Dispense del corso di Istituzioni di Logica Matematica A.A.2006-2007 Versione definitiva

Alessandro Andretta
alessandro.andretta@unito.it

Indice

Introduzione

Queste Dispense contengono gli argomenti trattati nel corso di Istituzioni di Logica Matematica per l'a.a. 2006–2007. Oltre agli argomenti d'esame, le Dispense contengono molti altri argomenti che, per mancanza di tempo, non siamo riusciti a coprire a lezione, per esempio il Capitolo IV sulle funzioni calcolabili.

Elenco dettagliato degli argomenti del corso

- Capitolo I: tutto *eccetto* la sezione 6 (Gli ordinali e la topologia).
- Cap II: tutto tranne le sezioni seguenti: 10.E (Il teorema di Cantor-Lawvere), la sezione 15 (Applicazioni dell'Assioma di Scelta) e la sezione 17 (Il teorema di Ramsey).
- Capitolo III:
  - dalla sezione 19 alla sezione 23 tranne: §22.B (Due teorie molto particolari) e Il Teorema di Ramsey nel caso finito 23.12.
  - la sezione 24:
    §24.A: tutto;
    §24.B: *escluso*;
    §24.C: solo la definizione di sottostruttura elementare, il Teorema di Tarski-Vaught 24.13 e il Corollario 24.14;
    §24.D: fino al Corollario 24.18 *escluso*
  - la sezione 25: fino a §25.B *escluso*
  - la sezione 27: tutto *eccetto* §27.D
  - la sezione 28: tutto.

Il Capitolo IV, pur essendo presente nelle Dispense, *non è parte del programma d'esame*. L'esame consiste in una prova orale. Gli studenti

interessati a sostenere la prova sono pregati di contattarmi per fissare la data.

tel: 011-6702918

e-mail: `alessandro.andretta@unito.it`

Capitolo I

Teoria elementare degli insiemi

1. Gli assiomi

La teoria degli insiemi è onnipresente in matematica—i vari oggetti studiati in algebra, analisi, geometria, sono definiti come insiemi dotati di qualche struttura addizionale. Intuitivamente, un insieme A è un aggregato di oggetti e l'espressione $x \in A$ significa che "l'oggetto x fa parte dell'aggregato A" ovvero "x appartiene ad A". La caratteristica principale di un insieme è che esso è completamente determinato dai suoi elementi. In altre parole: due insiemi che hanno gli stessi elementi coincidono. Questo è noto come assioma di estensionalità ed è il fondamento della teoria degli insiemi:

(∗) Supponiamo che A e B siano insiemi e che, per ogni x, $x \in A$ se e soltanto se $x \in B$. Allora $A = B$.

Un'altra caratteristica della nozione intuitiva di insieme è che data una proprietà φ, possiamo considerare l'insieme di tutti gli x che soddisfano a φ,

$$\{\, x \mid \varphi(x) \,\}.$$

Osserviamo che questo insieme è completamente determinato grazie a (∗). Parrebbe quindi ragionevole postulare che:

(∗∗) Se φ è una proprietà, allora esiste l'insieme $\{\, x \mid \varphi(x) \,\}$.

Tuttavia, come ha osservato Bertrand Russell nel 1901, (∗∗) contraddice (∗)! Consideriamo la proprietà $\varphi(x)$ che asserisce "x è un insieme e $x \notin x$": sia

R la totalità di tutti gli insiemi che non appartengono a sé stessi

$$\mathrm{R} = \{\, x \mid x \notin x \,\}. \tag{1}$$

Per $(**)$ R è un insieme e quindi possiamo chiederci se soddisfi o meno la proprietà φ, cioè se $\mathrm{R} \notin \mathrm{R}$ oppure $\mathrm{R} \in \mathrm{R}$. Ma

$$\mathrm{R} \in \mathrm{R} \text{ implica che } \mathrm{R} \notin \mathrm{R} \text{ e} \tag{2}$$

$$\mathrm{R} \notin \mathrm{R} \text{ implica che } \mathrm{R} \in \mathrm{R}, \tag{3}$$

una contraddizione in entrambi i casi. È quindi necessario restringere in qualche modo la nozione intuitiva di insieme, limitando il principio enunciato in $(**)$. Il paradosso di Russell riportato qui sopra non è l'unica antinomia presente nella trattazione ingenua della teoria degli insiemi, ma questa e tutte le altre antinomie utilizzano $(**)$ per definire collezioni molto "grandi". In altre parole, le antinomie della teoria ingenua degli insiemi non coinvolgono mai insiemi "piccoli", come quelli che si incontrano nella pratica matematica. Per risolvere queste contraddizioni, sono state introdotte varie teorie assiomatiche, che delimitano con precisione quali costruzioni insiemistiche sono ammissibili e quali no. La teoria assiomatica che presentiamo in questa sezione è stata introdotta da A.P. Morse e J. Kelly e prende il nome di MK.

1.A. Insiemi e classi. Assumeremo come nozione primitiva quella di **classe** e di relazione di appartenenza $\in$ tra classi. Diremo che una classe A è un **insieme** se e solo se esiste una classe B a cui A appartiene, cioè

$$\exists B(A \in B).$$

Una classe che non sia un insieme si dice **classe propria**. Nella trattazione insiemistica ingenua si distingue tra insiemi (o classi) e oggetti. Ma la nozione di insieme (e di classe) è così flessibile che possiamo fare a meno degli oggetti che non sono insiemi, dato che—come vedremo—tutti gli oggetti matematici comuni possono essere identificati con insiemi, i cui elementi sono insiemi, i cui elementi sono insiemi, e così via. In altre parole, d'ora in poi assumiamo che gli *elementi di una classe siano a loro volta delle classi*, anzi degli insiemi. Il principio enunciato in $(*)$ deve essere esteso in modo da permettere ad A e B di variare sulle classi (e non solo sugli insiemi), vale a dire

Assioma di Estensionalità. *Supponiamo che A e B siano classi tali che $\forall x(x \in A \Leftrightarrow x \in B)$. Allora $A = B$.*

1.B. Le formule della teoria degli insiemi. Se vogliamo formalizzare adeguatamente l'enunciato in $(**)$ dobbiamo prima trovare una controparte rigorosa alla nozione—per ora un po' ambigua—di *proprietà*. La nozione

rigorosa è quella di **formula della teoria degli insiemi**.[1] Utilizzeremo—più per desiderio di concisione che per reale necessità—la simbologia logica, cioè i quantificatori $\forall x \dots$ e $\exists x \dots$ che significano, rispettivamente, "per ogni $x \dots$" ed "esiste un $x \dots$" e i connettivi proposizionali: $\neg\varphi$, $\varphi \Rightarrow \psi$, $\varphi \Leftrightarrow \psi$, $\varphi \wedge \psi$ e $\varphi \vee \psi$ che significano rispettivamente "non φ", "se φ allora ψ", "φ se e solo se ψ", "φ e ψ", "φ o ψ", dove la disgiunzione "o" corrisponde al latino *vel*, ossia non si esclude che entrambe le affermazioni φ e ψ valgano. Le formule sono costruite a partire da lettere o variabili, usando il simbolo di appartenenza $\in$, il simbolo di uguaglianza $=$, i connettivi e i quantificatori.

Definizione 1.1. Le espressioni del tipo

$$x = y \qquad \text{e} \qquad x \in y\,,$$

dove x e y denotano variabili arbitrarie[2] si dicono formule atomiche.

Tutte le formule atomiche sono formule e la famiglia delle formule è ottenuta da quelle atomiche applicando un numero finito di volte i connettivi logici $\neg$, $\vee$, $\wedge$, $\Rightarrow$, $\Leftrightarrow$, e i quantificatori $\exists$ e $\forall$. Le lettere greche φ, ψ, e χ variano sulle formule.

L'espressione $\varphi \wedge \psi \vee \chi$ è ambigua dato che potrebbe significare:

- applico $\wedge$ a φ e ψ e poi applico $\vee$ alla formula risultante e χ, oppure
- applico $\wedge$ a φ e alla formula ottenuta dall'applicazione di $\vee$ a ψ e χ.

Per evitare queste ambiguità useremo le parentesi "(" e ")" e scriveremo, rispettivamente, $(\varphi \wedge \psi) \vee \chi$ e $\varphi \wedge (\psi \vee \chi)$. Allo stesso tempo, al fine di evitare un'eccessiva proliferazione delle parentesi, useremo la convenzione che $\neg$ lega più fortemente degli altri connettivi logici; quindi, per esempio, $\neg\varphi \wedge \psi$ sta per $(\neg\varphi) \wedge \psi$. Inoltre le espressioni $\neg(x = y)$ e $\neg(x \in y)$ si abbreviano $x \neq y$ e $x \notin y$.

Ogni formula contiene una quantità finita di variabili: nella seguente definizione individuiamo quelle variabili che compaiono **libere** nella formula.

Definizione 1.2. Sia φ una formula.

- Se φ è atomica allora ogni variabile di φ è libera.
- Se φ è della forma $\neg\psi$ allora le variabili libere di φ sono quelle di ψ.
- Se φ è della forma $\psi \,\square\, \chi$, dove $\square$ è $\wedge$, $\vee$, $\Rightarrow$ o $\Leftrightarrow$, allora le variabili libere di φ sono quelle di ψ e quelle di χ.
- Se φ è della forma $\exists x\psi$ oppure $\forall x\psi$, le variabili libere di φ sono quelle di ψ *eccetto* x. Vale a dire se y è una variabile distinta da x, allora y è libera in φ se e solo se è libera in ψ.

[1] Le formule della teoria degli insiemi sono casi speciali di formule di un linguaggio del prim'ordine, come vedremo in seguito.

[2] Non assumiamo che x e y siano distinte.

Un'occorrenza che non sia libera si dice **vincolata**.

L'espressione

$$\varphi(x_1, \ldots, x_n)$$

significa che le variabili che occorrono libere in φ sono tra le $x_1, \ldots, x_n$. (Non richiediamo che *tutte* le $x_1, \ldots, x_n$ compaiano libere o meno in φ.)

Vediamo qualche esempio.

1.B.1. *La formula del paradosso di Russell.* La formula $x \notin x$ usata nel paradosso di Russell, ha un un'unica variabile x, che è anche libera.

1.B.2. *I quantificatori vincolano le variabili.* La formula $\exists y(x \in y)$ asserisce che la classe x è un insieme. Questa formula, la cui unica variabile libera è x, è del tutto equivalente a $\exists z(x \in z)$, dove z è una qualsiasi altra variabile distinta da x. Se invece sostituiamo y con x otteniamo $\exists x(x \in x)$, una formula priva di variabili libere che asserisce l'esistenza di una classe x che appartiene a sé stessa. Quest'ultimo esempio è simile a quanto avviene in analisi: le espressioni $\int_0^1 f(x,y)\,\mathrm{d}y$ e $\int_0^1 f(x,z)\,\mathrm{d}z$ sono del tutto equivalenti e denotano una funzione nella variabile x, mentre $\int_0^1 f(x,x)\,dx$ denota un numero.

1.B.3. *Occorrenze libere e vincolate.* La formula φ

$$(x \in y) \wedge \exists y(y \in x)$$

dice che x appartiene a y e x è non vuoto. Entrambe x e y sono libere in φ e in $x \in y$, mentre soltanto x è libera in $\exists y(y \in x)$. Notiamo che φ è equivalente a $(x \in y) \wedge \exists z(z \in x)$.

1.C. Classi definite da formule. Il seguente assioma (che in realtà è uno schema di assiomi—uno per ogni φ) rende rigoroso il principio enunciato in $(**)$.

Assioma di Comprensione. *Sia $\varphi(x, y_1, \ldots, y_n)$ una formula in cui la variabile x compare libera e sia A una variabile differente da $x, y_1, \ldots, y_n$. Allora*

$$\forall y_1 \ldots \forall y_n\, \exists A \forall x\, (x \in A \Leftrightarrow \exists z(x \in z) \wedge \varphi(x, y_1, \ldots, y_n))\,.$$

Questo assioma è spesso detto Assioma di Costruzione di Classi. La classe A definita da φ e da $y_1, \ldots, y_n$ è la classe di tutti gli *insiemi* x per cui $\varphi(x, y_1, \ldots, y_n)$ vale. Per l'Assioma di Estensionalità, la classe A è unica e la si denota con

$$\{\, x \mid \varphi(x, y_1, \ldots, y_n) \,\}\,.$$

Osservazione 1.3. In matematica, ogni qual volta si dimostra che

$$\forall x_1 \ \ldots \ \forall x_n\, \exists! y\ \varphi(x_1, \ldots, x_n, y)$$

si introduce un nuovo simbolo $\mathtt{t}(x_1, \ldots, x_n)$ che denota l'unico y per cui vale $\varphi(x_1, \ldots, x_n, y)$. Capita quindi spesso di imbattersi in della forma

$$\{\, \mathtt{t}(x_1, \ldots, x_n) \mid x_1 \in X_1, \ldots, x_n \in X_n \,\}\,. \tag{4}$$

Bisogna quindi verificare che una classe così definita è ottenibile mediante l'Assioma di Comprensione. Per far questo basta osservare che la classe in questione è

$$\{\, y \mid \exists x_1 \ldots \exists x_n \,(x_1 \in X_1 \wedge \cdots \wedge x_n \in X_n \wedge \varphi(x_1, \ldots, x_n, y))\,\}$$

dove φ è la formula che definisce $\mathtt{t}$.

Riguardiamo il paradosso di Russell: per l'Assioma di Comprensione, la classe $\mathrm{R} = \{\, x \mid x \notin x \,\}$ esiste e l'implicazione in (2) dimostra che $\mathrm{R} \in \mathrm{R}$ non può valere e quindi $\mathrm{R} \notin \mathrm{R}$. Se R fosse un insieme, potremmo applicare (3) e ottenere una contraddizione come prima. Viceversa, se R è una classe propria il problema non si pone. Ne segue che R *è una classe propria*.

Se A è una classe e $\varphi(x, y_1, \ldots, y_n)$ è una formula come sopra,

$$\{\, x \in A \mid \varphi(x, y_1, \ldots, y_n)\,\}$$

è la classe determinata dalla formula $x \in A \wedge \varphi(x, y_1, \ldots, y_n)$, ovvero

$$\{\, x \in A \mid \varphi(x, y_1, \ldots, y_n)\,\} = \{\, x \mid x \in A \wedge \varphi(x, y_1, \ldots, y_n)\,\}\,.$$

Le usuali operazioni insiemistiche si applicano anche alle classi: se A e B sono classi, allora

- $A \cap B = \{\, x \mid x \in A \wedge x \in B \,\} = \{\, x \in A \mid x \in B \,\}$ è la classe intersezione di A e B,
- $A \cup B = \{\, x \mid x \in A \vee x \in B \,\}$ è la classe unione di A e B,
- $A \setminus B = \{\, x \mid x \in A \wedge x \notin B \,\}$ è la differenza tra le classi A e B e
- $A \triangle B = (A \setminus B) \cup (B \setminus A)$.

Dall'Assioma di Estensionalità segue che $A \cap B = B \cap A$, $A \cup B = B \cup A$ e $A \triangle B = B \triangle A$.

L'Assioma di Comprensione ci assicura l'esistenza di molte classi, ma da solo non è in grado di assicurare l'esistenza di *insiemi*. Postuliamo quindi che esista almeno un insieme, cioè

Assioma di Esistenza di Insiemi. $\exists A\, \exists B (A \in B)$.

1.D. Insieme potenza. Diremo che A è una **sotto-classe** di B,

$$A \subseteq B\,,$$

se $x \in A \Rightarrow x \in B$, per ogni x. Se $A \subseteq B$ e $A \neq B$, diremo che A è una **sottoclasse propria** di B e scriveremo $A \subset B$.

Assioma dell'Insieme Potenza. *Per ogni insieme A c'è un insieme P tale che*

$$\forall B\,(B \subseteq A \Leftrightarrow B \in P)\,.$$

In altre parole: se A è un insieme ogni sua sottoclasse è un insieme e la collezione di tutti i sottoinsiemi di A forma a sua volta un insieme. L'insieme P di cui sopra si indica con $\mathscr{P}(A)$ e si dice **insieme delle parti** o **insieme potenza** di A.

Corollario 1.4. *Se B è un insieme e $A \subseteq B$ allora A è un insieme. Equivalentemente: se A è una classe propria e $A \subseteq B$ allora B è una classe propria.*

Sia A un insieme. Allora anche

$$\{\, x \in A \mid x \neq x \,\} \tag{5}$$

è un insieme. Poiché ogni x è uguale a sé stesso, questo significa che nessun x può appartenere all'insieme in (5) e per l'Assioma di Estensionalità, una qualsiasi altra classe priva di elementi deve coincidere con questo insieme. In altre parole l'insieme in (5) non dipende dall'insieme A e si dice **insieme vuoto** e lo si indica con $\emptyset$.

1.E. Coppie. Dati due insiemi x e y, l'Assioma di Comprensione ci garantisce l'esistenza di $\{x, y\}$, la classe contenente soltanto x e y. Richiediamo—come è naturale—che questa classe sia un insieme:

Assioma della Coppia. *Se x e y sono insiemi, allora $\{x, y\}$ è un insieme.*

Osserviamo che non si richiede che x e y siano distinti. In particolare, dato un insieme x possiamo costruire il singoletto $\{x\} = \{x, x\}$.

Esercizio 1.5. Dimostrare che $\{x, y\} = \{z, w\}$ implica che

$$(x = z \wedge y = w) \vee (x = w \wedge y = z)\,.$$

In matematica più che gli insiemi della forma $\{x, y\}$ è necessario considerare le **coppie ordinate** (x, y): l'insieme (x, y) deve codificare x e y e deve essere sufficientemente asimmetrico per poter distinguere questi due insiemi. La definizione di coppia ordinata che si adotta in teoria degli insiemi è dovuta a Kazimirez Kuratowski: se x e y sono insiemi poniamo

$$(x, y) \stackrel{\text{def}}{=} \{\{x\}, \{x, y\}\}. \tag{6}$$

Il risultato seguente esercizio giustifica questa definizione.

Proposizione 1.6. *Per ogni insieme x, y, z, w,*

$$(x, y) = (z, w) \quad \Leftrightarrow \quad x = z \ \wedge \ y = w\,.$$

Dimostrazione. Supponiamo che $(x, y) = (z, w)$: vogliamo provare che $x = z$ e $y = w$.

Se $x = y$ allora $(x, y) = \{\{x\}\} = (z, w) = \{\{z\}, \{z, w\}\}$, quindi $\{x\} = \{z, w\} = \{z\}$, cioè $x = z = w$. Ne consegue che $x = y \Rightarrow z = w$ e poiché l'implicazione inversa segue similmente, possiamo supporre che

$$x \neq y \quad \text{e} \quad z \neq w\,. \tag{7}$$

Poiché $\{x\} \in (x, y) = (z, w) = \{\{z\}, \{z, w\}\}$ ne segue che $\{x\} = \{z\}$ oppure $\{x\} = \{z, w\}$, da cui $x = z$ oppure $x = z = w$. La seconda possibilità va scartata per via di (7), quindi

$$x = z\,.$$

Da $\{x, y\} \in (x, y) = (z, w) = (x, w)$ segue che $\{x, y\} = \{x\}$ oppure $\{x, y\} = \{x, w\}$. La prima possibilità non sussiste per (7) e dalla seconda otteniamo $y \in \{x, w\}$, cioè $y = x$ oppure $y = w$: nuovamente per (7) otteniamo

$$y = w\,.$$

L'implicazione inversa è immediata. □

Osservazione 1.7. La definizione data in (6) non è l'unica possibile, ma è probabilmente la più semplice. La prima definizione di coppia ordinata è dovuta a Norbert Wiener nel 1914:

$$(x, y)_{\mathrm{W}} = \{\{\emptyset, \{x\}\}, \{\{y\}\}\}\,.$$

Un'altra variante possibile definizione di coppia ordinata è una variante della definizione di Kuratowski:

$$(x, y)_{\mathrm{K}'} = \{x, \{x, y\}\}\,.$$

Lo svantaggio di quest'ultima definizione è che si richiede l'Assioma di Fondazione (definito qui sotto) per dimostrarne la sua adeguatezza—si veda l'Esercizio 1.22.

1.F. Fondazione. Se $A \in B$ è naturale considerare A più semplice, più elementare, più primitivo di B. Da questo punto di vista, l'insieme vuoto deve essere considerato come l'insieme più semplice in assoluto. Se gli elementi di un insieme sono più semplici dell'insieme stesso, allora nessun insieme dovrebbe appartenere a sé stesso. Il seguente assioma assicura tutto questo:

Assioma della Fondazione. *Se A è una classe non vuota esiste un $B \in A$ tale che $A \cap B = \emptyset$.*

Se per qualche classe si avesse che $A \in A$, allora A sarebbe un insieme e quindi esisterebbe $\{A\}$. Per l'Assioma di Fondazione deve esistere un $B \in \{A\}$ tale che $B \cap \{A\} = \emptyset$; ma B deve essere A e per ipotesi $A \in A = B$ e quindi $A \in B \cap \{A\}$: contraddizione. Poiché nessun insieme appartiene

a sé stesso, la classe R in (1) è la classe di *tutti* gli insiemi e solitamente è denotata con V. Usualmente la si definisce così:

$$\mathrm{V} \stackrel{\text{def}}{=} \{\, x \mid x = x \,\}. \tag{8}$$

Per questo motivo V viene detto l'**universo degli insiemi** o anche **classe totale**.

1.G. Unioni e intersezioni. Le operazioni di unione generalizzata $\bigcup_{x\in A} x$ e di intersezione generalizzata $\bigcap_{x\in A} x$ su una classe di insiemi A sono definite nel modo solito:

$$\bigcup A = \bigcup_{x\in A} x = \{\, y \mid \exists x \in A(y \in x) \,\}$$

è la collezione di tutti gli elementi contenuti in qualche x di A mentre

$$\bigcap A = \bigcap_{x\in A} x = \{\, y \mid \forall x \in A(y \in x) \,\},$$

con la convenzione che se $A = \emptyset$ allora $\bigcap A = \emptyset$. Poiché $\bigcap A \subseteq x$, per ogni $x \in A$, il Corollario 1.4 implica che $\bigcap A$ è sempre un insieme un insieme. (L'analogo risultato per $\bigcup A$ non vale—Esercizio 1.26.) Tuttavia, se A è una classe "piccola" (cioè un insieme) è ragionevole supporre che la sua unione sia tale.

Assioma dell'Unione. *Se A è un insieme allora anche $\bigcup A$ è un insieme.*

Quindi, se x e y sono insiemi, allora anche $\{x, y\}$ lo è per l'Assioma della Coppia e così pure $x \cup y = \bigcup\{x, y\}$.

Il **prodotto cartesiano** di due classi A e B è la classe

$$\begin{aligned} A \times B &= \{\, (x, y) \mid x \in A, y \in B \,\} \\ &= \{\, c \mid \exists a\, \exists b\, (a \in A \wedge b \in B \wedge c = (a, b)) \,\}, \end{aligned}$$

che esiste per l'Assioma di Comprensione

Proposizione 1.8. *Se A e B sono insiemi, anche $A \times B$ è un insieme.*

Dimostrazione. Per dimostrare che $A \times B$ è un insieme è sufficiente trovare un insieme che lo contenga. Se $x \in A$ e $y \in B$, allora $\{x\}, \{x, y\} \subseteq A \cup B$ e quindi $(x, y) = \{\{x\}, \{x, y\}\} \subseteq \mathscr{P}(A \cup B)$. Ne segue che $A \times B \subseteq \mathscr{P}(\mathscr{P}(A \cup B))$ e poiché quest'ultimo è un insieme la dimostrazione è completa. □

Usando gli Assiomi di Coppia e Unione siamo in grado di costruire infiniti nuovi insiemi a partire da $\emptyset$, per esempio

$$\{\emptyset\},\ \{\{\emptyset\}\},\ \{\{\{\emptyset\}\}\},\ \{\{\{\{\emptyset\}\}\}\},\quad \ldots$$

oppure

$$\{\emptyset\} = \mathbf{S}(\emptyset),\ \{\emptyset, \{\emptyset\}\} = \mathbf{S}(\{\emptyset\}),\ \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} = \mathbf{S}(\{\emptyset, \{\emptyset\}\}),\ \ldots \tag{9}$$

dove

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

è il **successore** di x. Non è difficile convincersi che gli insiemi in (9) sono tutti distinti.

1.H. Insiemi infiniti. Le varie costruzioni insiemistiche introdotte fin'ora ci consentono di costruire infiniti insiemi. Tuttavia esse non sono sufficientemente potenti da garantire l'esistenza di un insieme infinito, quale, per esempio, $\mathbb{N}$. Ma come possiamo formulare nel linguaggio insiemistico un principio che asserisca l'esistenza di un insieme infinito? La tentazione è di dire che esiste la classe A degli insiemi in (9) e poi stabilire che A è un insieme. Tuttavia non è chiaro quale sia la formula φ che caratterizza tutti e soli gli oggetti in (9) per poter applicare l'Assioma di Comprensione. Introduciamo quindi la seguente definizione: una classe I si dice **induttiva** se

$$\emptyset \in I \ \wedge \ \forall x \, (x \in I \Rightarrow \mathbf{S}(x) \in I) \, .$$

Chiaramente esistono classi induttive, per esempio V. Il seguente assioma ci garantisce che esistono *insiemi* induttivi.

Assioma dell'Infinito. *Esiste un insieme induttivo.*

Osserviamo che l'Assioma dell'Infinito, poiché asserisce l'esistenza di un *insieme* con certe proprietà, rende superfluo l'Assioma di Esistenza di Insiemi.

Sia $\mathcal{S}$ la classe di tutti gli insiemi induttivi. Poniamo

$$\mathbb{N} \stackrel{\text{def}}{=} \bigcap \mathcal{S}. \tag{10}$$

Quindi $\mathbb{N}$ è il più piccolo insieme contenente $\emptyset$ e chiuso per successori. Definiamo anche

$$0 = \emptyset, \quad 1 = \mathbf{S}(0), \quad 2 = \mathbf{S}(1) = \mathbf{S}(\mathbf{S}(0)), \quad \ldots$$

Proposizione 1.9. $\mathbb{N} \in \mathcal{S}$ *e se* $n \in \mathbb{N}$, *allora* $n = 0$ *oppure* $n = \mathbf{S}(m)$ *per qualche* $m \in \mathbb{N}$.

Dimostrazione. Sia I un elemento di $\mathcal{S}$—per l'Assioma dell'Infinito un insieme siffatto esiste. Poiché $0 \in I$ e poiché I è arbitrario, possiamo concludere che $0 \in \bigcap \mathcal{S} = \mathbb{N}$. Sia n un elemento di $\mathbb{N}$. Per ogni $I \in \mathcal{S}$ si ha che $n \in I$ e quindi $\mathbf{S}(n) \in I$: essendo $I \in \mathcal{S}$ arbitrario, otteniamo che $\mathbf{S}(n) \in \bigcap \mathcal{S} = \mathbb{N}$. Quindi $\mathbb{N} \in \mathcal{S}$.

