} :]n, n+1[\cap \mathbb{N} = \emptyset\} \;,$$

possiamo dire che $0 \in C$ e che $(n+1) \in C$ ogniqualvolta $n \in C$. Ne segue $C = \mathbb{N}$, per cui $\mathbb{N}$ soddisfa anche la (5.4).

Infine, sia $\mathbb{N}'$ un altro sottoinsieme di $\mathbb{R}$ verificante le (5.2), (5.3) e (5.4). Ne segue che anche per $\mathbb{N}'$ vale la (5.5). Consideriamo allora $A = \mathbb{N} \cap \mathbb{N}'$. Si ha $0 \in A$ e da $n \in A$ segue $n + 1 \in A$. Pertanto $A = \mathbb{N}$, ossia $\mathbb{N} \subseteq \mathbb{N}'$. Analogamente risulta anche $\mathbb{N}' \subseteq \mathbb{N}$, per cui $\mathbb{N}' = \mathbb{N}$. ■

Ricordiamo che gli elementi di $\mathbb{N}$ si chiamano *numeri naturali*, per cui $\mathbb{N}$ è l'insieme dei numeri naturali.

(5.6) Teorema *Valgono i seguenti fatti:*

(a) ogni sottoinsieme non vuoto di $\mathbb{N}$ *ammette minimo;*

(b) ogni sottoinsieme di $\mathbb{N}$ *non vuoto e limitato superiormente ammette massimo;*

(c) *per ogni* $m, n \in \mathbb{N}$ *si ha* $m + n \in \mathbb{N}$ *e* $mn \in \mathbb{N}$.

Dimostrazione.
(a) Sia X un sottoinsieme non vuoto di $\mathbb{N}$ e sia $a = \inf X$. Evidentemente risulta $a \geq 0$. Poiché $a + 1 > a$, esiste $n \in X$ tale che $n < a + 1$. Naturalmente si ha $a \leq n$. Deve risultare $a = n$, perché da $a < n$ segue che esiste $m \in X$ con $m < n$. Poiché $a \leq m$, risulta $n < a + 1 \leq m + 1$, quindi $n \in]m, m + 1[$, il che è assurdo. In conclusione, si ha $n \in X$ e $n = \inf X$, per cui $n = \min X$.
(b) Si tratta di una semplice variante della dimostrazione precedente.
(c) Fissato $m \in \mathbb{N}$, consideriamo

$$A_m = \{n \in \mathbb{N} : \, m + n \in \mathbb{N}\} \, .$$

Evidentemente $0 \in A_m$. Inoltre, se $n \in A_m$, risulta

$$m + (n + 1) = (m + n) + 1 \in \mathbb{N} \, ,$$

per cui $n + 1 \in A_m$. Ne segue $A_m = \mathbb{N}$, ossia $m + n \in \mathbb{N}$ per ogni $n \in \mathbb{N}$.

Ragionando sull'insieme

$$B_m = \{n \in \mathbb{N} : \, mn \in \mathbb{N}\}$$

e tenendo conto che

$$m(n + 1) = mn + m \, ,$$

si deduce in maniera simile che $mn \in \mathbb{N}$ per ogni $n \in \mathbb{N}$. ∎

6 Insiemi numerici al più numerabili

(6.1) Teorema *L'insieme* $\mathbb{Z}$ *è al più numerabile.*

Dimostrazione. Per definizione di $\mathbb{Z}$ si ha che l'applicazione $g : \mathbb{N} \times \mathbb{N} \to \mathbb{Z}$ definita da $g(m, n) = m - n$ è suriettiva. D'altronde per il Teorema (1.16) esiste un'applicazione suriettiva $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$. Allora $g \circ f$ è un'applicazione suriettiva da $\mathbb{N}$ su $\mathbb{Z}$. ∎

(6.2) Teorema *L'insieme $\mathbb{Q}$ è al più numerabile.*

Dimostrazione. Per definizione di $\mathbb{Q}$ si ha che l'applicazione $g : \mathbb{Z}\times(\mathbb{Z}\setminus\{0\}) \to \mathbb{Q}$ definita da $g(m,n) = m/n$ è suriettiva.

Per il teorema precedente esiste un'applicazione suriettiva $\varphi : \mathbb{N} \to \mathbb{Z}$. Allora l'applicazione $\psi : \mathbb{N} \to \mathbb{Z}\setminus\{0\}$ definita da

$$\psi(n) = \begin{cases} \varphi(n) & \text{se } \varphi(n) \neq 0\,, \\ 1 & \text{se } \varphi(n) = 0 \end{cases}$$

è pure suriettiva, per cui anche $\mathbb{Z}\setminus\{0\}$ è al più numerabile.

Per il Teorema (1.16) esiste un'applicazione suriettiva $f : \mathbb{N} \to \mathbb{Z}\times(\mathbb{Z}\setminus\{0\})$. Allora $g \circ f$ è un'applicazione suriettiva da $\mathbb{N}$ su $\mathbb{Q}$. ■

(6.3) Teorema *L'insieme dei numeri reali algebrici è al più numerabile.*

Dimostrazione. Dal momento che $\mathbb{Q}$ è al più numerabile, anche $\mathbb{Q}\setminus\{0\}$ è al più numerabile. Ne segue che, per ogni $n \geq 1$, è al più numerabile

$$\mathbb{Q}^n \times (\mathbb{Q}\setminus\{0\})\,.$$

Per ogni $a = (a_0, \ldots, a_n) \in \mathbb{Q}^n \times (\mathbb{Q}\setminus\{0\})$, sia P_a il polinomio definito da

$$P_a(x) = \sum_{k=0}^{n} a_k x^k\,.$$

Allora

$$\{x \in \mathbb{R} : \; P_a(x) = 0\}$$

è al più numerabile, avendo al più n elementi. Allora, per ogni $n \geq 1$, è al più numerabile

$$\bigcup_{a\in\mathbb{Q}^n\times(\mathbb{Q}\setminus\{0\})} \{x \in \mathbb{R} : \; P_a(x) = 0\}$$

