Teoria degli insiemi minimale

PAOLO LIPPARINI

Questo lavoro è protetto dalle leggi riguardanti il diritto di autore. Ne è consentita la copia esclusivamente per uso personale per motivi di studio.

Questi appunti sono stati scritti molto di fretta, potrebbero contenere molti errori! Cercherò di rivederli non appena possibile, nel frattempo faccio notare che è molto meritorio da parte degli studenti scoprire errori negli appunti dei docenti!

Questa è una versione incompleta, verrà aggiunto altro materiale.

1. Teoria degli insiemi minimale

Premessa. Lo scopo di questa sezione è quello di presentare nella maniera più breve e semplice possibile, evitando dettagli eccessivamente tecnici, alcune nozioni e idee di teoria degli insiemi che per uno studente, ad esempio di matematica, sarebbe opportuno conoscere. Le sezioni indicate con un asterisco e le note possono essere saltate in prima lettura.

1.1. Nozione intuitiva di insieme. Molte delle definizioni in questa sotto-sezione potrebbero essere già note al lettore. Preferiamo riepilgarle comunque per completezza e affinché non sussista alcun dubbio riguardo a terminologia e notazioni.

Intuitivamente, un *insieme* è una collezione, un aggregato, un raggruppamento di oggetti. Se x è un insieme, e l'oggetto A appartiene ad x , si scrive $A \in x$ e si dice che A è *un elemento di x* , che A *sta in x* , o altre simili espressioni. Per brevità, talvolta si scriverà $A, B \in x$ per intendere che contemporaneamente $A \in x$ e $B \in x$. Se A non appartiene ad x , si scrive $A \notin x$.

1.1.1. Uguaglianza fra insiemi. Due insiemi x e y si considerano *uguali*, cioè identici, e si scrive $x = y$, se x e y contengono *esattamente* gli stessi oggetti^{1 2}.

Work performed under the auspices of G.N.S.A.G.A. Work partially supported by PRIN 2012 "Logica, Modelli e Insiemi" and by MIUR CUP E83C18000100006.

¹ L'introduzione dell'uguaglianza come presentata sopra a prima vista potrebbe sembrare una semplice definizione, ma in realtà si tratta di un'assunzione forte. Si richiede che due insiemi uguali soddisfino esattamente le stesse proprietà; cioè, ad esempio, se $x = y$, allora, per ogni insieme z , deve valere $x \in z$ se e solo se $y \in z$.

² In generale, nel calcolo dei predicati, una *teoria con uguaglianza* ha un simbolo speciale di relazione binario $=$ tale che le seguenti formule sono assiomi (o comunque dimostrabili):

$x = x$,

$x = y \Rightarrow t(z_0, z_1, \dots, z_{i-1}, x, z_{i+1}, \dots) = t(z_0, z_1, \dots, z_{i-1}, y, z_{i+1}, \dots)$, per ogni termine t ,

$x = y \Rightarrow (\varphi(z_0, z_1, \dots, z_{i-1}, x, z_{i+1}, \dots) \Rightarrow \varphi(z_0, z_1, \dots, z_{i-1}, y, z_{i+1}, \dots))$,

per ogni formula φ .

La precedente affermazione è chiamata *Principio di estensionalità*. Ad esempio, gli insiemi descritti dalle seguenti clausole (a) - (c') sono uguali:

(a) L'insieme $\{4, 6, 8\}$ che contiene esattamente i numeri 4, 6, 8.

(a') L'insieme $\{6, 8, 4\}$.

(b) L'insieme $\{x \in \mathbb{N} \mid x \text{ è un numero naturale pari e } 3 \leq x \leq 9\}$ costituito da tutti i numeri naturali pari compresi fra 3 e 9. Ricordiamo che i numeri naturali sono 0, 1, 2... e che l'insieme di tutti i numeri naturali³ si indica con $\mathbb{N}$.

(c) L'insieme $\{2t \mid t \in \mathbb{N} \text{ e } 1 < t < 5\}$ di tutti i numeri che possono essere espressi nella forma $2t$ al variare di t fra i numeri naturali strettamente compresi fra 1 e 5.

(c') L'insieme $\{n \in \mathbb{N} \mid \text{esiste un } t \in \mathbb{N} \text{ tale che } t = 2n \text{ e } 1 < t < 5\}$ (l'espressione fra graffe in (c) può essere considerata un'abbreviazione dell'espressione indicata qui in (c')).

Quindi l'uguaglianza fra due insiemi dipende solo dagli elementi che essi contengono, ed è completamente indipendente dal modo in cui questi insiemi vengono definiti o descritti; in particolare, è indipendente dall'ordine in cui vengono eventualmente elencati i loro elementi. In altre parole, almeno in linea di principio, un insieme x risulta ben definito quando esiste una netta e precisa distinzione fra gli elementi che appartengono ad x e quelli che non vi appartengono, cioè quando è perfettamente chiaro⁴ cosa appartiene e cosa non appartiene ad x .

Le condizioni si possono indebolire, ed esistono molte formulazioni equivalenti, vedi ad esempio la Sezione 8 nel Capitolo 2 del libro del Mendelson. Solitamente si assume che in un modello di una teoria con uguaglianza il simbolo $=$ venga effettivamente interpretato come la relazione di uguaglianza fra gli elementi del modello; i modelli per cui questo avviene si chiamano modelli *normali*.

³ Alcuni autori non includono il numero 0 fra i numeri naturali (questo corrisponde all'origine storica dell'idea di numero naturale); altri autori includono il numero 0 e indicano con $\mathbb{N}^*$ oppure con $\mathbb{N}^+$ l'insieme dei numeri naturali escluso lo 0. Dovrebbe risultare chiaro che non si tratta di una questione sostanziale, ma esclusivamente di convenzioni di comodo. Non sempre esistono notazioni e convenzioni universalmente accettate in matematica. In questo e altri casi, quando si tratta di convenzioni e definizioni, è sempre opportuno consultare il testo che si sta leggendo, facendo riferimento con attenzione alle notazioni usate. Beninteso, può essere difficoltoso passare da un testo all'altro, specie se i testi fanno uso di notazioni e definizioni molto diverse.

⁴ Esiste una teoria degli insiemi "sfumati", dove l'appartenenza di qualche oggetto ad un insieme è incerta o ha valori probabilistici. Qui ci limiteremo alla teoria classica.

È anche ovvio che espressioni del tipo "precisa distinzione", "chiaro" etc. sono altrettanto vaghe quanto "aggregato", "raggruppamento" etc. Questa osservazione non costituisce certo un problema, visto che in questa sottosezione ci limitiamo a presentare le nozioni intuitivamente. Va però fatto notare che, mentre la definizione (o meglio, presentazione) degli insiemi come collezioni non sembra poter dare adito a molti tipi diversi di interpretazione, invece parlare di "netta distinzione" può dar luogo a differenti interpretazioni. Esistono collezioni, dette *ricorsivamente enumerabili* per cui esiste una procedura effettiva che elenca tutti gli elementi di una tale collezione. Ma non sempre è detto che esista una procedura effettiva che elenca tutti gli elementi che *non* vi appartengono (qui supponiamo per semplicità di considerare solo collezioni di numeri naturali). Certamente qualcuno potrebbe interpretare come "non perfettamente chiara" la definizione di tale insieme, perchè non si è in grado di conoscere con esattezza quali numeri non vi appartengono (e, comunque, il problema si presenterebbe per il suo complementare). Questo è il motivo per cui abbiamo precisato "in linea di principio". Problemi di questo tipo non si presenteranno nella teoria assiomatica, dove si precisa in ogni

Non solo, un dato elemento non può appartenere ad un insieme “più di una volta”, in altre parole, nella nozione di appartenenza non si considerano “molteplicità”. Gli insiemi $\{4, 6, 8\}$ e $\{4, 4, 6, 6, 8, 8, 8\}$ vanno considerati come lo stesso insieme⁵.

D’ora in poi le lettere romane corsive minuscole $a, b, \dots, x, y \dots$ (e talvolta anche maiuscole $A, B, \dots$) indicheranno sempre insiemi, anche senza che questo venga dichiarato esplicitamente.

1.1.2. Sottoinsiemi. Se tutti gli elementi di un certo insieme x appartengono ad un altro insieme y , si dice che x è un *sottoinsieme* di y , oppure che x è *contenuto* in y , o anche che y *contiene* x , e si scrive $x \subseteq y$. In altre parole, $x \subseteq y$ significa che, per ogni z , si ha che $z \in x$ implica $z \in y$.

Osserviamo che la nozione di appartenenza $\in$ e quella di essere sottoinsieme $\subseteq$ sono ben distinte fra di loro. Per esempio, per ogni insieme x , è vero che $x \subseteq x$. Invece non sempre⁶ è vero che $x \in x$. Ad esempio, se $\emptyset$ indica l’insieme che non ha elementi, sicuramente $\emptyset \notin \emptyset$. È perciò curioso notare che la maggior parte degli autori che hanno usato la teoria degli insiemi all’inizio sembra confondessero (per lo meno a livello di notazione) i due concetti. La distinzione esplicita fra le due nozioni sembra dovuta a Giuseppe Peano.

Se $x \subseteq y$ e $x \neq y$, si dice che x è un *sottoinsieme proprio* di y , e si scrive $x \subset y$, oppure $x \subsetneq y$. Osserviamo che, per ragioni tipografiche, molti testi, specie in passato, usavano $x \subset y$ col significato che abbiamo attribuito qui a $x \subseteq y$. Ribadiamo che, per quanto riguarda convenzioni, notazioni e definizioni, è sempre opportuno fare riferimento al testo che si sta utilizzando, leggendo con attenzione le parti introduttive.

In particolare, $x = y$ vale se e solo se valgono sia $x \subseteq y$ e $y \subseteq x$.

1.1.3. Variabili e costanti*. È importante notare che le lettere x e t nelle condizioni (b) e (c) precedenti sono da considerare come *variabili*, nel senso che possono essere sostituite da altre lettere senza modificare la definizione⁷.

dettaglio quali sono gli insiemi di cui si assume l’esistenza. Resta il fatto che nella teoria assiomatica usuale è richiesta l’esistenza di insiemi di natura molto astratta che qualcuno potrebbe non ritenere corrispondente alla nozione intuitiva appena descritta.

⁵ Esiste la nozione di “multiinsieme”, in cui si tiene conto di eventuali molteplicità. I multiinsiemi sono talvolta utili, particolarmente nella combinatoria finita. Sembra comunque più comodo definire i multiinsiemi in termini di insiemi, anziché viceversa. In questo senso, un multiinsieme può essere definito formalmente come una coppia (X, m) dove m è una funzione da X in $\mathbb{N}$, o eventualmente in un insieme di cardinali, se si ammettono molteplicità infinite.

⁶ In effetti, solitamente si assume addirittura che $x \in x$ non valga mai. Esistono comunque teorie “alternative” degli insiemi in cui è ammessa la possibilità di insiemi che appartengono a se stessi.

⁷ Avendo naturalmente l’accortezza di non utilizzare lettere già utilizzate in precedenza, cioè di non sovrapporre le notazioni. Ad esempio, posso sostituire n con m nella condizione (c’) precedente, ottenendo $\{m \in \mathbb{N} \mid \text{esiste un } t \in \mathbb{N} \text{ tale che } t = 2m \text{ e } 1 < t < 5\}$. Ma se invece sostituissi n con t , otterrei $\{t \in \mathbb{N} \mid \text{esiste un } t \in \mathbb{N} \text{ tale che } t = 2t \text{ e } 1 < t < 5\}$, definizione di dubbia comprensibilità, e che fornisce l’insieme che non ha nessun elemento, visto che non esiste nessun t tale che contemporaneamente $t = 2t$ e $1 < t < 5$. In alcune delle definizioni che seguono daremo per scontato che non si verificano situazioni come quella appena descritta. In senso strettamente formale, a volte andrebbe precisata una condizione in cui si dichiara che

Per esempio, la definizione data in (b) sarebbe completamente equivalente se scritta nella forma $\{y \in \mathbb{N} \mid y \text{ è un numero naturale pari e } 3 \leq y \leq 9\}$. Concettualmente, questa osservazione non dovrebbe comportare particolari difficoltà. Per fare il paragone con una situazione più elementare, risolvere l'equazione $x^3 - 1$ (nella variabile x) equivale a risolvere l'equazione $y^3 - 1$ (nella variabile y). Del resto (come succede anche nel caso della risoluzione di equazioni quando compaiono parametri!) a volte solo dal contesto si è in grado di capire quali sono le variabili e quali sono le costanti. Ad esempio, si consideri la seguente frase:

Sia r un numero reale fissato e sia $X = \{nr \mid n \in \mathbb{N}\} \dots$

Nella definizione di X la variabile è n , e r va considerato come una costante, o un parametro. Una descrizione più concreta di X potrebbe essere $X = \{0, r, 2r, 3r, \dots\}$.

Secondo la convenzione più comune in matematica (ma talvolta vi sono eccezioni) si ammette che variabili distinte possano assumere lo stesso valore, per esempio $2 \in \{n^2 + m^2 \mid n, m \in \mathbb{N}\}$, perché posso considerare $m = n = 1$.