Sia $n \in \mathbb{N} \setminus \{0\}$ e supponiamo per assurdo che $n \neq \mathbf{S}(m)$ per ogni $m \in \mathbb{N}$. Allora l'insieme $J = \mathbb{N} \setminus \{n\}$ soddisferebbe la formula che definisce $\mathcal{S}$ e quindi $J \in \mathcal{S}$. Da questo segue che $J \supseteq \bigcap \mathcal{S} = \mathbb{N}$, ma per costruzione $J \subset \mathbb{N}$: contraddizione. $\square$

Proposizione 1.10 (Principio di Induzione su $\mathbb{N}$ —prima formulazione)**.** *Sia $I \subseteq \mathbb{N}$ tale che $0 \in I$ e tale che $\forall n\,(n \in I \Rightarrow \mathbf{S}(n) \in I)$. Allora $I = \mathbb{N}$.*

Dimostrazione. $I \in \mathcal{S}$, quindi $I \supseteq \mathbb{N}$. □

Vedremo una seconda formulazione del principio di induzione nell'Esercizio 3.15.

1.I. Relazioni e funzioni. Una **relazione binaria** (o più brevemente: una relazione) è una classe tale che tutti i suoi elementi sono coppie ordinate. Una relazione F si dice **funzionale** se $(x, y), (x, y') \in F$ implica $y = y'$; talvolta useremo l'espressione **classe-funzione** invece di relazione funzionale. Spesso scriveremo $x\ R\ y$ invece di $(x, y) \in R$ e, nel caso in cui R sia una relazione funzionale, $R(x)$ denota l'unico y (se esiste) tale che $(x, y) \in R$. In genere il termine **funzione** indica una relazione funzionale che sia un insieme.

Il **dominio**, l'**immagine**[3] e il **campo** di una classe R sono, rispettivamente,

$$\begin{aligned} \mathrm{dom}(R) &= \{\, x \mid (x, y) \in R, \text{ per qualche } y \,\} \\ \mathrm{ran}(R) &= \{\, y \mid (x, y) \in R, \text{ per qualche } x \,\} \\ \mathrm{fld}(R) &= \mathrm{dom}(R) \cup \mathrm{ran}(R). \end{aligned}$$

Per verificare che, per esempio, $\mathrm{dom}(R)$ è una classe si applica l'Assioma di Costruzione di Classi alla formula $\varphi(x, R)$

$$\exists y\, \exists z\, (z = (x, y) \wedge z \in R)$$

dove l'espressione "$z = (x, y)$" è una formula insiemistica (Esercizio 1.21). La definizione è sensata per ogni classe R, non soltanto per le relazioni; se R non contiene coppie ordinate, $\mathrm{dom}(R) = \mathrm{ran}(R) = \mathrm{fld}(R) = \emptyset$. Il prodotto cartesiano $A \times B$ è una relazione di dominio A, immagine B e campo $A \cup B$.

Proposizione 1.11. *Se R è un insieme, allora* $\mathrm{dom}(R)$, $\mathrm{ran}(R)$, $\mathrm{fld}(R)$ *sono insiemi.*

Dimostrazione. Per dimostrare che $\mathrm{dom}(R)$ è un insieme, basta trovare un insieme che contenga $\mathrm{dom}(R)$: se $x \in \mathrm{dom}(R)$ allora $x \in \{x\} \in (x, y) \in R$, per qualche y, quindi $x \in \bigcup(\bigcup R)$, quindi $\mathrm{dom}(R) \subseteq \bigcup(\bigcup R)$. I casi di $\mathrm{ran}(R)$ e $\mathrm{fld}(R)$ sono analoghi. □

Se F è una relazione funzionale e A una classe poniamo

$$\begin{aligned} F[A] &= \{\, F(x) \mid x \in A \cap \mathrm{dom}(F) \,\} \\ F \restriction A &= \{\, (x, y) \in F \mid x \in A \,\}. \end{aligned}$$

[3] In inglese oltre a *image* si usa *range*, da cui ran.

Si noti che non si richiede che $A \subseteq \mathrm{dom}(F)$. Se entrambe F ed A sono classi proprie può accadere che $F[A]$ sia una classe propria: per esempio, se F è la relazione funzionale identica

$$F = \{\, (x, x) \mid x \in \mathrm{V} \,\}$$

allora $F[A] = A$ non è un insieme. È facile verificare (Esercizio 1.25) che se F è un insieme anche $F[A]$ è un insieme, ma che accade se F è una classe propria e A un insieme? Se le classi piccole sono insiemi, dato che ad ogni elemento di A corrisponde al più un elemento di $F[A]$, la classe dovrebbe essere piccola.

Assioma del Rimpiazzamento. *Se F è una relazione funzionale e A un insieme, allora $F[A]$ è un insieme.*

Questo completa la lista degli assiomi di MK. A questi assiomi se ne aggiunge spesso un altro, l'Assioma di Scelta che vedremo nella sezione 14.

Se F è una (classe-)funzione di dominio A e immagine contenuta in B diremo che F è una (classe-)funzione da A a B e lo indicheremo con $F\colon A \to B$. La collezione di tutte queste F è denotata

$$^{A}B = B^{A} = \{\, F \mid F\colon A \to B \,\}.$$

(Per l'Esercizio 1.27 questa nozione è interessante soltanto quando A è un insieme.)

Proposizione 1.12. *Se A e B sono insiemi, allora B^A è un insieme.*

Dimostrazione. $B^A \subseteq \mathscr{P}(A \times B)$. □

Osservazione 1.13. Le notazioni ^{A}B e B^A sono entrambe comuni in teoria degli insiemi, ma la seconda è quella comunemente usata nelle altre parti della matematica. Il motivo per scrivere ^{A}B invece del più comune B^A è che in certi casi la seconda notazione può essere ambigua: per esempio $^{2}3$ è la classe (anzi: l'insieme, per la Proposizione 1.12) di tutte le funzioni dall'insieme $2 = \{0, 1\}$ all'insieme $3 = \{0, 1, 2\}$, mentre 3^2 è il numero 9. Quando non c'è pericolo di confusione useremo liberamente B^A.

Se $F \in B^A$ diremo che F è:

iniettiva se $\forall a_1, a_2 \in A\,(a_1 \neq a_2 \Rightarrow F(a_1) \neq F(a_2))$,

suriettiva se $\forall b \in B\,\exists a \in A\,(F(a) = b)$,

bijettiva se è iniettiva e suriettiva.

Useremo i simboli $F\colon A \rightarrowtail B$ e $F\colon A \twoheadrightarrow B$ per dire che F è iniettiva e, rispettivamente, suriettiva. Se F è iniettiva

$$F^{-1} = \{\, (b, a) \mid (a, b) \in F \,\}$$

è una (classe-)funzione e si dice (classe-)funzione inversa.

Esercizio 1.14. Dimostrare che se A è una classe propria e B un insieme, allora non esiste nessuna $F\colon A \to B$ iniettiva.

Due insiemi sono **equipotenti** o **in bijezione** se esiste una bijezione da un insieme sull'altro.

Teorema 1.15. *Non esiste nessuna funzione f tale che* $\mathrm{dom}(f) = \mathbb{N}$ *e*

$$\forall n \in \mathbb{N}\ f(\mathbf{S}(n)) \in f(n)\,.$$

Dimostrazione. Per assurdo, supponiamo esista una f siffatta. Poiché $\emptyset \neq \mathrm{ran}(f)$, per l'assioma di Fondazione c'è un $y \in \mathrm{ran}(f)$ tale che $y \cap \mathrm{ran}(f) = \emptyset$. Sia $n \in \mathbb{N}$ tale che $y = f(n)$. Ma $f(\mathbf{S}(n)) \in f(n) \cap \mathrm{ran}(f)$: contraddizione. □

1.J. Successioni. Spesso in matematica si usa la notazione F_x invece di $F(x)$ e quando si scrivono espressioni come "a_i $(i \in I)$" oppure "$(a_i)_{i\in I}$" stiamo in realtà asserendo l'esistenza di una funzione a di dominio I che ad un $i \in I$ associa a_i. Per descrivere in modo conciso tutto ciò useremo le espressioni $I \ni i \mapsto a_i$ oppure $\langle a_i \mid i \in I\rangle$. La notazione $\langle a_i \mid i \in I\rangle$ è particolarmente utile quando $I \in \mathbb{N}$, cioè quando si ha a che fare con le **sequenze finite**, o **stringhe**. Per esempio, $s = \langle a_0, a_1, \ldots, a_{n-1}\rangle$ è la funzione di dominio $n = \{0, 1, \ldots, n-1\}$ che ad ogni $i < n$ associa l'insieme a_i; l'ordinale $n = \mathrm{dom}(s)$ si dice **lunghezza** di s e viene indicato con $\mathrm{lh}(s)$. Benché la sequenza $\langle a, b\rangle$ di lunghezza 2 e la coppia ordinata (a, b) possano essere identificate, esse sono insiemi distinti. Il vantaggio di usare le sequenze invece delle coppie è evidente quando vogliamo parlare n-uple ordinate: se definissimo—come è del tutto lecito fare—una tripla ordinata (a, b, c) come $((a, b), c)$ non riusciremmo a distinguere gli insiemi che sono triple da quelli che sono coppie. Un altro difetto dell'usuale definizione di coppia ordinata è che il prodotto cartesiano non è associativo e quindi l'espressione $X \times \cdots \times X$ è ambigua—per esempio: quando scriviamo $\mathbb{R}^3$ intendiamo $(\mathbb{R} \times \mathbb{R}) \times \mathbb{R}$ oppure $\mathbb{R} \times (\mathbb{R} \times \mathbb{R})$? Per questo motivo, per evitare fastidiose (e banali) ambiguità, conviene assumere implicitamente che il prodotto cartesiano $X^n \times X^m$ denoti, in realtà, l'insieme X^{n+m}. Se X è una classe

$$X^{<\mathbb{N}} = \{\, s \mid s \text{ è una stringa finita e } \mathrm{ran}(s) \subseteq X \,\}\,. \tag{11}$$

Esercizio 1.16. Dimostrare che se X è un insieme, allora $X^{<\mathbb{N}} = \{\, X^n \mid n \in \mathbb{N} \,\}$ è un insieme.

Per semplicità notazionale useremo spesso l'espressione $\bar{x}$ invece di $\langle x_0, \ldots, x_{n-1}\rangle$ o di $(x_0, \ldots, x_{n-1})$ quando questo non è motivo di confusione; inoltre se

$\mathrm{dom}(f) \subseteq \bigcup_{n\in\mathbb{N}} X^n$, allora scriveremo $f(\bar{x})$ o $f(x_0, \ldots, x_{n-1})$ invece del più corretto, ma barocco, $f(\langle x_0, \ldots, x_{n-1}\rangle)$.

Se I è un insieme e $\langle A_i \mid i \in I\rangle$ è una successione di insiemi, il **prodotto cartesiano generalizzato** è

$$\text{(12)}\quad \bigtimes_{i\in I} A_i = \{\, f \mid f \text{ è una funzione, } \mathrm{dom}(f) = I \text{ e } \forall i \in I\,(f(i) \in A_i)\,\}\,.$$

Quindi se $A_i = A$ per ogni $i \in I$, allora $\bigtimes_{i\in I} A_i = A^I$.

Esercizio 1.17. Dimostrare che $\bigtimes_{i\in I} A_i$ è un insieme e che se $I = \{0, 1\}$ allora $\bigtimes_{i\in I} A_i$ può essere identificato (cioè è in bijezione) con $A_0 \times A_1$.

Se $\langle A_i \mid i \in I\rangle$ è una successione di insiemi e $A_{i_0} = \emptyset$ per qualche $i_0 \in I$, allora $\bigtimes_{i\in I} A_i = \emptyset$. Supponiamo invece che $\forall i \in I\ A_i \neq \emptyset$. È veri che $\bigtimes_{i\in I} A_i \neq \emptyset$? La risposta è affermativa se I è costituito da due elementi, per l'esercizio precedente e, più in generale, la risposta continua ad essere affermativa se I è finito (vedi pag.33), cioè se è in bijezione con un numero naturale (Esercizio 1.29). Ma che dire di una successione indicizzata da un insieme I non finito? Intuitivamente $\bigtimes_{i\in I} A_i \neq \emptyset$ dovrebbe continuare a valere, dato che posso prendere un elemento $a_i \in A_i$ e considerare la funzione $f(i) = a_i$. Tuttavia questo semplice ragionamento utilizza un principio insiemistico che non abbiamo ancora introdotto: l'Assioma di Scelta, che vedremo in dettaglio nella sezione 14. Per il momento osserviamo soltanto che se gli A_i sono tutti uguali ad un $A \neq \emptyset$, allora $\bigtimes_{i\in I} A_i = A^I$ è non vuoto, dato che posso considerare una funzione costante $i \mapsto a \in A$.

1.K. Operazioni. Una **funzione finitaria** o **operazione su** X è una

$$f\colon X^n \to X$$

dove $n = \mathrm{ar}(f)$ si dice **arietà** di f. Se $n = 0$ allora $f\colon \{\emptyset\} \to X$, quindi f è completamente determinata dal valore $f(\emptyset) \in X$. Ne segue che le funzioni 0-arie su X possono essere identificate con gli elementi di X. Un $Y \subseteq X$ si dice **chiuso per** f se $f[Y^n] \subseteq Y$.

Esercizio 1.18. Sia $Y \subseteq X$ e sia

$$\mathcal{C} = \{\, Z \subseteq X \mid Y \subseteq Z \wedge Z \text{ chiuso per } f\,\}\,.$$

Dimostrare che $\mathcal{C} \neq \emptyset$ e che $\bigcap \mathcal{C}$ è il più piccolo sottoinsieme di X contenente Y e chiuso per f.

L'insieme $\bigcap \mathcal{C}$ si dice **chiusura di** Y **sotto** f e lo si indica con

$$\mathrm{Cl}_f(Y)\,.$$

La definizione di insieme chiuso e di chiusura si generalizzano al caso di una famiglia $\mathcal{F}$ di funzioni finitarie su X; in questo caso la chiusura di Y sotto la famiglia $\mathcal{F}$ si scrive $\mathrm{Cl}_{\mathcal{F}}(Y)$.

1.L. Coppie e successioni di classi. La coppia ordinata (x, y) è stata definita in (6) solo quando *entrambi* x e y sono insiemi. Tuttavia ci sono situazioni in matematica in cui è necessario lavorare con coppie di classi proprie, o, addirittura, con successioni di classi proprie. (Si veda la sezione 10 per esempio.) Se A e B sono classi e almeno una tra A e B è una classe propria, poniamo

$$\langle A, B\rangle \stackrel{\text{def}}{=} \{0\} \times A \cup \{1\} \times B\,.$$

Poiché $A = \{\, x \mid (0, x) \in \langle A, B\rangle \,\}$ e $B = \{\, x \mid (1, x) \in \langle A, B\rangle \,\}$, la classe $\langle A, B\rangle$ codifica entrambe A e B. Più in generale, se A è una classe propria di coppie ordinate, allora possiamo considerare A come una successione $\langle A_i \mid i \in I\rangle$, dove $I = \mathrm{dom}(A)$ e $A_i = \{\, x \mid (i, x) \in A \,\}$.

1.M. Le teorie MK e ZF. L'assiomatizzazione della teoria degli insiemi è stata introdotta per risolvere le antinomie che il paradosso di Russell aveva generato. Una possibile assiomatizzazione è quella che abbiamo visto nelle sezioni precedenti: la teoria Morse-Kelly, MK. Prima di tutto abbiamo introdotto (informalmente) il linguaggio della teoria degli insiemi LST che consiste di variabili, dei simboli di appartenenza $\in$, di uguaglianza $=$, delle parentesi $(,)$, dei connettivi logici e dei quantificatori. A partire da questo abbiamo costruito le formule della teoria degli insiemi (pagina 3 e seguenti) che sono enti *pre-insiemistici* che ci servono per parlare di insiemi e classi. Lo studio delle formule della teoria degli insiemi (in realtà appena abbozzato nella sezione 1) è un'impresa matematica che avviene in un ambiente antecedente allo sviluppo tecnico della teoria degli insiemi e della matematica usuale. Questo ambiente prende nome di *metamatematica* ed è caratterizzato da un approccio *concreto* e *finitistico*: le formule di LST sono oggetti analizzabili in modo algoritmico e quindi sono, in linea di principio, implementabili in un programma. Per far ciò dobbiamo specificare un po' meglio cosa intendiamo per variabili: formalmente questi sono simboli di una lista prefissata e riconoscibili in modo meccanico

$$\mathsf{v}_0, \quad \mathsf{v}_1, \quad \mathsf{v}_2, \quad \mathsf{v}_3, \quad \ldots$$

Quindi l'assioma di estensionalità dovrebbe essere scritto così

$$\forall \mathsf{v}_0\, \forall \mathsf{v}_1\, (\forall \mathsf{v}_2\, (\mathsf{v}_2 \in \mathsf{v}_0 \Leftrightarrow \mathsf{v}_2 \in \mathsf{v}_1) \Rightarrow \mathsf{v}_0 = \mathsf{v}_1)\,.$$

Tuttavia per non appesantire la notazione useremo impunemente le lettere dell'alfabeto variamente decorate per denotare le variabili.

Torniamo al problema di assiomatizzare la teoria ingenua degli insiemi: il sistema MK descrive degli enti matematici: le classi. Queste si dividono un due sottofamiglie: quelle "piccole" cioè gli insiemi e quelle "grandi" cioè le classi proprie. Gli assiomi di MK sono:

Estensionalità: $\forall x\, \forall y\, (\forall z (z \in x \Leftrightarrow z \in y) \Rightarrow x = y)$.

Comprensione (schema di assiomi): Per ogni formula di LST

$$\varphi(x, y_1, \ldots, y_n)$$

in cui x compare libera e per ogni variabile A differente da $x, y_1, \ldots, y_n$,

$$\forall y_1 \ldots \forall y_n \, \exists A \forall x \, (x \in A \Leftrightarrow \exists z (x \in z) \wedge \varphi(x, y_1, \ldots, y_n)) \, .$$

Esistenza di Insiemi: $\exists x \, \exists y (x \in y)$.

Potenza: $\forall x \, (\exists y \, (x \in y) \Rightarrow \exists z \, \exists w \, (z \in w \wedge \forall t \, (t \in z \Leftrightarrow t \subseteq z)))$.

Coppia: $\forall x \, \forall y \, (\exists a \, (x \in a) \wedge \exists b \, (y \in b) \Rightarrow \exists z \, \exists c \, (z \in c \wedge z = \{x, y\}))$.

Fondazione: $\forall A \, (A \neq \emptyset \Rightarrow \exists x \, (x \in A \wedge x \cap A = \emptyset))$.

Unione: $\forall A \, (\exists B \, (A \in B) \Rightarrow \exists C \, \exists D \, (C \in D \wedge C = \bigcup A))$.

Infinito: $\exists I \, \exists J \, (I \in J \wedge \emptyset \in I \wedge \forall x \, (x \in I \Rightarrow \exists y \, (y = \mathbf{S}(x) \wedge y \in I)))$.

Rimpiazzamento:

$$\forall F \, \forall A \, \big(\big(\forall x \, \exists! y \, (x, y) \in F \wedge \exists B \, (A \in B) \big) \Rightarrow \exists C \, (F[A] \in C) \big) \, . \tag{13}$$

Osserviamo che l'Assioma di Comprensione è in realtà una lista infinita di assiomi, uno per ogni formula φ come sopra e per questo motivo diremo che è uno *schema di assiomi*. Poiché è possibile stabilire in modo meccanico se o meno un'espressione è un'istanza di questo schema di assiomi, ne segue che è possibile stabilire in modo effettivo, meccanico se una certa formula è o meno un assioma di MK. È anche possibile generare la lista degli assiomi di MK mediante un programma: per prima cosa si elencano gli assiomi di Estensionalità, Potenza, Coppia, Fondazione, Unione, Infinito e Rimpiazzamento, per poi passare ad elencare una dopo l'altra le istanze dell'Assioma di Comprensione.

Gli assiomi qui sopra sono solo parzialmente formalizzati nel linguaggio LST dato che abbiamo usato termini definiti quali $\subseteq$, $\{x, y\}$, $\cap$, $\emptyset$, $\bigcup$, $\mathbf{S}$ e $F[A]$. Lasciamo al lettore l'ulteriore sforzo di eliminare questi simboli definiti (Esercizio 1.23). In oltre abbiamo usato varie lettere maiuscole e minuscole nel tentativo di rendere più trasparente il significato degli assiomi. Per esempio, nel caso dell'assioma di rimpiazzamento, la lettera F suggerisce che si sta parlando di una funzione. Nell'assioma di comprensione le lettere (vale a dire: le variabili) $y_1, \ldots, y_n$ denotano dei parametri, mentre la lettera maiuscola A indica la classe $\{ \, x \mid \varphi(x, y_1, \ldots, y_n) \, \}$ la cui esistenza è postulata dall'assioma. Se volessimo essere formalmente precisi dovremmo scrivere l'assioma di comprensione come segue:

> *Sia* φ *una formula di* LST *e sia* v_{k_0} *una variabile che occorre libera in* φ*, supponiamo che le altre variabili libere di*

φ siano tra le $\mathsf{v}_{k_1}, \ldots, \mathsf{v}_{k_n}$ e siano m, h e i indici diversi da $k_0, \ldots, k_n$. Allora

$$\forall \mathsf{v}_{k_1} \ldots \forall \mathsf{v}_{k_n}\, \exists \mathsf{v}_m \forall \mathsf{v}_h\, (\mathsf{v}_h \in \mathsf{v}_m \Leftrightarrow \exists \mathsf{v}_i (\mathsf{v}_m \in \mathsf{v}_i) \wedge \varphi(\mathsf{v}_m, \mathsf{v}_{k_1}, \ldots, \mathsf{v}_{k_n}))\,.$$

Un'altra assiomatizzazione della teoria degli insiemi è dovuta a Ernst Zermelo e Adolf Frænkel ed è nota con l'acronimo ZF. Come MK è formulata nel linguaggio LST, quindi la nozione di formula della teoria degli insiemi non cambia, ma, a differenza di MK, è una teoria che parla solo di insiemi e null'altro. Quindi la classe V di tutti gli insiemi è un ente che non ha diritto di cittadinanza in ZF. Gli assiomi di Estensionalità e Fondazione sono esattamente come in MK; gli assiomi della Coppia, Potenza, Unione e Infinito sono *essenzialmente* come in MK, eccetto che non è necessario asserire che si sta parlando di insiemi:

Coppia: $\forall x \forall y \exists z\, (z = \{x, y\})$.

Potenza: $\forall x \exists y \forall z\, (z \in y \Leftrightarrow z \subseteq z)$.

Unione: $\forall x \exists y \forall z\, (z \in y \Leftrightarrow \exists u\, (u \in x \wedge z \in u))$.

Infinito: $\exists x\, (\emptyset \in x \wedge \forall y\, (y \in x \Rightarrow \mathbf{S}(y) \in x))$.

Lo Schema di Assiomi di Comprensione è sostituito da

Separazione (schema di assiomi): *Per ogni formula di* LST

$$\varphi(x, B, y_1, \ldots, y_n)$$

in cui x compare libera e per ogni variabile A differente da $x, B, y_1, \ldots, y_n$,

$$\forall y_1 \ldots \forall y_n \forall B \exists A \forall x\, (x \in A \Leftrightarrow x \in B \wedge \varphi(x, B, y_1, \ldots, y_n))\,.$$

In altre parole: per ogni insieme A e ogni proprietà φ esiste l'insieme $\{\, x \in A \mid \varphi(x, y_1, \ldots, y_n)\,\}$.

L'Assioma del Rimpiazzamento è sostituito dal seguente schema di assiomi:

Rimpiazzamento (schema di assiomi): *Per ogni formula di* LST

$$\varphi(x, y, A, z_1, \ldots, z_n)$$

e per ogni variabile B differente da $x, y, A, z_1, \ldots, z_n$,

$$\begin{aligned}(14)\quad \forall A \forall z_1 \ldots \forall z_n\, (\forall x\, (x \in A \Rightarrow \exists! y\, \varphi(x, y, A, z_1, \ldots, z_n)) \Rightarrow \\ \exists B \forall y\, (y \in B \Leftrightarrow \exists x\, (x \in A \wedge \varphi(x, y, A, z_1, \ldots, z_n))))\,.\end{aligned}$$

In altre parole: fissati gli insiemi $A, z_1, \ldots, z_n$, se la formula φ definisce una funzione $x \mapsto y$ sull'insieme A, allora c'è un insieme B che consiste esattamente di tutti questi y.

Osserviamo che (13) è un singolo assioma, mentre lo Schema di Assiomi del Rimpiazzamento[4] di ZF è una lista infinita di assiomi, uno per ogni φ. Anche in questo caso è possibile stabilire in modo effettivo se un'espressione è o meno un assioma di ZF e la lista degli assiomi di ZF può essere generata in modo algoritmico, elencando prima gli assiomi di Estensionalità, Potenza, Coppia, Fondazione, Unione e Infinito, per poi passare ad elencare una dopo l'altra le istanze dell'Assioma di Separazione e di Rimpiazzamento.[5] Il paradosso di Russell è neutralizzato da ZF nel seguente modo. innanzitutto la collezione R in (1) non è stata definita mediante l'assioma di separazione, quindi non possiamo concludere a questo punto che che sia un insieme, cioè un oggetto legittimo di ZF. Supponiamo R sia un insieme: allora le implicazioni (2) e (3) continuano a valere portandoci quindi ad una contraddizione. Ne segue che R *non* è un insieme e quindi il paradosso di Russell non sussiste più.

Osserviamo infine che esiste un terzo approccio alla teoria assiomatica degli insiemi, quella introdotta da von Neumann e sviluppata da Kurt Gödel e Paul Bernays e che va sotto il nome di NGB. Non diremo nulla su questa teoria se non che, come MK, è una teoria degli insiemi e delle classi, ma, a differenza di quest'ultima, le formule usate nell'Assioma di Comprensione devono essere di tipo particolare. A differenza di MK e ZF, la teoria NGB è finitamente assiomatizzabile.

Benché la stragrande maggioranza degli oggetti studiati dai matematici siano insiemi, è spesso utile poter parlare della classe di tutti i gruppi, o della classe degli spazi topologici, o della classe degli insiemi finiti—questo è particolarmente vero quando si utilizza il linguaggio della teoria delle categorie (sezione 10). Per questo motivo taluni matematici preferiscono una teoria come MK o NGB. D'altra parte neppure queste teorie sembrano poi così soddisfacenti, visto che non è possibile considerare classi-di-classi come $\mathscr{P}(\mathrm{V})$, o classi-di-classi-di-classi come $\mathscr{P}(\mathscr{P}(\mathrm{V}))$, etc. In realtà, aggiungendo a ZF opportuni rafforzamenti dell'Assioma dell'Infinito è possibile, in un certo senso, catturare il concetto di classe, classe-di-classi, classe-di-classi-di-classi,... e molto altro ancora. Per questo motivo la quasi totalità della ricerca contemporanea in teoria degli insiemi avviene nel sistema ZF.

Le classi proprie in ZF sono solo degli oggetti meta-matematici, delle formule che descrivono una totalità a cui non corrisponde una controparte nella teoria. Per esempio: invece della classe di tutti i gruppi si considera la formula $\gamma(x)$ che asserisce che x è un gruppo, ovverosia x è una coppia ordinata $(G, *)$ dove G è un insieme non vuoto e $*$ è un'operazione binaria

[4]Per distinguere la versione del rimpiazzamento in MK (un singolo assioma) da quello in ZF (uno schema di assiomi), il primo viene spesso detto Rimpiazzamento Forte.