Infine è al più numerabile

$$\bigcup_{n\in\mathbb{N}\setminus\{0\}} \left(\bigcup_{a\in\mathbb{Q}^n\times(\mathbb{Q}\setminus\{0\})} \{x \in \mathbb{R} : \; P_a(x) = 0\} \right)\,,$$

che è proprio l'insieme dei numeri reali algebrici. ■

(6.4) Teorema *Sia X uno spazio metrico completo, non vuoto e privo di punti isolati. Allora X non è al più numerabile.*

Dimostrazione. Sia $f : \mathbb{N} \to X$ un'applicazione. Non può essere $X = \{f(0)\}$, perché $f(0)$ sarebbe un punto isolato in X. Sia quindi $x_0 \in X$ con $x_0 \neq f(0)$. Sia poi $r_0 \in]0, 1]$ tale che $f(0) \notin \overline{\mathrm{B}\,(x_0, r_0)}$. Non può essere $\mathrm{B}\,(x_0, r_0) = \{f(1)\}$, perché $f(1)$ sarebbe un punto isolato in X. Sia quindi $x_1 \in \mathrm{B}\,(x_0, r_0)$ con $x_1 \neq f(1)$. Sia poi $r_1 \in]0, 1/2]$ tale che $f(1) \notin \overline{\mathrm{B}\,(x_1, r_1)}$ e tale che $\overline{\mathrm{B}\,(x_1, r_1)} \subseteq \mathrm{B}\,(x_0, r_0)$.

Procedendo ricorsivamente, si possono costruire una successione (x_n) in X ed una successione (r_n) in $]0, +\infty[$ tali che

$$\forall n \in \mathbb{N} : \; f(n) \notin \overline{\mathrm{B}\,(x_n, r_n)}\,,$$

$$\forall n \in \mathbb{N} : \; \overline{\mathrm{B}\,(x_{n+1}, r_{n+1})} \subseteq \mathrm{B}\,(x_n, r_n)\;,$$

$$\forall n \in \mathbb{N} : \; r_n \leq \frac{1}{n+1}\,.$$

Osserviamo che (x_n) è di Cauchy in X. Infatti, dato $\varepsilon > 0$, esiste $\overline{n} \in \mathbb{N}$ con $2r_{\overline{n}} < \varepsilon$. Se $m, n \geq \overline{n}$, ne segue $x_m, x_n \in \mathrm{B}\,(x_{\overline{n}}, r_{\overline{n}})$, quindi

$$d(x_m, x_n) < 2r_{\overline{n}} < \varepsilon\,,$$

per cui (x_n) è di Cauchy. Sia ℓ il suo limite.

Poiché

$$\forall m \geq n : \; x_m \in \overline{\mathrm{B}\,(x_n, r_n)}\,,$$

si ha $\ell \in \overline{\mathrm{B}\,(x_n, r_n)}$ per ogni $n \in \mathbb{N}$. Ne segue $\ell \neq f(n)$ per ogni $n \in \mathbb{N}$. ■

(6.5) Corollario *L'insieme $\mathbb{R}$ non è al più numerabile.*

7 Spazi metrici separabili

(7.1) Definizione *Uno spazio metrico X si dice* separabile*, se esiste un sottoinsieme al più numerabile D in X tale che D sia denso in X (cioè con $\overline{D} = X$).*

(7.2) Proposizione *Siano X e Y due spazi metrici e sia $f : X \to Y$ un'applicazione continua e suriettiva.*

Allora, se X è separabile, anche Y è separabile.

Dimostrazione. Sia D un sottoinsieme al più numerabile denso in X. Evidentemente $f(D)$ è al più numerabile. Dimostriamo che $f(D)$ è denso in Y. Sia $y \in Y$ e sia V un intorno di y. Sia $x \in X$ tale che $f(x) = y$ e sia U un intorno di x tale che $f(U) \subseteq V$. Sia infine $\xi \in D \cap U$. Allora $f(\xi) \in f(D) \cap V$, da cui la tesi. ■

(7.3) Proposizione *Sia X uno spazio metrico e sia (Y_h) una successione di sottoinsiemi separabili di X.*

Allora, se l'insieme $\bigcup\limits_{h\in\mathbb{N}} Y_h$ è denso in X, anche X è separabile.

Dimostrazione. Sia D_h un sottoinsieme al più numerabile denso in Y_h. Allora $D = \bigcup\limits_{h\in\mathbb{N}} D_h$ è un insieme al più numerabile. Dimostriamo che D è denso in X. Siano $x \in X$ ed U un intorno aperto di x. Sia $y \in U \cap \bigcup\limits_{h\in\mathbb{N}} Y_h$ Sarà $y \in U \cap Y_h$ per un certo $h \in \mathbb{N}$. Sia $z \in U \cap D_h$. Allora $z \in U \cap D$, da cui la tesi. ■

(7.4) Proposizione *Sia X uno spazio metrico separabile e sia $Y \subseteq X$. Allora Y è separabile.*

Dimostrazione. Sia $\{x_h : h \in \mathbb{N}\}$ un sottoinsieme al più numerabile denso in X. Se $Y = \emptyset$, la tesi è banalmente vera. Se $Y \neq \emptyset$, sia $\overline{y} \in Y$. Per ogni $h, k \in \mathbb{N}$ scegliamo $y_{h,k} \in \mathrm{B}(x_h, 1/(k+1)) \cap Y$, se tale intersezione non è vuota, altrimenti poniamo $y_{h,k} = \overline{y}$.