1.1.4. Operazioni fra insiemi. Possono essere definite in maniera naturale molte operazioni fra insiemi. Per esempio, l'*intersezione* $x \cap y$ di due insiemi x e y è l'insieme z che ha per elementi esattamente gli oggetti che sono elementi sia di x che di y . In altre parole, z è il più grande insieme contenuto sia in x che in y .

In maniera simile, l'*unione* $x \cup y$ di due insiemi x e y è l'insieme z che ha per elementi esattamente gli oggetti che sono elementi di almeno uno fra x che di y (è compreso il caso in cui un elemento stia contemporaneamente in x e y). Stavolta, z è il più piccolo insieme che contiene sia x che y .

Il *complemento di y in x* è l'insieme $x \setminus y = \{z \in x \mid z \notin y\}$. Come accennato in precedenza, è ammesso come insieme l'insieme che non ha elementi; esso viene chiamato *insieme vuoto* e indicato con $\emptyset$. Per il principio di estensionalità tutti gli insiemi senza elementi sono uguali o, più brevemente, l'insieme vuoto è unico. Questo giustifica l'uso dell'articolo determinativo quando diciamo *l'insieme vuoto*. Sempre per il principio di estensionalità, tutti gli insiemi che abbiamo introdotto poco sopra sono definiti univocamente, e questo giustifica l'introduzione della notazione che li indica. Notiamo che $x \setminus x = \emptyset$, per ogni insieme x .

Gli insiemi possono contenere altri insiemi come oggetti. In effetti, tutti gli insiemi che considereremo avranno come loro elementi esclusivamente altri insiemi⁸.

una certa variabile va scelta fra variabili non ancora utilizzate.

⁸ Si può sviluppare tutta o praticamente tutta la matematica utilizzando solo gli insiemi, cioè codificando sotto forma di insiemi tutti gli oggetti matematici di cui si ha necessità. O, se si preferisce, costruendo una copia "isomorfa" all'interno della teoria degli insiemi di ciascuna struttura matematica di cui si ha necessità. Ad esempio, vedremo in seguito un metodo per introdurre i numeri naturali sotto forma di insiemi. Da un lato questo modo di trattare gli oggetti matematici può apparire artificioso; d'altro canto ha il vantaggio concettuale di "non moltiplicare le entità". In ogni caso, è stato fatto notare che è tipico della matematica studiare i propri oggetti indipendentemente dal modo in cui vengono presentati o costruiti, cioè basandosi solo sulle relazioni che si suppone valgano fra di loro. Quindi il problema di stabilire se gli (altri) oggetti matematici vadano effettivamente considerati insiemi oppure no è sicuramente un problema di scarso interesse matematico.

Questo aspetto non è comunque fondamentale per la teoria degli insiemi. Si possono dividere gli oggetti di cui si tratta in due categorie, gli insiemi veri e propri e gli altri "oggetti" che

Per esempio, il *singoleto* $\{x\}$ è l'insieme che ha x come unico elemento. Cioè, per qualunque z , si ha $z \in \{x\}$ se e solo se $z = x$.

La *coppia (non ordinata)* $\{x, y\}$ è l'insieme che ha come unici elementi x e y . Osserviamo che, per il principio di estensionalità, $\{x, y\} = \{y, x\}$. Inoltre, $\{x, x\} = \{x\}$.

È spesso utile considerare una *coppia ordinata* (x, y) di due insiemi x e y . Si richiede che questa nozione di coppia ordinata soddisfi alla seguente proprietà:

(C) dati x, y, x_1, y_1 qualunque, si ha che $(x, y) = (x_1, y_1)$ vale se e solo se valgono contemporaneamente $x = x_1$ e $y = y_1$.

Naturalmente, si potrebbe pensare di introdurre una nuova nozione di “insieme ordinato”. Questo non è però necessario: la nozione di coppia ordinata si può comunque introdurre senza “moltiplicare le entità”; una possibile definizione è $(x, y) = \{\{x\}, \{x, y\}\}$. Lasciamo al lettore il compito di verificare che la coppia ordinata definita come sopra⁹ soddisfa effettivamente alla proprietà (C). Suggerimento: trattare separatamente i casi $x \neq y$ e $x = y$.

Il *prodotto (cartesiano)* $A \times B$ di due insiemi A e B è l'insieme $\{(a, b) \mid a \in A, b \in B\}$ di tutte le coppie ordinate con primo elemento in A e secondo elemento in B . Una *relazione* R da A verso B è un sottoinsieme di $A \times B$. In questo modo si può definire la nozione di funzione e, in seguito, tutte¹⁰ le nozioni usate in matematica, le cui definizioni (nei rari casi in cui avremo bisogno di usarle) supporteremo generalmente note al lettore.

1.1.5. *Uso degli insiemi come linguaggio e uso sostanziale**. [...] (per ora chi fosse interessato all'argomento può consultare la prefazione di G. Lolli, *Guida alla teoria degli insiemi*, 2008)

1.2. L'impostazione assiomatica. Le argomentazioni nella sottosezione precedente sono esclusivamente intuitive. Le argomentazioni matematiche, solitamente, richiedono invece una maggiore precisione, in particolare, si richiede di specificare esattamente tutte le ipotesi che vengono usate. Alcune assunzioni

non sono insiemi (spesso chiamati “urelementi”, dal tedesco). Solo gli insiemi possono avere elementi, e questi elementi possono essere sia altri insiemi sia “urelementi”. Invece gli urelementi non possono avere elementi. Il principio di estensionalità si applica solo agli insiemi, e gli “urelementi” si distinguono fra di loro per aspetti che stanno al di fuori della teoria degli insiemi e si considerano noti in altro modo. Esistono pochi ambiti molto tecnici e specialistici in cui l'uso degli urelementi si rivela necessario. Noi non avremo la necessità di considerare urelementi.

⁹ Naturalmente questa definizione di coppia ordinata può apparire artificiosa e poco naturale. Se, da un lato, si tratta comunque di una convenzione, è ovvio che invece lavorare con due nozioni distinte di insieme (non ordinato e ordinato) comporterebbe alla lunga complicazioni ben peggiori. L'unico fatto importante, comunque, è che la proprietà (C) è soddisfatta.

¹⁰ o quasi, secondo l'opinione di alcuni. Rimandiamo il lettore interessato, ad esempio, all'interessante articolo (su sviluppi recenti del dibattito sui fondamenti della matematica) di P. Maddy, *Set-theoretic foundations* apparso in Andrés Eduardo Caicedo, James Cummings, Peter Koellner, Paul B. Larson (editors), *Foundations of Mathematics, Logic at Harvard, Essays in Honor of W. Hugh Woodin's 60th Birthday March 27–29, 2015, Harvard University, Cambridge, MA*, Contemporary Mathematics Volume 690, 2017. Può essere anche utile consultare gli ulteriori riferimenti bibliografici ivi indicati.

vengono prese come basi di partenza, e chiamate *assiomi*. A partire da queste assunzioni, mediante ragionamenti logici, si otterranno i teoremi e le altre conclusioni. I ragionamenti così effettuati dovrebbero risultare validi indipendentemente dalla concezione intuitiva degli oggetti trattati. Questo modo di procedere prende il nome di *metodo assiomatico*¹¹.

Quasi tutte le branche della matematica sono state trattate in maniera assiomatica, anche nel caso in cui le nozioni usate non comportassero nessuna problematicità. Illustri matematici hanno invece spesso messo in dubbio la liceità dell'uso degli insiemi in matematica. Questa constatazione, unita ai problemi e paradossi a cui accenneremo in seguito, suggerisce che in questo caso esiste l'effettiva necessità di una trattazione assiomatica. È importante notare che la trattazione assiomatica non è assolutamente un mezzo per liberarsi dalle controverse o per garantire un tipo di validità assoluta ai metodi che fanno uso degli insiemi. Tutto il contrario! Semplicemente, se si deve discutere su quali metodi possono essere considerati validi o meno, meglio specificare con precisione ciò su cui si sta discutendo.

Grossomodo e a volte con particolari precisazioni, gli assiomi che indicheremo riguardo agli insiemi sono accettati dalla comunità dei matematici¹². Siccome il

¹¹ Nella concezione moderna, gli assiomi non sono interpretati come verità assolute imposte in maniera dogmatica. A volte li si intende come verità intuitivamente evidenti riguardanti certi oggetti particolari, altre volte semplicemente come ipotesi di lavoro che possono o meno essere valide. Secondo questo modo di vedere, l'attività del matematico non fornirebbe verità assolute, presenterebbe solo ragionamenti del tipo: *ammettendo queste e queste ipotesi si ottengono queste e queste conclusioni*. Va da sé che in molti casi queste deduzioni sono tutt'altro che ovvie, sono di una complessità notevole e talvolta vengono giudicate di estrema bellezza o profondità. Ci premeva soltanto sottolineare che decidere sulla validità o meno delle ipotesi non viene considerato solitamente un problema di tipo matematico; il problema viene demandato ad altri, ad esempio, ai fisici (o, qualora non sia necessaria una soluzione immediata, ai filosofi).

Naturalmente, se si richiedesse un rigore assoluto, si dovrebbero specificare esattamente anche quali sono i metodi di ragionamento da considerare validi. Questo può essere fatto, ma esula dall'argomento della presente nota. Rimandiamo il lettore interessato ad un qualunque testo di logica matematica, ad esempio il testo di Mendelson che citeremo nella sezione sulle altre letture. Allo stesso modo di quanto osserveremo riguardo agli assiomi, dichiarare esplicitamente i metodi logici che vengono utilizzati non implica necessariamente la loro validità. D'altro canto, fra la maggior parte dei matematici, risulta esserci un consenso implicito su quali siano i ragionamenti corretti. Noi accetteremo questa pratica senza ulteriori precisazioni, rimandando di nuovo il lettore al libro citato o ad altri testi dedicati esplicitamente ai fondamenti della matematica.

¹² Molte parti della matematica tradizionale possono essere sviluppate facendo uso di sistemi di assiomi molto più deboli di quello che presenteremo. Il campo di ricerca che si occupa di trovare le ipotesi minimali necessarie per dimostrare teoremi classici va sotto il nome di *reverse mathematics* e ha ottenuto risultati di particolare interesse, ad esempio l'identificazione di un piccolo numero di sistemi di assiomi che "misurano" esattamente la complessità delle ipotesi necessarie in un gran numero di casi. Si veda S. G. Simpson, *Subsystems of Second Order Arithmetic*, Second edition, 2009. È modesto parere di chi scrive che questo campo di ricerca è ingiustamente trascurato e non sta ricevendo tutta l'attenzione che meriterebbe. In fondo, è caratteristico della matematica cercare di dimostrare teoremi utilizzando ipotesi minimali.

Come argomento collegato, ma da una prospettiva diametralmente opposta, alcuni problemi matematici complessi non sono risolvibili nella teoria standard degli insiemi, e hanno soluzione solo assumendo ulteriori assiomi. Le tecniche che si occupano di questi argomenti

nostro scopo è di presentare gli argomenti evitando quanto più possibile i dettagli tecnici, trascureremo alcuni assiomi senza descriverli in dettaglio. Questi assiomi sarebbero necessari per realizzare certi obiettivi particolari. Facciamo riferimento ai testi che verranno indicati in seguito per una trattazione più completa e rigorosa. Ci sentiamo corroborati in questa nostra scelta di privilegiare la semplicità alla completezza dal fatto che alcuni dei dettagli tecnici che sarebbero necessari sfuggirono, a suo tempo, anche a grandi personalità matematiche.

1.2.1. Nozioni primitive. Oltre agli assiomi, è necessario precisare anche le nozioni di cui si tratta. Altre nozioni e concetti potranno essere introdotti mediante definizioni, ma le nozioni di partenza non possono essere definite, a meno di non cadere in un circolo vizioso. In teoria degli insiemi gli unici concetti di base sono quelli di *insieme* e di *appartenenza*. Per comodità utilizzeremo anche la nozione di uguaglianza, supponendo che per essa valgano le proprietà intuitive.

1.2.2. Principio di estensionalità. Come precisato sopra, due insiemi si considerano uguali se e solo se hanno esattamente gli stessi elementi. Il nostro primo assioma sarà dunque il seguente¹³.

(PRINCIPIO DI ESTENSIONALITÀ) Due insiemi sono uguali se e solo se hanno esattamente gli stessi elementi.

Intuitivamente il Principio di estensionalità fornisce una “definizione” di insieme, corrispondente alla nozione informale introdotta nella precedente sottosezione. Va comunque considerato come un assioma vero e proprio. Ovviamente, il Principio di estensionalità non può essere usato per dimostrare l’esistenza di insiemi. È quindi necessario introdurre ulteriori assiomi.

1.2.3. Assiomi per la costruzione di insiemi.

(ASSIOMA DELLA COPPIA) Dati due insiemi qualunque x e y , esiste un insieme $\{x, y\}$ che ha per elementi esattamente¹⁴ x e y .