[5]Per fare ciò il programma lavora in simultanea sulle due liste, dividendo il suo tempo sull'una e sull'altra.

su G che induce una struttura di gruppo. Analogamente al posto della classe degli spazi topologici si considera la formula $\tau(x)$ che asserisce che x è uno spazio topologico, ovverosia x è una coppia ordinata $(Y, \mathcal{O})$ dove Y è un insieme non vuoto e $\mathcal{O}$ è una topologia su Y. Nella teoria MK è possibile dimostrare teoremi della forma

$$\exists X\,(\neg\exists Y(X \in Y) \wedge \ldots X \ldots) \tag{15}$$

e

$$\forall X\,(\neg\exists Y(X \in Y) \Rightarrow \ldots X \ldots) \tag{16}$$

cioè affermazioni del tipo: "Esiste una classe propria X tale che..." e "Per ogni classe propria X succede che...". O, naturalmente enunciati anche più complessi, del tipo $\forall X\,\exists Y\,\ldots$ In ZF capita di dimostrare affermazioni esistenziali come in (15): in questo caso dobbiamo esplicitamente *esibire esplicitamente una formula* φ che definisce la classe propria X con le proprietà richieste. In MK la richiesta è più modesta e potremmo, per esempio, dimostrare (15) per assurdo, cioè che se ogni classe propria X non soddisfa alla proprietà in questione, allora si ottiene una contraddizione in MK. Le affermazioni del tipo (16) sono anche più problematiche: infatti un "teorema" del genere deve essere dimostrato caso per caso, uno per ogni formula φ che definisca una classe X. Si parla in questo caso di *schema di teoremi* o *metateorema*.

La discussione precedente può far sorgere il sospetto che la differenza tra MK e ZF riguardi solo fatti astrusi su classi proprie, mentre i teoremi riguardanti gli insiemi non presentano differenza tra le due teorie. Ogni teorema di ZF è anche un teorema di MK, ma non vale il viceversa: ci sono dei teoremi sui numeri naturali che sono dimostrabili in MK, ma non in ZF. Di più: questi teoremi sono della forma

$$\forall n \in \mathbb{N}\ P(n)$$

dove la proprietà $P(n)$ è verificabile in modo meccanico a partire dall'input n. Tuttavia enunciati di questo genere sono molto rari e per la maggior parte, un risultato sugli *insiemi* dimostrato in MK è dimostrabile anche in ZF, essenzialmente con la stessa dimostrazione.

Esercizi

Esercizio 1.19. Dimostrare che se A è un insieme allora $A \cap B$ è un insieme; se B è una classe propria allora $A \cup B$ è una classe propria.

Se $x_1, \ldots, x_n$ sono insiemi, anche $\{x_1, \ldots, x_n\}$ è un insieme.

Esercizio 1.20. Dimostrare che $\mathrm{V} \setminus x$ è una classe propria, per ogni insieme x.

Esercizio 1.21. Dare formule $\varphi(x, y, z)$ e $\psi(x, y, z)$ che asseriscono, rispettivamente, "$z = \{x, y\}$" e "$z = (x, y)$."

Esercizio 1.22. Dimostrare che:

$$\{\{\emptyset, \{x\}\}, \{\{y\}\}\} = \{\{\emptyset, \{z\}\}, \{\{w\}\}\} \Rightarrow x = z \ \wedge \ y = w \qquad \text{e}$$
$$\{x, \{x, y\}\} = \{z, \{z, w\}\} \Rightarrow x = z \ \wedge \ y = w\,.$$

(Per la seconda implicazione utilizzare l'Assioma della Fondazione.) Quindi le definizioni di coppia ordinata $(x, y)_{\mathrm{W}}$ e $(x, y)_{\mathrm{K}'}$ dell'Osservazione 1.7 sono adeguate.

Esercizio 1.23. Formalizzare nel linguaggio LST i seguenti assiomi di MK: Potenza, Coppia, Fondazione, Unione, Infinito e Rimpiazzamento. Analogamente per gli assiomi di ZF.

Esercizio 1.24. Dimostrare che per ogni insieme x non esiste alcun y tale che $x \in y$ e $y \in \mathbf{S}(x)$.

Esercizio 1.25. Dimostrare che se f è un insieme anche $f[A]$ è un insieme.

Esercizio 1.26. Dimostrare che:

(i) $\{\, \{x\} \mid x \in \mathrm{V} \,\}$ è una classe propria;

(ii) se $y \neq \emptyset$, allora la classe degli insiemi equipotenti ad y

$$\{\, x \mid \exists f \colon x \to y \text{ bijezione} \,\}$$

è una classe propria.

(iii) Trovare un esempio di classe propria A tale che $\bigcup A$ è una classe propria.

Esercizio 1.27. Dimostrare che:

(i) se A è una classe propria oppure $B = \emptyset \neq A$, allora $B^A = \emptyset$,

(ii) se $A \neq \emptyset$ è un insieme e B una classe propria, allora B^A è una classe propria,

(iii) se $A = \emptyset$, allora $B^A = \{\emptyset\}$.

Esercizio 1.28. Dimostrare che se C è una classe propria, anche C^n ($n \neq 0$) e $C^{<\mathbb{N}}$ sono classi proprie.

Esercizio 1.29. Dimostrare che se $\langle A_i \mid i \in I \rangle$ è una sequenza di insiemi (o di classi) non-vuoti e I è in bijezione con un numero naturale, allora $\bigtimes_{i \in I} A_i \neq \emptyset$.

Esercizio 1.30. Dimostrare che:

(i) In presenza degli altri assiomi di MK, l'assioma di rimpiazzamento (13) è equivalente alla sua versione iniettiva:

> Se F è una relazione funzionale iniettiva e A è un insieme, allora $F[A]$ è un insieme.

(ii) Analogamente, in presenza degli altri assiomi di ZF, lo schema di assiomi di rimpiazzamento (14) è equivalente alla sua versione iniettiva:

Sia $\varphi(x, y, A, z_1, \ldots, z_n)$ una formula di LST e supponiamo B sia differente da $x, y, A, z_1, \ldots, z_n$. Per ogni A, z_1, …, z_n se

$$\forall x \, (x \in A \Rightarrow \exists! y \, \varphi(x, y, A, z_1, \ldots, z_n))$$

e se

$$\forall x \, \forall x' \, \forall y \, \forall y' \, \big(x \in A \wedge x' \in A \wedge x \neq x' \wedge \varphi(x, y, A, z_1, \ldots, z_n) \wedge \varphi(x', y', A, z_1, \ldots, z_n) \Rightarrow y \neq y'\big)$$

allora

$$\exists B \, \forall y \, (y \in B \Leftrightarrow \exists x \, (x \in A \wedge \varphi(x, y, A, z_1, \ldots, z_n))) \, .$$

(iii) In presenza degli altri assiomi di ZF, lo schema di assiomi di rimpiazzamento (14) implica lo schema di assiomi di separazione.

Note e osservazioni

La teoria degli insiemi è stata inventata da Georg Cantor (1845–1918) verso il 1870 per risolvere un problema di Bernhard Riemann (1826–1866) sulle serie trigonometriche. L'assiomatizzazione della teoria degli insiemi è stata portata a termine solo nella prima metà del secolo scorso ad opera di molti matematici tra cui Ernst Zermelo (1871–1953), A.A. Frænkel (1891–1965), Johan Von Neumann (1903–1957), Kurt Gödel (1906–1978), Paul Bernays (1888–1977), John L. Kelley (1916–1999) e Antony P. Morse. In particolare, la teoria MK qui esposta è stata sviluppata indipendentemente da Kelley e Morse: una lista di assiomi essenzialmente equivalenti a quelli qui presentati si trova nell'appendice del libro di Kelley di topologia generale [**Kel55**], mentre la monografia di Morse [**Mor65**] presenta (in modo assai idiosincratico)

una trattazione dettagliata della teoria degli insiemi MK. L'esposizione in queste dispense segue abbastanza fedelmente il libro di [**Mon69**]. Un ottimo testo di teoria degli insiemi in cui viene sviluppata ZF è [**Lev02**]. Per una panoramica storica sulla teoria degli insiemi si consiglia [**Lol94**].

2. Insiemi ordinati

2.A. Definizioni. Sia X una classe e sia $R \subseteq X \times X$. Diremo che R è:

- **riflessiva su** X se $\forall x \in X(x\ R\ x)$;
- **irriflessiva su** X se $\neg\exists x \in X(x\ R\ x)$;
- **simmetrica su** X se $\forall x \in X\, \forall y \in X(x\ R\ y \Rightarrow y\ R\ x)$;
- **antisimmetrica su** X se $\forall x \in X\, \forall y \in X\big((x\ R\ y \wedge y\ R\ x) \Rightarrow x = y\big)$;
- **connessa su** X se $\forall x \in X\, \forall y \in X(x = y \vee x\ R\ y \vee y\ R\ x)$;
- **transitiva su** X se $\forall x \in X\, \forall y \in X\, \forall z \in X\big((x\ R\ y \wedge y\ R\ z) \Rightarrow x\ R\ z\big)$;
- **regolare su** X se $\{\, y \in X \mid y\ R\ x \,\}$ è un insieme, per ogni $x \in X$.

Se R è un insieme allora R è regolare, quindi questa nozione è significativa solo quando R è una classe propria. Se R è una relazione su X e $Y \subseteq X$, la restrizione di R ad Y è

$$R \restriction Y = R \cap (Y \times Y)\,.$$

Spesso, se non c'è pericolo di confusione, diremo che R è una relazione su Y. Una **relazione di equivalenza** è una $E \subseteq X \times X$ riflessiva, simmetrica e transitiva. Le relazioni di equivalenza solitamente si denotano con

$$\sim, \quad \approx, \quad \equiv, \quad \cong, \quad \ldots$$

La classe di $\sim$-equivalenza di un elemento $x \in X$ è

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

Se $\sim$ è regolare, allora le classi di equivalenza sono insiemi e possiamo costruire il quoziente[6]

$$X/\!\sim\ = \{\, [x]_\sim \mid x \in X \,\}\,.$$

Esercizio 2.1. Dimostrare che:

(i) se R è una relazione riflessiva su X, allora R è un insieme se e solo se X è un insieme.

(ii) se R è una relazione su X, $Y \subseteq X$ e R è riflessiva (simmetrica, antisimmetrica, transitiva) su X allora anche $R \restriction Y$ è riflessiva (simmetrica, antisimmetrica, transitiva) su Y. In particolare la restrizione di una relazione di equivalenza è ancora di equivalenza.

[6] Una costruzione di X/E, per E non regolare, è data nell'Esercizio 4.27.

(iii) Se $\sim$ è una relazione di equivalenza su un insieme X, allora $X/\sim$ è un insieme.

(iv) La relazione di equipotenza (pag.12) tra insiemi è una relazione di equivalenza su V non regolare.

Un **ordine parziale** o più semplicemente un **ordine su** X è una relazione $R \subseteq X \times X$ riflessiva, antisimmetrica e transitiva su X; se R è anche connessa su X diremo che è un **ordine lineare** o **ordine totale** su X. Un **pre-ordine** o **quasi-ordine** su X una relazione binaria riflessiva e transitiva su X. I pre-ordini sono una generalizzazione degli ordini e delle relazioni d'equivalenza. Gli ordini (parziali o totali) e i pre-ordini vengono usualmente denotati con i simboli

$$\leq, \quad \preccurlyeq, \quad \sqsubseteq, \quad \dots .$$

Dato un pre-ordine $\preccurlyeq$ su X sia $\sim$ la relazione di equivalenza su X indotta dal pre-ordine

$$x \sim y \quad \Leftrightarrow \quad x \preccurlyeq y \wedge y \preccurlyeq x \,.$$

Se $\sim$ è regolare, l'ordine $\leq$ indotto da $\preccurlyeq$ su $X/\sim$ è

$$[x] \leq [y] \quad \Leftrightarrow \quad x \preccurlyeq y \,.$$

Un **ordine stretto**[7] (parziale o totale) su X è una relazione che è la parte irriflessiva di un ordine (parziale o totale) su X, dove la **parte irriflessiva di una relazione** $R \subseteq X \times X$ è definita come

$$R \setminus \{\, (x,y) \mid (x,y) \in R \wedge (y,x) \in R \,\} \,.$$

Un **pre-ordine stretto** è la parte irriflessiva di un pre-ordine Gli ordini stretti (parziali o totali) e i pre-ordini stretti si denotano con

$$<, \quad \prec, \quad \sqsubset, \quad \dots .$$

Chiaramente, ad ogni (pre-)ordine $(\leq, \preccurlyeq, \sqsubseteq, \dots)$ possiamo associare la sua versione stretta $(<, \prec, \sqsubset, \dots)$ e viceversa. Spesso la proprietà di connessione per gli ordini stretti si dice proprietà di **tricotomia** poiché asserisce che deve valere una una delle tre possibilità mutualmente esclusive:

$$x < y, \quad x = y, \quad x > y \,.$$

Se $\leq$ è un pre-ordine, $x \not\leq y$ significa che $x \leq y$ non vale; nel caso degli ordini lineari questo significa che $y < x$, ma ciò non vale in generale per i pre-ordini o gli ordini parziali.

Un **segmento iniziale** di un (pre-)ordine $\leq$ su X è un $Y \subseteq X$ tale che

$$\forall y \in Y \, \forall x \in X \, (x \leq y \Rightarrow x \in Y) \,;$$

[7] La terminologia è un po' infelice, visto che un ordine stretto *non* è un ordine.

analogamente si definisce la nozione di **segmento finale**. Una **catena** in un ordine $\leq$ su X è un $C \subseteq X$ tale che C è linearmente ordinato da $\leq$, vale a dire

$$\forall x, y \in C\,(x \leq y \ \vee \ y \leq x)\,.$$

Se $\leq$ è un ordine su X, un $I \subseteq X$ tale che

$$\forall x, y \in I\,\forall z \in X\,(x \leq z \leq y \Rightarrow z \in I)$$

si dice **intervallo**. Se $x \leq y$ le classi

$$\begin{aligned}(x;y) &= \{\, z \in X \mid x < z < y \,\}\\ [x;y] &= \{\, z \in X \mid x \leq z \leq y \,\}\\ (x;y] &= \{\, z \in X \mid x < z \leq y \,\}\\ [x;y) &= \{\, z \in X \mid x \leq z < y \,\}\end{aligned}$$

sono intervalli e si dicono, rispettivamente intervallo aperto, chiuso, semiaperto inferiormente, semiaperto superiormente determinato da x e y. Se $x < y$ diremo che x è un predecessore di y, ovvero che y è un successore di x. Se $(x;y) = \emptyset$ diremo che x è un **predecessore immediato** di y e che y è un **successore immediato di** di x. (Se $\leq$ è lineare, il predecessore immediato e il successore immediato di un elemento, se esistono, sono unici.) Diremo che $D \subseteq X$ è **denso in** X se $(x;y) \cap D \neq \emptyset$ per ogni $x < y$. Nel caso in cui $D = X$, cioè $(x;y) \neq \emptyset$ diremo che l'ordine è denso. Quando X è un insieme diremo che $\langle X, \leq\rangle$ è un insieme (pre-)ordinato se $\leq$ è un (pre-)ordine su X, e analogamente $\langle X, <\rangle$ è un insieme strettamente ordinato se $<$ è un ordine stretto su X.

Sia $\langle X, \leq\rangle$ un insieme pre-ordinato e sia $Y \subseteq X$. Diremo che $\bar{x} \in X$ è un:

- **maggiorante** di Y se $\forall y \in Y\,(y \leq \bar{x})$;
- **minorante** di Y se $\forall y \in Y\,(\bar{x} \leq y)$;
- **elemento massimale** di Y se $\bar{x} \in Y$ e

  $$\neg\exists y \in Y\,(\bar{x} \leq y \wedge y \not\leq \bar{x})\,,$$

  ovvero $\neg\exists y \in Y\,(\bar{x} < y)$ dove $<$ è la parte stretta di $\leq$. Se $\leq$ è un ordine (invece che un pre-ordine) questa condizione diventa

  $$\neg\exists y \in Y\,(\bar{x} \leq y \wedge \bar{x} \neq y)\,;$$

- **elemento minimale** di Y se $\bar{x} \in Y$ e

  $$\neg\exists y \in Y\,(y \leq \bar{x} \wedge \bar{x} \not\leq y)\,,$$

  ovvero $\neg\exists y \in Y\,(y < \bar{x})$ dove $<$ è la parte stretta di $\leq$. Se $\leq$ è un ordine (invece che un pre-ordine) questa condizione diventa $\neg\exists y \in Y\,(y \leq \bar{x} \wedge \bar{x} \neq y)$;

- **massimo** di Y se è un maggiorante di Y e $\bar{x} \in Y$;
- **minimo** di Y se è un minorante di Y e $\bar{x} \in Y$;
- **estremo superiore** di Y se è un maggiorante di Y e se $\bar{x}$ è un minorante di $\{ x \in X \mid x \text{ è un maggiorante di } Y \}$.
- **estremo inferiore** di Y se è un minorante di Y e se $\bar{x}$ è un maggiorante di $\{ x \in X \mid x \text{ è un minorante di } Y \}$.

Osservazione 2.2. Nel caso degli ordini, la proprietà antisimmetrica implica che se $\bar{x}$ è un massimo o un minimo di Y, allora è unico e viene denotato con $\max Y$, ovvero $\min Y$. Analogamente , poiché l'estremo superiore e l'estremo inferiore di Y, se esistono, sono $\max \{ x \in X \mid x \text{ è un minorante di } Y \}$ e $\min \{ x \in X \mid x \text{ è un maggiorante di } Y \}$, allora sono unici e vengono denotati con $\sup Y$ e $\inf Y$.

Un insieme $Y \subseteq X$ si dice limitato superiormente (inferiormente) se esiste un $\bar{x} \in X$ maggiorante (minorante) di Y. Un pre-ordine $\leq$ su X si dice

- **diretto superiormente** se $\forall x, y \in X \, \exists z \in X \, (x \leq z \wedge y \leq z)$,
- **diretto inferiormente** se $\forall x, y \in X \, \exists z \in X \, (z \leq x \wedge z \leq y)$.

Se richiediamo che $\leq$ sia un ordine (e non solo un pre-ordine) e che $\sup\{x, y\}$ (oppure $\inf\{x, y\}$) esista, per ogni $x, y \in X$ otteniamo la nozione di **semi-reticolo superiore** (rispettivamente: **semi-reticolo inferiore**). Un **reticolo** è un semi-reticolo superiore ed inferiore. Ogni ordine lineare è un reticolo.

Proposizione 2.3. *Sia $\mathcal{F}$ una classe di funzioni e supponiamo $\subseteq$ sia diretto superiormente su $\mathcal{F}$. Allora $\bigcup \mathcal{F}$ è una relazione funzionale.*

Dimostrazione. $\bigcup \mathcal{F}$ è una classe di coppie ordinate. Supponiamo $(x, y) \in \bigcup \mathcal{F}$ e $(x, z) \in \bigcup \mathcal{F}$ e quindi $(x, y) \in f$ e $(x, z) \in g$, per qualche $f, g \in \mathcal{F}$. Sia $h \in \mathcal{F}$ tale che $f, g \subseteq h$: allora $(x, y), (x, z) \in h$ e quindi $y = z$. □

2.B. Esempi di ordini. Vediamo qualche esempio di ordine parziale. Useremo liberamente concetti (*finito*, *numerabile*, etc) ed enti ($\mathbb{Q}$, $\mathbb{R}$, etc.) che saranno introdotti ufficialmente solo tra qualche pagina, ma che sono (o dovrebbero essere) ben noti. Il lettore più scettico può saltare per il momento questa sezione e ritornarci una volta che questi fatti sono stati sviluppati in modo formale.

2.B.1. *L'insieme potenza.* Se A è un insieme, allora $\langle \mathscr{P}(A), \subseteq \rangle$ è un insieme ordinato; è totalmente ordinato se e solo se A è un singoletto o $A = \emptyset$. Se $b \in B \subseteq A$ allora $B \setminus \{b\}$ è un predecessore immediato di B e se $a \in A \setminus B$ allora $B \cup \{a\}$ è un successore immediato di B. Ogni sottoinsieme

$\mathcal{A}$ di $\mathscr{P}(A)$ ammette un estremo superiore $\bigcup\mathcal{A}$ e un estremo inferiore $\bigcap\mathcal{A}$ e quindi $\langle\mathscr{P}(A),\subseteq\rangle$ è un reticolo. Il massimo e il minimo di $\mathscr{P}(A)$ sono, rispettivamente A e $\emptyset$.

2.B.2. *I razionali ed i reali.* $\mathbb{R}$ e $\mathbb{Q}$ con l'usuale ordinamento sono linearmente ordinati e densi in sé stessi. Non hanno né massimo né minimo. Tuttavia ogni sottoinsieme superiormente (inferiormente) limitato di $\mathbb{R}$ ha un estremo superiore (inferiore). L'analoga affermazione in $\mathbb{Q}$ è falsa.

2.B.3. *Gli intorni di un punto.* Sia $\mathcal{U}(\bar{x})$ l'insieme degli intorni di un punto fissato $\bar{x}\in\mathbb{R}$, ordinato da $\subseteq$. $\langle\mathcal{U}(\bar{x}),\subseteq\rangle$ è un ordine non totale e un reticolo. Come nell'Esempio 2.B.1, ogni elemento di $\mathcal{U}(\bar{x})$ ha un predecessore e, se diverso da $\mathbb{R}$, un successore. Ogni sottoinsieme di $\mathcal{U}(\bar{x})$ ha un estremo superiore, ma, in generale, non ha estremo inferiore; in particolare $\mathcal{U}(\bar{x})$ non ha minimo, ma ha massimo: $\mathbb{R}$.

2.B.4. *Dominazione di funzioni.* Se $f,g\in\mathbb{N}^{\mathbb{N}}$ poniamo

$$f\leq^* g\Leftrightarrow\exists k\,\forall m\geq k\,(f(m)\leq g(m))\,.$$

e diciamo che g **domina** f **quasi ovunque**. $\leq^*$ è un pre-ordine (ma non un ordine) su $\mathbb{N}^{\mathbb{N}}$ la cui relazione d'equivalenza associata è

$$f=^* g\Leftrightarrow\exists k\,\forall m\geq k\;f(m)=g(m)\,.$$

L'ordine $\leq$ sul quoziente $\mathbb{N}^{\mathbb{N}}/=^*$ non è totale, ma non ha massimo. Per ogni $f,g\in\mathbb{N}^{\mathbb{N}}$ le funzioni

$$\begin{aligned} f\wedge g\colon&\quad n\mapsto\min\{f(n),g(n)\}\\ f\vee g\colon&\quad n\mapsto\max\{f(n),g(n)\}\end{aligned}$$

sono tali che $[f\wedge g]=\inf\{[f],[g]\}$ e $[f\vee g]=\sup\{[f],[g]\}$. Quindi

$$\langle\mathbb{N}^{\mathbb{N}}/=^*,\leq\rangle$$

è un reticolo. Ogni famiglia numerabile di elementi di $\mathbb{N}^{\mathbb{N}}$ ha un maggiorante e un minorante, ma non ha necessariamente un sup o un inf (Esercizio 2.9).

2.B.5. *Inclusione a meno di insiemi finiti.* La relazione $\subseteq^*$ su $\mathscr{P}(\mathbb{N})$

$$A\subseteq^* B\Leftrightarrow A\setminus B\text{ è finito}$$

è un pre-ordine la cui relazione di equivalenza associata è

$$A=^* B\Leftrightarrow A\triangle B\text{ è finito.}$$

$A\subset^* B$ significa che $A\subseteq^* B$ e $B\not\subseteq^* A$, vale a dire $A\subseteq^* B$ e $B\neq^* A$. L'ordine parziale $\leq$ indotto sul quoziente

$$\mathcal{P}\stackrel{\text{def}}{=}(\mathscr{P}(\mathbb{N})/=^*)$$

è un reticolo, ponendo $\sup\{[A],[B]\}=[A\cup B]$ e $\inf\{[A],[B]\}=[A\cap B]$ (Esercizio 2.10).

Se $[A] < [B]$, cioè $A \subset^* B$, allora $B \setminus A$ è un insieme infinito $\{k_0 < k_1 < \dots\}$ e quindi $[A] < [C] < [B]$ dove $C = A \cup \{ k_{2i} \mid i \in \mathbb{N} \}$. Ne segue che $\langle \mathcal{P}, \leq \rangle$ è denso in sé stesso. Se consideriamo il sottoinsieme $\mathcal{P} \setminus \{[\emptyset], [\mathbb{N}]\}$, otteniamo un ordine denso in sé stesso, privo di elementi massimali o minimali.

Proposizione 2.4. *Se $A_0 \subset^* A_1 \subset^* A_2 \subset^* \dots$ è una catena $\subset^*$-crescente allora c'è un $B \neq^* \mathbb{N}$ tale che*

$$\forall n \in \mathbb{N}\, (A_n \subset^* B)$$

In altre parole: ogni successione $<$-crescente in $\mathcal{P}$ ha un maggiorante.

Dimostrazione. Innanzi tutto possiamo supporre che $A_0 \neq \emptyset$ altrimenti basta rimpiazzare A_0 con $\{0\}$: l'ipotesi continua a valere e ogni C che sia un $\subseteq^*$-maggiorante di $\{0\}, A_1, A_2, \dots$ è anche un $\subseteq^*$-maggiorante di $A_0, A_1, A_2, \dots$. Poiché $A_n \cup A_{n-1} \cup \dots \cup A_0 = A_n \cup (A_{n-1} \setminus A_n) \cup (A_{n-2} \setminus A_{n-1}) \cup \dots \cup (A_0 \setminus A_0)$

$$\begin{aligned} B_{n+1} &= A_{n+1} \setminus (A_n \cup A_{n-1} \cup \dots \cup A_0) \\ &= A_{n+1} \setminus (A_n \cup (A_{n-1} \setminus A_n) \cup (A_{n-2} \setminus A_{n-1}) \cup \dots \cup (A_0 \setminus A_1)) \\ &= (A_{n+1} \setminus A_n) \setminus ((A_{n-1} \setminus A_n) \cup (A_{n-2} \setminus A_{n-1}) \cup \dots \cup (A_0 \setminus A_1)) \end{aligned}$$

è infinito in quanto differenza tra un insieme infinito $A_{n+1} \setminus A_n$ ed un'unione finita di insiemi finiti: $A_{n-1} \setminus A_n$, $A_{n-2} \setminus A_{n-1}$,… $A_0 \setminus A_1$. Definiamo induttivamente $k_0 \in A_0$ e $k_{n+1} \in B_{n+1}$ in modo che che i k_i siano tutti distinti. Poiché $k_m \notin A_i$ se $i \leq m$, ne segue che $A_n \cap \{ k_m \mid m \in \mathbb{N} \} \subseteq \{k_0, \dots, k_n\}$ e quindi

$$A_n \subseteq^* C \stackrel{\text{def}}{=} \mathbb{N} \setminus \{ k_m \mid m \in \mathbb{N} \}\,.$$

Quindi C è un maggiorante di $\{ A_n \mid n \in \mathbb{N} \}$ e $C \subset^* \mathbb{N}$ dato che $\mathbb{N} \setminus C = \{ k_m \mid m \in \mathbb{N} \}$ è infinito. □

Ogni suo sottoinsieme numerabile ha un maggiorante e un minorante, ma non ha necessariamente un massimo o un minimo (Esercizio 2.11).