Allora $\{y_{h,k} : h, k \in \mathbb{N}\}$ è un sottoinsieme al più numerabile di Y. Proviamo che è denso in Y. Dati $y \in Y$ ed $\varepsilon > 0$, sia $k \in \mathbb{N}$ tale che $2/(k+1) < \varepsilon$ e sia $x_h \in \mathrm{B}(y, 1/(k+1))$. Allora $y \in \mathrm{B}(x_h, 1/(k+1))$, per cui $\mathrm{B}(x_h, 1/(k+1)) \cap Y \neq \emptyset$.

Ne segue che $y_{h,k} \in \mathrm{B}\,(x_h, 1/(k+1)) \cap Y$, quindi

$$d(y, y_{h,k}) \leq d(y, x_h) + d(x_h, y_{h,k}) < \frac{1}{k+1} + \frac{1}{k+1} < \varepsilon\,,$$

da cui la tesi. ■

(7.5) Teorema *Ogni spazio normato di dimensione finita è separabile.*

Dimostrazione. Consideriamo dapprima alcuni casi particolari. Lo spazio $\mathbb{R}^n$ è separabile, perché contiene il sottoinsieme denso $\mathbb{Q}^n$, che è numerabile. Per la Proposizione (7.2) è separabile anche $\mathbb{C}^n$, che è isometrico a $\mathbb{R}^{2n}$. Quindi $\mathbb{K}^n$ è separabile per $\mathbb{K} = \mathbb{R}, \mathbb{C}$.

Sia ora X uno spazio normato su $\mathbb{K}$ di dimensione finita n. Esiste un'applicazione $f : \mathbb{K}^n \to X$ lineare e biiettiva. Essenda f continua, la separabilità di X discende dalla Proposizione (7.2). ■

(7.6) Teorema *Sia X uno spazio normato. Allora X è separabile se e solo se esiste una successione (x_h) in X che genera un sottospazio vettoriale denso in X.*

Dimostrazione. Supponiamo che X sia separabile e sia $\{x_h : h \in \mathbb{N}\}$ un insieme al più numerabile denso in X. Allora a maggior ragione (x_h) è una successione che genera un sottospazio vettoriale denso in X.

Viceversa, sia (x_h) una successione che genera un sottospazio vettoriale Y denso in X. Sia Y_h il sottospazio vettoriale generato da $\{x_1, \ldots, x_h\}$. Per il Teorema (7.5) ciascun Y_h è separabile. Poiché $Y = \bigcup\limits_{h \in \mathbb{N}} Y_h$, la separabilità di X discende dalla Proposizione (7.3).
■

8 La funzione esponenziale

(8.1) Teorema (Prodotto secondo Cauchy di due serie) *Siano* $\sum_{n=0}^{\infty} x_n$ *e* $\sum_{n=0}^{\infty} y_n$ *due serie assolutamente convergenti in* $\mathbb{C}$ *e sia*

$$z_n = \sum_{k=0}^{n} x_k y_{n-k}\,.$$

Allora la serie $\sum_{n=0}^{\infty} z_n$ *è assolutamente convergente e*

$$\sum_{n=0}^{\infty} z_n = \left(\sum_{n=0}^{\infty} x_n\right)\left(\sum_{n=0}^{\infty} y_n\right)\,.$$

Dimostrazione. Risulta

$$\sum_{n=0}^{N} |z_n| \leq \sum_{n=0}^{N}\sum_{k=0}^{n} |x_k|\,|y_{n-k}| \leq \left(\sum_{n=0}^{N} |x_n|\right)\left(\sum_{n=0}^{N} |y_n|\right)\,,$$

per cui la serie $\sum_{n=0}^{\infty} z_n$ è assolutamente convergente, quindi convergente.

Risulta anche

$$\begin{aligned}
\left|\sum_{n=0}^{2N} z_n - \left(\sum_{k=0}^{N} x_k\right)\left(\sum_{m=0}^{N} y_m\right)\right| &= \left|\sum_{k=0}^{N-1}\left(x_k \sum_{m=N+1}^{2N-k} y_m\right) + \sum_{k=N+1}^{2N}\left(x_k \sum_{m=0}^{2N-k} y_m\right)\right| \leq \\
&\leq \sum_{k=0}^{N-1}\left(|x_k| \sum_{m=N+1}^{2N-k} |y_m|\right) + \sum_{k=N+1}^{2N}\left(|x_k| \sum_{m=0}^{2N-k} |y_m|\right) \leq \\
&\leq \left(\sum_{k=0}^{\infty} |x_k|\right)\left(\sum_{m=N+1}^{\infty} |y_m|\right) + \\
&\quad + \left(\sum_{k=N+1}^{\infty} |x_k|\right)\left(\sum_{m=0}^{\infty} |y_m|\right)\,.
\end{aligned}$$

Passando al limite per $N \to +\infty$, ne segue che

$$\sum_{n=0}^{\infty} z_n - \left(\sum_{k=0}^{\infty} x_k\right)\left(\sum_{m=0}^{\infty} y_m\right) = 0\,,$$

per cui la dimostrazione è completa. ■

(8.2) Proposizione *Per ogni* $z \in \mathbb{C}$ *la serie*

$$\sum_{n=0}^{\infty} \frac{z^n}{n!}$$

è assolutamente convergente.

Dimostrazione. Se $z = 0$ il fatto è evidente. Se $z \neq 0$, risulta

$$\lim_n \frac{|z|^{n+1}}{(n+1)!} \frac{n!}{|z|^n} = \lim_n \frac{|z|}{n+1} = 0\,.$$

La tesi discende allora dal criterio del rapporto. ■

(8.3) Definizione *Per ogni* $z \in \mathbb{C}$ *poniamo*

$$\exp z := \sum_{n=0}^{\infty} \frac{z^n}{n!}\,.$$

La funzione $\exp : \mathbb{C} \to \mathbb{C}$ *si chiama* esponenziale complesso.