L’assioma della coppia si può esprimere in linguaggio simbolico come

$$\forall xy \exists z \forall w (w \in z \Leftrightarrow (w = x \vee w = y)),$$

sono estremamente sofisticate e includono, fra gli altri, il cosiddetto *forcing*, i *modelli interni*, i *grandi cardinali*, l’*ipotesi di determinatezza*. Il lettore interessato può approfondire l’argomento dapprima studiando il libro di Jech e, in seguito, l’*Handbook of Set Theory*, entrambi citati nella sezione sulle ulteriori letture.

¹³ ** (Le note a pie’ di pagina contrassegnate da due asterischi non sono strettamente necessarie per la comprensione del testo e possono essere “saltate” da chi lo desidera, oppure in una prima lettura. Contengono osservazioni e precisazioni che ci sarebbe sembrato improprio omettere.)

Se, come stiamo facendo, si assume la nozione di uguaglianza come primitiva. In caso contrario, il principio, come stiamo per introdurlo, risulta una definizione. In tal caso è necessario richiedere poi un assioma che dice che due insiemi uguali, nel modo così definito, soddisfano alle stesse proprietà. Preciseremo in seguito cosa debba intendersi per “proprietà”. Il lettore che risultasse perplesso da questo commento non si preoccupi: a volte anche studiosi esperti nel settore confondono i due approcci.

¹⁴ ** Utilizzando l’assioma di separazione, che enunceremo in seguito, è sufficiente richiedere la seguente forma più debole dell’assioma della coppia: *Dati due insiemi qualunque x e y , esiste almeno un insieme u tale che $x \in u$ e $y \in u$.*

dove $\vee$ significa “oppure” (in senso inclusivo, ovvero nel senso che può verificarsi una o l'altra possibilità, e possono anche verificarsi entrambe contemporaneamente). Lasciamo per esercizio al lettore di verificare che tutti gli assiomi che enunceremo si possono scrivere in un linguaggio simbolico come sopra. Mentre cercheremo di essere il meno formali possibile, la necessità di un simile trattamento formale apparirà chiara quando enunceremo l'assioma di separazione più sotto.

Per il principio di estensionalità, data una qualunque coppia di insiemi x e y , l'insieme la cui esistenza è stabilita dall'assioma della coppia è unico, e quindi può essere effettivamente indicato¹⁵ con $\{x, y\}$. D'ora in poi quando un assioma implica l'esistenza di un insieme definito univocamente per estensionalità, daremo direttamente un nome a quest'insieme senza ulteriori precisazioni. Va comunque notato che è necessario fare uso dell'assioma di estensionalità, affinché ciò sia giustificato.

Nell'enunciato dell'assioma della coppia è possibile avere $x = y$; in questo caso si otterrà il singoletto $\{x\}$. In particolare, la coppia ordinata $(x, y) = \{\{x\}, \{x, y\}\}$ si può costruire iterando l'assioma della coppia.

Enunceremo adesso l'assioma dell'unione. Questo assioma ci permette di costruire l'unione $x \cup y$ due insiemi qualunque x e y . Come già precisato $x \cup y$ ha per elementi esattamente tutti gli insiemi che sono elementi di x oppure sono elementi di y (oppure di entrambi). Più in generale, data una famiglia di insiemi

¹⁵ La possibilità di introdurre nuovi simboli per oggetti di cui si dimostrano esistenza ed unicità può apparire lecita al di là di ogni possibile ombra di dubbio e non suscettibile di creare problemi logici. Effettivamente l'introduzione di nuovi simboli è lecita in questa situazione, ma ad un esame più approfondito la questione risulta parecchio delicata.

Una prima possibilità è quella di considerare i nuovi simboli introdotti come abbreviazioni. Ad esempio, tutte le volte che si usa l'espressione $\{x, y\}$ all'interno di un'altra espressione, si suppone che $\{x, y\}$ vada sostituita utilizzando la sua effettiva definizione. Ad esempio, la formula $\{x, y\} \in h$ può essere considerata come un'abbreviazione della formula più complessa $\exists z(\forall w(w \in z \Leftrightarrow (w = x \vee w = y)) \wedge z \in h)$. In questo modo non si introduce nessun nuovo assioma, e i nuovi simboli introdotti sono intesi semplicemente come abbreviazioni utili per migliorare la leggibilità delle formule.

Un approccio più complesso, ma in un certo senso più elegante è quello di introdurre un nuovo assioma per ogni oggetto di cui si dimostrano esistenza ed unicità. A titolo di esempio, l'assioma che descrive il significato che attribuiamo ad $\{x, y\}$ è $\forall w(w \in \{x, y\} \Leftrightarrow (w = x \vee w = y))$. Questo metodo moltiplica il numero dei concetti e degli assiomi usati. Ma la complessità aggiunta è solo apparente. Si può dimostrare che introdurre un nome per ogni oggetto di cui è dimostrabile l'esistenza e l'unicità, insieme ad assiomi che ne caratterizzano le proprietà, produce una *estensione conservativa* della teoria precedente all'introduzione di questi nuovi simboli ed assiomi. Ciò significa che se un enunciato utilizza *solo* il linguaggio della teoria precedente (quella senza i simboli e gli assiomi aggiuntivi), questo enunciato è dimostrabile nella teoria precedente se e solo se è dimostrabile nella teoria “nuova” (quella con i nuovi simboli e i nuovi assiomi). In altre parole, *se ci si limita agli enunciati che non fanno uso esplicito dei nuovi simboli*, in questo caso, ad esempio, del simbolo $\{x, y\}$, si ottengono esattamente gli stessi teoremi. In altri termini ancora, l'aggiunta di questi nuovi simboli ed assiomi può essere considerata inessenziale. Vedi ad esempio la Proposizione 2.29 nel libro di Mendelson.

In qualunque modo si consideri la questione, gli argomenti precedenti ci autorizzano ad introdurre nuovi simboli, cosa che faremo per semplificare la leggibilità

$\{A_i \mid i \in I\}$, l'assioma ci permette di costruire un insieme $\bigcup_{i \in I} A_i$ tale che, per ogni insieme z , si ha che $z \in \bigcup_{i \in I} A_i$ se e solo se esiste $i \in I$ tale che $z \in A_i$.

Qui l'espressione *famiglia* è sinonimo di insieme, ed è usata solo per evitare ripetizioni. La presentazione appena fornita dell'assioma dell'unione ci sembra intuitivamente chiara, ma dovremmo dare un significato preciso all'espressione $\{A_i \mid i \in I\}$. In seguito questo significato verrà reso esplicito, ma va notato che non sempre abbiamo la possibilità di dimostrare l'esistenza di "famiglie" del tipo $\{A_i \mid i \in I\}$, in base ai soli assiomi che abbiamo introdotto finora. In ogni caso, per enunciare la versione rigorosa e "ufficiale" dell'assioma dell'unione non c'è la necessità di considerare famiglie "indicizzate", quindi, formalmente, l'eventuale indicizzazione risulta una complicazione anziché una semplificazione. Tuttavia, forse, il seguente enunciato dell'assioma può apparire meno intuitivo. L'insieme $\mathcal{F}$ considerato nell'assioma seguente va comunque pensato come una famiglia di insiemi.

(ASSIOMA DELL'UNIONE) Dato un qualunque insieme $\mathcal{F}$, esiste l'insieme $\bigcup \mathcal{F} = \{z \mid \text{esiste } h \in \mathcal{F} \text{ tale che } z \in h\}$.

Cioè, per ogni z , $z \in \bigcup \mathcal{F}$ se e solo se esiste $h \in \mathcal{F}$ tale che $z \in h$.

Osserviamo che non è scontato che la forma finita dell'assioma dell'unione segue dalla forma generale. Dobbiamo usare l'assioma della coppia per costruire $\{x, y\}$. Dopodiché $x \cup y = \bigcup \{x, y\}$.

Usando gli assiomi della coppia e dell'unione¹⁶ possiamo costruire terne $\{x, y, z\}$ come $\{x, y\} \cup \{z\}$, e così via. È invece curioso osservare che non abbiamo bisogno dell'assioma dell'unione per costruire le *terne ordinate*, mediante la definizione $(x, y, z) = ((x, y), z)$.

(ASSIOMA DELL'INSIEME POTENZA (O DELLE PARTI)) Dato un insieme qualunque x , esiste l'insieme $\mathcal{P}(x)$ che ha per elementi esattamente tutti i sottoinsiemi di x .

Usando gli assiomi introdotti finora, si può tentare di costruire il prodotto cartesiano $A \times B$ di due insiemi A e B . Se $a \in A$ e $b \in B$, per l'assioma della coppia esistono il singoletto $\{a\}$ e la coppia $\{a, b\}$. Applicando di nuovo l'assioma della coppia con $x = \{a\}$ e $y = \{a, b\}$, abbiamo la coppia ordinata $(a, b) = \{\{a\}, \{a, b\}\}$. Inoltre, siccome $a \in A$, abbiamo $\{a\} \subseteq A$ e, quindi, $\{a\} \in \mathcal{P}(A)$. Siccome $a, b \in A \cup B$, abbiamo anche $\{a, b\} \subseteq A \cup B$ e $\{a, b\} \in \mathcal{P}(A \cup B)$. Siccome $A \subseteq A \cup B$, abbiamo inoltre $\mathcal{P}(A) \subseteq \mathcal{P}(A \cup B)$ (perché ogni sottoinsieme di A è anche sottoinsieme di $A \cup B$). In conclusione, sia $\{a\}$ che $\{a, b\}$ appartengono a $\mathcal{P}(A \cup B)$, quindi $\{\{a\}, \{a, b\}\} \subseteq \mathcal{P}(A \cup B)$, da cui segue $(a, b) = \{\{a\}, \{a, b\}\} \in \mathcal{P}\mathcal{P}(A \cup B)$. Quindi abbiamo che, se $A \times B$ esiste, $A \times B \subseteq \mathcal{P}\mathcal{P}(A \cup B)$. Ma, naturalmente, $A \times B \neq \mathcal{P}\mathcal{P}(A \cup B)$. Per poter costruire $A \times B$ abbiamo quindi bisogno di un assioma che, dato un insieme W ,

¹⁶ ** Va comunque precisato che l'assioma della coppia e più in generale l'esistenza delle n -uple sono una conseguenza degli altri assiomi, quando si consideri la teoria completa.

ci autorizzi a costruire il sottoinsieme di W costituito da tutti gli elementi di W che soddisfano ad una certa proprietà. Costruzioni di questo tipo vengono effettuate in continuazione in matematica, lo studente avrà ascoltato numerose volte frasi del tipo “Sia X l’insieme di tutti i numeri reali tali che ...” e simili, dove al posto dei puntini possono apparire svariate espressioni di vario tipo, a volte anche estremamente complesse. L’assioma che ci serve è dunque il seguente.

(ASSIOMA DI SEPARAZIONE) Per ogni insieme W e ogni “proprietà” φ , esiste l’insieme $\{x \in W \mid \varphi(x)\}$, cioè l’insieme costituito da tutti gli elementi di W per cui vale la proprietà φ .

Formalmente, l’assioma di separazione viene considerato non come un singolo assioma, ma come un’infinità di assiomi, uno per ogni “proprietà” φ . Questo si esprime solitamente dicendo che si tratta di uno *schema* di assiomi.

Più sostanziale è la richiesta di definire esattamente cosa si intenda per “proprietà”. Sebbene esistano possibilità alternative, per *proprietà* si intende solitamente (una proprietà definita da) un’espressione simbolica che può essere costruita in maniera naturale¹⁷ utilizzando i simboli^{18 19} $\in$ e $=$, i connettivi logici $\wedge$ (e), $\vee$ (o), $\neg$ (non), $\Rightarrow$ (implica), variabili $x_1, x_2, \dots$ e i quantificatori $\forall$ (per ogni) e $\exists$ (esiste).

Tornando all’esempio precedente, cioè al tentativo di costruire $A \times B$, gli assiomi della coppia, dell’unione e della potenza ci consentono di costruire $\mathcal{P}\mathcal{P}(A \cup B)$. Esiste una formula φ che esprime l’affermazione “ x è una coppia ordinata con

¹⁷ È abbastanza intuitivo capire quali sono le regole di costruzione per le possibili “formule” φ ammesse nello schema di assiomi di separazione. Per il lettore che richiedesse i dettagli formali, la definizione è data dalle seguenti clausole.

- (1) Se x e y sono variabili, allora sia $x \in y$ che $x = y$ sono formule.
- (2) Se φ e ψ sono formule e x è una variabile, allora tutte le seguenti sono formule: $\varphi \wedge \psi$, $\varphi \vee \psi$, $\neg\varphi$, $\varphi \Rightarrow \psi$, $\forall x\varphi$ e $\exists x\varphi$.
- (3) Sono formule tutte e sole le espressioni simboliche che possono essere ottenute in un numero finito di passi applicando (1) e (2).

Alcune condizioni sono pleonastiche, nel senso che, ad esempio, alcuni connettivi o quantificatori possono essere definiti in termini di altri. A volte è necessario inserire opportune parentesi nella costruzione delle formule come sopra, affinché esse risultino di interpretazione non ambigua. I dettagli sono intuitivamente ovvi.