2.C. Un teorema di punto fisso. Se $R \subseteq X \times X$ e $S \subseteq Y \times Y$, un **morfismo** $f\colon \langle X, R\rangle \to \langle Y, S\rangle$ è una funzione $f\colon X \to Y$ tale che

$$\forall x_1, x_2 \in X\, (x_1\, R\, x_2 \Rightarrow f(x_1)\, S\, f(x_2))\,.$$

Se inoltre f è una bijezione tra X e Y e $f^{-1}\colon \langle Y, S\rangle \to \langle X, R\rangle$ è un morfismo, diremo che f è un **isomorfismo**. Nel caso di pre-ordini, un morfismo $f\colon \langle X, \leq\rangle \to \langle Y, \preccurlyeq\rangle$ si dice funzione **(debolmente) crescente**; se è anche un morfismo per i pre-ordini stretti associati $\langle X, <\rangle \to \langle Y, \prec\rangle$ allora f si dice **strettamente crescente**.

Teorema 2.5. *Sia $\langle X, \leq \rangle$ un insieme ordinato tale che ogni $Y \subseteq X$ ha un estremo superiore. Se $f\colon X \to X$ è crescente esiste un punto fisso per f, vale a dire*

$$\exists a \in X\, (f(a) = a)\,.$$

Dimostrazione. Sia $A = \{\, x \in X \mid x \leq f(x) \,\}$ e sia $a = \sup A$. Se $x \in A$, allora $x \leq a$ e $x \leq f(x)$ da cui

$$x \leq f(x) \leq f(a)\,.$$

Quindi $f(a)$ è un maggiorante di A. Da questo segue che $a \leq f(a)$ e quindi $f(a) \leq f(f(a))$, per la crescenza di f. Ne segue che $f(a) \in A$, da cui $f(a) \leq a$. Quindi $a = f(a)$. □

Mediante questo risultato di punto fisso possiamo dimostrare il seguente importante risultato:

Teorema 2.6 (Shröder-Bernstein)**.** *Se $F\colon A \to B$ e $G\colon B \to A$ sono iniettive allora $\exists H\, (H\colon A \to B$ bijettiva$)$.*

Dimostrazione. L'insieme ordinato $\langle \mathscr{P}(A), \subseteq \rangle$ e la funzione $\Phi\colon \mathscr{P}(A) \to \mathscr{P}(A)$

$$\Phi(C) = A \setminus G[B \setminus F[C]]$$

soddisfano le ipotesi del Teorema 2.5, quindi esiste un $C \subseteq A$ tale che $\Phi(C) = C$, ovvero $A \setminus C = G[B \setminus F[C]]$ e quindi

$$G^{-1} \restriction (A \setminus C)\colon A \setminus C \to B \setminus F[C]$$
$$F \restriction C\colon C \to F[C]$$

sono bijezioni. Quindi $H = G^{-1} \restriction (A \setminus C) \cup F \restriction C$ è la bijezione cercata. □

Esercizi

Esercizio 2.7. Siano $\langle X, \leq\rangle$ e $\langle Y, \preccurlyeq\rangle$ insiemi ordinati e $f\colon X \to Y$ crescente. Dimostrare che se $\langle X, \leq\rangle$ è lineare,

$$\forall x_1, x_2 \in X\, (f(x_1) \prec f(x_2) \Rightarrow x_1 < x_2)\,.$$

In particolare, se $\langle X, \leq\rangle$ è lineare e f è strettamente crescente

$$\forall x_1, x_2 \in X\, (x_1 \leq x_2 \Leftrightarrow f(x_1) \preccurlyeq f(x_2))\,.$$

Mostrare con un controesempio che l'ipotesi "$\langle X, \leq\rangle$ è lineare" non può essere rimossa.

Esercizio 2.8. Se $\langle X, \leq\rangle$ e $\langle Y, \preccurlyeq\rangle$ sono insiemi ordinati, possiamo definire due ordini su $X \times Y$, l'ordine prodotto $\trianglelefteq$ e l'ordine lessicografico $\leq_{\text{lex}}$:

$$(x_1, y_1) \trianglelefteq (x_2, y_2) \Leftrightarrow (x_1 \leq x_2 \wedge y_1 \preccurlyeq y_2)$$
$$(x_1, y_1) \leq_{\text{lex}} (x_2, y_2) \Leftrightarrow (x_1 < x_2 \vee (x_1 = x_2 \wedge y_1 \preccurlyeq y_2))\,.$$

Quali delle proprietà viste (essere un reticolo, avere massimi, minimi, etc.) si preservano passando agli ordini prodotto e lessicografico?

Esercizio 2.9. Dimostrare che per ogni successione di funzioni $f_n \in \mathbb{N}^{\mathbb{N}}$ esiste $g \in \mathbb{N}^{\mathbb{N}}$ tale che $f_n \leq^* g$, per ogni $n \in \mathbb{N}$. Dare un esempio di sottoinsieme numerabile di $\mathbb{N}^{\mathbb{N}}/=^*$ che non ha estremo superiore e uno che non ha estremo inferiore.

Esercizio 2.10. Verificare che $\langle \mathcal{P}, \leq\rangle$ dell'Esempio 2.B.5 è un reticolo.

Esercizio 2.11. Siano $A_n, B_n \subseteq \mathbb{N}$ tali che

$$n < m \quad \Rightarrow \quad A_n \subset^* A_m \subset^* B_m \subset^* B_n$$

dove $\subseteq^*$ e $\subset^*$ sono come nell'Esempio 2.B.5. Dimostrare che c'è un $C \subseteq \mathbb{N}$ tale che

$$\forall n \in \mathbb{N}\, (A_n \subseteq^* C \subseteq^* B_n)\,.$$

Esercizio 2.12. Dimostrare che esiste un $\mathcal{C} \subseteq \mathscr{P}(\mathbb{N})$ tale che $\langle \mathcal{C}, \subseteq\rangle$ è isomorfo ad $\langle \mathbb{R}, <\rangle$. (Suggerimento: $\mathbb{N}$ è in bijezione con $\mathbb{Q}$.)

3. Ordinali

Definizione 3.1. Sia X una classe e $R \subseteq X \times X$ una relazione irriflessiva su X. Diremo che R è **ben-fondata** se ogni sotto-classe non-vuota di X contiene un elemento R-minimale cioè

$$\forall Y \subseteq X\, (Y \neq \emptyset \Rightarrow \exists y \in Y\, \forall z \in Y\, (z \neq y \Rightarrow (z, y) \notin R))\,.$$

Se R non è ben fondata su X diremo che è **mal-fondata**.

L'Assioma della Fondazione implica che la relazione di appartenenza

$$\{\,(x,y) \in \mathrm{V} \mid x \in y\,\}$$

è irriflessiva e ben-fondata e poiché $\{\,y \mid y \in x\,\} = x$ è un insieme per ogni $x \in \mathrm{V}$, è anche regolare.

Definizione 3.2. Un **buon ordine** è un ordine lineare stretto, ben-fondato e regolare. Con abuso di linguaggio diremo che un ordine $\leq$ è un buon ordine se lo è il suo ordine stretto associato $<$.

Esercizio 3.3. (i) Dimostrare che se $<$ è un buon ordine su X e $Y \subseteq X$, allora lo è anche l'ordine indotto $< \restriction Y$ su Y. Quando non c'è pericolo di confusione l'ordine indotto viene indicato con $<$.

(ii) Siano $<$ e $\prec$ buoni ordini su X e Y, rispettivamente, e siano $\lhd$ e $<_{\mathrm{lex}}$ l'ordinamento prodotto stretto e l'ordinamento lessicografico stretto su $X \times Y$ (cioè gli ordini stretti associati agli ordini $\trianglelefteq$ e $\leq_{\mathrm{lex}}$). Allora $<_{\mathrm{lex}}$ è un buon ordine su $X \times Y$ e $\lhd$ è una relazione ben fondata su $X \times Y$. Sotto quali ipotesi $\lhd$ è un buon-ordine?

Gli ordinali sono esempi canonici di buoni ordini.

Definizione 3.4. Una classe A si dice **transitiva** se $\bigcup A \subseteq A$, cioè se

$$\forall a\, \forall x\, ((a \in A \wedge x \in a) \Rightarrow x \in A)\,.$$

Un **ordinale** è un insieme transitivo tale che tutti i suoi elementi sono transitivi. Gli ordinali vengono generalmente denotati con lettere greche minuscole α, β, ... e Ord è la classe degli ordinali.

Esercizio 3.5. (i) Il singoletto $\{x\}$ è transitivo se e solo se $x = \emptyset$. Nessuna coppia ordinata (x, y) è un insieme transitivo.

(ii) La classe V è transitiva, mentre la classe $\{\,\{x\} \mid x \in \mathrm{V}\,\}$ non lo è.

(iii) Se x è transitivo, anche $\mathbf{S}(x)$ è transitivo. Se α è un ordinale, anche $\mathbf{S}(\alpha)$ è un ordinale.

(iv) Se x è transitivo, anche $\bigcup x$ è transitivo.

(v) Se α è un ordinale, allora ogni $\beta \in \alpha$ è un ordinale.

(vi) Se x è un insieme di ordinali, allora $\bigcup x$ è un ordinale.

(vii) $\alpha \in \beta \Leftrightarrow \mathbf{S}(\alpha) \in \mathbf{S}(\beta)$.

Proposizione 3.6. Ord *è una classe propria.*

Dimostrazione. Se $\alpha \in$ Ord e $\beta \in \alpha$, allora $\beta \in$ Ord per la parte (v) dell'Esercizio 3.5. Quindi Ord è una classe transitiva. Se Ord fosse un insieme, allora sarebbe un ordinale e quindi Ord $\in$ Ord, contraddicendo l'Assioma di Fondazione. $\square$

Teorema 3.7. *Se* $\alpha, \beta \in \mathrm{Ord}$

$$\alpha \in \beta \quad \vee \quad \alpha = \beta \quad \vee \quad \beta \in \alpha\,.$$

Dimostrazione. Dobbiamo dimostrare che

$$A = \{\, \alpha \in \mathrm{Ord} \mid \exists \beta \in \mathrm{Ord}\,(\alpha \notin \beta \ \wedge\ \alpha \neq \beta \ \wedge\ \beta \notin \alpha)\,\}$$

è vuota. Se $A \neq \emptyset$, allora per l'Assioma di Fondazione esiste $\bar{\alpha} \in A$ tale che

$$\bar{\alpha} \cap A = \emptyset\,. \tag{17}$$

Allora

$$B = \{\, \beta \in \mathrm{Ord} \mid \beta \notin \bar{\alpha} \ \wedge\ \beta \neq \bar{\alpha} \ \wedge\ \bar{\alpha} \notin \beta\,\}$$

è una classe non vuota e di nuovo per l'Assioma di Fondazione esiste $\bar{\beta} \in B$ tale che $\bar{\beta} \cap B = \emptyset$. Se $\gamma \in \bar{\alpha}$ allora, per la (17), $\gamma \notin A$, quindi, in particolare

$$\bar{\beta} \in \gamma \quad \vee \quad \bar{\beta} = \gamma \quad \vee \quad \gamma \in \bar{\beta}\,.$$

Le prime due possibilità e la transitività di $\bar{\alpha}$ implicano $\bar{\beta} \in \bar{\alpha}$, contraddicendo il fatto che $\bar{\beta} \in B$. Quindi $\gamma \in \bar{\beta}$. Essendo γ arbitrario, otteniamo $\bar{\alpha} \subseteq \bar{\beta}$. Analogamente $\bar{\beta} \subseteq \bar{\alpha}$ e quindi $\bar{\alpha} = \bar{\beta}$: contraddizione. □

Corollario 3.8. $\in$ *è un buon ordine stretto su* Ord *e quindi su ogni ordinale* α.

Per questo motivo scriveremo

$$\alpha < \beta \quad \text{e} \quad \alpha \leq \beta$$

al posto di $\alpha \in \beta$ e $(\alpha \in \beta \vee \alpha = \beta)$, rispettivamente. Quindi, se $\emptyset \neq A \subseteq \mathrm{Ord}$, l'elemento $<$-minimale di A è il minimo di A.

Proposizione 3.9. *Se* $A \neq \emptyset$ *è una classe non vuota di ordinali, allora* $\min A = \bigcap A$.

Dimostrazione. Supponiamo $\emptyset \neq A \subseteq \mathrm{Ord}$ e sia $\bar{\alpha} \in A$ tale che $\bar{\alpha} \cap A = \emptyset$. È immediato verificare che $\forall \alpha \in A\,(\bar{\alpha} \subseteq \alpha)$, quindi $\bigcap A = \bar{\alpha} = \min A$. □

Come caso particolare del Teorema 1.15 otteniamo

Corollario 3.10. *Non esiste nessuna catena discendente di ordinali, vale a dire*

$$\neg \exists f\,(f \colon \mathbb{N} \to \mathrm{Ord} \wedge \forall n (f(\mathbf{S}(n)) < f(n)))\,.$$

Lemma 3.11. (a) *Ogni numero naturale è un ordinale.*

(b) *Se* $n \in \mathbb{N}$ *e* $x \in n$ *allora* $x \in \mathbb{N}$.

Dimostrazione. (a) Per assurdo, supponiamo $X = \mathbb{N} \setminus \mathrm{Ord}$ sia non vuoto e sia $n \in X$ tale che $n \cap X = \emptyset$. Poiché 0 è un ordinale, ne segue $n > 0$ e quindi, per la Proposizione 1.9, $n = \mathbf{S}(m)$ per qualche $m \in \mathbb{N}$. Allora $m \in \mathrm{Ord}$ e quindi $\mathbf{S}(m) \in \mathrm{Ord} \cap \mathbb{N}$: una contraddizione.

(b) Per assurdo supponiamo che $X = \{\, n \in \mathbb{N} \mid \exists x \in n\,(x \notin \mathbb{N}) \,\}$ sia non vuoto e sia $\bar{n} \in X$ tale che $\bar{n} \cap X = \emptyset$. Fissiamo $\bar{x} \in \bar{n}$ tale che $\bar{x} \in \bar{n} \setminus \mathbb{N}$. Per la Proposizione 1.9 $\bar{n} = \mathbf{S}(\bar{m})$, per qualche $\bar{m} \in \mathbb{N}$, quindi $\bar{x} \in \bar{m}$ o $\bar{x} = \bar{m}$. È immediato verificare che entrambe le possibilità portano ad un assurdo. □

Un ordinale α è **successore** se $\alpha = \mathbf{S}(\beta)$, per qualche β. Chiaramente $\alpha < \mathbf{S}(\alpha)$ e per il Esercizio 1.24, non esiste alcun β tale che $\alpha < \beta < \mathbf{S}(\alpha)$. In altre parole $\mathbf{S}(\alpha)$ è il successore di α nell'ordinamento dato da $\in$. Se un ordinale non è successore e non è 0, allora si dice **limite**.

Teorema 3.12. *$\mathbb{N}$ è il più piccolo ordinale limite.*

Dimostrazione. $\mathbb{N}$ è un ordinale per il Lemma 3.11 e per la Proposizione 1.9 non esistono ordinali limite minori di $\mathbb{N}$. Basta quindi verificare che $\mathbb{N}$ non è successore. Se, per assurdo, $\mathbb{N} = \mathbf{S}(\alpha)$, allora $\alpha \in \mathbb{N}$, da cui $\mathbf{S}(\alpha) \in \mathbb{N}$, cioè $\mathbb{N} \in \mathbb{N}$: contraddizione. □

In teoria degli insiemi si è soliti denotare l'ordinale $\mathbb{N}$ con

$$\omega\,.$$

Proposizione 3.13. (a) $\alpha < \beta \Leftrightarrow \alpha \subset \beta$;

(b) $\alpha \leq \beta \Leftrightarrow \alpha \subseteq \beta$;

(c) $\alpha < \beta \Leftrightarrow \mathbf{S}(\alpha) \leq \beta$;

(d) $x \subseteq \alpha \Rightarrow (\bigcup x = \alpha \ \vee \ \bigcup x < \alpha)$;

(e) $\bigcup(\mathbf{S}(\alpha)) = \alpha$;

(f) $\alpha = \mathbf{S}(\bigcup \alpha) \ \vee \ \alpha = \bigcup \alpha$;

(g) $\bigcup \alpha = \alpha \Leftrightarrow (\alpha = 0 \ \vee \ \alpha$ *limite*$) \Leftrightarrow \langle \alpha, < \rangle$ *non ha massimo.*

Dimostrazione. (a) Se $\alpha \in \beta$ allora $\alpha \subseteq \beta$ per transitività. L'Assioma di Fondazione implica $\alpha \neq \beta$, quindi $\alpha \subset \beta$. Vice versa supponiamo $\alpha \subset \beta$: l'Assioma di Fondazione implica $\beta \notin \alpha$ e poiché $\beta \neq \alpha$ segue che $\alpha \in \beta$.

(b) è analogo ad (a).

(c) Sia $\alpha < \beta$. Poiché $\beta \in \mathbf{S}(\alpha)$ è impossibile, segue che $\beta = \mathbf{S}(\alpha)$ o $\mathbf{S}(\alpha) \in \beta$. L'implicazione inversa è immediata.

(d) $\bigcup x$ è un ordinale per l'Esercizio 3.5 quindi è confrontabile con α. Ma $\alpha \in \bigcup x$ implica che $\alpha \in \beta \in x \subseteq \alpha$, per qualche β: una contraddizione. Quindi $\bigcup x \leq \alpha$.

(e) $\beta \in \bigcup \mathbf{S}(\alpha)$ se e solo se $\beta \in \gamma \in \alpha$ per qualche γ oppure $\beta \in \alpha$. Quindi $\beta \in \bigcup \mathbf{S}(\alpha) \Leftrightarrow \beta \in \alpha$.

(f) Da (e) otteniamo $\bigcup \alpha \leq \alpha$. Se $\bigcup \alpha < \alpha$, allora per (c) $\mathbf{S}(\bigcup \alpha) \leq \alpha$, quindi è sufficiente dimostrare che non vale la disuguaglianza stretta: se $\mathbf{S}(\bigcup \alpha) \in \alpha$ allora $\bigcup \alpha \in \mathbf{S}(\bigcup \alpha)$ implica che $\bigcup \alpha \in \bigcup \alpha$: contraddizione.

(g) segue da (e) e (f). □

Proposizione 3.14. *Se A è un insieme di ordinali, allora $\bigcup A = \sup A$, il più piccolo ordinale che maggiora tutti gli elementi di A.*

Dimostrazione. Sia A sia un insieme di ordinali. L'insieme $\bigcup A$ è il più piccolo insieme contenete ogni $\alpha \in A$ e dato che $\bigcup A$ è un ordinale (Esercizio 3.5) e che l'inclusione coincide con $\leq$ sugli ordinali (Proposizione 3.13), ne segue che $\bigcup A = \sup A$. □

Esercizio 3.15. (i) Sia A un ordinale o $A = \mathrm{Ord}$. Supponiamo che $I \subseteq A$ sia tale per cui

$$\big(\forall \beta \in A\,(\beta < \alpha \Rightarrow \beta \in I)\big) \Rightarrow \alpha \in I\,,$$

per ogni $\alpha \in A$. Allora $I = A$.

In particolare (Principio di Induzione su $\mathbb{N}$ —seconda formulazione) se $I \subseteq \mathbb{N}$ è tale che per ogni $n \in \mathbb{N}$,

$$\big(\forall m \in \mathbb{N}\,(m < n \Rightarrow m \in I)\big) \Rightarrow n \in I\,,$$

allora $I = \mathbb{N}$.

(ii) Sia A un ordinale o $A = \mathrm{Ord}$. Supponiamo che $I \subseteq A$ sia tale per cui
- $0 \in I$,
- $\forall \alpha \in A\big(\exists \beta(\alpha = \mathbf{S}(\beta) \ \wedge \ \beta \in I) \Rightarrow \alpha \in I\big)$,
- $\forall \alpha \in A\big((\alpha \text{ limite e } \forall \beta < \alpha \ \beta \in I) \Rightarrow \alpha \in I\big)$.

Allora $I = A$.

Proposizione 3.16. (a) *Sia $f\colon \alpha \to \beta$ strettamente crescente. Allora*

$$\forall \gamma \in \alpha\,(\gamma \leq f(\gamma)) \tag{18}$$

e $\alpha \leq \beta$.

(b) *Se $f\colon \alpha \to \beta$ è un isomorfismo, allora $\alpha = \beta$ e f è l'identità.*

Dimostrazione. (a) Supponiamo, per assurdo, che

$$A = \{\, \gamma \in \alpha \mid f(\gamma) \in \gamma \,\} \neq \emptyset$$

e sia $\bar\gamma = \min(A)$. Poiché $f(\bar\gamma) \notin A$, $f(\bar\gamma) \leq f(f(\bar\gamma))$ da cui $\bar\gamma \leq f(\bar\gamma)$: contraddizione. Questo prova la (18).

Se, per assurdo, $\beta \in \alpha$ allora $f(\beta) \in \beta$, contraddicendo quanto appena dimostrato, quindi $\alpha \leq \beta$

(b) Per la parte (a) $\alpha \leq \beta$ e poiché anche $f^{-1}\colon \beta \to \alpha$ è crescente, $\beta \leq \alpha$, da cui $\alpha = \beta$. Usando la (18) con f e f^{-1} otteniamo $\gamma \leq f(\gamma)$ e $\gamma \leq f^{-1}(\gamma)$, cioè f è l'identità. □

In modo del tutto analogo si dimostra che se $f\colon \mathrm{Ord} \to \mathrm{Ord}$ è strettamente crescente allora $\gamma \leq f(\gamma)$ e se f è anche suriettiva allora è l'identità.

3.A. Cardinali. Un insieme di dice **finito** se è in bijezione con un numero naturale, altrimenti si dice **infinito**. Se un insieme è finito, allora è in bijezione con un unico $n \in \mathbb{N}$, come discende dalla parte (a) del seguente risultato, noto come *principio dei cassetti* o *principio di Dirichlet*: se riponiamo n oggetti in m cassetti e $m < n$, allora uno dei cassetti dovrà contenere almeno due oggetti.

Teorema 3.17. (a) *Se $n, m \in \mathbb{N}$ ed esiste $f\colon n \rightarrowtail m$, allora $n \leq m$. In particolare: se n e m sono in bijezione, allora $n = m$.*

(b) *$\mathbb{N}$ è infinito.*

Dimostrazione. (a) Per induzione su $n \in \mathbb{N}$. Se $n = 0$ è banale, quindi possiamo supporre $n = \mathbf{S}(n')$ e $f\colon n \rightarrowtail m$. Chiaramente $m > 0$, cioè $m = \mathbf{S}(m')$. Sia $g\colon m \to m$ la bijezione che scambia $f(n')$ con m' e lascia invariato il resto. Allora $(g \circ f) \restriction n'\colon n' \rightarrowtail m'$ e quindi, per ipotesi induttiva, $n' \leq m'$. La parte (vii) dell'Esercizio 3.5 implica che $n \leq m$.

(b) Se $\mathbb{N}$ fosse in bijezione con $n \in \mathbb{N}$, da $\mathbf{S}(n) \rightarrowtail \mathbb{N}$ e $\mathbb{N} \rightarrowtail n$, otterremmo $\mathbf{S}(n) \rightarrowtail n$ contraddicendo la parte (a). □

Osservazione 3.18. Se $f\colon n \to X$ è una bijezione e $n > 0$, allora possiamo elencare gli elementi di X mediante f

$$X = \{x_0, \ldots, x_{n-1}\}$$

dove $x_i = f(i)$. Quando diciamo "Consideriamo un insieme finito $X = \{x_0, \ldots, x_{n-1}\}$ ...", stiamo in realtà dando una bijezione tra il numero naturale n e l'insieme X.

Esercizio 3.19. Dimostrare che se X è finito e $Y \subseteq X$ allora Y è finito.

Definizione 3.20. Un **cardinale** è un ordinale κ che non è in bijezione con nessun ordinale $\alpha < \kappa$. I cardinali sono generalmente denotati con lettere greche quali κ, λ, ... e Card è la classe dei cardinali. Per ogni $\alpha \in \mathrm{Ord}$, la **cardinalità** di α, in simboli $|\alpha|$, è il più piccolo ordinale β in bijezione con α.

Chiaramente $|\alpha| \leq \alpha$. Il Teorema 3.17 implica che ogni numero naturale è un cardinale e che ω è il primo cardinale infinito. Invece $\mathbf{S}(\omega)$, $\mathbf{S}(\mathbf{S}(\omega))$, $\mathbf{S}(\mathbf{S}(\mathbf{S}(\omega)))$,... non sono cardinali—Proposizione 3.22.

Proposizione 3.21. *Se κ e λ sono cardinali,*

(a) *$\kappa = \lambda$ se e solo se κ e λ sono in bijezione,*

(b) *$\kappa \leq \lambda$ se e solo se c'è una funzione iniettiva $f\colon \kappa \to \lambda$.*

Dimostrazione. (a) Supponiamo che κ e λ siano in bijezione e che $\kappa \neq \lambda$, per esempio $\kappa < \lambda$. Allora λ sarebbe in bijezione con un ordinale più piccolo: contraddizione.

(b) Supponiamo $f\colon \kappa \to \lambda$ sia iniettiva. Se, per assurdo, $\lambda < \kappa$, allora sia $j\colon \lambda \to \kappa$ la funzione identica. Per il Teorema di Shröder-Bernstein 2.6 κ e λ sono in bijezione, quindi $\kappa = \lambda$ per (a): contraddizione. □

Proposizione 3.22. (a) *Se $\alpha \geq \omega$ allora $|\alpha| = |\mathbf{S}(\alpha)|$,*

(b) *$|\alpha| \leq \beta \leq \alpha \Rightarrow |\alpha| = |\beta|$,*

(c) *$|\alpha| = |\beta|$ se e solo se α e β sono in bijezione,*

(d) *$|\alpha| \leq |\beta|$ se e solo se esiste $f\colon \alpha \to \beta$ iniettiva.*

Dimostrazione. (a) $f\colon \mathbf{S}(\alpha) \to \alpha$

$$f(\beta) = \begin{cases} \mathbf{S}(\beta) & \text{se } \beta < \omega, \\ \beta & \text{se } \omega \leq \beta < \alpha, \\ 0 & \text{se } \beta = \alpha, \end{cases}$$

è una bijezione.

(b) Sia $f\colon \alpha \to |\alpha|$ una bijezione. Poiché $f\colon \alpha \to \beta$ è iniettiva e β si inietta in α, $|\alpha| = |\beta|$ per il Teorema di Shröder-Bernstein 2.6 e la Proposizione 3.21.