(8.4) Teorema *La funzione* $\exp : \mathbb{C} \to \mathbb{C}$ *è continua. Inoltre valgono i seguenti fatti:*

$$\exp 0 = 1\,,$$

$$\forall z, w \in \mathbb{C} :\ \exp(z + w) = (\exp z)(\exp w)\,,$$

$$\forall z \in \mathbb{C} :\ \exp z \neq 0\,,$$

$$\forall z \in \mathbb{C} :\ \exp(-z) = (\exp z)^{-1}\,,$$

$$\forall z \in \mathbb{C} :\ \exp \bar{z} = \overline{\exp z}\,,$$

$$\lim_{z \to 0} \frac{\exp z - 1}{z} = 1\,.$$

Dimostrazione. Evidentemente $\exp 0 = 1$. Per la formula del binomio di Newton si ha

$$\frac{1}{n!}(z + w)^n = \frac{1}{n!} \sum_{k=0}^{n} \binom{n}{k} z^k w^{n-k} = \sum_{k=0}^{n} \frac{1}{k!} z^k \frac{1}{(n-k)!} w^{n-k}\,.$$

Per il teorema sul prodotto secondo Cauchy di due serie, ne segue

$$\exp(z + w) = (\exp z)(\exp w)\,.$$

Poiché

$$1 = \exp 0 = \exp(z + (-z)) = (\exp z)(\exp(-z))\,,$$

si ha $\exp z \neq 0$ ed $\exp(-z) = (\exp z)^{-1}$.

Risulta

$$\sum_{n=0}^{N} \frac{\overline{z}^n}{n!} = \overline{\sum_{n=0}^{N} \frac{z^n}{n!}}\,.$$

Passando al limite per $N \to +\infty$ e tenendo conto della continuità della funzione coniugato, si ottiene $\exp \overline{z} = \overline{\exp z}$.

Per ogni $z \in \mathbb{C}$ con $|z| \leq 1$ si ha

$$\begin{aligned} |(\exp z) - 1 - z| &= \left|\sum_{n=2}^{\infty} \frac{z^n}{n!}\right| = |z|^2 \left|\sum_{n=0}^{\infty} \frac{z^n}{(n+2)!}\right| \leq \\ &\leq |z|^2 \sum_{n=0}^{\infty} \frac{|z|^n}{(n+2)!} \leq |z|^2 \sum_{n=0}^{\infty} \frac{1}{n!} = (\exp 1)|z|^2\,. \end{aligned}$$

Ne segue

$$\left|\frac{\exp z - 1}{z} - 1\right| \leq (\exp 1)|z|\,,$$

da cui

$$\lim_{z\to 0} \frac{\exp z - 1}{z} = 1\,.$$

A maggior ragione si ha

$$\lim_{z\to 0} \exp z = 1\,,$$

per cui

$$\lim_{w\to z} \exp w = \lim_{w\to z} \exp(z + (w - z)) = \lim_{w\to z} \big(\exp z \exp(w - z)\big) = \exp z\,.$$

Pertanto la funzione exp è continua. ∎

(8.5) Corollario *Sia $z \in \mathbb{C}$ e sia $f : \mathbb{R} \to \mathbb{C}$ la funzione definita da $f(x) = \exp(zx)$. Allora f è derivabile e*

$$\forall x \in \mathbb{R} :\; f'(x) = z \exp(zx)\,.$$

Dimostrazione. Se $z = 0$, il fatto è ovvio. Altrimenti si ha

$$\lim_{\xi\to x} \frac{\exp(z\xi) - \exp(zx)}{\xi - x} = \lim_{\xi\to x} \left(z \exp(zx) \frac{\exp(z\xi - zx) - 1}{z\xi - zx} \right) = z \exp(zx)\,,$$

da cui la tesi. ■

(8.6) Proposizione *Per ogni* $x \in \mathbb{R}$ *si ha* $\exp x \in \mathbb{R}$.

Dimostrazione. Se $x \in \mathbb{R}$, si ha $\overline{x} = x$. Ne segue

$$\overline{\exp x} = \exp \overline{x} = \exp x \,.$$

Pertanto $\exp x \in \mathbb{R}$. ■

(8.7) Definizione *La funzione* $\exp_{|\mathbb{R}} : \mathbb{R} \to \mathbb{R}$ *si chiama* esponenziale *(*reale*). Per semplicità viene denotata con lo stesso simbolo* exp*.*

(8.8) Teorema *Per ogni* $x, y \in \mathbb{R}$ *si ha*

$$\exp(x + y) = (\exp x)(\exp y) \,,$$

$$\exp x \geq 1 + x \,.$$

Inoltre exp *è l'unica funzione da* $\mathbb{R}$ *in* $\mathbb{R}$ *con tali proprietà.*

Dimostrazione. La formula riguardante $\exp(x + y)$ discende dalla corrispondente formula in ambito complesso.

D'altronde, per ogni $x \in \mathbb{R}$, risulta

$$\exp x = \left(\exp \frac{x}{2}\right)^2 \geq 0 \,.$$

Inoltre dal Corollario (8.5) segue che la funzione exp è derivabile con

$$\forall x \in \mathbb{R} : \ (\exp)'(x) = \exp x \,,$$

per cui exp è derivabile due volte con

$$\forall x \in \mathbb{R} : \ (\exp)''(x) = \exp x \,.$$

Se $x > 0$, dalla Formula di Taylor col resto di Lagrange si deduce che esiste $t \in]0, x[$ tale che

$$\exp x = 1 + x + \frac{1}{2}\,(\exp t)x^2 \geq 1 + x \,.$$

Se $x < 0$, la dimostrazione è analoga.