Inoltre si assume la possibilità che φ dipenda da altri parametri, non solo da x . L’assioma garantisce l’esistenza dell’insieme $\{x \in W \mid \varphi(x)\}$ per ogni valore che può assumere ogni eventuale parametro (facendo uso degli altri assiomi, ci si può comunque ridurre equivalentemente al caso di un solo parametro).

¹⁸ Come precisato in precedenza, all’atto pratico si possono usare ulteriori simboli in φ , purchè le formule che contengono questi simboli siano interpretabili come un’abbreviazione di un’altra formula che non contiene i nuovi simboli.

Sarebbe anche molto importante osservare che qui stiamo identificando i simboli con la loro interpretazione. Le due nozioni sono in realtà ben distinte.

¹⁹ Quando scriviamo $A \in x$ intendiamo che la relazione $\in$ vale realmente per certi insiemi A ed x . Invece, quando parliamo della *formula* $x \in y$, allora $\in$ va inteso come un simbolo grafico. Allo stesso modo, nella *formula* $x \in y$ le lettere x e y sono semplici simboli che si pensano possibilmente interpretabili come insiemi, ma, in questo caso, non vanno considerate *esse stesse* insiemi. Il lettore che decidesse di dedicarsi allo studio della logica matematica, in particolare della teoria dei modelli, sarebbe costretto molto presto a rendersi conto dell’importanza di questa distinzione, che a prima vista potrebbe apparire dovuta esclusivamente a pignoleria.

primo elemento in A e secondo elemento in B ". Dunque l'assioma di separazione ci consente di costruire l'insieme $\{x \in \mathcal{P}\mathcal{P}(A \cup B) \mid x \text{ è una coppia ordinata con primo elemento in } A \text{ e secondo elemento in } B\}$. Per quanto detto sopra, questo insieme è proprio $A \times B$.

1.2.4. L'assioma dell'infinito. Gli assiomi presentati finora ci garantiscono la possibilità di costruire certi insiemi a partire da uno o più insiemi dati, ma finora non abbiamo nulla che ci dimostri l'esistenza di almeno un insieme. Se si assume l'esistenza di almeno un insieme W , l'assioma di separazione ci fornisce il vuoto, dato da $\{x \in W \mid x \neq x\}$. Usando poi l'assioma della coppia possiamo costruire altri insiemi come $\{\emptyset\}$, $\{\{\emptyset\}\}$, $\{\emptyset, \{\emptyset\}\}$ ecc.

Anziché richiedere l'esistenza di un insieme qualunque, richiederemo l'esistenza di un insieme che soddisfi ad una particolare proprietà.

(ASSIOMA DELL'INFINITO) (versione informale) Esiste un insieme infinito.

Forse la definizione di "infinito" può sembrare ovvia. In realtà non è affatto così; addirittura, esistono diverse definizioni di "infinito" che non sono equivalenti, se non sotto certe assunzioni, anche se ciascuna cattura alcune proprietà che intuitivamente caratterizzano le collezioni infinite.

Per esprimere con precisione l'assioma dell'infinito, chiederemo l'esistenza di un insieme che contiene tutti i numeri naturali. Detto in questo modo si tratta di un circolo vizioso, poiché, insiemisticamente, un numero naturale è esattamente un elemento di $\mathbb{N}$. Ma è proprio $\mathbb{N}$ che vogliamo definire! All'inconveniente si può ovviare nel modo che stiamo per spiegare, ma prima descriviamo informalmente i numeri naturali. I primi numeri naturali si definiscono (o si interpretano, se si preferisce) nel seguente modo:

$$\begin{aligned} 0 &= \emptyset, \\ 1 &= 0 \cup \{0\} = \emptyset \cup \{\emptyset\} = \{\emptyset\} = \{0\}, \\ 2 &= 1 \cup \{1\} = \{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\} = \{0, 1\}, \\ 3 &= 2 \cup \{2\} = \{0, 1\} \cup \{2\} = \{0, 1, 2\}, \text{ e così via.} \end{aligned}$$

Potremmo pensare di iterare queste definizioni al seguente modo:

$$\begin{aligned} 0 &= \emptyset, \\ s(n) &= n + 1 = n \cup \{n\}, \quad \text{per ogni naturale } n, \end{aligned} \tag{*}$$

ma questa definizione "ricorsiva" è lecita solo se ammettiamo già di conoscere i numeri naturali²⁰. La conoscenza dei numeri naturali non è affatto una richiesta forte, ma preferiamo comunque che la teoria che presentiamo sia completamente autosufficiente²¹. Osserviamo che, in base alle definizioni precedenti, abbiamo

²⁰ ** L'uso della struttura di tutti i numeri naturali è implicito nell'espressione "e così via". Beninteso, possiamo iterare le definizioni date in precedenza un numero finito di volte, cioè possiamo definire un qualunque numero naturale, grande quanto si vuole. Quello che non possiamo ancora fare è considerare la definizione precedente come una definizione che comprende contemporaneamente *tutti* i numeri naturali.

²¹ In effetti, anche la definizione di formula, in una nota precedente relativa all'assioma di separazione, è implicitamente data per induzione, quindi comporta la conoscenza di alcune proprietà dei numeri naturali. Il punto sostanziale è che si tratta di due livelli differenti, la

(intuitivamente) che un numero naturale è l'insieme di tutti i suoi predecessori, e che il numero n ha esattamente n elementi.

Il trucco per “definire l'infinito senza fare uso dell'infinito”, essenzialmente dovuto a Dedekind (e formalizzato in questa maniera probabilmente da von Neumann), è il seguente. Diciamo che un insieme I è *induttivo* se $\emptyset \in I$ e, ogni volta che un insieme x appartiene ad I , allora anche il suo *successore* $s(x) = x \cup \{x\}$ appartiene ad I . Così, ricordando le definizioni precedenti, un insieme induttivo contiene $0 = \emptyset$. Ma allora contiene anche $1 = 0 \cup \{0\}$, $2 = 1 \cup \{1\}$...

Quindi l'enunciato formale dell'assioma dell'infinito è il seguente.

(ASSIOMA DELL'INFINITO) Esiste un insieme induttivo I .

Come abbiamo detto, intuitivamente un insieme induttivo contiene tutti i numeri naturali. La definizione di $\mathbb{N}$ sarà dunque la seguente: $\mathbb{N}$ è l'insieme che contiene tutti gli elementi che appartengono a tutti gli insiemi induttivi. La definizione è giustificata in base all'assioma di separazione e siccome, in base all'assioma dell'infinito, esiste almeno un insieme induttivo I . Formalmente,

$\mathbb{N} = \{n \in I \mid n \text{ appartiene ad ogni insieme induttivo}\}$,

dove è facile costruire una formula che esprime la frase in parole contenuta nell'espressione precedente. Dunque $\mathbb{N}$ esiste, per l'assioma di separazione, ed è facile vedere che la definizione di $\mathbb{N}$ non dipende dalla particolare scelta di un insieme induttivo I . Inoltre è facile controllare che $\mathbb{N}$ stesso è induttivo, quindi contiene $0, 1, \dots$

Si può vedere che $\mathbb{N}$ con l'operazione di successore soddisfa agli assiomi di Peano-Dedekind²², che se $n \neq m \in \mathbb{N}$, allora non esiste una biiezione fra m ed n , e che se $n \in \mathbb{N}$, allora non esiste una biiezione fra n ed $\mathbb{N}$. Si possono dunque finalmente dare le seguenti definizioni. Un insieme x si dice *finito* se esistono un $n \in \mathbb{N}$ ed una biiezione fra x ed n . Un insieme x si dice *infinito* se non è finito; così, per quanto affermato sopra, abbiamo che $\mathbb{N}$ è infinito. Un insieme si dice *numerabile*^{23 24} se può essere messo in corrispondenza biunivoca con $\mathbb{N}$.

nozione di formula è *metamatematica*, ed è praticamente impossibile sviluppare la metamatematica in maniera significativa senza dare per note alcune nozioni e proprietà riguardanti l'aritmetica elementare (o, per lo meno, questa è l'opinione largamente diffusa. Per opinioni diverse, che vengono talvolta classificate sotto il nome *ultrafinitismo*, si veda [...]). Invece, a livello della teoria formale che stiamo sviluppando, tutte le nuove nozioni devono essere definite, inclusa quella di numero naturale. Per maggiori dettagli sulla distinzione fra matematica e metamatematica facciamo riferimento al libro di Mendelson, o a libri più specificatamente dedicati ai fondamenti della matematica.

²² ** L'operazione di successore $s : \mathbb{N} \rightarrow \mathbb{N}$ data da $s(n) = n \cup \{n\}$ è effettivamente definita, poichè, pensandola come un insieme di coppie ordinate, è $s = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid y = x \cup \{x\}\}$, e l'esistenza di questo insieme segue dagli assiomi.

²³ Alcuni autori usano “numerabile” nel senso di “finito oppure numerabile”. In lingua inglese, solitamente *denumerable* significa “numerabile” secondo la nostra definizione, mentre *countable* significa “finito oppure numerabile”.

²⁴ ** Per quanto le convenzioni non abbiano particolare importanza, purché esplicitamente dichiarate, e per quanto, limitatamente alla matematica o alla scienza in generale, la praticità d'uso abbia sicuramente la preminenza su questioni di purismo linguistico, l'uso italiano del termine “contabile” al posto di “finito oppure numerabile” ci apparirebbe una violenza non giustificata alla nostra lingua.

1.2.5. Costruzioni ulteriori. Una volta “costruito” l’insieme $\mathbb{N}$ dei numeri naturali, lo si può dotare delle consuete operazioni²⁵. Infatti, disponendo dei prodotti cartesiani, un’operazione binaria su $\mathbb{N}$ è (o si può pensare) come un sottoinsieme di $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$. Una volta costruito $\mathbb{N}$, si può costruire l’insieme $\mathbb{Z}$ dei numeri interi (positivi e negativi), per esempio pensandolo come opportuno quoziente di $\mathbb{N} \times \mathbb{N}$. In questo modo, come è ben noto, risulta facile estendere le operazioni da $\mathbb{N}$ a $\mathbb{Z}$. La struttura $\mathbb{Q}$ dei numeri razionali può poi essere introdotta facendo uso di un quoziente di $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$. Supponiamo che queste costruzioni siano note al lettore. In base agli esempi dati, appare evidente come gli assiomi che abbiamo presentato giustifichino queste costruzioni.

La struttura dei numeri reali $\mathbb{R}$ può poi essere introdotta facendo uso delle sezioni di Dedekind, o (di certe classi di equivalenza) delle successioni di Cauchy di numeri razionali, secondo costruzioni che (anche queste!) dovrebbero essere ben note al lettore.

È importante osservare che, mentre i passaggi da $\mathbb{N}$ a $\mathbb{Z}$ e da $\mathbb{Z}$ a $\mathbb{Q}$ non fanno uso sostanziale della teoria degli insiemi (ad esempio, si può sempre considerare un numero razionale come una coppia di interi ridotta ai minimi termini; anzi, è ciò che si fa abitualmente quando i numeri razionali si scrivono sotto forma di “frazioni”), d’altro canto l’introduzione dei numeri reali fa effettivamente uso essenziale degli insiemi. Per esempio, le sezioni di Dedekind sono coppie di *sottoinsiemi* di $\mathbb{Q}$. Qualunque opinione si abbia sulla teoria degli insiemi, ammettere la possibilità di lavorare con numeri reali arbitrari (non definibili da particolari regole od espressioni, come è invece possibile per $\sqrt{2}$ o π , ad esempio), significa comunque ammettere la validità di una teoria equivalente ad un frammento non insignificante della teoria degli insiemi che qui abbiamo presentato. La stessa presentazione assiomatica dei numeri reali, come campo ordinato, archimedeo e completo, dà per nota la conoscenza dei sottoinsiemi di numeri reali (nella definizione di completezza).

1.2.6. I paradossi. [...] (per ora vedi l’introduzione del libro di Mendelson, p. 10–12)

1.2.7. L’assioma di scelta. [...] (per ora si può guardare la Sez. 5 del Capitolo IV del libro di Mendelson, notando che però presenta un’assiomatizzazione diversa)

1.2.8. Brevi cenni ad ulteriori assiomi*. Come abbiamo accennato all’inizio, l’elenco degli assiomi che abbiamo presentato non è del tutto completo. È assolutamente necessario considerare una forma più forte dell’assioma di separazione che, detto in maniera molto approssimativa, ci consenta di costruire certe famiglie $\{A_i \mid i \in I\}$ di

²⁵ ** mediante le definizioni “ricorsive”

$$n + 0 = n,$$

$$n + s(m) = s(n + m),$$

$$n \cdot 0 = 0,$$

$$n \cdot s(m) = n \cdot m + n.$$

Mentre è intuitivamente chiaro che le precedenti condizioni definiscono effettivamente due operazioni su $\mathbb{N}$, una giustificazione rigorosa richiederebbe alcuni dettagli per i quali rimandiamo ad un qualunque testo di teoria degli insiemi.[...]

insiemi la cui esistenza non seguirebbe dagli altri assiomi. Come già detto, la questione è talmente delicata che ha tratto in inganno illustri matematici.