(c) e (d) discendono dalla Proposizione 3.21. □

Gli unici esempi di cardinali visti fin'ora sono i numeri naturali e ω. Sorge quindi spontanea la domanda: esistono cardinali più che numerabili? Sia $\alpha \geq \omega$ e sia

$$B = \{\, (\beta, f) \mid \beta \in \mathrm{Ord} \text{ e } f\colon \beta \to \alpha \text{ è una bijezione} \,\}.$$

Ad ogni $(\beta, f) \in B$ associamo il buon ordine $W_{(\beta,f)}$ su α indotto dalla bijezione f:

$$\nu \; W_{(\beta,f)} \; \xi \quad \Leftrightarrow \quad f^{-1}(\nu) < f^{-1}(\xi)\,.$$

Quindi $f : \langle \beta, < \rangle \to \langle \alpha, W_{(\beta,f)} \rangle$ è un isomorfismo. Se $(\beta, f), (\gamma, g) \in B$ e $W_{(\beta,f)} = W_{(\gamma,g)}$ allora $g^{-1} \circ f\colon \langle \beta, < \rangle \to \langle \gamma, < \rangle$ è un isomorfismo e quindi $\beta = \gamma$ e $f = g$ per la Proposizione 3.16. In altre parole: la funzione

$$B \to \mathscr{P}(\alpha \times \alpha) \qquad (\beta, f) \mapsto W_{(\beta,f)}$$

è iniettiva e quindi per gli assiomi del rimpiazzamento e dell'insieme potenza B è un insieme. Quindi la sua proiezione sulla prima coordinata

$$A = \{\, \beta \in \mathrm{Ord} \mid \beta \text{ è in bijezione con } \alpha \,\}$$

è un insieme. Sia

$$\alpha^+ \stackrel{\text{def}}{=} \bigcup A\,.$$

Per la parte (a) della Proposizione 3.22, l'insieme A è chiuso sotto l'operazione **S** di successore per cui non ha un massimo, cioè $\alpha^+ \notin A$. Inoltre se $|\alpha^+| < \alpha^+$, sia $\beta \in A$ tale che e $|\alpha^+| \leq \beta < \alpha^+$: allora $|\alpha| = |\beta| = |\alpha^+|$ e quindi $\alpha^+ \in A$: una contraddizione. Questo implica che α^+ è un cardinale. Abbiamo quindi dimostrato il seguente

Teorema 3.23. *Se $\alpha \geq \omega$ allora*

$$\alpha^+ = \bigcup \{\, \beta \mid |\beta| = |\alpha| \,\}$$

è il più piccolo cardinale strettamente maggiore di α.

Un insieme finito o in bijezione con ω si dice **numerabile** altrimenti si dice non-numerabile o più che numerabile.

Esercizio 3.24. Dimostrare che un insieme non vuoto è numerabile se e solo se è immagine suriettiva di ω.

Il cardinale ω^+ viene denotato con

$$\omega_1$$

ed è il primo cardinale più che numerabile.

Teorema 3.25. *Se X è un insieme di cardinali, allora* $\sup X$ *è un cardinale ed è il più piccolo cardinale $\geq \kappa$, per ogni $\kappa \in X$.*

Dimostrazione. Se $\lambda = \bigcup X$ non fosse un cardinale allora λ sarebbe in bijezione con qualche $\alpha < \lambda$ e $\lambda \notin X$. Ma allora $\alpha < \kappa < \lambda$ per qualche $\kappa \in X$ e quindi $|\alpha| = |\kappa| = |\lambda|$, cioè κ non sarebbe un cardinale: contraddizione. □

Corollario 3.26. Card *è una classe propria.*

Esercizi

Esercizio 3.27. Sia $R \subseteq X \times X$ una relazione irriflessiva, transitiva[8] e regolare. Allora R è ben-fondata se e solo se ogni sotto-*insieme* non-vuoto di X ha un elemento R-minimale.

Esercizio 3.28. Siano $\langle X, < \rangle$ e $\langle Y, \prec \rangle$ due insiemi bene ordinati. Dimostrare che:

(i) La relazione

$$\begin{aligned} \lhd = {} & \{\, ((x,0),(x',0)) \mid x, x' \in X \wedge x < x' \,\} \cup \\ & \{\, ((y,1),(y',1)) \mid y, y' \in Y \wedge y \prec y' \,\} \cup \\ & \{\, ((x,0),(y,1)) \mid x \in X \wedge y \in Y \,\} \end{aligned}$$

è un buon ordine su $X \times \{0\} \cup Y \times \{1\}$.

(ii) La relazione $\ll \subseteq (X \times Y) \times (X \times Y)$ definita da

$$(x,y) \ll (x',y') \;\Leftrightarrow\; (x < x') \vee (x = x' \wedge y \prec y')$$

è un buon ordine su $X \times Y$.

Esercizio 3.29. Dimostrare che se $\alpha \geq \omega$, allora $\alpha^+ = \{\, \beta \mid \exists f\, (f \colon \beta \rightarrowtail \alpha) \,\}$.

Esercizio 3.30. Dimostrare che non esiste nessuna funzione $f \colon \omega_1 \to \mathbb{R}$ strettamente crescente o strettamente decrescente.

4. Costruzioni per ricorsione

Supponiamo di avere una funzione f da un insieme A in sé stesso e di voler definire la successione $\langle f^{(n)} \mid n \in \mathbb{N} \rangle$ delle iterate,

$$f^{(n)} = \begin{cases} h & \text{se } n = 0, \\ f \circ f^{(n-1)} & \text{se } n > 0. \end{cases}$$

dove $h \colon A \to A$ è la funzione identica. L'esistenza di ciascuna $f^{(n)}$ è chiara—per esempio

$$f^{(2)} = \{\, (x,y) \in A \times A \mid \exists z\, ((x,z) \in f \wedge (z,y) \in f) \,\}.$$

Ma che dire della *successione* $G = \langle f^{(n)} \mid n \in \mathbb{N} \rangle$ delle iterate? Non è per nulla ovvio che i vari assiomi di MK o di ZF siano sufficienti per garantire l'esistenza della successione G, $n \mapsto f^{(n)}$, la quale è definita in modo "dinamico:" la definizione ricorsiva di G suggerisce un'espressione del tipo

$$G = \{\, (n,g) \mid \varphi(n,g,G) \,\},$$

[8] Vedremo nell'Esercizio 4.28 che l'ipotesi di transitività può essere rimossa.

ma questa non è un'applicazione lecita dell'assioma di comprensione, dato che G, la classe che si intende definire mediante la formula φ, compare nella formula stessa.

In questa sezione dimostreremo un teorema sufficientemente generale per garantire l'esistenza di una G siffatta. Innanzi tutto osserviamo che ogni $G \restriction n$ è una funzione $p\colon n \to A^A$, per qualche $n \in \mathbb{N}$, tale che se $0 < n$ allora $p(0) = h$ e se $m+1 < n$ allora $p(m+1) = f \circ p(m)$. Diremo che una p siffatta è un'approssimazione di G. È facile verificare che due approssimazioni sono sempre compatibili, nel senso che una delle due estende l'altra e che data una $p = \langle f^{(0)}, \dots, f^{(n-1)} \rangle$ possiamo costruire un'approssimazione migliore $\langle f^{(0)}, \dots, f^{(n-1)}, F(n,p) \rangle$ dove $F(n,p)$ è definita da

$$F(n,p) = f \circ p(n-1)\,. \tag{19}$$

Queste idee si traducono nel seguente

Teorema 4.1. *Siano A, B insiemi, $h\colon A \to B$ una funzione e sia $F\colon A \times \omega \times \mathcal{G} \to B$, dove $\mathcal{G} = \{\, p \subseteq (A \times \omega) \times B \mid p \text{ è una funzione} \,\}$. Allora esiste un'unica $G\colon A \times \omega \to B$ tale che per ogni $a \in A$ e ogni $n \in \omega$*

$$\begin{aligned} G(a,0) &= h(a) \\ G(a, \mathbf{S}(n)) &= F(a, n, G \restriction \{\, (a,m) \mid m \leq n \,\}) \end{aligned}$$

Il Teorema 4.1 discende dal più generale Teorema 4.2 della sezione 4.B, ma prima di addentrarci nella dimostrazione, vediamo qualche applicazione.

4.A. Esempi. Vediamo come questo risultato viene usato per giustificare in MK o in ZF le definizioni ricorsive.

4.A.1. *Iterazione di una funzione.* Prendendo $A = B$, $h\colon A \to A$ la funzione identica e F come in (19) otteniamo $G\colon A \times \omega \to A$ tale che $G(a,n) = f^{(n)}(a)$.

4.A.2. *Addizione.* La funzione somma $+\colon \omega \times \omega \to \omega$ è definita ricorsivamente nella seconda variabile mediante le equazioni

$$\begin{aligned} n + 0 &= n \\ n + \mathbf{S}(m) &= \mathbf{S}(n+m) \end{aligned}$$

Questa può essere ottenuta come $G(n,m) = n + m$ dal teorema ponendo $A = \omega \times \omega$, $B = \omega$, $h\colon \omega \to \omega$ è la funzione identità e

$$F((n,k),m,p) = \begin{cases} \mathbf{S}(p(n,k)) & \text{se } \mathbf{S}(k) = m \text{ e } (n,k) \in \operatorname{dom} p, \\ 0 & \text{altrimenti.} \end{cases}$$

4.A.3. *Moltiplicazione.* A partire dall'addizione (la cui esistenza è stata stabilita nell'esempio precedente) possiamo definire il prodotto mediante le equazioni

$$\begin{aligned} n \cdot 0 &= 0 \\ n \cdot \mathbf{S}(m) &= (n \cdot m) + n\,. \end{aligned}$$

In questo caso la funzione $h\colon \omega \to \omega$ è identicamente 0 mentre

$$F((n,k),m,p) = \begin{cases} p(n,k) + n & \text{se } \mathbf{S}(k) = m \text{ e } (n,k) \in \operatorname{dom} p, \\ 0 & \text{altrimenti.} \end{cases}$$

4.A.4. *Fattoriale.* La funzione fattoriale $G\colon \omega \to \omega$ è ottenuta ponendo $A = \{0\}$, $B = \omega$, $h\colon A \to B$, $h(0) = 1$ e

$$F(0,n,p) = \begin{cases} p(k) \cdot n & \text{se } \mathbf{S}(k) = n, \\ 0 & \text{se } n = 0. \end{cases}$$

Gli argomenti di questa sezione e, segnatamente, i Teoremi 4.1 e 4.2 risultano spesso ostici la prima volta che li si incontra, non tanto per le loro dimostrazioni, per altro abbastanza semplici, quanto per le motivazioni dei teoremi. Spesso gli studenti si chiedono: *Che bisogno c'è di dimostrare questi risultati? Non è ovvio che le operazioni di somma, prodotto, fattoriale e, più in generale, le funzioni definite per ricorsione sono ben definite in matematica?* Il punto fondamentale è che vogliamo *dimostrare* a partire dagli assiomi che queste funzioni esistono e questo richiede i teoremi di questa sezione. Le funzioni definite per ricorsione risultano problematiche quando compaiono in enunciati che devono essere scritti nel linguaggio della teoria degli insiemi, cioè usando soltanto i simboli di appartenenza $\in$, di uguaglianza $=$, i quantificatori e i connettivi. Per esempio, supponiamo di voler formalizzare nel linguaggio LST la formula

$$\forall n, m \in \omega\,(n + m = m + n)\,. \tag{20}$$

Vediamo subito che sono presenti due simboli non primitivi: il simbolo ω e il simbolo $+$. Il primo lo possiamo rimpiazzare con la variabile u e la formula

$$\exists u[\varphi(u) \wedge \forall n, m(n \in u \wedge m \in u \Rightarrow n + m = m + n)$$

dove $\varphi(u)$ è la formula che asserisce che u è un ordinale limite ed è il più piccolo siffatto. Per eliminare il simbolo $+$ possiamo ricorrere alla perifrasi: c'è una funzione $f\colon \omega \times \omega \to \omega$ che soddisfa gli assiomi della somma e tale che $f(n,m) = f(m,n)$, per tutti gli n, m. Il Teorema 4.1 ci garantisce che

tale funzione esiste ed è unica. Quindi la formula (20) diventa

$$\begin{aligned}\exists u[\varphi(u) \wedge \exists f\colon u \times u \to u\, \forall n(n \in u \wedge f(n,0) = n) \wedge \\ \forall n, m(n \in u \wedge m \in u \Rightarrow f(n, \mathbf{S}(m)) = \mathbf{S}(f(n,m)) \wedge \\ \forall n, m(n \in u \wedge m \in u \Rightarrow f(n,m) = f(m,n))\end{aligned}$$

Questa non è ancora una vera formula di LST in quanto sono ancora presenti dei simboli definiti, quali $\times$, 0 e $\mathbf{S}$, ma questi possono essere eliminati come abbiamo fatto per ω.

4.B. Il Teorema di Ricorsione. Il Teorema 4.1 benché molto utile non è sufficiente per molte applicazioni, per cui si dimostra una versione più generale sostituendo ω ed il suo ordinamento con una classe (eventualmente propria) X ed una relazione R ben-fondata su di essa.

Teorema 4.2. *Siano X e Z classi, sia $R \subseteq X \times X$ irriflessiva, regolare e ben-fondata e sia $F\colon Z \times X \times \mathrm{V} \to \mathrm{V}$. Allora esiste un'unica $G\colon Z \times X \to \mathrm{V}$ tale che per ogni $(z,x) \in Z \times X$*

$$G(z,x) = F(z, x, G \restriction \{\, (z,y) \mid y\ R\ x \,\})\,. \tag{21}$$

Dimostrazione. Supponiamo che $G, G'\colon Z \times X \to \mathrm{V}$ soddisfino (21) e che $G \neq G'$. Fissiamo uno $\bar{z} \in Z$ per cui $Y = \{\, x \in X \mid G(\bar{z},x) \neq G'(\bar{z},x) \,\} \neq \emptyset$ e sia $\bar{x} \in Y$ un elemento R-minimale. Allora

$$G \restriction \{\, (\bar{z},y) \mid y\ R\ \bar{x} \,\} = G' \restriction \{\, (\bar{z},y) \mid y\ R\ \bar{x} \,\}$$

e sia $\bar{p}$ questa funzione. La regolarità di R e l'Assioma del Rimpiazzamento implicano che $\bar{p}$ è un insieme e allora $G(\bar{z},\bar{x}) = F(\bar{z},\bar{x},\bar{p}) = G'(\bar{z},\bar{x})$: una contraddizione. Quindi l'unicità è stabilita.

Sia $\mathcal{G}$ la classe delle funzioni p tali che

(i) $\mathrm{dom}(p) \subseteq Z \times X$,

(ii) $\forall (z,x) \in \mathrm{dom}(p)\, \forall y \in X\, (y\ R\ x \Rightarrow (z,y) \in \mathrm{dom}(p))$,

(iii) $\forall (z,x) \in \mathrm{dom}(p)\, (p(z,x) = F(z,x, p \restriction \{\, (z,y) \mid y\ R\ x \,\}))$.

Osserviamo che se $p, q \in \mathcal{G}$ allora $p \cup q$ è una funzione: supponiamo per assurdo che

$$\{\, x \in X \mid \exists z \in Z\, ((z,x) \in \mathrm{dom}(p) \cap \mathrm{dom}(q)\ \wedge\ p(z,x) \neq q(z,x)) \,\}$$

sia non vuoto e per la ben fondatezza sia $\bar{x}$ un elemento R-minimale di questa classe. Sia $\bar{z} \in Z$ tale che $(\bar{z},\bar{x}) \in \mathrm{dom}(p) \cap \mathrm{dom}(q)$ e $p(\bar{z},\bar{x}) \neq q(\bar{z},\bar{x})$. Per (ii)

$$\{\, (\bar{z},y) \mid y\ R\ \bar{x} \,\} \subseteq \mathrm{dom}(p) \cap \mathrm{dom}(q)$$

e per la R-minimalità di $\bar{x}$

$$p \restriction \{\, (\bar{z},y) \mid y\ R\ \bar{x} \,\} = q \restriction \{\, (\bar{z},y) \mid y\ R\ \bar{x} \,\} \stackrel{\mathrm{def}}{=} \bar{r}$$

da cui, utilizzando (iii) $p(\bar{z},\bar{x}) = F(\bar{z},\bar{x},\bar{r}) = q(\bar{z},\bar{x})$, contrariamente alla nostra ipotesi. È facile verificare che $p \cup q \in \mathcal{G}$, e quindi $\mathcal{G}$ è un semi-reticolo superiore rispetto all'inclusione. Per la Proposizione 2.3, $G = \bigcup \mathcal{G}$ è una relazione funzionale di dominio $\subseteq Z \times X$. Se $Z \times X \setminus \mathrm{dom}(G) \neq \emptyset$, sia $\bar{x}$ un elemento R-minimale di $\{\, x \in X \mid \exists z \in Z\ (z,x) \notin \mathrm{dom}(G) \,\}$ e sia $\bar{z} \in Z$ tale che $(\bar{z},\bar{x}) \notin \mathrm{dom}(G)$. Allora

$$p = G \restriction \{\, (\bar{z},y) \mid y\ R\ \bar{x} \,\}$$

è un insieme per l'Assioma del Rimpiazzamento e per la regolarità di R. È facile verificare che $p \cup \{((\bar{z},\bar{x}),F(z,x,p))\} \in \mathcal{G}$, da cui $(\bar{z},\bar{x}) \in \mathrm{dom}(G)$, contrariamente alla nostra assunzione. Ne segue che G è la relazione funzionale cercata. □

Osservazione 4.3. Il teorema così formulato è un enunciato di MK che asserisce che per ogni classe-funzione F c'è una ed una sola classe-funzione G con certe proprietà. Se vogliamo formulare (e dimostrare) il Teorema 4.2 in ZF, dobbiamo usare la perifrasi: date due formule φ_X, φ_Z con un'unica variabile libera e data una formula φ_R con due variabili libere che definiscono (eventualmente con parametri) le classi X, Z e R e data una formula φ_F che definisce (eventualmente con parametri) una classe-funzione F come nell'enunciato, *allora* c'è una formula φ_G che definisce (eventualmente con parametri) la classe-funzione G che soddisfa (21). Inoltre, se ψ è un'altra formula che definisce una classe-funzione G' che soddisfa (21) allora $G = G'$, cioè

$$\forall y,z,u\,(\varphi_G(x,y,u) \Leftrightarrow \psi(x,y,u))$$

Quindi in ZF non si ha un *singolo enunciato* bensì uno *schema di teoremi*, uno per ogni scelta di φ_X, φ_Z, φ_R e φ_F: per ogni scelta di formule possiamo costruire esplicitamente la formula φ_G

Corollario 4.4. *Sia X un ordinale oppure $X = \mathrm{Ord}$ e sia Z una classe. Siano H, K e L funzioni di dominio Z, $Z \times \{\, \alpha \in X \mid \alpha$ successore$\,\} \times \mathrm{V}$ e $Z \times \{\, \alpha \in X \mid \alpha$ limite$\,\} \times \mathrm{V}$, rispettivamente. Allora esiste un'unica $G\colon Z \times X \to \mathrm{V}$ tale che*

$$G(z,\alpha) = \begin{cases} H(z) & \text{se } \alpha = 0, \\ K(z,\alpha,G \restriction \{z\} \times \alpha) & \text{se } \alpha \text{ è successore,} \\ L(z,\alpha,G \restriction \{z\} \times \alpha) & \text{se } \alpha \text{ è limite.} \end{cases}$$

Dimostrazione. Basta porre R la relazione $<$ su X e $F\colon Z \times X \times \mathrm{V} \to \mathrm{V}$,

$$F(z,\alpha,p) = \begin{cases} H(z) & \text{se } \alpha = 0, \\ K(z,\alpha,p) & \text{se } \alpha \text{ è successore,} \\ L(z,\alpha,p) & \text{se } \alpha \text{ è limite} \end{cases}$$

□

In molti casi la classe Z è irrilevante, quindi otteniamo

Corollario 4.5. *Sia X un ordinale oppure $X = \mathrm{Ord}$, sia Y un insieme e siano K e L funzioni di dominio $\{\, \alpha \in X \mid \alpha \text{ successore} \,\} \times \mathrm{V}$ e $\{\, \alpha \in X \mid \alpha \text{ limite} \,\} \times \mathrm{V}$, rispettivamente. Allora esiste un'unica $G\colon X \to \mathrm{V}$ tale che*

$$G(\alpha) = \begin{cases} Y & \text{se } \alpha = 0, \\ K(\alpha, G \restriction \alpha) & \text{se } \alpha \text{ è successore,} \\ L(\alpha, G \restriction \alpha) & \text{se } \alpha \text{ è limite.} \end{cases}$$

Chiaramente, quando $X \leq \omega$ possiamo fare a meno della funzione L.

Vediamo come il Corollario implichi l'esistenza della successione $\langle g^{(n)} \mid n \in \omega \rangle$ delle iterate di una $g\colon A \to A$. Siano $X = \omega$ e sia $Y\colon A \to A$ la funzione identità. Sia $K(n,p) = g \circ p(z, \bigcup n)$ se p è una funzione definita in $(z, \bigcup n)$ e $p(z, \bigcup n)\colon A \to A$; oppure $K(n,p) = \emptyset$, altrimenti. Allora $G(n) = g^{(n)}$ per ogni $n \in \omega$.

Un'altra semplice applicazione di questo Corollario è data dalla seguente:

Proposizione 4.6. *Ogni ordine stretto $\prec$ su un insieme finito non vuoto X ha elementi massimali e elementi minimali. In particolare $\prec$ è una relazione ben fondata su X.*

Dimostrazione. Considerando l'ordinamento $\prec^*$

$$x \prec^* y \Leftrightarrow y \prec x$$

è sufficiente dimostrare che esistono elementi massimali. Per contraddizione, supponiamo che $\forall x \in X\, \exists y \in X\, (x \prec y)$. Fissiamo un'enumerazione $\{\, x_i \mid i \leq n \,\}$ di X e definiamo $g\colon \omega \to \mathbf{S}(n)$

$$\begin{aligned} g(0) &= 0\,, \\ g(\mathbf{S}(i)) &= \min \left\{\, j \leq n \mid x_{g(i)} \prec x_j \,\right\}. \end{aligned}$$

(Per ipotesi l'insieme $\left\{\, j \leq n \mid x_{g(i)} \prec x_j \,\right\}$ è non vuoto, quindi $g(i)$ è definito per tutti gli $i \in \omega$.) Verifichiamo, per induzione su $j \in \omega$ che

$$\forall i < j \left(x_{g(i)} \prec x_{g(j)} \right).$$

Se $j = 0$ il risultato è banale, quindi possiamo supporre che $j = \mathbf{S}(m)$. Se $i < m$, allora $x_{g(i)} \prec x_{g(m)}$ per ipotesi induttiva e $x_{g(m)} \prec x_{g(\mathbf{S}(m))} = x_{g(j)}$ per costruzione e quindi $x_{g(i)} \prec x_{g(j)}$; se $i = m$, allora $x_{g(i)} \prec x_{g(j)}$ per costruzione. Quindi che g è iniettiva, ma questo contraddice il fatto che X sia finito.

La seconda parte dell'enunciato discende dalla prima e dall'Esercizio 3.19. □

Poiché ad ogni ordine stretto $\prec$ possiamo associare l'ordine (non-stretto) associato $\preceq$ e viceversa, si ha il seguente

Corollario 4.7. *Ogni ordine $\preceq$ su un insieme finito non vuoto X ha elementi massimali e elementi minimali. In particolare $\preceq$ è una relazione ben fondata su X.*

Proposizione 4.8. *Per ogni insieme finito X e ogni ordine parziale $\preceq$ su X c'è un ordine totale $\leq$ su X che estende $\preceq$, cioè*

$$\forall x, y \in X \, (x \preceq y \Rightarrow x \leq y) \, .$$

Dimostrazione. Procediamo per induzione su $|X|$, la cardinalità di X. Se $|X| \leq 1$, il risultato è banale, quindi possiamo supporre che $|X| \geq 2$. Per il Corollario 4.7 fissiamo un $\bar{x} \in X$ minimale: per ipotesi induttiva c'è un ordine totale $\leq$ su $X \setminus \{\bar{x}\}$ che estende $\preceq$ su $X \setminus \{\bar{x}\}$. Allora $\leq \cup \{ (\bar{x}, y) \mid y \in X \}$ è un ordine totale su X che estende $\preceq$. □

Nel Capitolo III vedremo che la Proposizione 4.8 vale per ogni X (Teorema 14.11.)

4.C. Applicazioni ed esempi. Vediamo alcuni esempi di funzioni costruite mediante il Teorema 4.2.

4.C.1. *Rango di una relazione ben-fondata.* Se R è una relazione irriflessiva, regolare e ben-fondata su X, la relazione funzionale

$$\boldsymbol{\varrho}_{R,X} \colon X \to \mathrm{Ord}$$

che soddisfa

$$\boldsymbol{\varrho}_{R,X}(x) = \bigcup \{ \mathbf{S}(\boldsymbol{\varrho}_{R,X}(y)) \mid y \; R \; x \}$$

si dice **rango di R su X**. Osserviamo innanzitutto che $\mathrm{ran}(\boldsymbol{\varrho}_{R,X}) \subseteq \mathrm{Ord}$: se $\boldsymbol{\varrho}_{R,X}(y) \in \mathrm{Ord}$ per ogni y tale che $y \; R \; x$, allora $\boldsymbol{\varrho}_{R,X}(x) \in \mathrm{Ord}$ per l'Esercizio 3.5. Inoltre $\mathrm{ran}(\boldsymbol{\varrho}_{R,X})$ è un segmento iniziale di Ord, cioè

$$\mathrm{ran}(\boldsymbol{\varrho}_{R,X}) \in \mathrm{Ord} \;\vee\; \mathrm{ran}(\boldsymbol{\varrho}_{R,X}) = \mathrm{Ord} :$$

se, per assurdo esistesse un $\bar{x} \in X$ tale che $\boldsymbol{\varrho}_{R,X}(x) \notin \mathrm{Ord}$, allora prendendo $\bar{x}$ R-minimale e $\alpha \in \boldsymbol{\varrho}_{R,X}(x) \setminus \mathrm{ran}(\boldsymbol{\varrho}_{R,X})$ esisterebbe un $y \; R \; \bar{x}$ tale che $\alpha < \mathbf{S}(\boldsymbol{\varrho}_{R,X}(y))$. Poiché $\alpha = \boldsymbol{\varrho}_{R,X}(y)$ e questo contraddice la R-minimalità di $\bar{x}$.

Esercizio 4.9. Verificare che l'esistenza di $\boldsymbol{\varrho}_{R,X}$ discende dal Teorema 4.2 e dimostrare che:

(i) $x \; R \; y \Rightarrow \boldsymbol{\varrho}_{R,X}(x) < \boldsymbol{\varrho}_{R,X}(y)$,

(ii) $\boldsymbol{\varrho}_{R,X}(x) = \inf \{ \alpha \mid \forall y \, (y \; R \; x \Rightarrow \boldsymbol{\varrho}_{R,X}(y) < \alpha) \}$.

Quindi $\boldsymbol{\varrho}_{R,X}(x) = 0$ se e solo se x è R-minimale in X e $\boldsymbol{\varrho}_{R,X}(x) = \alpha$ se e solo se x è R-minimale in $X \setminus \{\, y \in X \mid \boldsymbol{\varrho}_{R,X}(y) < \alpha \,\}$.

L'ordinale $\boldsymbol{\varrho}_{R,X}(x)$, quando $X = \mathrm{V}$ e R è la relazione di appartenenza, si dice **rango di** x e si denota con $\mathrm{rank}(x)$.