Infine, sia $g : \mathbb{R} \to \mathbb{R}$ un'altra funzione tale che

$$\forall x, y \in \mathbb{R} : \; g(x+y) = g(x)g(y)\,, \qquad g(x) \geq 1 + x\,.$$

Risulta che $g(0) = 1$ e che g è derivabile con $g'(x) = g(x)$ per ogni $x \in \mathbb{R}$. Posto $\varphi(x) = \dfrac{g(x)}{\exp x}$, si ha che $\varphi : \mathbb{R} \to \mathbb{R}$ è derivabile con

$$\varphi'(x) = \frac{g'(x)\exp x - g(x)\exp x}{(\exp x)^2} = \frac{g(x)\exp x - g(x)\exp x}{(\exp x)^2} = 0\,.$$

Ne segue che φ è costante. Poiché $\exp 0 = g(0) = 1$, deve essere $\varphi = 1$, ossia $g = \exp$. ■

(8.9) Osservazione *Evidentemente risulta*

$$e = \sum_{h=0}^{\infty} \frac{1}{h!}\,.$$

9 Le funzioni circolari

(9.1) Definizione *Per ogni $z \in \mathbb{C}$ poniamo*

$$\cos z := \frac{\exp(iz) + \exp(-iz)}{2}\,,$$

$$\sin z := \frac{\exp(iz) - \exp(-iz)}{2i}\,.$$

Le funzioni $\cos : \mathbb{C} \to \mathbb{C}$ *e* $\sin : \mathbb{C} \to \mathbb{C}$ *si chiamano rispettivamente* coseno *e* seno.

(9.2) Teorema *Le funzioni* $\cos : \mathbb{C} \to \mathbb{C}$ *e* $\sin : \mathbb{C} \to \mathbb{C}$ *sono continue. Inoltre valgono i seguenti fatti:*

$$\forall z \in \mathbb{C} : \; \exp(iz) = \cos z + i \sin z\,,$$

$$\cos 0 = 1\,, \qquad \sin 0 = 0\,,$$

$$\forall z, w \in \mathbb{C} : \; \cos(z+w) = \cos z \cos w - \sin z \sin w\,,$$

$$\forall z, w \in \mathbb{C}: \ \sin(z+w) = \sin z \cos w + \cos z \sin w \,,$$

$$\forall z \in \mathbb{C}: \ \cos(-z) = \cos z \,, \qquad \sin(-z) = -\sin z \,,$$

$$\forall z \in \mathbb{C}: \ \cos^2 z + \sin^2 z = 1 \,,$$

$$\forall z \in \mathbb{C}: \ \cos \overline{z} = \overline{\cos z} \,, \qquad \sin \overline{z} = \overline{\sin z} \,,$$

$$\lim_{z \to 0} \frac{\cos z - 1}{z} = 0 \,, \qquad \lim_{z \to 0} \frac{\sin z}{z} = 1 \,,$$

$$\forall z \in \mathbb{C}: \ \cos z = \sum_{n=0}^{\infty} (-1)^n \, \frac{z^{2n}}{(2n)!} \,, \qquad \sin z = \sum_{n=0}^{\infty} (-1)^n \, \frac{z^{2n+1}}{(2n+1)!} \,.$$

Dimostrazione. La continuità di coseno e seno segue per composizione dalla continuità dell'esponenziale complesso. Dalla definizione segue immediatamente che

$$\forall z \in \mathbb{C}: \ \exp(iz) = \cos z + i \sin z \,,$$

$$\cos 0 = 1 \,, \qquad \sin 0 = 0 \,.$$

Inoltre si ha

$$\begin{aligned}
\cos z \cos w - \sin z \sin w &= \frac{\exp(iz)+\exp(-iz)}{2} \frac{\exp(iw)+\exp(-iw)}{2} + \\
&\quad - \frac{\exp(iz)-\exp(-iz)}{2i} \frac{\exp(iw)-\exp(-iw)}{2i} = \\
&= \frac{1}{4} \big(\exp(iz+iw) + \exp(iz-iw) + \exp(iw-iz) + \\
&\quad + \exp(-iz-iw) + \exp(iz+iw) - \exp(iz-iw) + \\
&\quad - \exp(iw-iz) + \exp(-iz-iw) \big) = \\
&= \frac{\exp(iz+iw)+\exp(-iz-iw)}{2} = \cos(z+w) \,.
\end{aligned}$$

In modo simile risulta

$$\begin{aligned}
\sin z \cos w + \cos z \sin w &= \frac{\exp(iz)-\exp(-iz)}{2i} \frac{\exp(iw)+\exp(-iw)}{2} + \\
&\quad + \frac{\exp(iz)+\exp(-iz)}{2} \frac{\exp(iw)-\exp(-iw)}{2i} = \\
&= \frac{1}{4i} \big(\exp(iz+iw) + \exp(iz-iw) - \exp(iw-iz) + \\
&\quad - \exp(-iz-iw) + \exp(iz+iw) - \exp(iz-iw) + \\
&\quad + \exp(iw-iz) - \exp(-iz-iw) \big) = \\
&= \frac{\exp(iz+iw)-\exp(-iz-iw)}{2i} = \sin(z+w) \,.
\end{aligned}$$

Dalla definizione di cos e sin segue direttamente che

$$\forall z \in \mathbb{C}: \ \cos(-z) = \cos z\,, \qquad \sin(-z) = -\sin z\,,$$

$$\forall z \in \mathbb{C}: \ \cos^2 z + \sin^2 z = 1\,,$$

$$\forall z \in \mathbb{C}: \ \cos \overline{z} = \overline{\cos z}\,, \qquad \sin \overline{z} = \overline{\sin z}\,.$$