[...] (vedi anche [...] sotto)

Altre letture. Un libro molto utile, apparentemente elementare ma in realtà decisamente denso, dove (a dispetto del titolo) si presenta la teoria degli insiemi in maniera assiomatica anche se non formalizzata è Paul Halmos, *Naive Set Theory*, varie edizioni, trad. it., *Teoria elementare degli insiemi*, varie ristampe.

Utile materiale in lingua italiana si può trovare ai seguenti indirizzi:

(Alessandro Andretta)

<http://www.logicatorino.altervista.org/materiale/Elementi.pdf>

(Mauro Di Nasso) <http://www.dm.unipi.it/cluster-pages/dinasso/eti-2014.html>

(Piero Plazzi) <http://campus.unibo.it/74334/1/Insiemi.pdf>

Il manuale ormai classico riguardante la teoria degli insiemi è Thomas Jech, *Set Theory. The Third Millennium Edition, revised and expanded*, 2002, successive ristampe con correzioni.

Un manuale aggiornato agli sviluppi più recenti è Matthew Foreman, Akihiro Kanamori (Editors), *Handbook of Set Theory*, 2010, tre volumi.

Come testo di base riguardante la logica matematica consigliamo, fra le tante possibilità, il libro di Elliot Mendelson, *Introduction to Mathematical Logic*, varie edizioni, trad. it. *Introduzione alla Logica Matematica*. Di sicuro interesse per lo studente che voglia approfondire le questioni fondazionali è il libro di Gabriele Lolli, *Filosofia della matematica*, 2002.

2. Insiemi bene ordinati

In questa sezione studiamo le relazioni di buon ordine, che hanno fatto parte della teoria degli insiemi fin dagli inizi, e che hanno trovato applicazioni di tipo molto vario. Prima di dare la definizione di insieme bene ordinato, presentiamo alcuni esempi (fra i tanti possibili) che forniscono motivazioni per lo studio della nozione generale.

2.1. Iterazioni transfinitive. In matematica abbondano procedimenti che possono essere iterati un numero finito ma arbitrariamente alto di volte. Abbiamo visto sopra le definizioni ricorsive di successore, e della somma e del prodotto fra naturali. Un altro esempio tipico è la definizione di fattoriale di un numero naturale, data da $0! = 1$ e $(n + 1)! = n!(n + 1)$.

In alcuni casi è possibile considerare un passo “all’infinito”, per esempio, se $(a_n)_{n \in \mathbb{N}}$ è una successione di numeri reali, si possono considerare le somme finite (parziali) degli elementi a_n definite ovviamente da

$$\begin{aligned} S_0 &= 0, \\ S_{m+1} &= S_m + a_m, \end{aligned}$$

cioè, $S_m = \sum_{n < m} a_n = a_0 + a_1 + \dots + a_{m-1}$. Allora, come ben noto, la serie $\sum_{n \in \mathbb{N}} a_n$ è definita come $\lim_{m \in \mathbb{N}} S_m$, naturalmente supponendo che il limite esista.

In alcuni casi è addirittura possibile procedere ancora oltre, come stiamo per vedere²⁶.

2.1.1. Gruppi risolubili generalizzati. Ricordiamo che se H e K sono sottogruppi di un gruppo G , il loro commutatore $[H, K]$ è il sottogruppo di G generato da $\{hkh^{-1}k^{-1} \mid h \in H, k \in K\}$. Non è necessario conoscere approfonditamente la teoria dei gruppi per seguire questo esempio, basta sapere che $[H, K]$ è un sottogruppo contenuto sia in H che in K , in particolare, $G^{(1)} = [G, G]$ è un sottogruppo di G , $G^{(2)} = [G^{(1)}, G^{(1)}]$ è un sottogruppo di $G^{(1)}$ (quindi anche un sottogruppo di G), e così via. In dettaglio, se definiamo

$$G^{(0)} = G, \text{ e}$$

$$G^{(n+1)} = [G^{(n)}, G^{(n)}], \text{ per } n \in \mathbb{N},$$

otteniamo una successione decrescente²⁷ $(G^{(n)})_{n \in \mathbb{N}}$ di sottogruppi di G .

Un gruppo si dice *risolubile* se esiste $n \in \mathbb{N}$ tale che $G^{(n)} = \{e\}$, il sottogruppo minimo. Ricordiamo che un gruppo G è *abeliano* se $hk = kh$, per tutti gli $h, k \in G$. Siccome un gruppo è abeliano se e solo se $G^{(1)} = [G, G] = \{e\}$, la nozione di gruppo risolubile estende quella di gruppo abeliano. Intuitivamente un gruppo è risolubile se e solo se può essere costruito usando “blocchi” abeliani. Esistono definizioni equivalenti di gruppo risolubile che rendono più precisa questa intuizione. In particolare, se $G^{(1)} = [G, G] = G$, allora G è invece “il meno abeliano possibile”.

Ovviamente, se $G^{(\bar{n}+1)} = G^{(\bar{n})}$, per qualche $\bar{n}$, allora la successione si stabilizza, cioè $G^{(\bar{n}+2)} = [G^{(\bar{n}+1)}, G^{(\bar{n}+1)}] = [G^{(\bar{n})}, G^{(\bar{n})}] = G^{(\bar{n}+1)} = G^{(\bar{n})}$, dove abbiamo usato a turno la definizione di $G^{(n+2)}$ o di $G^{(n+1)}$ e l'ipotesi $G^{(\bar{n}+1)} = G^{(\bar{n})}$. Continuando allo stesso modo, se $G^{(\bar{n}+1)} = G^{(\bar{n})}$, allora $G^{(m)} = G^{(\bar{n})}$, per ogni $m \geq \bar{n}$.

Se G è un gruppo finito, la successione $(G^{(n)})_{n \in \mathbb{N}}$ si stabilizza da un certo punto in poi, e sono possibili entrambi i casi estremi $G^{(1)} = G$, e quindi $G^{(n)} = G$, per ogni $n \in \mathbb{N}$, oppure $G^{(\bar{n})} = \{e\}$, per qualche $\bar{n}$, e quindi $G^{(m)} = \{e\}$ per ogni $m \geq \bar{n}$.

Se invece G è infinito, è possibile che la successione $(G^{(n)})_{n \in \mathbb{N}}$ sia strettamente decrescente. In questo caso il sottogruppo $G^{(\omega)} = \bigcap_{n \in \mathbb{N}} G^{(n)}$ è un gruppo strettamente contenuto in ciascuno dei $G^{(n)}$. Si ha quindi una generalizzazione

²⁶ ** In realtà anche la somma si può iterare “oltre l'infinito”. Se $(b_n)_{n \in \mathbb{N}}$ è un'altra successione di numeri reali, possiamo definire $S_\omega = \sum_{n \in \mathbb{N}} a_n$, poi $S_{\omega+1} = S_\omega + b_0$, e $S_{\omega+2} = S_\omega + b_0 + b_1$ e, in generale, $S_{\omega+m} = S_\omega + \sum_{n < m} b_n$ e prendere ancora il limite, sempre supponendo che esista, $S_{\omega+\omega} = \lim_{m \in \mathbb{N}} (S_\omega + \sum_{n < m} b_n)$. Non sembrano esserci però molte applicazioni di questa iterazione transfinita della somma (vedi comunque per argomenti correlati il Capitolo IV di Udo Hebisch, Hanns Joachim Weinert, *Semirings: Algebraic Theory and Applications in Computer Science*, 1998). Invece le definizioni che presentiamo nelle prossime sottosezioni hanno molte applicazioni interessanti.

²⁷ decrescente rispetto alla relazione di inclusione; qui con *decrescente* si intende decrescente in senso non necessariamente stretto.

della nozione di gruppo risolubile, quella di gruppo risolubile di indice ω , cioè un G tale che $G^{(\omega)} = \{e\}$.

Fino a qui il nostro esempio non ha nulla di sostanzialmente diverso dal caso delle serie discusso in precedenza. Ma in questo caso possiamo continuare oltre. Avendo definito

$$G^{(\omega)} = \bigcap_{n \in \mathbb{N}} G^{(n)},$$

possiamo porre

$$G^{(\omega+1)} = [G^{(\omega)}, G^{(\omega)}],$$

$$G^{(\omega+2)} = [G^{(\omega+1)}, G^{(\omega+1)}], \dots$$

(qui, almeno per ora, gli esponenti ω , $\omega + 1$, $\omega + 2$ non hanno un significato particolare, li stiamo semplicemente usando come indici con significato intuitivo. Il simbolo ω rappresenta l'infinito, anzi, *un* infinito, visto che poi consideriamo subito dopo "infiniti ancor più grandi". Tutto il discorso verrà reso rigoroso fra qualche sezione). In generale, poniamo

$$G^{(\omega+n+1)} = [G^{(\omega+n)}, G^{(\omega+n)}], \text{ per } n \in \mathbb{N},$$

e così abbiamo definito $G^{(\omega+n)}$, per ogni $n \in \mathbb{N}$. Ormai che abbiamo iniziato, sarebbe limitativo fermarsi qui! Poniamo

$$G^{(\omega+\omega)} = \bigcap_{n \in \mathbb{N}} G^{(\omega+n)},$$

e, ancora,

$$G^{(\omega+\omega+n+1)} = [G^{(\omega+\omega+n)}, G^{(\omega+\omega+n)}], \text{ per } n \in \mathbb{N},$$

$$G^{(\omega+\omega+\omega)} = \bigcap_{n \in \mathbb{N}} G^{(\omega+\omega+n)}.$$

È convenzione (dovuta a motivi storici che sarebbero lunghi da spiegare) scrivere $\omega 2$ (anziché 2ω) per $\omega+\omega$, scrivere $\omega 3$ per $\omega+\omega+\omega$ e così via. Procedendo come sopra, possiamo definire $G^{(\omega m+n)}$, per ogni $m, n \in \mathbb{N}$. Ma possiamo andare ancora oltre. Sia

$$G^{(\omega^2)} = \bigcap_{m \in \mathbb{N}} G^{(\omega m)}.$$

Il lettore si potrebbe chiedere perchè non abbiamo invece definito

$$G^{(\omega^2)} = \bigcap_{m, n \in \mathbb{N}} G^{(\omega m+n)}.$$

È chiaro che queste definizioni di $G^{(\omega^2)}$ risultano equivalenti; basta controllare che $G^{(\omega(m+1))} \subseteq G^{(\omega m+n)} \subseteq G^{(\omega m)}$, per ogni $m, n \in \mathbb{N}$.

Quanto a lungo si può continuare con costruzioni di questo tipo? Il problema è semplicemente quello di stabilire un opportuno insieme di indici (ma questo compito è tutt'altro che banale!). Per questo appropriato insieme di indici, diciamo, $\alpha \in A$, deve essere ben definito $G^{(\alpha+1)}$ ogni qual volta è definito $G^{(\alpha)}$, e inoltre, se α non ha nessun immediato predecessore (come, ad esempio, ω oppure $\omega + \omega$ nella costruzione precedente), $G^{(\alpha)}$ deve essere definito in funzione solo dei $G^{(\beta)}$, con β che varia fra tutti gli elementi che "precedono" α . Questo "sistema di indici" deve essere congegnato in modo che questo tipo di definizioni garantiscano davvero che $G^{(\alpha)}$ è definito *per ogni* $\alpha \in A$.

Stabiliremo in seguito un sistema di indici che soddisfa alle proprietà desiderate; supponiamo di averlo definito e lo chiameremo On . Avvertiamo da subito che On risulterà una classe propria, non un insieme. Ovviamente, in ogni singolo caso pratico, sarà sempre possibile considerare come sistema di indici un *insieme*

A contenuto in On .

Sotto queste ipotesi, possiamo definire:

$$G^{(0)} = G,$$

$$G^{(\alpha+1)} = [G^{(\alpha)}, G^{(\alpha)}], \text{ e}$$

$G^{(\alpha)} = \bigcap_{\beta < \alpha} G^{(\beta)}$, se α è *limite*, cioè se non ha un immediato predecessore, cioè ancora se non è della forma $\alpha = \beta + 1$, per qualche β .

Nella definizione precedente, $\beta < \alpha$ significa che β è un indice che è stato costruito, o considerato, prima di α ; tutto questo verrà reso rigoroso in seguito.

Un gruppo *risolubile generalizzato* è un gruppo G tale che $G^{(\alpha)} = \{e\}$, per qualche $\alpha \in On$. I gruppi risolubili generalizzati costituiscono un'estensione molto ampia della classe dei gruppi risolubili. Un'introduzione all'argomento si può trovare nel libro di Robinson *Generalized solvable groups*.

Costruzioni analoghe alla precedente possono svolgersi in un ambito molto ampio: basta disporre di un oggetto iniziale X_0 , avere una regola che definisce $X_{\alpha+1}$ ogni volta che si conosce X_α , e infine poter costruire X_α quando α non ha predecessori immediati; quest'ultima costruzione deve dipendere solo dagli X_β precedenti; solitamente, in questo "caso limite" X_α è l'intersezione (oppure l'unione) di tutti gli X_β precedenti²⁸.