Esercizio 4.10. (i) $x \in y \Rightarrow \mathrm{rank}(x) < \mathrm{rank}(y)$.

(ii) $x \subseteq y \Rightarrow \mathrm{rank}(x) \leq \mathrm{rank}(y)$.

(iii) $\mathrm{rank}(\alpha) = \alpha$.

Proposizione 4.11. (a) $\mathrm{rank}(\mathscr{P}(x)) = \mathbf{S}(\mathrm{rank}(x))$.

(b) $\mathrm{rank}(\bigcup x) = \sup\{\, \mathrm{rank}(y) \mid y \in x \,\}$.

Dimostrazione. (a) Poiché $x \in \mathscr{P}(x)$ si ha che $\mathbf{S}(\mathrm{rank}(x)) \leq \mathrm{rank}(\mathscr{P}(x))$. Viceversa se $y \subseteq x$, allora $\mathbf{S}(\mathrm{rank}(y)) \leq \mathbf{S}(\mathrm{rank}(x))$ per l'Esercizio 4.10 e quindi $\mathrm{rank}(\mathscr{P}(x)) = \sup\{\, \mathbf{S}(\mathrm{rank}(y)) \mid y \subseteq x \,\} \leq \mathbf{S}(\mathrm{rank}(x))$.

(b) Se $y \in x$ allora $y \subseteq \mathrm{rank}(\bigcup x)$ e quindi $\sup\{\, \mathrm{rank}(y) \mid y \in x \,\} \leq \mathrm{rank}(\bigcup x)$. $\mathrm{rank}(\bigcup x) = \sup\{\, \mathrm{rank}(y) \mid y \in x \,\}$. Viceversa, se $z \in y \in x$ allora $\mathbf{S}(\mathrm{rank}(z)) \leq \mathrm{rank}(y)$ e quindi $\mathbf{S}(\mathrm{rank}(z)) \leq \sup\{\, \mathrm{rank}(y) \mid y \in x \,\}$. Per l'arbitrarietà di z, $\mathrm{rank}(\bigcup x) \leq \sup\{\, \mathrm{rank}(y) \mid y \in x \,\}$. □

Definizione 4.12. $\mathrm{V}_\alpha = \{\, x \mid \mathrm{rank}(x) < \alpha \,\}$.

Teorema 4.13. V_α *è un insieme transitivo e*

$$\mathrm{V}_\alpha = \bigcup_{\beta<\alpha} \mathscr{P}(\mathrm{V}_\beta)\,. \tag{22}$$

Dimostrazione. Se $y \in x \in \mathrm{V}_\alpha$ allora $\mathrm{rank}(y) < \mathrm{rank}(x) < \alpha$ da cui $y \in \mathrm{V}_\alpha$. Quindi V_α è una classe transitiva. Per induzione su α dimostriamo che V_α è un insieme e che (22). Supponiamo il risultato valga per tutti i $\beta < \alpha$: allora $\{\, \mathscr{P}(\mathrm{V}_\beta) \mid \beta < \alpha \,\}$ è un insieme e quindi è sufficiente dimostrare (22). Per l'Esercizio 4.10 $x \subseteq \mathrm{V}_{\mathrm{rank}(x)}$ e quindi $\mathrm{rank}(x) < \alpha \Rightarrow x \in \bigcup_{\beta<\alpha} \mathscr{P}(\mathrm{V}_\beta)$. Viceversa, se $x \in \bigcup_{\beta<\alpha} \mathscr{P}(\mathrm{V}_\beta)$, allora $x \subseteq \mathrm{V}_\beta$, per qualche $\beta < \alpha$ e quindi $\mathrm{rank}(y) < \beta$ per ogni $y \in x$, da cui $\mathrm{rank}(x) \leq \beta < \alpha$. □

Corollario 4.14. (a) $\mathrm{V}_0 = \emptyset$.

(b) *Se* $\alpha < \beta$ *allora* $\mathrm{V}_\alpha \in \mathrm{V}_\beta$ *e* $\mathrm{V}_\alpha \subset \mathrm{V}_\beta$.

(c) $\mathrm{V}_{\mathbf{S}(\alpha)} = \mathscr{P}(\mathrm{V}_\alpha)$.

(d) $\mathrm{V}_\lambda = \bigcup_{\alpha<\lambda} \mathrm{V}_\alpha$, *se* λ *limite.*

(e) $\mathrm{V} = \bigcup_{\alpha\in\mathrm{Ord}} \mathrm{V}_\alpha$.

4.C.2. Se R è una relazione irriflessiva, regolare e ben fondata su X, la funzione

$$\boldsymbol{\pi}_{R,X} \colon X \to \mathrm{V}$$

definita da

$$\boldsymbol{\pi}_{R,X}(x) = \{\, \boldsymbol{\pi}_{R,X}(y) \mid y \mathrel{R} x \,\}$$

si dice **funzione collassante di Mostowski**. La classe $\overline{X} = \mathrm{ran}(\boldsymbol{\pi}_{R,X})$ si dice **collasso di Mostowski di R e X**.

Esercizio 4.15. Dimostrare che:

(i) $\overline{X}$ è transitiva e

(ii) $\forall x, y \in X\, (x \mathrel{R} y \Rightarrow \boldsymbol{\pi}_{R,X}(x) \in \boldsymbol{\pi}_{R,X}(y))$.

Definizione 4.16. Una relazione $R \subseteq X \times X$ è **estensionale su** X se

$$\forall x, y \in X\, (\forall z \in X\, (z \mathrel{R} x \Leftrightarrow z \mathrel{R} y) \Rightarrow x = y)\,,$$

Esercizio 4.17. (i) Se X è una classe transitiva, allora $\in \restriction X = \{\, (y, x) \in X \times X \mid y \in x \,\}$ è estensionale su X.

(ii) Se R è un buon ordine stretto su X, allora R è estensionale su X.

Proposizione 4.18. (a) *Se R è estensionale su X, allora $\boldsymbol{\pi}_{R,X}$ è iniettiva e $\boldsymbol{\pi}_{R,X} \colon X \to \overline{X}$ è un isomorfismo tra R su X e $\in$ su $\overline{X}$, cioè $\boldsymbol{\pi}_{R,X}$ è bijettiva e*

$$\forall x, y \in X\, (x \mathrel{R} y \Leftrightarrow \boldsymbol{\pi}_{R,X}(x) \in \boldsymbol{\pi}_{R,X}(y))\,. \tag{23}$$

(b) *Se R è un buon ordine stretto su X le funzioni $\boldsymbol{\pi}_{R,X}$ e $\boldsymbol{\varrho}_{R,X}$ coincidono.*

Dimostrazione. (a) Verifichiamo che $\boldsymbol{\pi}_{R,X}$ è iniettiva. Per assurdo, sia $\bar{x}$ R-minimale tale che $\boldsymbol{\pi}_{R,X}(\bar{x}) = \boldsymbol{\pi}_{R,X}(\bar{y})$, per qualche $'\bar{y} \neq \bar{x}$. Sia $z \mathrel{R} \bar{x}$: poiché $\boldsymbol{\pi}_{R,X}(z) \in \boldsymbol{\pi}_{R,X}(\bar{x}) = \boldsymbol{\pi}_{R,X}(\bar{y})$, c'è un $w \mathrel{R} \bar{y}$ tale che $\boldsymbol{\pi}_{R,X}(z) = \boldsymbol{\pi}_{R,X}(w)$. Ma per la minimalità di $\bar{x}$, $z = w$. Quindi

$$z \mathrel{R} \bar{x} \Rightarrow z \mathrel{R} \bar{y}\,.$$

Analogamente, se $z \mathrel{R} \bar{y}$ allora esiste $w \mathrel{R} \bar{x}$ tale che $\boldsymbol{\pi}_{R,X}(z) = \boldsymbol{\pi}_{R,X}(w)$ e quindi $z = w$, cioè

$$z \mathrel{R} \bar{y} \Rightarrow z \mathrel{R} \bar{x}\,.$$

Quindi, per estensionalità, $\bar{y} = \bar{x}$, contrariamente alla nostra ipotesi. Ne segue che $\boldsymbol{\pi}_{R,X}$ è una bijezione tra X e $\overline{X}$.

Se $\boldsymbol{\pi}_{R,X}(x) \in \boldsymbol{\pi}_{R,X}(y) = \{\, \boldsymbol{\pi}_{R,X}(z) \mid z \mathrel{R} y \,\}$, allora per l'iniettività, $x \mathrel{R} y$. Quindi per l'Esercizio 4.15 (23) vale.

(b) Supponiamo che $\boldsymbol{\varrho}_{R,X}(y) = \boldsymbol{\pi}_{R,X}(y)$, per ogni $y \mathrel{R} x$. Allora $\boldsymbol{\pi}_{R,X}(x) = \{\, \boldsymbol{\pi}_{R,X}(y) \mid y \mathrel{R} x \,\} = \{\, \boldsymbol{\varrho}(y) \mid y \mathrel{R} x \,\}$ è un insieme di ordinali. Se $\boldsymbol{\pi}_{R,X}(z) \in \boldsymbol{\pi}_{R,X}(y) \in \boldsymbol{\pi}_{R,X}(x)$, allora $z \mathrel{R} y \mathrel{R} x$, da cui $z \mathrel{R} x$, cioè $\boldsymbol{\pi}_{R,X}(x)$ è

transitivo e quindi è un ordinale. Per costruzione $\boldsymbol{\pi}_{R,X}(x)$ è l'estremo superiore degli ordinali $\mathbf{S}(\boldsymbol{\pi}_{R,X}(y)) = \mathbf{S}(\boldsymbol{\varrho}_{R,X}(y))$ con $y\ R\ x$, vale a dire $\boldsymbol{\pi}_{R,X}(x) = \boldsymbol{\varrho}_{R,X}(x)$. □

Definizione 4.19. Se R è un buon ordine su X la classe

$$\mathrm{ot}(R, X) = \mathrm{ran}(\boldsymbol{\pi}_{R,X}) = \mathrm{ran}(\boldsymbol{\varrho}_{R,X})$$

è un ordinale oppure è Ord e si dice **tipo d'ordine di R su X**. $\mathrm{ot}(R, X)$ è un insieme se e solo se X lo è. La funzione

$$\boldsymbol{\pi}^{-1}_{R,X} = \boldsymbol{\varrho}^{-1}_{R,X} \colon \mathrm{ot}(R, X) \to X$$

si dice **funzione enumerante**.

Osserviamo che se f è la funzione enumerante di un buon ordine R su X, allora $f(0)$ è il minimo di X, $f(\mathbf{S}(\alpha)$ è il successore immediato di $f(\alpha)$ e se λ è limite, $f(\lambda)$ è il più piccolo $x \in X$ tale che $f(\alpha)\ R\ x$, per ogni $\alpha < \lambda$.

Teorema 4.20. *Se $\langle X, R\rangle$ è un insieme bene ordinato esiste uno ed un solo ordinale α ed un'unica f tale che $f \colon \langle \alpha, <\rangle \to \langle X, R\rangle$ è un isomorfismo.*

Dimostrazione. L'esistenza di α e f è assicurata dalla Proposizione 4.18. L'unicità discende dalla Proposizione 3.16. □

4.C.3. Sia A un ordinale, oppure $A = \mathrm{Ord}$. Una funzione crescente $f \colon A \to \mathrm{Ord}$ si dice **continua** se

$$\forall \lambda \in A \big(\lambda \text{ limite } \Rightarrow f(\lambda) = \sup_{\alpha<\lambda} f(\alpha)\big)\,. \tag{24}$$

Esercizio 4.21. Se $f \colon \mathrm{Ord} \to \mathrm{Ord}$ è crescente e continua, allora per ogni limite λ e ogni $X \subseteq \lambda$ tale che $\sup X = \lambda$,

$$f(\lambda) = \sup_{\nu\in X} f(\nu)\,.$$

Se f è anche strettamente crescente, allora $f(\lambda)$ è un ordinale limite.

Lemma 4.22. *Se $f \colon \mathrm{Ord} \to \mathrm{Ord}$ è strettamente crescente e continua, allora*

$$\forall \alpha\, \exists \bar\alpha > \alpha\, (f(\bar\alpha) = \bar\alpha)\,.$$

Dimostrazione. Per ricorsione definiamo la successione $\langle \alpha_n \mid n \in \omega\rangle$ ponendo $\alpha_0 = \mathbf{S}(\alpha)$ e $\alpha_{\mathbf{S}(n)} = f(\alpha_n)$ e sia $\bar\alpha = \sup_n \alpha_n$. Se $f(\alpha_0) = \alpha_0$, allora $\forall n\, (\alpha_0 = \alpha_n)$ e quindi $\bar\alpha = \alpha_0$. Se invece $\alpha_0 < f(\alpha_0) = \alpha_1$, allora $\alpha_n < \alpha_{\mathbf{S}(n)}$

e quindi $\bar\alpha$ è limite. Allora

$$\begin{aligned} f(\bar\alpha) &= \sup_{\nu<\bar\alpha} f(\nu) \\ &= \sup_n f(\alpha_n) && \text{(per l'Esercizio 4.21)} \\ &= \sup_n \alpha_{\mathbf{S}(n)} \\ &= \bar\alpha\,. \end{aligned}$$

In ogni caso $\bar\alpha$ è il più piccolo punto fisso per f maggiore di α. □

Definizione 4.23. $\aleph\colon \mathrm{Ord} \to \mathrm{Card} \setminus \omega$ è la funzione che enumera la classe dei cardinali infiniti, cioè

$$\begin{aligned} \aleph_0 &= \omega \\ \aleph_{\mathbf{S}(\alpha)} &= (\aleph_\alpha)^+ \\ \aleph_\lambda &= \sup_{\alpha<\lambda} \aleph_\alpha\,. \end{aligned}$$

La definizione di $\aleph_\lambda$, per λ limite, è ben posta per il Teorema 3.25. Poiché $\aleph\colon \mathrm{Ord} \to \mathrm{Ord}$ è strettamente crescente e continua, esistono cardinali κ tali che $\kappa = \aleph_\kappa$, il più piccolo dei quali è l'estremo superiore di

$$\aleph_0, \quad \aleph_{\aleph_0}, \quad \aleph_{\aleph_{\aleph_0}}, \quad \aleph_{\aleph_{\aleph_{\aleph_0}}}, \quad \dots$$

4.C.4. La **chiusura transitiva** di una classe X è la classe

$$\mathrm{trcl}(X) = \Big\{ x \mid \exists n>0\, \exists f \in {}^{\mathbf{S}(n)}\mathrm{V} \big[x = f(0) \wedge f(n) \in X \wedge \forall i < n\ f(i) \in f(\mathbf{S}(i)) \big] \Big\}$$

In altre parole $x \in \mathrm{trcl}(X)$ se e solo se esistono $x_0, \dots, x_n$ tali che

$$x = x_0 \in x_1 \in \cdots \in x_n \in X\,.$$

Esercizio 4.24. Dimostrare che $\mathrm{trcl}(X)$ è la più piccola classe transitiva contenente X. Se X è un insieme anche $\mathrm{trcl}(X)$ lo è e $\mathrm{trcl}(X) = \bigcup_n X_n$, dove $X_0 = X$ e $X_{n+1} = \bigcup X_n$.

4.C.5. La **chiusura transitiva** di una relazione R su X è la relazione

$$\tilde R = \Big\{ (x,y) \in X\times X \mid \exists n>0\, \exists f \in {}^{\mathbf{S}(n)}X \big[x = f(0) \wedge y = f(n) \wedge \forall i < n\ (f(i), f(\mathbf{S}(i))) \in R \big] \Big\}$$

In altre parole $x\ \tilde R\ y$ se e solo se esistono $x_0, \dots, x_n$ tali che

$$x = x_0\ R\ x_1 \cdots x_{n-1}\ R\ x_n = y\,.$$

Esercizio 4.25. La relazione $\tilde R$ è transitiva su X.

Proposizione 4.26. *Se R è regolare su X, allora anche $\tilde{R}$ è regolare su X.*

Dimostrazione. Fissato un $\bar{x} \in X$, definiamo per ricorsione gli insiemi Z_n $(n \geq 1)$

$$\begin{aligned} Z_1 &= \{\, y \in X \mid y \; R \; \bar{x} \,\} \\ Z_{n+1} &= \{\, y \in X \mid \exists z \in Z_n \, (y \; R \; z) \,\} \\ &= \bigcup_{z \in Z_n} \{\, y \in X \mid y \; R \; z \,\}. \end{aligned}$$

Allora $\left\{ y \in X \mid y \; \tilde{R} \; \bar{x} \right\} = \bigcup_{n \geq 1} Z_n$ è un insieme. □

Esercizi

Esercizio 4.27. In questo esercizio vedremo una costruzione—dovuta a D. Scott—per rendere rigorosa la costruzione della classe quoziente quando la relazione d'equivalenza non è regolare, cioè quando le classi d'equivalenza sono classi proprie.

Sia E una relazione d'equivalenza non regolare su una classe propria X. Definiamo

$$\begin{aligned} [\![x]\!]_E &= \{\, y \in X \mid y \; E \; x \;\wedge\; \text{rank}(y) \text{ è minimo} \,\} \\ &= \{\, y \in X \mid y \; E \; x \;\wedge\; \forall z \in X \, (z \; E \; y \Rightarrow \text{rank}(z) \geq \text{rank}(y)) \,\}. \end{aligned}$$

Dimostrare che ogni $[\![x]\!]_E$ è un insieme e quindi

$$X/E = \{\, [\![x]\!]_E \mid x \in X \,\}$$

è una classe. Dimostrare che

(i) $x \; E \; y \Leftrightarrow [\![x]\!]_E = [\![y]\!]_E$,
(ii) $\neg(x \; E \; y) \Leftrightarrow [\![x]\!]_E \cap [\![y]\!]_E = \emptyset$.

Esercizio 4.28. Sia $R \subseteq X \times X$ una relazione regolare, vale a dire: per ogni $y \in X$

$$R^{(y)} = \{\, x \in X \mid x \; R \; y \,\}$$

è un insieme. Se $Y \subseteq X$ è un insieme definiamo

$$\begin{aligned} Y_0 &= Y \\ Y_{k+1} &= \bigcup \left\{ R^{(y)} \mid y \in Y_k \right\}. \end{aligned}$$

(i) Dimostrare che $\bar{Y} = \bigcup_k Y_k$ è un insieme.

(ii) Generalizzare l'Esercizio 3.27 dimostrando che se è irriflessiva, regolare e tale che ogni sotto-*insieme* di X ammette un elemento R-minimale, allora R è ben fondata su X.

Esercizio 4.29. Dimostrare che da una successione di ordinali α_n si può estrarre una sotto-successione α_{n_k} debolmente crescente. In altre parole: per ogni $f\colon \omega \to \mathrm{Ord}$ c'è una $g\colon \omega \to \omega$ strettamente crescente tale che $f \circ g\colon \omega \to \mathrm{Ord}$ è debolmente crescente.

5. Aritmetica ordinale

Per il Corollario 4.4 possiamo definire le operazioni di somma $\alpha \dot{+} \beta$, prodotto $\alpha \cdot \beta$ ed esponenziazione $\alpha^{\cdot\beta}$ sugli ordinali come le uniche funzioni $\mathrm{Ord} \times \mathrm{Ord} \to \mathrm{Ord}$ che soddisfano certe proprietà. (I simboli $\alpha + \beta$, $\alpha \cdot \beta$ e α^β vengono riservati per le operazioni di somma, prodotto ed esponenziazione *cardinale*, come vedremo nella sezione 8.)

5.A. Addizione. La **somma** $\alpha \dot{+} \beta$ di due ordinali è definita da:

$$\alpha \dot{+} \beta = \begin{cases} \alpha & \text{se } \beta = 0, \\ \mathbf{S}(\alpha \dot{+} \gamma) & \text{se } \beta = \mathbf{S}(\gamma), \\ \sup_{\gamma<\beta} \alpha \dot{+} \gamma & \text{se } \beta \text{ è limite.} \end{cases}$$

Proposizione 5.1. (a) $\beta < \beta' \Rightarrow \alpha \dot{+} \beta < \alpha \dot{+} \beta'$.

(b) *Se λ è limite e $\lambda = \sup_{i\in I} \lambda_i$, allora* $\alpha \dot{+} \lambda = \sup_{i\in I} \alpha \dot{+} \lambda_i$.

(c) $(\alpha \dot{+} \beta) \dot{+} \gamma = \alpha \dot{+} (\beta \dot{+} \gamma)$.

(d) $\alpha < \alpha' \Rightarrow \alpha \dot{+} \beta \leq \alpha' \dot{+} \beta$.

(e) $0 \dot{+} \beta = \beta$.

(f) $\beta \leq \alpha \dot{+} \beta$.

(g) $\alpha \leq \beta \Leftrightarrow \exists!\gamma\, (\alpha \dot{+} \gamma = \beta)$.

Dimostrazione. (a) Per induzione su β'. Il caso $\beta' = 0$ vale per motivi banali, quindi possiamo supporre β' successore o limite. Se $\beta' = \mathbf{S}(\beta'') > \beta$ allora $\beta'' \geq \beta$: per ipotesi induttiva $\alpha \dot{+} \beta \leq \alpha \dot{+} \beta''$ e

$$\alpha \dot{+} \beta'' < \mathbf{S}(\alpha \dot{+} \beta'') = \alpha \dot{+} \beta' \,,$$

da cui l'asserto. Se β' è limite e $\beta' > \beta$, allora

$$\alpha \dot{+} \beta' = \sup_{\gamma<\beta'} \alpha \dot{+} \gamma \geq \alpha \dot{+} \mathbf{S}(\beta) > \alpha \dot{+} \beta \,.$$

(b) La funzione $\nu \mapsto \alpha \dot{+} \nu$ è crescente e continua, quindi $\alpha \dot{+} \lambda$ è limite per l'Esercizio 4.21. Se $\lambda = \sup_{i\in I} \lambda_i$, allora $\alpha \dot{+} \lambda_i \leq \alpha \dot{+} \lambda$ e quindi $\sup_{i\in I} \alpha \dot{+} \lambda_i \leq \alpha \dot{+} \lambda$. Viceversa, se $\beta < \alpha \dot{+} \lambda$, allora fissiamo $\gamma < \lambda$ tale

che $\beta < \alpha \dot{+} \gamma$ e fissiamo $j \in I$ tale che $\gamma < \lambda_j$. Allora $\beta < \alpha \dot{+} \gamma < \alpha \dot{+} \lambda_j$, da cui segue l'asserto.

(c) Per induzione su γ. Il caso $\gamma = 0$ è banale. Supponiamo la proprietà valga per un γ:

$$\begin{aligned}(\alpha \dot{+} \beta) \dot{+} \mathbf{S}(\gamma) &= \mathbf{S}((\alpha \dot{+} \beta) \dot{+} \gamma) && \text{(per definizione di } \dot{+}) \\ &= \mathbf{S}(\alpha \dot{+} (\beta \dot{+} \gamma)) && \text{(per ipotesi induttiva)} \\ &= \alpha \dot{+} \mathbf{S}(\beta \dot{+} \gamma) && \text{(per definizione di } \dot{+}) \\ &= \alpha \dot{+} (\beta \dot{+} \mathbf{S}(\gamma)) && \text{(per definizione di } \dot{+})\end{aligned}$$

Supponiamo γ limite e quindi $\beta \dot{+} \gamma$ limite, per (b). Supponiamo inoltre che la proprietà valga per tutti i $\gamma' < \gamma$:

$$\begin{aligned}(\alpha \dot{+} \beta) \dot{+} \gamma &= \sup_{\gamma' < \gamma} (\alpha \dot{+} \beta) \dot{+} \gamma' && \text{(per definizione di } \dot{+}) \\ &= \sup_{\gamma' < \gamma} \alpha \dot{+} (\beta \dot{+} \gamma') && \text{(per ipotesi induttiva)} \\ &= \alpha \dot{+} (\beta \dot{+} \gamma) && \text{(per (a) e } \beta \dot{+} \gamma \text{ limite)}\end{aligned}$$

(d),(e) ed (f) seguono da una semplice induzione su β.

(g) L'unicità di γ discende da (a), quindi è sufficiente dimostrarne l'esistenza. Per (d) l'insieme

$$\{\, \xi \mid \alpha \dot{+} \xi < \beta \,\}$$

è un sottoinsieme di β e per (a) è un ordinale γ e poiché $\gamma \in \gamma$ è impossibile, ne segue che $\alpha \dot{+} \gamma \geq \beta$. È sufficiente dimostrare che $\alpha \dot{+} \gamma \leq \beta$. Se $\gamma = 0$, allora $\alpha \dot{+} \gamma = \alpha \leq \beta$. Se $\gamma = \mathbf{S}(\delta)$, allora $\alpha \dot{+} \delta < \beta$ e quindi $\alpha \dot{+} \gamma \leq \beta$. Se invece γ è limite, $\alpha \dot{+} \gamma = \sup_{\xi < \gamma} \alpha \dot{+} \xi \leq \beta$. □

È possibile dare una descrizione alternativa dell'operazione di somma. Sia $\lhd$ il buon ordine[9] su $\alpha \times \{0\} \cup \beta \times \{1\}$

$$(\gamma, i) \lhd (\eta, j) \Leftrightarrow (\gamma < \eta \wedge i = j) \vee (i = 0 \wedge j = 1)$$

Allora $f \colon \langle \alpha \dot{+} \beta, < \rangle \to \langle \alpha \times \{0\} \cup \beta \times \{1\}, \lhd \rangle$

$$f(\xi) = \begin{cases} (\xi, 0) & \text{se } \xi < \alpha, \\ (\gamma, 1) & \text{se } \xi = \alpha \dot{+} \gamma. \end{cases}$$

è un isomorfismo. Quindi $\alpha \dot{+} \beta$ è il tipo d'ordine di una copia di α seguita da una copia di β e

$$|\alpha \dot{+} \beta| = |\alpha \times \{0\} \cup \beta \times \{1\}| \tag{25}$$

Esercizio 5.2. Dimostrare che

(i) $\forall \alpha \, (\alpha \dot{+} 1 = \mathbf{S}(\alpha))$ e

[9] Si veda il Esercizio 3.28.

(ii) $\forall\alpha\,(\alpha \geq \omega \Rightarrow 1 \dot{+} \alpha = \alpha)$.

Quindi l'addizione sugli ordinali non è un'operazione commutativa.

Vediamo qualche esempio di sotto-insieme bene ordinato di $\mathbb{R}$.[10]

5.A.1. Gli insiemi di reali $\left\{ \frac{n}{n+1} \mid n \in \omega \right\}$ e $\{0\} \cup \left\{ \frac{n}{n+1} \mid n \in \omega \right\}$ hanno entrambi tipo d'ordine ω. L'insieme $\left\{ \frac{n}{n+1} \mid n \in \omega \right\} \cup \{1\}$ ha tipo d'ordine $\omega \dot{+} 1$.

5.A.2. Gli insiemi di reali $\left\{ \frac{n}{n+1} \mid n \in \omega \right\} \cup \left\{ \frac{2n+1}{n+1} \mid n \in \omega \right\}$ e $\left\{ \frac{n}{n+1} \mid n \in \omega \right\} \cup \left\{ \frac{2n+1}{n+1} \mid n \in \omega \right\} \cup \{2\}$ hanno tipo d'ordine $\omega \dot{+} \omega$ e $\omega \dot{+} \omega \dot{+} 1$, rispettivamente.