Risulta

$$\frac{\cos z - 1}{z} = \frac{\exp(iz) + \exp(-iz) - 2}{2z} = \frac{i}{2}\left(\frac{\exp(iz)-1}{iz} - \frac{\exp(-iz)-1}{-iz}\right)\,,$$

per cui

$$\lim_{z\to 0} \frac{\cos z - 1}{z} = 0\,.$$

In modo simile si ha

$$\frac{\sin z}{z} = \frac{\exp(iz) - \exp(-iz)}{2iz} = \frac{1}{2}\left(\frac{\exp(iz)-1}{iz} + \frac{\exp(-iz)-1}{-iz}\right)\,,$$

da cui

$$\lim_{z\to 0} \frac{\sin z}{z} = 1\,.$$

Infine risulta

$$\begin{aligned}
\cos z &= \frac{\exp(iz) + \exp(-iz)}{2} = \\
&= \frac{1}{2}\left(\sum_{n=0}^{\infty} \frac{(iz)^n}{n!} + \sum_{n=0}^{\infty} \frac{(-iz)^n}{n!}\right) = \\
&= \frac{1}{2}\sum_{n=0}^{\infty} (1 + (-1)^n)\, i^n \frac{z^n}{n!} = \\
&= \frac{1}{2}\sum_{n=0}^{\infty} 2i^{2n} \frac{z^{2n}}{(2n)!} = \sum_{n=0}^{\infty} (-1)^n \frac{z^{2n}}{(2n)!}\,.
\end{aligned}$$

Analogamente si ha

$$\begin{aligned}
\sin z &= \frac{\exp(iz) - \exp(-iz)}{2i} = \\
&= \frac{1}{2i}\left(\sum_{n=0}^{\infty} \frac{(iz)^n}{n!} - \sum_{n=0}^{\infty} \frac{(-iz)^n}{n!}\right) = \\
&= \frac{1}{2i}\sum_{n=0}^{\infty} (1 - (-1)^n)\, i^n \frac{z^n}{n!} = \\
&= \frac{1}{2i}\sum_{n=0}^{\infty} 2i^{2n+1} \frac{z^{2n+1}}{(2n+1)!} = \sum_{n=0}^{\infty} (-1)^n \frac{z^{2n+1}}{(2n+1)!}\,,
\end{aligned}$$

da cui la tesi. ■

(9.3) Proposizione *Per ogni $x \in \mathbb{R}$ si ha $\cos x \in \mathbb{R}$ e $\sin x \in \mathbb{R}$.*

Dimostrazione. Poiché $\overline{x} = x$, risulta

$$\overline{\cos x} = \cos \overline{x} = \cos x \,,$$

$$\overline{\sin x} = \sin \overline{x} = \sin x \,,$$

da cui $\cos x \in \mathbb{R}$ e $\sin x \in \mathbb{R}$ ■

(9.4) Definizione *Le funzioni $\cos_{|\mathbb{R}} : \mathbb{R} \to \mathbb{R}$ e $\sin_{|\mathbb{R}} : \mathbb{R} \to \mathbb{R}$ vengono ancora chiamate con gli stessi nomi* coseno *e* seno *e denotate con gli stessi simboli* cos *e* sin.

(9.5) Teorema *Per ogni $x, y \in \mathbb{R}$ si ha*

$$\cos^2 x + \sin^2 x = 1 \,,$$

$$\cos(x + y) = \cos x \cos y - \sin x \sin y \,,$$

$$\sin(x + y) = \sin x \cos y + \cos x \sin y \,,$$

$$0 < |x| \leq 1 \implies \cos x \leq \frac{\sin x}{x} \leq 1 \,.$$

Inoltre $(\cos, \sin)$ è l'unica coppia di funzioni da $\mathbb{R}$ in $\mathbb{R}$ con tali proprietà.

Dimostrazione. Le prime tre formule discendono dalle corrispondenti formule in ambito complesso.

Sia ora $x \in \mathbb{R}$ con $0 < |x| \leq 1$. Osserviamo anzitutto che per ogni $k \geq 1$ risulta

$$\sum_{n=2k-1}^{2k} (-1)^n \frac{x^{2n}}{(2n)!} \leq \sum_{n=2k-1}^{2k} (-1)^n \frac{x^{2n}}{(2n+1)!} \leq 0 \,.$$

In effetti questo equivale a

$$-\frac{x^{4k-2}}{(4k-2)!} + \frac{x^{4k}}{(4k)!} \leq -\frac{x^{4k-2}}{(4k-1)!} + \frac{x^{4k}}{(4k+1)!} \leq 0$$

ossia

$$-(4k+1)4k(4k-1) + (4k+1)x^2 \leq -(4k+1)4k + x^2 \leq 0$$

che a sua volta equivale a

$$x^2 \leq (4k+1)(4k-2)\,.$$

Quest'ultima disuguaglianza è certamente vera per $|x| \leq 1$ e $k \geq 1$.