Nell'esempio intuitivo precedente, quando ci siamo fermati a $G^{(\omega^2)}$, abbiamo considerato un insieme numerabile di indici. La costruzione può essere prolungata con insiemi di indici non numerabili, anzi, di qualunque cardinalità (assumendo l'assioma di scelta).

È invece molto significativo che la costruzione che presentiamo nella sottosezione seguente si stabilizza sempre dopo un numero finito oppure un'infinità numerabile di passi, anche se, sempre restando nel numerabile, la costruzione può risultare lunga a piacere.

2.1.2. *Il derivato di uno spazio topologico e cenni al teorema di Cantor-Bendixson.* [...] Per ora chi fosse interessato può guardare i Teoremi 4.5 e 4.6 del libro di Jech.

Storicamente questa costruzione sembra essere stata la prima in cui si fa uso di insiemi bene ordinati, anzi, sembra essere stata la motivazione principale di Cantor per introdurre la nozione di buon ordine.

2.1.3. *La gerarchia V_α di von Neumann.* Possiamo definire

$$V_0 = \emptyset,$$

$$V_{n+1} = \mathcal{P}(V_n).$$

In questo modo otteniamo una successione crescente (rispetto all'inclusione) di insiemi $(V_n)_{n < \omega}$. È quindi naturale definire

$$V_\omega = \bigcup_{n \in \mathbb{N}} V_n, \text{ e, iterando come sopra,}$$

²⁸ ** In realtà, le condizioni precedenti si possono sia unificare che generalizzare richiedendo che, per ogni α , X_α sia definito in funzione di tutti gli X_β , con β che precede α . Grossomodo, la differenza è simile alla differenza fra l'induzione "semplice" e l'induzione forte, cosiddetta "sul decorso dei valori". Rimandiamo a qualunque libro di teoria degli insiemi per i dettagli tecnici. In realtà questi dettagli, a nostro parere, illuminano l'idea principale, ma non sembrano comunque adatti per chi si stia avvicinando all'argomento.

$$V_{\omega m+n+1} = \mathcal{P}(V_{\omega m+n}),$$

$$V_{\omega(m+1)} = \bigcup_{n \in \mathbb{N}} V_{\omega m+n}.$$

In generale, supponendo, come nelle sezioni precedenti, di aver introdotto un opportuno sistema di indici, possiamo definire:

$$V_0 = \emptyset,$$

$$V_{\alpha+1} = \mathcal{P}(V_\alpha),$$

$$V_\alpha = \bigcup_{\beta < \alpha} V_\beta, \text{ se } \alpha \text{ è limite, cioè se non ha un immediato predecessore.}$$

[...]

2.1.4. Iterare l'operazione di successore. Ricordiamo che avevamo definito il successore $s(x)$ di un insieme x come $s(x) = x \cup \{x\}$. In particolare, abbiamo costruito i numeri naturali definendo $0 = \emptyset$ e $n+1 = s(n) = n \cup \{n\}$. Ricordiamo che questa definizione è delicata e le abbiamo potuto dare un senso preciso solo dopo l'introduzione dell'assioma dell'infinito. Con questa definizione ogni numero naturale n ha cardinalità n ed è l'insieme di tutti i numeri naturali più piccoli.

Possiamo iterare l'operazione di successore come negli esempi precedenti, utilizzando l'operazione di unione nel caso "limite" (intuitivamente questo è giustificato poiché vogliamo che qualunque insieme costruito in questo modo sia l'insieme di tutti gli oggetti "minori").

Quindi la definizione di successore generalizzato sarebbe la seguente:

$$s_0 = \emptyset,$$

$$s_{\alpha+1} = s_\alpha \cup \{s_\alpha\},$$

$$s_\alpha = \bigcup_{\beta < \alpha} s_\beta, \text{ se } \alpha \text{ è limite.}$$

Intuitivamente, un *ordinale* è un insieme che si può ottenere nel modo precedente iterando al transfinito l'operazione di successore. In realtà, la classe degli ordinali sarà esattamente la classe degli indici appropriata per le iterazioni transfinito di cui abbiamo dato esempi in questa e nelle sottosezioni precedenti. Quindi sarebbe circolare dare la definizione di ordinale nel modo appena presentato. Può forse comunque essere intuitivamente utile.

2.2. Metodi per controllare che un programma termini dopo un numero finito di passi. Quando si lavora con numeri naturali, spesso si usa il fatto che non esistono successioni infinite strettamente decrescenti di numeri naturali.

Ad esempio, se si calcola il massimo comun divisore di due numeri naturali m ed n utilizzando l'algoritmo delle divisioni successive, si ottiene una successione²⁹ decrescente di resti. Questa successione dunque termina dopo un numero finito di passi, per quanto detto sopra, e ciò significa che prima o poi si ottiene un resto nullo (se il resto non fosse nullo il procedimento potrebbe continuare).

²⁹ Per comodità in questa sezione *successione* può significare sia successione numerabile nel senso usuale in matematica, sia una successione finita, cioè una n -upla ordinata di oggetti, per qualche $n \in \mathbb{N}$.

L'algoritmo, che supponiamo noto al lettore, ci dice che l'ultimo resto non nullo è il massimo comun divisore dei due numeri dati³⁰.

Considereremo adesso dei programmi in cui, in alcuni passi, può essere richiesto all'utilizzatore di inserire numeri naturali arbitrari. Ogni passo del programma, generalmente, viene effettuato scegliendo una fra due o più opzioni. La modalità in cui viene effettuata questa scelta non ci interessa, può essere effettuata dall'utilizzatore, o dipendere da un qualche stato interno della macchina, o anche semplicemente essere effettuata in base ad una scelta casuale. Vogliamo però che il programma termini *sempre* dopo un numero finito (anche se arbitrario, cioè non prefissato in partenza) di passi, qualunque siano i numeri inseriti dall'utilizzatore, e in qualunque modo venga effettuata la scelta fra le eventuali opzioni ad ogni passo.

Un esempio è il seguente:

(a) All'inizio il programma chiede all'utilizzatore di inserire due numeri naturali a e b .

(b) Ad ogni passo successivo il programma esegue una delle seguenti due operazioni³¹:

$a \mapsto a + 1$ e $b \mapsto b - 2$, oppure

$a \mapsto a - 2$ e $b \mapsto b + 1$.

(c) Il programma termina se almeno uno fra a e b assume un valore strettamente negativo. Altrimenti una delle operazioni in (b) viene eseguita nuovamente.

Questo programma prima o poi termina, poiché la funzione $\rho(a, b) = a + b$ assume sempre valori naturali e decresce strettamente ad ogni passo (a rigore $\rho(a, b)$ potrebbe assumere valori interi negativi, ma allora almeno uno fra a e b è negativo, e questo implica che il programma termina). Che un programma del tipo precedente prima o poi termini non è affatto scontato, in generale. Se avessimo invece considerato la seguente condizione (b*) al posto di (b):

(b*) Ad ogni passo successivo il programma esegue una delle seguenti due operazioni:

$a \mapsto a + 1$ e $b \mapsto b - 1$

oppure

$a \mapsto a - 1$ e $b \mapsto b + 1$

allora vi sono situazioni in cui il programma può continuare all'infinito senza fermarsi. Ad esempio, basta scegliere $a > 0$ e $b > 0$ ed eseguire alternativamente le due opzioni.

Altro esempio:

³⁰ Ci sembra importante osservare che la divisione con resto è possibile per numeri reali arbitrari t ed s . Dati tali t ed $s \neq 0$ reali esistono e sono unici $q \in \mathbb{Z}$ ed $r \in \mathbb{R}$ tali che $t = qs + r$ e $0 \leq r < |s|$. Ma, nel caso di numeri reali, l'algoritmo delle divisioni successive non sempre termina. Il lettore saprebbe precisare quali sono i casi in cui termina?

³¹ Qui quando scriviamo, ad esempio, $a \mapsto a + 1$, intendiamo che il programma *asigna* alla variabile a il valore precedente aumentato di 1. Siccome questo è un lavoro rivolto anche ai matematici, si creerebbero troppe ambiguità usando a questo scopo invece il simbolo $=$, come avviene in molti linguaggi di programmazione.

(b**) Ad ogni passo il programma esegue una delle seguenti operazioni:

$$a \mapsto a + 1 \text{ e } b \mapsto b - 2$$

oppure

$$a \mapsto a - 1 \text{ e } b \mapsto b + 1$$

Questo programma termina sempre, poiché $\rho(a, b) = 3a + 2b$ è strettamente decrescente ad ogni passo. Osserviamo che in questo caso la funzione $\rho(a, b) = a + b$ non sarebbe servita, poiché non *strettamente* decrescente.

Esistono però situazioni in cui la dimostrazione che il programma termina è più complessa. Consideriamo il seguente esempio (le condizioni (a) e (c) restano sempre invariate).

(b***) Ad ogni passo il programma esegue una delle seguenti operazioni:

$$a \mapsto a - 1 \text{ e } b \text{ viene sostituito da un numero positivo qualunque,}$$

oppure

$$a \text{ resta invariato e } b \mapsto b - 1.$$

È intuitivo che questo programma prima o poi termina, poiché a non può mai crescere, e prima o poi deve calare, perché nel caso in cui a resti invariato è b che decresce. Ma in questo caso si può dimostrare che non esiste una funzione $\rho(a, b)$ strettamente decrescente ad ogni passo e a valori in $\mathbb{N}$.

Per dimostrare che questo programma prima o poi termina conviene considerare le coppie di numeri naturali col seguente *ordine lessicografico*:

$$(a, b) < (a', b') \text{ se e solo se } \begin{cases} a = a' \text{ e } b < b', \text{ oppure} \\ a < a'. \end{cases}$$

Si può verificare (e lo faremo nella prossima sottosezione) che, con quest'ordine, non esistono successioni infinite strettamente decrescenti di coppie in $\mathbb{N} \times \mathbb{N}$. In questo caso la funzione ρ che serve per dimostrare che il programma termina è la funzione identica su $\mathbb{N} \times \mathbb{N}$.

Concludiamo con un esempio più sofisticato.

(a') Lo stato del programma è dato da una lista finita F di coppie di numeri naturali. All'inizio la lista F è vuota. Intuitivamente F rappresenta una lista di coppie "vietate"; inoltre, se (c, d) è una coppia vietata, allora anche tutte le coppie (a, b) con $a \geq c$ e $b \geq d$ sono "vietate". NB: il $\geq$ deve valere per *entrambe* le componenti.

(b') Ad ogni passo il programma chiede all'utilizzatore di inserire una coppia (a, b) di numeri naturali.

(c') Il programma confronta la coppia (a, b) inserita dall'utilizzatore con le coppie già presenti in F . Se esiste una coppia (c, d) nella lista F tale che $a \geq c$ e $b \geq d$, il programma termina. Altrimenti il programma aggiunge la coppia (a, b) ad F e si ripete il passo (b').

Questo programma termina sempre in qualunque modo l'operatore inserisca i dati? Se sì, in che modo lo si può verificare?

Chi desiderasse più informazioni sul problema della verificabilità dei programmi, può consultare Z. Manna, *Mathematical Theory of Computation*, 1974, trad. it. *Teoria matematica della computazione*, 1978.

2.3. Insiemi bene ordinati.

Definizione 2.1. Si dice che un insieme totalmente ordinato $\langle W, < \rangle$ è un *buon ordine*, o che W è *bene ordinato* (da $<$) se ogni sottoinsieme non vuoto di W ha un minimo (secondo l'ordine $<$). Come d'uso, se non vi è possibilità di equivoci, scriveremo W al posto di $\langle W, < \rangle$.

Se $w \in W$, definiamo l'insieme $w^\downarrow$ come $w^\downarrow = \{v \in W \mid v < w\}$. L'insieme $w^\downarrow$ è dotato di una struttura di ordine totale indotta da W , ed è immediato vedere che anche $w^\downarrow$ è un buon ordine. I sottoinsiemi di W della forma $w^\downarrow$ si dicono *segmenti iniziali (propri)* di W .³²

NB: nella precedente definizione ammettiamo la possibilità che W oppure $w^\downarrow$ siano l'insieme vuoto. Del resto, se W è bene ordinato e $W \neq \emptyset$, essendo W sottoinsieme di se stesso, lo stesso W ha un minimo w . Ma allora in questo caso $w^\downarrow$ è l'insieme vuoto.

Ogni insieme finito (e totalmente ordinato) è ovviamente bene ordinato³³. Vediamo adesso che esistono buoni ordini infiniti.

Proposizione 2.2. $\mathbb{N}$ (con l'ordine usuale) è bene ordinato.