5.B. Moltiplicazione ed esponenziazione. Il **prodotto** e l'**esponenziazione** di ordinali sono definite da

$$\alpha \cdot \beta = \begin{cases} 0 & \text{se } \beta = 0, \\ (\alpha \cdot \gamma) \dot{+} \alpha & \text{se } \beta = \mathbf{S}(\gamma), \\ \sup_{\gamma<\beta} \alpha \cdot \gamma & \text{se } \beta \text{ è limite.} \end{cases}$$

$$\alpha^{\cdot\beta} = \begin{cases} 1 & \text{se } \beta = 0, \\ \alpha^{\cdot\gamma} \cdot \alpha & \text{se } \beta = \mathbf{S}(\gamma), \\ \sup_{\gamma<\beta} \alpha^{\cdot\gamma} & \text{se } \beta \text{ è limite.} \end{cases}$$

Come nell'uso comune, la moltiplicazione lega più strettamente dell'addizione, cioè $\alpha \dot{+} \beta \cdot \gamma$ sta per $\alpha \dot{+} (\beta \cdot \gamma)$.

Proposizione 5.3. (a) *Supponiamo* $\alpha \neq 0$. *Allora* $\beta < \beta' \Rightarrow \alpha \cdot \beta < \alpha \cdot \beta'$.

(b) *Se* λ *è limite e* $\alpha \neq 0$ *allora* $\alpha \cdot \lambda$ *è limite e se* $\lambda = \sup_{i\in I} \lambda_i$ *allora* $\alpha \cdot \lambda = \sup_{i\in I} \alpha \cdot \lambda_i$.

(c) $\alpha \cdot (\beta \dot{+} \gamma) = \alpha \cdot \beta \dot{+} \alpha \cdot \gamma$.

(d) $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$.

(e) $\alpha < \alpha' \Rightarrow \alpha \cdot \beta \leq \alpha' \cdot \beta$.

(f) $0 \cdot \beta = 0$ *e* $1 \cdot \beta = \beta$.

(g) *Se* $\alpha \neq 0$ *allora* $\beta \leq \alpha \cdot \beta$.

(h) *Se* $0 < \alpha$ *allora* $\forall\beta > 0\, \exists!\gamma \leq \beta\, \exists!\delta < \alpha\, (\alpha \cdot \gamma \dot{+} \delta = \beta)$.

Dimostrazione. (a) e (b) si dimostrano come le analoghe affermazioni (a) e (b) della Proposizione 5.1.

(c) Per induzione su γ. Il caso $\gamma = 0$ è banale, quindi supponiamo γ successore o limite. Se $\gamma = \mathbf{S}(\delta)$ allora, utilizzando la proprietà associativa

[10] Usiamo qualche semplice fatto sui numeri reali, che verranno introdotti nella sezione 9.

di $\dot{+}$,

$$\begin{aligned}
\alpha \cdot (\beta \dot{+} \gamma) &= \alpha \cdot \mathbf{S}(\beta \dot{+} \delta) \\
&= \alpha \cdot (\beta \dot{+} \delta) \dot{+} \alpha && \text{(per ipotesi induttiva)} \\
&= (\alpha \cdot \beta \dot{+} \alpha \cdot \delta) \dot{+} \alpha \\
&= \alpha \cdot \beta \dot{+} (\alpha \cdot \delta \dot{+} \alpha) \\
&= \alpha \cdot \beta \dot{+} \alpha \cdot \mathbf{S}(\delta) \\
&= \alpha \cdot \beta \dot{+} \alpha \cdot \gamma \,.
\end{aligned}$$

Supponiamo γ limite e che la proprietà valga per tutti i $\gamma' < \gamma$. Poiché $\beta \dot{+} \gamma$ e $\alpha \cdot (\beta \dot{+} \gamma)$ sono limiti,

$$\begin{aligned}
\alpha \cdot (\beta \dot{+} \gamma) &= \sup_{\nu<\gamma} \alpha \cdot (\beta \dot{+} \nu) && \text{(per (b))} \\
&= \sup_{\nu<\gamma} (\alpha \cdot \beta \dot{+} \alpha \cdot \nu) && \text{(per ipotesi induttiva)} \\
&= \alpha \cdot \beta \dot{+} \sup_{\nu<\gamma} \alpha \cdot \nu && \text{(per (b))} \\
&= \alpha \cdot \beta \dot{+} \alpha \cdot \gamma \,.
\end{aligned}$$

(d)–(g) sono simili alle analoghe dimostrazioni nelle Proposizione 5.1.

(h) Cominciamo col verificare l'unicità di γ e δ. Se $\alpha \cdot \gamma \dot{+} \delta = \alpha \cdot \gamma' \dot{+} \delta'$ e $\gamma \neq \gamma'$, per esempio, $\gamma < \gamma'$, allora per (a)

$$\beta = \alpha \cdot \gamma \dot{+} \delta < \alpha \cdot (\gamma \dot{+} 1) \leq \alpha \cdot \gamma' \leq \alpha \cdot \gamma' \dot{+} \delta' = \beta \,,$$

contraddizione! Quindi $\gamma = \gamma'$. Se, per esempio $\delta < \delta'$ allora per la parte (a) della Proposizione 5.1

$$\beta = \alpha \cdot \gamma \dot{+} \delta < \alpha \cdot \gamma \dot{+} \delta' = \beta \,,$$

contraddizione!

Dimostriamo l'esistenza di γ e δ. Se $\alpha < \beta$ poniamo $\gamma = 0$ e $\delta = \beta$, quindi possiamo supporre che $\alpha \leq \beta$. Per (a) esistono ordinali γ tali che $\alpha \cdot \gamma > \beta$ e sia $\bar{\gamma}$ il loro minimo: poiché $\bar{\gamma} = 0$ o $\bar{\gamma}$ limite è impossibile, ne segue che $\bar{\gamma}$ è della forma $\mathbf{S}(\gamma)$. Quindi $\alpha \cdot \gamma \leq \beta$ e $\gamma \leq \beta$ per (g) e (a). Se vale l'uguaglianza, allora poniamo $\delta = 0$. Se invece $\alpha \cdot \gamma < \beta$, per la parte (g) della Proposizione 5.1 c'è un δ tale che $\alpha \cdot \gamma \dot{+} \delta = \beta$. Poiché $\alpha \cdot \gamma \dot{+} \alpha > \beta$, ne segue che $\delta < \alpha$. □

Supponiamo $\alpha, \beta \neq 0$ e diamo a $\beta \times \alpha$ l'ordinamento lessicografico $<_{\text{lex}}$. Per la Proposizione 5.3, per ogni $\xi < \alpha \cdot \beta$ esistono $\gamma < \beta$ e $\delta < \alpha$ tali che $\alpha \cdot \gamma \dot{+} \delta = \xi$ e la funzione

$$f \colon \langle \alpha \cdot \beta, < \rangle \to \langle \beta \times \alpha, <_{\text{lex}} \rangle \qquad \xi \mapsto (\gamma, \delta)$$

è un isomorfismo. Quindi $\alpha \cdot \beta$ è il tipo d'ordine di β copie di α, allineate una dopo l'altra. In particolare,

$$|\alpha \cdot \beta| = |\alpha \times \beta| \,. \tag{26}$$

Esercizio 5.4. Dimostrare che

(i) $\alpha \cdot 2 = \alpha \dotplus \alpha$ e

(ii) se λ è limite, allora $2 \cdot \lambda = \lambda$.

Il seguente risultato, la cui dimostrazione è lasciata per esercizio, è l'analogo delle Proposizioni 5.1 e 5.3.

Proposizione 5.5. (a) *Se* $\alpha > 1$ *allora* $\beta < \beta' \Rightarrow \alpha^{\cdot\beta} < \alpha^{\cdot\beta'}$.

(b) $\alpha^{\cdot(\beta \dotplus \gamma)} = \alpha^{\cdot\beta} \cdot \alpha^{\cdot\gamma}$.

(c) $(\alpha^{\cdot\beta})^{\cdot\gamma} = \alpha^{\cdot(\beta \cdot \gamma)}$.

(d) $\alpha < \alpha' \Rightarrow \alpha^{\cdot\beta} \leq \alpha'^{\cdot\beta}$.

(e) $1^{\cdot\beta} = 1$ *e* $0^{\cdot\beta} = 1$, *se* $\bigcup \beta = \beta$, $0^{\cdot\beta} = 0$ *se* β *è successore.*

(f) *Se* $\alpha > 1$ *allora* $\beta \leq \alpha^{\cdot\beta}$.

(g) *Se* $1 < \alpha$ *allora* $\forall \beta \, \exists! \gamma \leq \beta \, \exists! \delta < \alpha \, \exists! \varepsilon < \alpha^{\cdot\gamma} \, (\alpha^{\cdot\gamma} \cdot \delta \dotplus \varepsilon = \beta)$.

Vediamo qualche altro esempio di insieme bene ordinato in matematica.

5.B.1. L'insieme di reali $\left\{ \frac{n \cdot m - 1}{n} \mid n, m \in \omega \setminus \{0\} \right\}$ ha tipo d'ordine $\omega \cdot \omega$.

5.B.2. Se f e g sono funzioni reali di variabile reale, definiamo l'ordinamento

$$f \prec g \quad \Leftrightarrow \quad \exists M \, \forall x > M \, (f(x) < g(x)) \,. \tag{27}$$

L'ordine $\prec$ sull'insieme $\mathbb{N}[X]$ dei polinomi in una variabile X con coefficienti in $\mathbb{N}$ è un buon ordine di tipo $\omega^{\cdot\omega}$. Infatti $f \prec g$ se e solo se

- $\deg(f) < \deg(g)$, dove $\deg(f)$ denota il grado di f, oppure
- $\deg(f) = \deg(g) = n$, $f = a_n X^n + \cdots + a_0$, $g = b_n X^n + \cdots + b_0$ e se $k \leq n$ è il più piccolo indice tale che $a_k \neq b_k$, allora $a_k < b_k$.

Possiamo allora definire un isomorfismo $F \colon \langle \mathbb{N}[X], \prec \rangle \to \langle \omega^\omega, < \rangle$

$$F(a_n X^n + \cdots + a_1 X + a_0) = \omega^{\cdot n} \cdot a_n \dotplus \cdots \dotplus \omega \cdot a_1 \dotplus a_0 \,.$$

5.C. Aritmetica su $\mathbb{N}$. Ora che abbiamo definito le operazioni di somma, prodotto, esponenziazione sugli ordinali e quindi sui naturali, è possibile dimostrare gli usuali fatti dell'aritmetica di $\mathbb{N}$: proprietà delle operazioni, fattorizzazione in primi, etc. Come vedremo nella sezione 8 le operazioni di somma, prodotto ed esponenziazione *ordinale* coincidono con le loro controparti *cardinali* sui naturali, per cui utilizzeremo i simboli $n + m$, $n \cdot m$ e n^m per queste operazioni sui naturali. Come esempio verifichiamo che la somma su $\mathbb{N}$ è commutativa. La dimostrazione si sviluppa in tre passi.

(I) $\forall m\,(0+m=m+0)$
La proprietà è vera per $m=0$ e se vale per un m, allora $0+\mathbf{S}(m)=\mathbf{S}(0+m)=\mathbf{S}(m)=\mathbf{S}(m)+0$. Quindi per induzione la proprietà vale per tutti gli m.

(II) $\forall m\,(1+m=m+1)$.
La proprietà è vera per $m=0$ in quanto $1+0=1$ e $0+1=\mathbf{S}(0+0)=\mathbf{S}(0)=1$. Supponiamo la proprietà valga per un m, allora

$$1+\mathbf{S}(m)=\mathbf{S}(1+m)=\mathbf{S}(m+1)=\mathbf{S}(\mathbf{S}(m))=\mathbf{S}(m)+1$$

cioè la proprietà vale per $\mathbf{S}(m)$. Quindi per induzione la proprietà vale per tutti gli m.

(III) $\forall n\,\forall m\,(n+m=m+n)$.
La dimostrazione è per induzione su n, cioè si verifica che per ogni n vale $\forall m\,(n+m=m+n)$. Il caso $n=0$ è la parte (I), quindi possiamo supporre che la proprietà valga per un n e dimostrarla per $\mathbf{S}(n)$:

$$\begin{aligned}
\mathbf{S}(n)+m &= (n+1)+m \\
&= n+(1+m) && \text{(per la proprietà associativa)}\\
&= (1+m)+n && \text{(per ipotesi induttiva)}\\
&= (m+1)+n && \text{(per (II))}\\
&= m+(1+n) && \text{(per la proprietà associativa)}\\
&= m+(n+1) && \text{(per (II))}\\
&= m+\mathbf{S}(n)
\end{aligned}$$

La proprietà commutativa del prodotto si dimostra in modo analogo e viene lasciata al lettore. La relazione $n \mid m$ significa che $\exists k\,(nk=m)$, cioè n divide m.

Esercizio 5.6. Dimostrare che

(i) $\forall n\in\omega\,\exists!m\in\omega\,(n=2m\ \vee\ n=2m+1)$.

(ii) $\forall n\in\omega\,\forall k\in\omega\,\big(2^{k+1}\mid n\Rightarrow 2^k\mid n\big)$

(iii) $\forall n\in\omega\,(n<2^n)$ e quindi $\forall n\in\omega\,(2^n\not\mid n)$.

(iv) $\forall n\in\omega\setminus\{0\}\,\exists!k\in\omega\,\exists!h\in\omega\,\big(n=2^k(2h+1)\big)$.

Ne segue che la funzione $f\colon\omega\times\omega\to\omega\setminus\{0\}$, $f(n,m)=2^n(2m+1)$ è una bijezione. Se $n-1$ denota il predecessore di n, quando $n\in\omega\setminus\{0\}$, possiamo allora definire una bijezione $\omega\times\omega\to\omega$, $(n,m)\mapsto f(n,m)-1$. Abbiamo quindi dimostrato il seguente:

Teorema 5.7. *$\omega\times\omega$ è in bijezione con ω.*

Questo risultato sarà esteso dal Teorema 8.8 a tutti i cardinali infiniti.

Esercizi

Esercizio 5.8. Dimostrare che un ordinale limite se e solo se è della forma $\omega \cdot \nu$, per qualche $\nu > 0$.

Esercizio 5.9. Dimostrare che se $\omega \leq \alpha$, $0 \leq n < \omega$ e $0 < m < \omega$ allora $(\alpha \dot{+} n) \cdot m = \alpha \cdot m \dot{+} n$.

Esercizio 5.10. Dimostrare che se λ è un ordinale limite, $0 \leq n < \omega$ e $1 < m < \omega$, allora $(\lambda \dot{+} n)^{\cdot m} < \lambda^{\cdot m} \cdot 2$. Dedurre che $(\lambda \dot{+} n)^{\cdot \omega} = \lambda^{\cdot \omega}$.

Esercizio 5.11. Dimostrare che:

(i) se $\alpha < \beta$ allora $\omega^{\cdot \alpha} \dot{+} \omega^{\cdot \beta} = \omega^{\cdot \beta}$; [11]

(ii) se $\alpha < \beta$ allora $\omega^{\cdot \alpha} \cdot n \dot{+} \omega^{\cdot \beta} = \omega^{\cdot \beta}$;

(iii) se $\alpha < \omega^{\cdot \beta}$ allora $\alpha \dot{+} \omega^{\cdot \beta} = \omega^{\cdot \beta}$.

Un ordinale α si dice **additivamente indecomponibile** se

$$\forall \beta, \gamma < \alpha \, (\beta \dot{+} \gamma < \alpha) \, .$$

Esercizio 5.12. Dimostrare per ogni ordinale α sono equivalenti le seguenti affermazioni:

(i) α è additivamente indecomponibile;

(ii) $\forall \beta < \alpha \, (\beta \dot{+} \alpha = \alpha)$;

(iii) $\exists \beta \left(\alpha = \omega^{\cdot \beta}\right)$, oppure $\alpha = 0$.

Un ordinale α si dice **moltiplicativamente indecomponibile** se

$$\forall \beta, \gamma < \alpha \, (\beta \cdot \gamma < \alpha) \, .$$

Esercizio 5.13. Dimostrare per ogni ordinale α sono equivalenti le seguenti affermazioni:

(i) α è moltiplicativamente indecomponibile;

(ii) $\forall \beta < \alpha \, (\beta \cdot \alpha = \alpha)$;

(iii) $\exists \beta \left(\alpha = \omega^{\cdot \omega^{\cdot \beta}}\right)$, oppure $\alpha = 0, 1, 2$.

Un ordinale α si dice **esponenzialmente indecomponibile** se

$$\forall \beta, \gamma < \alpha \, (\beta^{\cdot \gamma} < \alpha) \, .$$

Esercizio 5.14. Dimostrare per ogni ordinale α sono equivalenti le seguenti affermazioni:

[11] Suggerimento: usare le Proposizioni 5.1 e 5.3.

(i) α è esponenzialmente indecomponibile;

(ii) $\forall \beta < \alpha\, (\beta^{\cdot\alpha} = \alpha)$;

Esercizio 5.15. (i) Dimostrare che $\forall \alpha > 2\, (\alpha \dot{+} \alpha < \alpha \cdot \alpha < \alpha^{\cdot\alpha})$.

(ii) Definiamo

$$E(0, \alpha) = \alpha$$
$$E(\mathbf{S}(n), \alpha) = E(n, \alpha)^{E(n,\alpha)}\,.$$

Dimostrare che

$$\forall n\, \forall m\, (E(n, \alpha) < E(n + m, \alpha))$$

e che $\sup_n E(n, \alpha)$ è il più piccolo ordinale esponenzialmente indecomponibile maggiore di α.

Gli ordinali esponenzialmente indecomponibili maggiore di ω si chiamano **ε-numeri**: il primo di questi è

$$\varepsilon_0 = \sup\{\omega, \omega^{\cdot\omega}, \omega^{\cdot\omega^{\cdot\omega}}, \omega^{\cdot\omega^{\cdot\omega^{\cdot\omega}}}, \dots\}\,,$$

Esercizio 5.16. Sia $\beta > 1$. Dimostrare che per ogni α esiste un $m \in \omega$ e esistono ordinali $\gamma_0, \dots, \gamma_{m-1}$ e $\delta_0, \dots, \delta_{m-1}$ con $\alpha \geq \gamma_0 > \gamma_1 > \cdots > \gamma_{m-1}$ e $0 < \delta_i < \beta$ per ogni $i < m$, tali che

$$\alpha = \beta^{\cdot\gamma_0} \cdot \delta_0 \dot{+} \beta^{\cdot\gamma_1} \cdot \delta_1 \dot{+} \cdots \dot{+} \beta^{\cdot\gamma_{m-1}} \cdot \delta_{m-1}\,.$$

Dimostrare che m, i γ_i e i δ_i sono unici. Questa espressione è lo sviluppo di α in base β. Nel caso $\beta = \omega$ i δ_i sono naturali e si parla di **forma normale di Cantor**.

Esercizio 5.17. Se f e g sono funzioni reali di variabile reale, poniamo

$$f \prec g \Leftrightarrow \exists M\, \forall x > M\ f(x) < g(x)\,.$$

Sia $\mathcal{F}$ il più piccolo insieme di funzioni contenente $\mathbb{N}[X]$ e chiuso sotto la somma e l'operazione $f \mapsto X^f$. (Quindi funzioni quali $X^{(X^{3X+2}+5X^X)} + 2X + 4$ sono in $\mathcal{F}$, ma $(X + 1)^X$ no.) Dimostrare che l'ordinamento $\prec$ definito in (27) su $\mathcal{F}$ è un buon ordine di tipo ε_0, il primo punto fisso della funzione $\alpha \mapsto \omega^{\cdot\alpha}$.

Esercizio 5.18. Sia b un numero naturale > 1. Lo sviluppo di n in pura base b si calcola come segue:

- si scrive n in base b, cioè $n = b^{k_0} h_0 + \cdots + b^{k_{m-1}} h_{m-1}$;
- si scrive ogni k_i in base b, cioè $k_i = b^{\bar{k}_0} \bar{h}_0 + \cdots + b^{\bar{k}_{m-1}} \bar{h}_{m-1}$;
- si scrive ogni $\bar{k}_i$ in base b, etc.

finché nello sviluppo compaiono solo cifre $\leq b$. Per esempio lo sviluppo di $n = 2004$ in pura base $b = 2, 3, 4$ è

$$\begin{aligned} 2004 &= 2^{2^{2+1}+2} + 2^{2^{2+1}+1} + 2^{2^{2+1}} + 2^{2^2+2+1} + 2^{2^2+2} + 2^{2^2} + 2^2 \\ &= 3^{3\cdot 2} \cdot 2 + 3^{3+2} \cdot 2 + 3^3 \cdot 2 + 3 \cdot 2 \\ &= 4^{4+1} + 4^4 \cdot 3 + 4^3 \cdot 3 + 4^2 + 4\,. \end{aligned}$$

Per ogni $n \in \mathbb{N}$, la sequenza di Goodstein di n

$$G_n(0), \quad G_n(1), \quad G_n(2), \quad G_n(3), \quad \dots$$

si calcola nel seguente modo: $G_n(0) = n$, $G_n(k+1)$ si ottiene scrivendo $G_n(k)$ in pura base $k+2$, sostituendo ogni $k+2$ con $k+3$ e poi sottraendo 1. Quindi $G_n(1)$ è ottenuto sostituendo tutti i 2 nello sviluppo in pura base 2 con dei 3 e poi sottraendo 1, $G_n(2)$ è ottenuto da $G_n(1)$ scrivendolo in pura base 3, sostituendo i 3 con i 4 e poi sottraendo 1, etc. I primi elementi della sequenza di Goodstein per $n = 2004$ sono

$$\begin{aligned} &2^{2^{2+1}+2} + 2^{2^{2+1}+1} + 2^{2^{2+1}} + 2^{2^2+2+1} + 2^{2^2+2} + 2^{2^2} + 2^2 \\ &3^{3^{3+1}+3} + 3^{3^{3+1}+1} + 3^{3^{3+1}} + 3^{3^3+3+1} + 3^{3^3+3} + 3^{3^3} + 3^2 \cdot 2 + 3 \cdot 2 + 2 \\ &4^{4^{4+1}+4} + 4^{4^{4+1}+1} + 4^{4^{4+1}} + 4^{4^4+4+1} + 4^{4^4+4} + 4^{4^4} + 4^2 \cdot 2 + 4 \cdot 2 + 1 \\ &5^{5^{5+1}+5} + 5^{5^{5+1}+1} + 5^{5^{5+1}} + 5^{5^5+5+1} + 5^{5^5+5} + 5^{5^5} + 5^2 \cdot 2 + 5 \cdot 2 \\ &\quad \vdots \end{aligned}$$

Dimostrare che ogni sequenza di Goodstein termina a 0, cioè

$$\forall n \in \mathbb{N}\, \exists k\ G_n(k) = 0\,.$$

6. Gli ordinali e la topologia*

Gli ordinali sono molto utili in topologia: molti spazi topologici sono definiti tramite una costruzione transfinita e gli ordinali stessi sono una classe interessante di spazi topologici.

6.A. Spazi secondo numerabili. Ricordiamo che uno spazio topologico soddisfa al secondo assioma di numerabilità se ha una base numerabile (pag. 249).

Proposizione 6.1. *Se X è uno spazio topologico secondo numerabile non esiste nessuna successione di aperti $\langle U_\alpha \mid \alpha < \omega_1 \rangle$ tale che*

$$\alpha < \beta \Rightarrow U_\alpha \subset U_\beta\,.$$

Analogamente non esiste nessuna successione di chiusi $\langle C_\alpha \mid \alpha < \omega_1 \rangle$ tale che

$$\alpha < \beta \Rightarrow C_\alpha \supset C_\beta\,.$$

Dimostrazione. Fissiamo una base $\{ V_n \mid n \in \omega \}$ di X. Se, per assurdo, esistesse una sequenza $\subset$-crescente $\langle U_\alpha \mid \alpha < \omega_1 \rangle$, la funzione $\omega_1 \mapsto \omega$,

$$\alpha \mapsto \min \{ n \mid V_n \subseteq U_{\alpha \dot{+} 1} \ \wedge \ V_n \not\subseteq U_\alpha \}$$

sarebbe un'iniezione: assurdo. Il caso dei chiusi si ottiene da quanto sopra considerando i complementi. □

Sia X uno spazio secondo numerabile. Se x è isolato in X, allora $\{x\}$ è un aperto di base, quindi i punti isolati di X formano un insieme numerabile. Poiché la proprietà di essere secondo numerabile si preserva per sottospazi, per ogni $A \subseteq X$ possiamo definire il **derivato** di A come

$$A' = \{ x \in A \mid x \text{ non è isolato in } A \}.$$

Esercizio 6.2. Dimostrare che A' è un chiuso di A.

È facile vedere che $A \setminus A'$ è al più numerabile: fissiamo una base $\{ U_n \mid n \in \omega \}$ di X e definiamo $F_A \colon A \setminus A' \rightarrowtail \omega$

$$F_A(x) = \min \{ n \in \omega \mid U_n \cap A = \{x\} \}.$$

Uno spazio topologico si dice **perfetto** se non contiene punti isolati, cioè se coincide col suo derivato. Se C è un chiuso di uno spazio separabile X, possiamo definire la successione

$$\begin{aligned} C^{(0)} &= C \\ C^{(\alpha \dot{+} 1)} &= (C^{(\alpha)})' \\ C^{(\lambda)} &= \bigcap_{\alpha < \lambda} C^{(\alpha)} \qquad\qquad \text{se } \lambda \text{ è limite.} \end{aligned}$$

Gli insiemi C_α sono chiusi in X e quindi per la Proposizione 6.1 c'è un $\bar\alpha < \omega_1$ tale che $C^{(\bar\alpha)} = C^{(\bar\alpha \dot{+} 1)}$. Ad ogni $x \in \bigcup_{\alpha < \bar\alpha} C^{(\alpha)} \setminus C^{(\alpha \dot{+} 1)}$ possiamo associare l'ordinale

$$\alpha_x = \min \left\{ \alpha < \bar\alpha \mid x \in C^{(\alpha)} \setminus C^{(\alpha \dot{+} 1)} \right\}.$$

Quindi la funzione $F \colon \bigcup_{\alpha < \bar\alpha} C^{(\alpha)} \setminus C^{(\alpha \dot{+} 1)} \to \bar\alpha \times \omega$ definita da

$$F(x) = (\alpha_x, F_{A^{(\alpha_x)}}(x))$$

è un'iniezione. Sia $g \colon \bar\alpha \rightarrowtail \omega$ un'iniezione: componendo F con la mappa $\bar\alpha \times \omega \rightarrowtail \omega \times \omega$ otteniamo un'iniezione di $\bigcup_{\alpha < \bar\alpha} C^{(\alpha)} \setminus C^{(\alpha \dot{+} 1)}$ in $\omega \times \omega$. Quindi per il Teorema 5.7 $\bigcup_{\alpha < \bar\alpha} C^{(\alpha)} \setminus C^{(\alpha \dot{+} 1)}$ è numerabile. Abbiamo quindi dimostrato che

Teorema 6.3 (Cantor-Bendixson)**.** *In uno uno spazio secondo numerabile ogni chiuso C può essere scritto come $C = P \cup S$, dove P è perfetto, S è numerabile e $P \cap S = \emptyset$.*

L'insieme P è la parte perfetta di C, mentre S è la parte sparsa[12] di C. L'ordinale $\bar\alpha$ della dimostrazione precedente si dice **rango di Cantor Bendixson** di C e lo si indica con $\|C\|_{\mathrm{CB}}$. La definizione di questo ordinale dipende solo dalla topologia relativa di C e non dallo spazio ambiente X ed è invariante per omeomorfismi, vale a dire: se C e D sono spazi topologici omeomorfi, secondo numerabili, allora $\|C\|_{\mathrm{CB}} = \|D\|_{\mathrm{CB}}$.