Risulta quindi

$$1 + \sum_{n=1}^{\infty} (-1)^n \frac{x^{2n}}{(2n)!} \leq 1 + \sum_{n=1}^{\infty} (-1)^n \frac{x^{2n}}{(2n+1)!} \leq 1\,,$$

ossia

$$\cos x \leq \frac{\sin x}{x} \leq 1\,.$$

Sia infine (f, g) una coppia di funzioni da $\mathbb{R}$ in $\mathbb{R}$ con le stesse proprietà. Risulta che $f(0) = 1$, $g(0) = 0$ e che f, g sono derivabili con $f'(x) = -g(x)$ e $g'(x) = f(x)$ per ogni $x \in \mathbb{R}$. Posto $\varphi(x) = \dfrac{f(x) + ig(x)}{\exp(ix)}$, si ha che $\varphi : \mathbb{R} \to \mathbb{C}$ è derivabile con

$$\begin{aligned} \varphi'(x) &= \frac{(f'(x) + ig'(x))\exp(ix) - i(f(x) + ig(x))\exp(ix)}{(\exp(ix))^2} = \\ &= \frac{(-g(x) + if(x))\exp(ix) - (if(x) - g(x))\exp(ix)}{(\exp(ix))^2} = 0\,. \end{aligned}$$

Ne segue che φ è costante. Poiché $\exp 0 = f(0) + ig(0) = 1$, deve essere $\varphi(x) = 1$, ossia $f(x) + ig(x) = \exp(ix) = \cos x + i \sin x$. Ne segue $f(x) = \cos x$ e $g(x) = \sin x$. ■

(9.6) Definizione *Per ogni* $z \in \mathbb{C}$ *con* $\cos z \neq 0$ *poniamo*

$$\tan z := \frac{\sin z}{\cos z}\,.$$

La funzione tan *si chiama* tangente.

10 Il teorema fondamentale dell'algebra

(10.1) Teorema (fondamentale dell'algebra) *Sia*

$$P(z) = \sum_{k=0}^{n} a_k z^k$$

una funzione polinomiale complessa con $n \geq 1$ *ed* $a_n \neq 0$.

Allora esiste $z \in \mathbb{C}$ *tale che* $P(z) = 0$.

Dimostrazione. Sia (ζ_h) una successione in $\mathbb{C}$ tale che

$$\forall h \in \mathbb{N} : \, |P(\zeta_h)| < \inf_{z \in \mathbb{C}} |P(z)| + \frac{1}{h+1} \, .$$

Per ogni $z \neq 0$ risulta

$$|P(z)| \geq |a_n||z|^n - \sum_{k=0}^{n-1} |a_k||z|^k = |z|^n \left(|a_n| - \sum_{k=0}^{n-1} |a_k||z|^{k-n} \right) .$$

Poiché

$$\lim_{t \to +\infty} t^n \left(|a_n| - \sum_{k=0}^{n-1} |a_k| t^{k-n} \right) = +\infty \, ,$$

esiste $R > 0$ tale che

$$\forall t > R : \, t^n \left(|a_n| - \sum_{k=0}^{n-1} |a_k| t^{k-n} \right) > \inf_{z \in \mathbb{C}} |P(z)| + 1 \, .$$

Ne segue $|\zeta_h| \leq R$ per ogni h, per cui la successione (ζ_h) è limitata.

Sia $(\zeta_{\nu(h)})$ una sottosuccessione convergente a $z_0 \in \mathbb{C}$. Per la continuità della funzione $|P|$, risulta

$$|P(z_0)| = \lim_h |P(\zeta_{\nu(h)})| = \inf_{z \in \mathbb{C}} |P(z)| \, .$$

Pertanto

$$\forall z \in \mathbb{C} : \, |P(z_0)| \leq |P(z)| \, .$$

La tesi sarà dimostrata, se proviamo che $P(z_0) = 0$.

Sia Q il polinomio definito da $Q(z) = P(z + z_0)$. Sarà

$$Q(z) = \sum_{k=0}^{n} b_k z^k$$

con $b_n = a_n$ ed inoltre

$$\forall z \in \mathbb{C} : \, |Q(0)| \leq |Q(z)| \, .$$

Si tratta di dimostrare che $Q(0) = 0$, ossia che $b_0 = 0$.

Sia j tale che $1 \leq j \leq n$, $b_j \neq 0$ e

$$Q(z) = b_0 + \sum_{k=j}^{n} b_k z^k \, .$$

Sia $w \in \mathbb{C}$ tale che $b_0 + b_j w^j = 0$. Allora si ha

$$\lim_{t \to 0} \frac{Q(tw) - b_0 - b_j(tw)^j}{t^j} = 0\,.$$

Se per assurdo fosse $b_0 \neq 0$, esisterebbe $t \in]0,1]$ tale che

$$|Q(tw) - b_0 - b_j(tw)^j| < \frac{1}{2}|b_0|t^j\,.$$

Ne seguirebbe

$$\begin{aligned} |Q(tw)| &\leq |Q(tw) - b_0 - b_j(tw)^j| + |b_0 + b_j(tw)^j| < \\ &< \frac{1}{2}|b_0|t^j + |b_0|(1 - t^j) = |b_0| - \frac{1}{2}|b_0|t^j < |Q(0)|\,, \end{aligned}$$

il che è assurdo. ■

11 Serie di potenze

(11.1) Definizione *Si chiama* serie di potenze in $\mathbb{C}$ *ogni espressione formale*

$$\sum_{n=0}^{\infty} c_n (z-a)^n$$

dove (c_n) *è una successione in* $\mathbb{C}$ *ed* $a \in \mathbb{C}$.

Si chiama raggio di convergenza *della serie il numero reale esteso*

$$\left(\limsup_n \sqrt[n]{|c_n|}\right)^{-1}$$

con le convenzioni $0^{-1} = +\infty$ *e* $(+\infty)^{-1} = 0$.

(11.2) Teorema *Sia*

$$\sum_{n=0}^{\infty} c_n (z-a)^n$$

una serie di potenze in $\mathbb{C}$ *e sia* $R \in [0, +\infty]$ *il suo raggio di convergenza.*

Allora per ogni $z \in \mathbb{C}$ *con* $|z-a| < R$ *la serie*

$$\sum_{n=0}^{\infty} c_n (z-a)^n$$

è assolutamente convergente in $\mathbb{C}$, mentre per ogni $z \in \mathbb{C}$ con $|z-a| > R$ tale serie non è convergente.