Dimostrazione. Sia $X \subseteq \mathbb{N}$ e $X \neq \emptyset$. Quindi $n \in X$ per qualche $n \in \mathbb{N}$. Allora $\{0, 1, \dots, n-1, n\} \cap X$ è finito e non vuoto, quindi ha un minimo, che è anche il minimo di X , poiché $n \in X$. $\square$

Proposizione 2.3. Se W è bene ordinato, allora non esiste una successione infinita strettamente decrescente di elementi di W .³⁴

Dimostrazione. Supponiamo per assurdo che esista una tale successione $(w_n)_{n \in \mathbb{N}}$. L'insieme $X = \{w_n \mid n \in \mathbb{N}\}$ è un sottoinsieme non vuoto di W , quindi ha un minimo, visto che W è bene ordinato. Sia w_n il minimo di X . Dall'ipotesi che $(w_n)_{n \in \mathbb{N}}$ è strettamente decrescente, otteniamo $w_{n+1} < w_n$; ma $w_{n+1} \in X$, e questo contraddice l'assunzione che w_n sia il minimo di X . $\square$

³² ** Alcuni testi considerano W stesso come segmento iniziale (improprio) di W . In questa nota *segmento iniziale* avrà sempre il significato di segmento iniziale *proprio*.

³³ Ad essere pignoli, si deve dimostrare che se W è totalmente ordinato e un sottoinsieme X non vuoto è finito, allora X ha un minimo. Il minimo fra due elementi di W esiste perchè W è totalmente ordinato. Se X è finito, allora per definizione X è in corrispondenza biunivoca con qualche $n \in \mathbb{N}$. L'affermazione desiderata si ottiene per induzione su $n \geq 1$.

³⁴ ** In realtà la proposizione fornisce una condizione equivalente, ma l'altra implicazione utilizza una forma dell'assioma di scelta. Supponiamo che W non sia bene ordinato, quindi esiste un sottoinsieme X non vuoto senza un minimo. Siccome X è non vuoto, esiste $x_1 \in X$. Per ipotesi x_1 non è il minimo di X , quindi esiste $x_2 \in X$ tale che $x_2 < x_1$. Ma neanche x_2 può essere il minimo di X , quindi iterando la costruzione si ottiene una successione strettamente decrescente di elementi di X , quindi anche di W .

$\mathbb{N}$ non è l'unico insieme infinito bene ordinato. Supponiamo che W sia bene ordinato, consideriamo un "nuovo" elemento $u \notin W$, e ordiniamo $W \cup \{u\}$ in modo che u sia maggiore di tutti gli elementi di W . Con questo ordine, $W \cup \{u\}$ è bene ordinato (perchè?). Faremo presto vedere che W e $W \cup \{u\}$ non sono mai isomorfi (che W e $W \cup \{u\}$ non siano isomorfi è intuitivamente ovvio nel caso in cui W è finito).

Osserviamo che non è affatto scontato che W e $W \cup \{u\}$ non siano isomorfi. Infatti possiamo compiere una costruzione simile quando W è un ordine totale qualunque, non necessariamente bene ordinato. Se $W = \mathbb{Z}^-$, l'insieme dei numeri interi negativi (o anche $\mathbb{N}$ con l'ordine inverso), allora $W \cup \{u\}$ è isomorfo a W .

2.3.1. Confrontabilità di buoni ordini.

Proposizione 2.4. *Se W è bene ordinato e $w^\downarrow$ è un suo segmento iniziale, allora W e $w^\downarrow$ non sono isomorfi.*

Dimostrazione. Supponiamo per assurdo che $f : W \rightarrow w^\downarrow$ sia un isomorfismo. Siccome $w \in W$, il valore $f(w)$ è definito, e inoltre $f(w) \in w^\downarrow$, cioè $f(w) < w$. Quindi $X = \{v \in W \mid f(v) < v\}$ è non vuoto. Siccome W è bene ordinato, X ha un minimo v . Siccome $v \in X$, abbiamo $f(v) < v$. Siccome f è un isomorfismo, abbiamo anche $f(f(v)) < f(v)$. Ma allora $z = f(v)$ è tale che $f(z) < z$ e inoltre $z < v$. Questo contraddice l'assunzione che v è il minimo di X , e abbiamo ottenuto l'assurdo desiderato. $\square$

Teorema 2.5. *Se W e V sono insiemi bene ordinati, allora si verifica una (ed una sola) delle seguenti condizioni.*

- (1) W e V sono isomorfi;
- (2) W è isomorfo ad un segmento iniziale di V ;
- (3) V è isomorfo ad un segmento iniziale di W .

Dimostrazione. Le condizioni sono incompatibili fra di loro. Ad esempio, supponiamo che valgano sia (2) che (3). Sia W isomorfo ad un segmento iniziale $v^\downarrow$ di V , come dato da (2), e sia f un isomorfismo da V ad un segmento iniziale di W , come dato da (3), e sia $w = f(v)$. L'isomorfismo f chiaramente induce un isomorfismo f' da $v^\downarrow$ a $w^\downarrow$. Componendo l'isomorfismo dato da (2) con f' otterremmo un isomorfismo fra W e $w^\downarrow$, assurdo per la Proposizione 2.4.

Le incompatibilità fra (1) e (2) e fra (1) e (3) si dimostrano in maniera simile e più semplice.

Dimostriamo adesso che almeno una delle condizioni si presenta. Si consideri la seguente relazione $R \subseteq W \times V$:

$$R = \{(w, v) \in W \times V \mid w^\downarrow \text{ e } v^\downarrow \text{ sono isomorfi}\}.$$

Abbiamo che l'inversa di R è univoca, cioè che se $(w, v) \in R$ e $(w_1, v) \in R$, allora $w = w_1$. Infatti, se fosse $w \neq w_1$, avremmo che $w > w_1$ oppure $w_1 > w$, siccome W è totalmente ordinato. Se, ad esempio, $w > w_1$, allora, componendo

l'isomorfismo dato da $(w, v) \in R$ con l'inverso dell'isomorfismo dato da $(w_1, v) \in R$, avremmo che $w^\downarrow$ sarebbe isomorfo a $w_1^\downarrow$, un suo segmento iniziale.

In maniera simmetrica abbiamo che R è univoca, cioè che se $(w, v) \in R$ e $(w, v_1) \in R$, allora $v = v_1$.

Inoltre, se $(w, v) \in R$ e $w_1 < w$, esiste $v_1 \in V$ tale che $(w_1, v_1) \in R$ e $v_1 < v$. Infatti, se f è l'isomorfismo dato da $(w, v) \in R$ e $v_1 = f(w_1)$, allora f induce un isomorfismo da $w_1^\downarrow$ a $v_1^\downarrow$.

Dalle considerazioni precedenti segue che, se $D = \{w \in W \mid \text{esiste un } v \in V \text{ tale che } (w, v) \in R\}$ è il dominio di R e $C = \{v \in V \mid \text{esiste un } w \in W \text{ tale che } (w, v) \in R\}$ è il codominio di R , allora

(*) R definisce un isomorfismo da D a C .

Dimostriamo adesso che almeno una delle seguenti due condizioni si verifica: o D è tutto W , oppure C è tutto V .

Infatti, se nessuna delle due condizioni si verifica, allora $W \setminus D$ e $V \setminus C$ sono entrambi non vuoti. Siccome W e V sono buoni ordini, esistono un minimo s di $W \setminus D$ ed un minimo t di $V \setminus C$. Quindi $D = s^\downarrow$ e $C = t^\downarrow$, perchè abbiamo dimostrato che se $w \in D$, allora $w^\downarrow \subseteq D$, e la condizione simmetrica vale per C . Ma allora, per (*), $(s, t) \in R$, ma questo contraddice $s \in W \setminus D$.

Quindi $D = W$, oppure $C = V$, oppure entrambi. Se si verificano entrambe le condizioni, R è un isomorfismo da W su V . Altrimenti, nel primo caso R è un isomorfismo da W su un segmento iniziale di V e nel secondo caso R è un isomorfismo da un segmento iniziale di W su V . $\square$

2.3.2. Somme e prodotti di buoni ordini. Se $(W, <_W)$ e $(V, <_V)$ sono buoni ordini e W e V sono disgiunti, allora $Z = W \cup V$ diventa un buon ordine rispetto alla relazione $<_Z$ definita da

$$s <_Z t \text{ se e solo se } \begin{cases} s <_W t \text{ e } s, t \in W, \text{ oppure} \\ s <_V t \text{ e } s, t \in V, \text{ oppure} \\ s \in W \text{ e } t \in V. \end{cases}$$

Intuitivamente, tutti gli elementi di V vengono "messi in cima", cioè considerati maggiori di qualunque elemento di W . Lasciamo per esercizio al lettore di dimostrare che, se W e V sono buoni ordini disgiunti, allora anche $W \cup V$ è un buon ordine. Nel caso W e V non fossero disgiunti, la costruzione precedente si può sempre effettuare (a meno di isomorfismo) considerando al posto di V un buon ordine V' isomorfo a V .

Prendendo V non vuoto otteniamo dal Teorema 2.5 che per ogni buon ordine W esiste un buon ordine strettamente maggiore, fatto a cui avevamo già accennato in precedenza, sostanzialmente considerando la stessa costruzione nel caso in cui V aveva un solo elemento.

Se W e V sono buoni ordini, si può definire l'*ordine lessicografico* su $W \times V$ nel seguente modo:

$$(w, v) < (w', v') \text{ se e solo se } \begin{cases} w = w' \text{ e } v < v', \text{ oppure} \\ w < w'. \end{cases}$$

Proposizione 2.6. *Se W e V sono buoni ordini, allora $W \times V$, dotato dell'ordine lessicografico, è un buon ordine.*

Dimostrazione. Lasciamo per esercizio al lettore di verificare che $W \times V$ è un ordine totale. Sia $X \subseteq W \times V$ e X non vuoto. Allora $A = \{w \in W \mid \text{esiste } v \in V \text{ tale che } (w, v) \in X\}$ è un sottoinsieme non vuoto di W , dunque A ha un minimo a . Anche $\{v \in V \mid (a, v) \in X\}$ è non vuoto, dunque ha un minimo b .

Dalla definizione dell'ordine lessicografico segue che (a, b) è il minimo di X . $\square$

2.3.3. Cenni agli ordinali. Un insieme A si dice *transitivo* se $x \in y \in A$ implica $x \in A$. Equivalentemente, A è transitivo se ogni elemento di A è un sottoinsieme di A . Un *ordinale* è un insieme transitivo e bene ordinato dalla relazione di appartenenza. Intuitivamente, gli ordinali si costruiscono iterando l'operazione di successore e prendendo unioni nel caso limite, come abbiamo accennato in 2.1.4, ma usare quella costruzione per definire gli ordinali necessiterebbe di parecchi dettagli aggiuntivi e comunque non è l'approccio usuale.

Si può dimostrare, ma la dimostrazione è delicata, che ogni buon ordine è isomorfo ad un ordinale, quindi gli ordinali possono essere presi come rappresentanti delle classi di equivalenza dei buoni ordini rispetto alla relazione di isomorfismo.³⁵

Si dimostra abbastanza facilmente che ogni ordinale è l'insieme degli ordinali precedenti (gli ordinali sono confrontabili fra di loro per il Teorema 2.5). Quindi ogni classe non vuota X di ordinali ha un minimo (se $\alpha \in X$ e α non è il minimo di X , $\alpha \cap X$ è un sottoinsieme non vuoto di α , dunque ha un minimo, che è anche il minimo di X). Quindi intuitivamente la *classe* di tutti i buoni ordini è bene ordinata, ma non può essere considerata un insieme, perchè abbiamo visto che per ogni insieme bene ordinato ne esiste uno strettamente maggiore. Questo è il paradosso di Burali-Forti. Nella teoria degli insiemi moderna, questo non è più un paradosso, semplicemente dimostra che non esiste un insieme che contiene tutti gli ordinali (così come il contenuto del paradosso di Russell diventa che non esiste un insieme che contiene tutti gli insiemi).

Si può dimostrare che l'assioma di scelta è equivalente all'assunzione che ogni insieme è bene ordinabile. Quindi, se si accetta l'assioma di scelta, si può definire la *cardinalità* di un insieme Y come il più piccolo ordinale α che può essere posto in biiezione con Y . Gli ordinali ottenibili in questo modo si chiamano *cardinali* e sono solo una piccola parte di tutti gli ordinali (perchè? Considerate ad esempio il caso degli ordinali numerabili...)

³⁵ In questo caso sarebbe stato problematico costruire il quoziente, poiché le classi di equivalenza non sono insiemi, ma classi proprie.

3. Appendice

Questa sezione contiene altro materiale (parecchio disparato!) per il corso di Logica 1, A.A. 2018–2019.

3.1. Il Teorema di Tarski. Supponiamo di lavorare in un'estensione non contraddittoria T dell'Aritmetica di Peano PA e di avere una gödelizzazione che ad ogni formula φ associa il numero $g(\varphi)$ con associato numerale $\ulcorner \varphi \urcorner = g(\bar{\varphi})$ (ricordiamo che, se $n \in \mathbb{N}$, il numerale $\bar{n}$ è il termine $0''''''''''$ con n apici; intuitivamente, $\bar{n}$ è il nome di n nel linguaggio di PA).