Inoltre, per ogni $r \in]0, R[$, la corrispondente serie in $\left(C\left(\overline{\mathrm{B}\,(a,r)};\mathbb{C}\right), \|\ \|_\infty\right)$ è totalmente convergente.

Dimostrazione. Se $z \in \mathbb{C}$ e $|z-a| > R$, si ha

$$\limsup_n \sqrt[n]{|c_n(z-a)^n|} > 1\,,$$

per cui risulta $|c_n(z-a)^n| > 1$ per infiniti n. Allora non può essere

$$\lim_n c_n(z-a)^n = 0$$

e la serie

$$\sum_{n=0}^{\infty} c_n(z-a)^n$$

non può quindi convergere in $\mathbb{C}$.

Sia ora $r \in]0, R[$. Risulta

$$\sup\left\{|c_n(z-a)^n| :\, z \in \overline{\mathrm{B}\,(a,r)}\right\} \leq |c_n| r^n\,.$$

Poiché

$$\limsup_n \sqrt[n]{|c_n| r^n} < 1\,,$$

la serie

$$\sum_{n=0}^{\infty} |c_n| r^n$$

è convergente in $\mathbb{R}$ per il criterio della radice. Ne segue la convergenza totale della serie

$$\sum_{n=0}^{\infty} c_n(z-a)^n$$

su $\overline{\mathrm{B}\,(a,r)}$.

In particolare, per ogni $z \in \mathbb{C}$ con $|z-a| < R$ la serie in questione è assolutamente convergente in $\mathbb{C}$. ■

(11.3) Teorema *Sia*

$$\sum_{n=0}^{\infty} c_n(z-a)^n$$

una serie di potenze in $\mathbb{C}$ *con raggio di convergenza* $R \in]0, +\infty]$, *sia*

$$A = \{z \in \mathbb{C} : \, |z - a| < R\}$$

e sia $f : A \to \mathbb{C}$ *la funzione definita da*

$$f(z) = \sum_{n=0}^{\infty} c_n (z-a)^n \, .$$

Valgono allora i seguenti fatti:

(a) *la serie di potenze*

$$\sum_{n=0}^{\infty} (n+1) c_{n+1} (z-a)^n$$

ha lo stesso raggio di convergenza R;

(b) *la funzione f è differenziabile (in senso complesso) e si ha*

$$\forall z \in A : \, f'(z) = \sum_{n=0}^{\infty} (n+1) c_{n+1} (z-a)^n \, .$$

Dimostrazione.

(a) Si ha

$$\limsup_n \sqrt[n]{(n+1)|c_{n+1}|} =$$

$$= \limsup_n \left(\sqrt[n+1]{n+1} \, \sqrt[n+1]{|c_{n+1}|} \right)^{\frac{n+1}{n}} = \limsup_n \sqrt[n]{|c_n|} \, .$$

(b) Definiamo $g : A \to \mathbb{C}$ ponendo

$$\forall z \in A : \, g(z) = \sum_{n=0}^{\infty} (n+1) c_{n+1} (z-a)^n \, .$$

Siano $z \in A$, $|z - a| < r < R$ e $w \in \mathbb{C} \setminus \{0\}$ con $|z - a| + |w| \leq r$. Per ogni $n \geq 1$, l'applicazione

$$\begin{gathered} [0,1] \to \mathbb{C} \\ s \mapsto (z + sw - a)^{n+1} - s(n+1)(z-a)^n w \end{gathered}$$

soddisfa le ipotesi della disuguaglianza di Lagrange. Sia $s_1 \in]0, 1[$ tale che

$$\left| (z + w - a)^{n+1} - (z-a)^{n+1} - (n+1)(z-a)^n w \right| \leq$$

$$\leq (n+1)|w|\,|(z+s_1w-a)^n-(z-a)^n| \; .$$

Riapplicando la disuguaglianza di Lagrange a

$$\begin{aligned}[0,s_1] &\to \mathbb{C}\\ \sigma &\mapsto (z+\sigma w-a)^n\end{aligned}$$

si ottiene $s_2 \in]0,s_1[$ tale che

$$|(z+s_1w-a)^n-(z-a)^n| \leq n|w|\left|(z+s_2w-a)^{n-1}\right| \leq n|w|r^{n-1}\,,$$

per cui

$$\left|(z+w-a)^{n+1}-(z-a)^{n+1}-(n+1)(z-a)^n w\right| \leq n(n+1)|w|^2 r^{n-1}\,.$$

Ne segue

$$\left|\sum_{n=0}^{k+1} c_n(z+w-a)^n-\sum_{n=0}^{k+1} c_n(z-a)^n-\sum_{n=0}^{k}(n+1)c_{n+1}(z-a)^n w\right| =$$

$$=\left|\sum_{n=0}^{k} c_{n+1}(z+w-a)^{n+1}-\sum_{n=0}^{k} c_{n+1}(z-a)^{n+1}-\sum_{n=0}^{k}(n+1)c_{n+1}(z-a)^n w\right| \leq$$

$$\leq |w|^2\sum_{n=0}^{k} n(n+1)|c_{n+1}|r^{n-1}\,.$$

Passando al limite per $k\to\infty$ e dividendo per $|w|$, si ottiene

$$\left|\frac{f(z+w)-f(z)}{w}-g(z)\right| \leq |w|\sum_{n=0}^{\infty} n(n+1)|c_{n+1}|r^{n-1}\,.$$

Passando infine al limite per $w\to 0$, si deduce che f è derivabile in z e che $f'(z)=g(z)$.

■

Elenco dei simboli

Indice analitico