Teorema 3.1. (Tarski) *Non esiste nessuna formula $\sigma(x, y)$ dipendente solo dalle variabili x e y e tale che, per ogni formula $\varphi(x)$ dipendente al massimo dalla variabile x ed ogni naturale $n \in \mathbb{N}$, il seguente enunciato sia un teorema di T*

$$\sigma(\ulcorner \varphi(x) \urcorner, \bar{n}) \Leftrightarrow \varphi(\bar{n}). \quad (3.1)$$

Dimostrazione. Supponiamo per assurdo che esista una siffatta σ . Sia $\varphi(x)$ la formula $\neg\sigma(x, x)$ e sia $\bar{n} = \ulcorner \varphi(x) \urcorner$. Quindi $\varphi(\bar{n})$ è $\neg\sigma(\bar{n}, \bar{n})$, cioè $\neg\sigma(\ulcorner \varphi(x) \urcorner, \bar{n})$. Sostituendo in (3.1) abbiamo

$$\sigma(\ulcorner \varphi(x) \urcorner, \bar{n}) \Leftrightarrow \neg\sigma(\ulcorner \varphi(x) \urcorner, \bar{n})$$

cioè una contraddizione. □

In particolare, se T è la teoria che contiene come assiomi tutti gli enunciati veri in (cioè soddisfatti da) $\mathbb{N}$, abbiamo³⁶ che non esiste nessuna formula che “esprime” la verità³⁷ in $\mathbb{N}$.

³⁶Qui per $\mathbb{N}$ intendiamo $(\mathbb{N}, 0', +, \cdot, =)$, eventualmente a cui sono aggiunte ulteriori operazioni o relazioni. T è non contraddittoria perchè per costruzione ha un modello. Naturalmente, l'esistenza di questo modello, pur intuitiva, è un'assunzione metamatematica forte.

³⁷** Per semplicità abbiamo sottinteso nell'affermazione precedente che sia sempre possibile esprimere il gödeliano di una formula ottenuta sostituendo una variabile con un termine, conoscendo il gödeliano della formula di partenza. Se non si vogliono mescolare i due aspetti, ci si deve chiedere se esiste una formula τ tale che

$$\tau(\ulcorner \psi \urcorner) \Leftrightarrow \psi \quad (3.2)$$

sia un teorema, per ogni enunciato ψ .

Supponiamo di avere una formula α che esprime il risultato di una sostituzione, cioè tale che $\alpha(u, v, w)$ esprime (nel senso del Capitolo III, Sezione 2 del libro del Mendelson) la relazione $R(\bar{u}, \bar{v}, \bar{w})$ definita da “ $\bar{u} = \ulcorner \varphi(x) \urcorner$, per qualche formula $\varphi(x)$, e $\bar{v} = \ulcorner \varphi(\bar{w}) \urcorner$ ”. Allora da una τ che soddisfa (3.2), otteniamo una σ che soddisfa (3.1) definendo $\sigma(u, v)$ come $\exists w(\tau(w) \wedge \alpha(u, v, w))$. Quindi sotto l'ipotesi dell'esistenza di α , (3.1) e (3.2) sono equivalenti.

Inoltre osserviamo che il Teorema 3.1 vale in realtà sotto ipotesi estremamente generali. È sufficiente avere un sistema formale con:

- due simboli di variabile,
- un insieme di espressioni che chiamiamo *termini*, che contengono le variabili,
- una nozione di *sostituzione* (di una variabile x con un termine t) che ad ogni formula φ associa un'altra formula $\varphi(x|t)$, per ogni variabile x ed ogni termine t . Si richiede che questa operazione di sostituzione soddisfi ad alcune proprietà naturali, la cui enunciazione esplicita lasciamo al lettore,
- un operatore di *negazione* che ad ogni formula φ associa un'altra formula $\neg\varphi$. Questo operatore di negazione deve commutare con l'operazione di sostituzione,
- una nozione di equivalenza e la richiesta che φ e $\neg\varphi$ non siano mai equivalenti.

Una funzione gödeliana in questo ambito è semplicemente una funzione (a livello metamatematico, e non necessariamente iniettiva) dall'insieme delle formule all'insieme dei termini. In realtà non è nemmeno necessario assumere che variabili e termini siano espressioni del linguaggio, l'unico aspetto importante è l'esistenza dell'operazione di sostituzione con le opportune proprietà. Anche la nozione di equivalenza non deve necessariamente essere espressa da un simbolo del sistema formale, per esempio, si possono considerare φ e ψ equivalenti se $\varphi \vdash \psi$ e $\psi \vdash \varphi$.

3.2. Congruenze in semigrupperi. Un *semigruppero* $\mathbf{S} = (S, \cdot)$ è un insieme S dotato di un'operazione binaria associativa $\cdot$ che in seguito indicheremo mediante giustapposizione, se questo non genererà confusione, cioè scriveremo st al posto di $s \cdot t$.

Se $\mathbf{S} = (S, \cdot)$ e $\mathbf{S}_1 = (S_1, \cdot)$ sono due semigrupperi, una funzione $\varphi : S \rightarrow S_1$ si dice *morfismo* se $\varphi(st) = \varphi(s)\varphi(t)$ o, in notazione non abbreviata,

$$\varphi(s \cdot t) = \varphi(s) \cdot \varphi(t), \text{ per ogni coppia di elementi } s, t \in S.$$

Nella formula precedente, l'operazione a sinistra è quella in $\mathbf{S}$ e l'operazione a destra è quella in $\mathbf{S}_1$.

Se $\varphi : A \rightarrow B$ è una funzione, φ induce una relazione di equivalenza su A , se si considerano "identificati" due elementi di A se e solo se hanno la stessa immagine secondo φ . Sarebbe naturale chiamare questa relazione di equivalenza "nucleo" di φ , ma, per evitare conflitti di terminologia, per esempio, col nucleo di un morfismo di gruppi, modificheremo leggermente la terminologia.

Definizione 3.2. Se $\varphi : A \rightarrow B$ è una funzione, il *nucleo di φ nel senso di relazione di equivalenza* di φ è la seguente relazione su A

$$KerEq(\varphi) = \{(a, b) \in A \times A \mid \varphi(a) = \varphi(b)\}.$$

È ovvio verificare che, sotto le ipotesi nella definizione, $KerEq(\varphi)$ è effettivamente una relazione di equivalenza su A . Finora le operazioni di semigruppero e la nozione di morfismo non sono intervenute.

3.2.1. Se però $A = S$ e $B = S_1$ sono semigrupperi, e φ è un morfismo da $\mathbf{S}$ ad $\mathbf{S}_1$, allora $\alpha = KerEq(\varphi)$ soddisfa all'ulteriore proprietà

$$(*) \text{ Per tutti gli elementi } s, s', t, t' \in S, \text{ se } s \alpha s' \text{ e } t \alpha t', \text{ allora } st \alpha s't',$$

dove abbiamo scritto $s \alpha s' \dots$ al posto di $(s, s') \in \alpha \dots$

Infatti, da $s \alpha s'$ e $t \alpha t'$ otteniamo, per definizione di $\alpha = KerEq(\varphi)$, che $\varphi(s) = \varphi(s')$ e $\varphi(t) = \varphi(t')$. Se poi φ è un morfismo, applicando due volte la proprietà di essere un morfismo, abbiamo $\varphi(st) = \varphi(s)\varphi(t) = \varphi(s')\varphi(t') = \varphi(s't')$, cioè $\varphi(st) = \varphi(s't')$ e quindi $st \alpha s't'$. Dunque (*) vale se φ è un morfismo di semigrupperi e $\alpha = KerEq(\varphi)$.

Osserviamo che la struttura di $\mathbf{S}_1$ non compare in (*), cioè (*) riguarda esclusivamente $\mathbf{S}$ ed α ; il morfismo φ ed $\mathbf{S}_1$ non compaiono in (*). In realtà, almeno in parte, le proprietà di φ seguono da (*), come vedremo.

Se $\mathbf{S}$ è un semigruppero, una relazione d'equivalenza su S che soddisfa ad (*) si dice una *congruenza su $\mathbf{S}$* .

3.2.2. Se α è un congruenza, indichiamo con s/α la classe di equivalenza di un elemento $s \in S$ e con S/α l'insieme delle classi di equivalenza. Su S/α definiamo la seguente operazione binaria

$$(**) s/\alpha \cdot t/\alpha = (s \cdot t)/\alpha, \text{ per } s/\alpha \in S/\alpha \text{ e } t/\alpha \in S/\alpha.$$

Naturalmente va verificato che la definizione è indipendente dal rappresentante scelto per ogni classe, cioè che $s/\alpha = s'/\alpha$ e $t/\alpha = t'/\alpha$ implicano $(s \cdot t)/\alpha = (s' \cdot t')/\alpha$. Ma $s/\alpha = s'/\alpha$ se e solo se $s \alpha s'$, e così via, quindi

la proprietà (*) garantisce che l'operazione introdotta su S/α è ben definita. È facile verificare che se S è un semigruppato, allora anche S/α è un semigruppato, con l'operazione appena introdotta.

Abbiamo quasi dimostrato la seguente proposizione.

Proposizione 3.3. *Se $\mathbf{S}$ è un semigruppato, allora una relazione binaria α su S è una congruenza se e solo se α è il nucleo $\alpha = \text{KerEq}(\varphi)$ di qualche morfismo φ da $\mathbf{S}$ ad $\mathbf{S}_1$, per qualche semigruppato $\mathbf{S}_1$.*

Dimostrazione. Se α è il nucleo $\text{KerEq}(\varphi)$ di un morfismo $\varphi : \mathbf{S} \rightarrow \mathbf{S}_1$, allora α è una congruenza per 3.2.1.

Viceversa, se α è una congruenza, sia $S_1 = S/\alpha$; abbiamo che S_1 diventa un semigruppato, se dotato dell'operazione introdotta in 3.2.2. Inoltre, la definizione stessa (***) di questa operazione implica che la proiezione π che ad ogni elemento $s \in S$ associa la sua classe $\pi(s) = s/\alpha$ è un morfismo di semigruppato, e $\alpha = \text{KerEq}(\pi)$ per costruzione. $\square$

Le costruzioni effettuate nella dimostrazione precedente sono, in un certo senso, una l'inversa dell'altra. Se $\varphi : \mathbf{S} \rightarrow \mathbf{S}_1$ è un morfismo di semigruppato, l'immagine di φ è $\varphi(S) = \{u \in S_1 \mid \text{esiste } s \in S \text{ tale che } \varphi(s) = u\}$. L'insieme $\varphi(S)$ diventa naturalmente un semigruppato con la (restrizione della) stessa operazione di S_1 . Un morfismo di semigruppato si dice *isomorfismo* se, in quanto funzione, è biettiva. Due semigruppato si dicono *isomorfi* se esiste un isomorfismo dall'uno all'altro.

Proposizione 3.4. *Se $\varphi : \mathbf{S} \rightarrow \mathbf{S}_1$ è un morfismo di semigruppato e $\alpha = \text{KerEq}(\varphi)$, allora $\mathbf{S}/\alpha$ è isomorfo all'immagine $\varphi(\mathbf{S})$ di φ .*

In particolare, se φ è suriettivo, allora $\mathbf{S}/\alpha$ e $\mathbf{S}_1$ sono isomorfi.

Dimostrazione. La funzione ψ che ad s/α associa $\varphi(s)$ è un isomorfismo da $\mathbf{S}/\alpha$ verso $\varphi(\mathbf{S})$.

Cosa ci assicura che ψ sia un morfismo?

Cosa ci assicura che ψ sia suriettiva?

C'è da effettuare un'altra verifica? $\square$

In altre parole, la seconda parte della Proposizione 3.4 ci fornisce un modo "interno ad $\mathbf{S}$ " per descrivere (a meno di isomorfismo) tutte le "immagini omomorfe" di $\mathbf{S}$.

Lo studente familiare con la teoria dei gruppi può confrontare le costruzioni precedenti con costruzioni simili effettuate per i gruppi. Se $\mathbf{S}$ è un gruppo, cos'è una congruenza, nella terminologia usata in teoria dei gruppi?

Lo studente saprebbe controllare che l'insieme delle congruenze di un semigruppato è un reticolo, rispetto alla relazione di inclusione?

Quali degli argomenti precedenti sono validi se si suppone che $\mathbf{S}$ sia dotato semplicemente di un'operazione binaria, senza l'ipotesi che l'operazione sia associativa (quindi senza nessuna ipotesi ulteriore sull'operazione)?

Quali dei ragionamenti precedenti sono validi nel caso in cui considerino al posto dei semigrupperi *strutture algebriche* qualunque, cioè insiemi con un certo numero di operazioni, eventualmente anche dipendenti da più di due argomenti?

3.2.3. Ulteriori letture. Un'introduzione al cosiddetto "problema della parola" per gruppi e semigrupperi si può trovare in Rotman, *An Introduction to the Theory of Groups*, Capitolo 12. Altro materiale, che riguarda anche parole di lunghezza infinita, nei capitoli IV e V del libro citato di Hebisch e Weinert, *Semirings: Algebraic Theory and Applications in Computer Science* e in D. Perrin, J.-E. Pin, *Infinite Words: Automata, Semigroups, Logic and Games*, 2004.

PAOLO LIPPARINI

Dipartimento di Matematica, Viale della Ricerca Insiemistica, Università di Roma "Tor Vergata", I-00133 ROME ITALY