In uno spazio separabile metrico completo[13] (X, d), la parte perfetta P di un chiuso C è vuota oppure è più che numerabile. Per verificare ciò supponiamo P sia non vuoto e numerabile: lo spazio P con la metrica d risulta essere completo privo di punti isolati e e separabile quindi, per un risultato che dimostreremo più avanti (Teorema 9.16), esisterebbe una funzione iniettiva $f\colon 2^{\mathbb{N}} \to 2$ e poiché $2^{\mathbb{N}}$ è più che numerabile si giunge ad una contraddizione.

Corollario 6.4. *In uno spazio separabile metrico completo, se K è un sottospazio compatto numerabile, allora $\|K\|_{\mathrm{CB}}$ è un ordinale successore.*

Dimostrazione. Per il Teorema di Cantor-Bendixson possiamo decomporre K nella sua parte perfetta P e la sua parte sparsa S. Per quanto osservato poco sopra, $P = K^{(\bar\alpha)} = \emptyset$, dove $\bar\alpha = \|K\|_{\mathrm{CB}}$. Se $\bar\alpha$ fosse limite allora $K^{(\bar\alpha)} = \bigcap_{\beta<\bar\alpha} K^{(\beta)}$ sarebbe intersezione vuota di una famiglia decrescente di compatti non vuoti, contro la proprietà dell'intersezione finita. □

Quindi dato un compatto metrico numerabile K, definiamo $\gamma = \gamma(K)$ come il predecessore di $\|K\|_{\mathrm{CB}}$ così che $K^{(\gamma)} \neq \emptyset$, ma $K^{(\gamma\dot{+}1)} = \emptyset$. L'insieme $K^{(\gamma)}$ non può essere infinito, altrimenti $\big\{\, \{x\} \mid x \in K^{(\gamma)} \,\big\}$ sarebbe un ricoprimento aperto privo di sotto-ricoprimenti finiti. Sia $n = n(K)$ la cardinalità di $K^{(\gamma)}$.

Il seguente teorema, di cui non diamo la dimostrazione, dice che $\gamma(K)$ e $n(K)$ individuano K a meno di omeomorfismi.

Teorema 6.5. *Dati K e H compatti metrici, numerabili e separabili, K e H sono omeomorfi se e solo se*

$$\gamma(K) = \gamma(H) \qquad e \qquad n(K) = n(H)\,.$$

6.B. La topologia degli ordinali. Ad ogni ordine lineare $\langle L, \leq\rangle$ possiamo associare la **topologia degli intervalli** generata dalle semirette aperte $\{\, x \in L \mid x < b \,\}$ e $\{\, x \in L \mid a < x \,\}$, con $a, b \in L$. Quindi ogni ordinale può essere visto come spazio topologico e la topologia dell'ordine si dice **topologia ordinale**.

Esercizio 6.6. Sia α un ordinale. Dimostrare che:

[12] In inglese: *scattered*.

[13] Ricordiamo che uno spazio separabile metrico è sempre secondo numerabile.

(i) La topologia su α ha come base gli intervalli $[\beta;\gamma)$ con $\beta < \gamma \leq \alpha$.

(ii) La topologia su α è di Hausdorff.

(iii) Se $\alpha' < \alpha$ allora la topologia su α' coincide con la topologia indotta da α, cioè α' è un sottospazio di α.

(iv) Se $\beta \in \alpha$, allora β è un punto isolato di α se e solo se β è successore o 0.

(v) $C \subseteq \alpha$ è chiuso di α se e solo se

$$\forall \lambda \in \alpha\, (\lambda \text{ limite e } \lambda = \textstyle\bigcup (C \cap \lambda) \Rightarrow \lambda \in C)\,.$$

Proposizione 6.7. *Un ordinale successore con la topologia ordinale è uno spazio compatto.*

Dimostrazione. Dimostriamo per induzione su α, che lo spazio $\alpha \dotplus 1$ è compatto. Se $\alpha = 0$ il risultato è immediato, quindi possiamo supporre che $\alpha > 0$ e che $\alpha' \dotplus 1$ sia compatto, per ogni $\alpha' < \alpha$. Sia $\mathcal{U}$ un ricoprimento aperto di $\alpha \dotplus 1$ e sia $U \in \mathcal{U}$ tale che $\alpha \in U$. Se α è un ordinale successore $\beta \dotplus 1$, allora per ipotesi induttiva c'è un $\mathcal{U}_0 \subseteq \mathcal{U}$ finito che ricopre $\beta \dotplus 1 = \alpha$, quindi $\mathcal{U}_0 \cup \{U\}$ è un ricoprimento aperto finito di $\alpha \dotplus 1$. Se α è limite prendiamo un $\beta < \alpha$ tale che $[\beta \dotplus 1; \alpha] \subseteq U$: per ipotesi induttiva $\beta \dotplus 1$ è compatto quindi posso trovare un sotto-ricoprimento finito $\mathcal{U}_0 \subseteq \mathcal{U}$ per esso. Ne segue che $\mathcal{U}_0 \cup \{U\}$ è un ricoprimento aperto finito di $\alpha \dotplus 1$. □

Teorema 6.8. *Se $\alpha < \omega_1$, allora α è immergibile in $\mathbb{R}$, cioè c'è una funzione $f\colon \alpha \to \mathbb{R}$ che preserva l'ordine e tale che* $\operatorname{ran}(f)$ *è un chiuso di $\mathbb{R}$.*

La dimostrazione è differita alla sezione 9 (Esercizio 9.34).

Esercizio 6.9. Se $f\colon \alpha \rightarrowtail \mathbb{R}$ è un'immersione, allora f è un omeomorfismo tra α e $\operatorname{ran}(f) \subseteq \mathbb{R}$.

Quindi gli spazi $\alpha \dotplus 1$ (con $\alpha < \omega_1$) sono esempi di spazi compatti, numerabili e completamente metrizzabili, cioè ammettono una metrica completa compatibile con la topologia ordinale. Benché siano tutti distinguibili come ordini, non sono tutti distinguibili come spazi topologici: per esempio se $\alpha \geq \omega$, la funzione $f\colon \alpha \dotplus 2 \to \alpha \dotplus 1$

$$f(\beta) = \begin{cases} \beta \dotplus 1 & \text{se } \beta < \omega, \\ \beta & \text{se } \omega \leq \beta \leq \alpha, \\ 0 & \text{se } \beta = \alpha \dotplus 1, \end{cases}$$

è un omeomorfismo.

Lemma 6.10. *Se $K = \alpha \dotplus 1 < \omega_1$, il β-esimo insieme derivato (con $\beta > 0$) è*

$$K^{(\beta)} = \left\{ \omega^{\cdot\beta} \cdot \nu \mid 0 < \nu \ \wedge \omega^{\cdot\beta} \cdot \nu \leq \alpha \right\}. \tag{28}$$

Dimostrazione. Cominciamo con due semplici osservazioni. La prima è che un ordinale $\gamma > 0$ è della forma $\omega^{\cdot\beta} \cdot \nu$, con $\nu > 0$ se e solo se, posto nella forma normale di Cantor (Esercizio 5.16)

$$\gamma = \omega^{\cdot\xi_1} \cdot n_1 \dotplus \cdots \dotplus \omega^{\cdot\xi_k} \cdot n_k$$

si ha $\beta \leq \xi_k$. Infatti se $\gamma = \omega^{\cdot\beta} \cdot \nu$ e $\nu = \omega^{\cdot\eta_1} \cdot n_1 \dotplus \cdots \dotplus \omega^{\cdot\eta_k} \cdot n_k$, allora $\gamma = \omega^{\cdot\beta\dotplus\eta_1} \cdot n_1 \dotplus \cdots \dotplus \omega^{\cdot\beta\dotplus\eta_k} \cdot n_k$ è in forma normale di Cantor e $\beta \leq \beta \dotplus \eta_k$. Viceversa se $\xi_k \leq \beta$ nella forma normale di Cantor di γ, allora posto η_i tale che $\xi_i = \beta \dotplus \eta_i$ e quindi

$$\gamma = \omega^{\cdot\beta} \cdot (\omega^{\cdot\eta_1} \cdot n_1 \dotplus \cdots \dotplus \omega^{\cdot\eta_k} \cdot n_k)$$

La seconda osservazione è che $K = K^{(0)} = \alpha \dotplus 1$ è l'insieme

$$\left\{ \omega^{\cdot 0} \cdot \nu \mid 0 \leq \nu \ \wedge \omega^{\cdot 0} \cdot \nu \leq \alpha \right\}.$$

In altre parole, l'unico motivo per considerare la formula (28) con $\beta > 0$ è che $0 \in K^{(0)}$, mentre $0 \notin K^{(\beta)}$, se $\beta > 0$.

I punti non isolati di K sono gli ordinali limite che, per l'Esercizio 5.8, sono della forma $\omega \cdot \nu$. Quindi la (28) vale per $\beta = 1$. Analogamente, se (28) vale per β, allora i punti non isolati di $K^{(\beta)}$ sono della forma $\omega^{\cdot\beta} \cdot \nu$ con ν limite. Per l'Esercizio 5.8 ν può essere scritto come $\omega \cdot \xi$ e quindi $K^{(\beta\dotplus 1)} = \left\{ \omega^{\cdot\beta\dotplus 1} \cdot \xi \mid 0 < \xi \ \wedge \ \omega^{\cdot\beta\dotplus 1} \cdot \xi \leq \alpha \right\}$. Supponiamo infine che β sia limite e che (28) valga per ogni $\beta' < \beta$. Sia $\lambda \in K^{(\beta)} = \bigcap_{\beta'<\beta} K^{(\beta')}$ e sia $\gamma = \omega^{\cdot\xi_1} \cdot n_1 \dotplus \cdots \dotplus \omega^{\cdot\xi_k} \cdot n_k$ la sua forma normale. Poiché λ è della forma $\omega^{\cdot\beta'} \cdot \nu'$, per ogni $\beta' < \beta$, segue che $\xi_k \geq \beta'$. Quindi λ è della forma $\omega^{\cdot\beta} \cdot \nu$, con $\nu > 0$. Viceversa, se $\lambda = \omega^{\cdot\beta} \cdot \nu$ e $\beta' < \beta$, allora $\lambda = \omega^{\cdot\beta'} \cdot (\omega^{\cdot\eta} \cdot \nu)$, dove $\beta' \dotplus \eta = \beta$ e quindi $\lambda \in K^{(\beta')}$. Poiché β' è arbitrario si ha che $\lambda \in \bigcap_{\beta'<\beta} K^{(\beta')} = K^{(\beta)}$. □

Corollario 6.11. *Se $K = \alpha \dotplus 1 < \omega_1$ ha come forma normale di Cantor*

$$\gamma = \omega^{\cdot\xi_1} \cdot n_1 \dotplus \cdots \dotplus \omega^{\cdot\xi_k} \cdot n_k \dotplus n_{k+1}$$

con $\xi_1 > \cdots > \xi_k > 0$ e $n_1, \ldots, n_k, n_{k+1} > 0$, allora $\gamma(K) = \xi_1$, $K^{(\xi_1)} = \{\omega^{\cdot\xi_1}, \omega^{\cdot\xi_1} \cdot 2, \ldots, \omega^{\cdot\xi_1} \cdot n_1\}$ e quindi $n(K) = n_1$.

Dal Corollario 6.11 e dal Teorema 6.5 otteniamo il seguente teorema di classificazione dei compatti metrici numerabili.

Teorema 6.12. *Gli spazi compatti metrici numerabili non vuoti sono, a meno di omeomorfismi, tutti e soli gli ordinali $\omega^{\cdot\gamma} \cdot n \dotplus 1$, con $0 < n < \omega$ e $\gamma < \omega_1$.*

Considerando α e β come spazi topologici, ci chiediamo: A quali condizioni deve soddisfare $f\colon \alpha \to \beta$ affinché sia una funzione **continua**? Chiaramente la continuità non è mai un problema sui $\gamma < \alpha$ ordinali successori, in

quanto sono punti isolati. Supponiamo quindi $\gamma < \alpha$ sia limite. Se $f(\gamma)$ è un successore, allora per la continuità di f, c'è un intervallo $[\beta;\gamma]$ che è mandato da f nel singoletto $\{f(\gamma)\}$; in altre parole: f è definitivamente costante al di sotto di γ. Se $f(\gamma)$ è limite, allora per ogni $\delta < f(\gamma)$ c'è un $\beta < \gamma$ tale che l'intervallo $[\beta;\gamma]$ è mandato da f nell'intervallo $[\delta; f(\gamma)]$.

Esercizio 6.13. (i) Dimostrare che se $f\colon \alpha \to \beta$ è crescente, allora f è continua (nel senso della topologia) se e solo se è continua nel senso della (24), cioè

$$\forall \lambda < \alpha \big(\lambda \text{ limite} \Rightarrow f(\lambda) = \sup_{\beta<\lambda} f(\beta)\big)\,. \tag{29}$$

(ii) Dimostrare che se ξ e λ sono ordinali limite, $f\colon \xi \to \lambda$ è crescente e continua e $\bigcup \mathrm{ran}(f) = \lambda$, allora $\mathrm{ran}(f)$ è un chiuso di λ.

Vale anche il converso della parte (ii) dell'Esercizio 6.13: se λ è limite e $C \subseteq \lambda$ è chiuso, allora esiste un'unica $f\colon \kappa \to \lambda$ continua e crescente con κ limite tali che $\mathrm{ran}(f) = C$ (Esercizio 6.16). Gli intervalli $[\beta;\gamma)$, al variare di β e γ definiscono una topologia su Ord la cui restrizione su ogni α induce la topologia qui definita. L'unico problema è che alcuni aperti di Ord sono classi proprie e quindi non appartengono a nessuna collezione. In altre parole, in MK (e a maggior ragione in ZF) non è consentito definire questa topologia. Tuttavia diremo che una classe $C \subseteq \mathrm{Ord}$ è chiusa se soddisfa (v) dell'Esercizio 6.6 e che una funzione crescente $f\colon \mathrm{Ord} \to \mathrm{Ord}$ è continua se soddisfa (29).

Esercizi

Esercizio 6.14. Dimostrare che ogni funzione $f\colon \omega \to \omega$ è continua.

Esercizio 6.15. Dimostrare che la funzione $\mathrm{Ord} \to \mathrm{Ord}$, $\alpha \mapsto \alpha \dotplus 1$, è discontinua su tutti gli ordinali limite.

Esercizio 6.16. Sia $C \subseteq \lambda$ chiuso, λ limite e $f\colon \kappa \to C$ la funzione che enumera C. Allora $f\colon \kappa \to \lambda$ è crescente e continua.

7. Successioni finite

Le operazioni aritmetiche su ω ci permettono di dimostrare rigorosamente fatti sulle successioni finite.

Definizione 7.1. Se s e t sono funzioni che hanno per dominio un ordinale e tali che $\mathrm{dom}(s) < \omega$ e $\mathrm{dom}(t) \leq \omega$, la **concatenazione** di s e t è la funzione

$s^\frown t$ di domino $\mathrm{dom}(s) \dot{+} \mathrm{dom}(t) \leq \omega$ definita da

$$s^\frown t(n) = \begin{cases} s(n) & \text{se } n \in \mathrm{dom}(s), \\ t(m) & \text{se } n = \mathrm{dom}(s) \dot{+} m. \end{cases}$$

Quindi se $s = \langle a_0, a_1, \ldots, a_{n-1} \rangle$ e $t = \langle b_0, b_1, \ldots, \rangle$, allora

$$s^\frown t = \langle a_0, a_1, \ldots, a_{n-1}, b_0, b_1, \ldots, \rangle \,.$$

Ricordiamo che $X^{<\omega}$ è l'insieme di tutte le successioni finite di elementi di X —vedi(11).

Esercizio 7.2. (i) Verificare che la definizione è ben data e che $\mathrm{dom}(s^\frown t) = \omega$ se e solo se $\mathrm{dom}(t) = \omega$.

(ii) Dimostrare che l'operazione di concatenazione su ${}^{<\omega}X$ è associativa.

Le strutture algebriche ${}^{<\omega}X$ con l'operazione di concatenazione si dicono **semigruppi liberi**.

Data una struttura algebrica (gruppo, anello, etc,) su un insieme A, e dato un $B \subseteq A$, la sotto-struttura generata da B è il più piccolo $C \neq \emptyset$ chiuso sotto le operazioni e tale che $B \subseteq C \subseteq A$. Nel caso degli anelli unitari, per esempio, si considera R l'anello primo di A (vale a dire il sotto-anello generato dall'unità) e l'insieme di tutti i polinomi in più variabili a coefficienti in R,

$$\bigcup_n R[X_1, \ldots, X_n] \,.$$

Il sotto-anello di A generato da B è l'insieme degli elementi della forma $p(b_1, \ldots, b_n)$ dove $p(X_1, \ldots, X_n) \in R[X_1, \ldots, X_n]$ e $b_1, \ldots, b_n \in B$. Queste costruzioni possono essere formulate in generale.

Definizione 7.3. Sia S un insieme non vuoto e sia $a\colon S \to \omega$ una funzione. L'insieme $\mathrm{Words}(S, a)$ delle **parole** su (S, a) è il più piccolo $W \subseteq S^{<\omega}$ contenente

$$\{\, \langle s \rangle \mid a(s) = 0 \,\}$$

e chiuso sotto l'operazione

$$s \in S \;\wedge\; w_1, \ldots, w_m \in W \;\wedge\; a(s) = m \;\Rightarrow\; \langle s \rangle^\frown w_1{}^\frown \ldots {}^\frown w_m \in W \,.$$

Lemma 7.4. *L'insieme* $\mathrm{Words}(S, a)$ *delle parole su* (S, a) *è* $\bigcup_n \mathrm{Words}_n(S, a)$ *dove*

$$\begin{aligned} \mathrm{Words}_0 &= \{\, \langle s \rangle \mid s \in S \;\wedge\; a(s) = 0 \,\} \\ \mathrm{Words}_{n+1} &= W_n \cup \{ \langle s \rangle^\frown w_1{}^\frown \cdots {}^\frown w_m \mid s \in S \wedge \\ &\qquad\qquad w_1, \ldots, w_m \in \mathrm{Words}_n \wedge a(s) = m \}. \end{aligned}$$

Dimostrazione. Per induzione su n si dimostra che $\text{Words}_n \subseteq \text{Words}$ e $\text{Words}_n \subseteq \text{Words}_m$, se $n < m$. Quindi è sufficiente dimostrare che se $w_1, \ldots, w_m \in \bigcup_n \text{Words}_n$, $a(s) = m$ allora $z = \langle s \rangle^\frown w_1{}^\frown \ldots {}^\frown w_m$ appartiene a $\bigcup_n \text{Words}_n$: ma se k è sufficientemente grande per cui $w_1, \ldots, w_m \in \text{Words}_k$, allora $z \in \text{Words}_{k+1} \subseteq \bigcup_n \text{Words}_n$. □

Definizione 7.5. L'**altezza** di una parola $w \in \text{Words}(S, a)$ è il più piccolo n tale che $w \in \text{Words}_n$.

$$\text{ht}\colon \text{Words}(S, a) \to \omega$$

è la funzione altezza.

Spesso, quando ciò non comporta confusione, una stringa di elementi di S è denotata con $s_1 s_2 \ldots s_n$ invece del più corretto, ma pesante, $\langle s_1, s_2, \ldots, s_n \rangle$. Chiaramente, non tutti gli elementi di $S^{<\omega}$ sono parole di (S, a). Se $w = s_1 s_2 \ldots s_n \in S^{<\omega}$, definiamo

$$\varphi(w) = \varphi(s_1) + \cdots + \varphi(s_n)$$

dove $\varphi(s) = a(s) - 1$, se $s \in S$.[14] Innanzitutto diamo una condizione necessaria e sufficiente affinché una stringa sia una parola.

Proposizione 7.6. *Sia $w = s_1 s_2 \ldots s_n \in S^{<\omega}$. Allora $w \in \text{Words}(S, a)$ se e solo se*

$$\varphi(w) = -1 \quad \wedge \quad \forall m < n \ \varphi(s_1 s_2 \ldots s_m) \geq 0\,. \tag{30}$$

Dimostrazione. Cominciamo col dimostrare per induzione su $\text{ht}(w)$ che se $w \in \text{Words}$ allora (30) vale. Se $w \in S$ e quindi $a(w) = 0$ il risultato è immediato, quindi posso supporre che $w = \langle s \rangle^\frown z_1{}^\frown \ldots {}^\frown z_n$ con $a(s) = m$. Per ipotesi induttiva $\varphi(z_1) = \cdots = \varphi(z_n) = -1$ e quindi $\varphi(w) = n - 1 + (-1) \cdot n = -1$. Inoltre, se w' è un segmento iniziale di w, allora $w' = \langle s \rangle^\frown z_1{}^\frown \ldots {}^\frown z_k{}^\frown u$, con $k < n$ e u un segmento iniziale di z_{k+1}. Per ipotesi induttiva applicata a z_{k+1}, si ha che $\varphi(u) \geq 0$ e quindi $\varphi(w') = \varphi(s) + \varphi(z_1) + \cdots + \varphi(z_k) + \varphi(u) = n - 1 + (-1) \cdot k + \varphi(u) \geq 0$.

Sia $w = s_1 s_2 \ldots s_n \in S^{<\omega}$. Dimostriamo per induzione su n che se w soddisfa (30), allora w è una parola. Se $n = 1$, allora $w = s_1$, quindi $-1 = \varphi(w) = a(s_1) - 1$, cioè $a(s_1) = 0$ e w è una parola. Possiamo quindi supporre $n > 1$. Sia $\varphi(s_1) = m \geq 0$ e quindi $a(s_1) = m + 1$. Distinguiamo due casi: $m = 0$ e $m > 0$. Se $m = 0$, allora la stringa $s_2 s_3 \ldots s_n$ soddisfa ancora (30) e quindi per ipotesi induttiva è una parola. Poiché $a(s_1) = 1$, segue che $s_1 s_2 \ldots s_n$ è una parola. Supponiamo quindi che $m > 0$. Poiché

[14] Usiamo qui qualche banale proprietà sui numeri interi relativi, anche se, formalmente, questi saranno introdotti solo nel capitolo seguente.

$\varphi(s_2 s_3 \dots s_n) = -m-1$ è possibile suddividere la stringa $s_2 s_3 \dots s_n$ in blocchi consecutivi $z_1, z_2, \dots, z_k, u$

$$\underbrace{\boxed{s_2 \dots s_{j_1}}}_{z_1}\underbrace{\boxed{s_{j_1+1} \dots s_{j_2}}}_{z_2} \cdots\cdots \underbrace{\boxed{s_{j_{k-1}+1} \dots s_{j_k}}}_{z_k}\underbrace{\boxed{s_{j_k+1} \dots s_n}}_{u}$$

di modo che $\varphi(z_i) = -1$ $(i = 1, \dots, k)$, $\varphi(u) \neq -1$ e che ogni segmento iniziale proprio v di un z_i o di u soddisfi $\varphi(v) \geq 0$. Ne segue che $\varphi(u) = \varphi(s_{j_k+1} \dots s_{n-1}) + \varphi(s_n) \geq 0$, dato che $\varphi(s_n) \geq -1$. Dimostreremo che $k = m + 1$ e che u è vuota e quindi

$$w = s_1{}^\frown z_1 \dots {}^\frown z_k$$

è una parola. Da

$$\begin{aligned} -1 &= \varphi(s_1 s_2 \dots s_n) \\ &= \varphi(s_1) + \varphi(z_1) + \cdots + \varphi(z_k) + \varphi(u) \\ &= m - k + \varphi(u) \end{aligned}$$

otteniamo che $k > m$. Se $k > m+1$, allora $\varphi(s_1{}^\frown z_1{}^\frown \dots {}^\frown z_{m+1}) = -1$, contro l'ipotesi (30), per cui otteniamo che $k = m+1$ e quindi u è la sequenza vuota e $w = s_1{}^\frown z_1{}^\frown \dots {}^\frown z_k$. □

Corollario 7.7. $\forall w, z \in \mathrm{Words}(S, a)\,(w \subseteq z \Rightarrow w = z)$.

Questo corollario ci garantisce che le parole su un insieme S possono essere lette in un unico modo. Quindi se dobbiamo dimostrare che ogni parola $w \in \mathrm{Words}$ gode si una certa proprietà, è possibile dimostrare ciò procedendo per induzione su $\mathrm{ht}(w)$; o, equivalentemente, dimostrando che tutte le parole in Words_0 godono di questa proprietà e che se tutte le parole in Words_n godono di questa proprietà, allora questo vale anche per le parole in Words_{n+1}.

7.A. Un'applicazione. Se $\mathcal{F}$ è una collezione di funzioni finitarie su X e $Y \subseteq X$, sia

$$S = \mathcal{F} \cup Y$$

e poniamo

$$a(s) = \begin{cases} 0 & \text{se } s \in Y, \\ \mathrm{ar}(s) & \text{se } s \in \mathcal{F}. \end{cases}$$

Usando la notazione del Lemma 7.4, osserviamo che $\mathrm{Words}_0 = Y \subseteq X$ e che se $w \in \mathrm{Words}_{n+1}$ allora esistono e sono unici $f \in \mathcal{F}$ e $w_1, \dots, w_m \in \mathrm{Words}_n$ tali che $w = \langle f \rangle{}^\frown w_1{}^\frown \dots {}^\frown w_m$, Per l'unicità della lettura delle parole, possiamo definire una mappa

$$\Phi\colon \mathrm{Words} \to X$$

ponendo $\Phi \restriction \mathrm{Words}_0 =$ l'identità su Y e

$$\Phi(\langle f\rangle^\frown w_1{}^\frown \ldots {}^\frown w_m) = f(\Phi(w_1),\ldots,\Phi(w_m))\,.$$

Sia $Y_n = \Phi[\mathrm{Words}_n]$. È facile verificare che

$$\begin{aligned} Y_0 &= Y \\ Y_{k+1} &= Y_k \cup \{\, f(x_1,\ldots,x_n) \mid f\in\mathcal{F} \wedge \mathrm{ar}(f)=n \wedge x_1,\ldots,x_n\in Y_k \,\} \end{aligned}$$

e che $Y_0 \subseteq Y_1 \subseteq \ldots$. Se $f \in \mathcal{F}$ è n-aria e $x_0,\ldots,x_{n-1} \in \bigcup_{k\in\mathbb{N}} Y_k$, fissiamo un $\bar{k}$ sufficientemente grande tale che $x_0,\ldots,x_{n-1}\in Y_{\bar{k}}$: allora $f(x_0,\ldots,x_{n-1}) \in Y_{\bar{k}+1} \subseteq \bigcup_{k\in\mathbb{N}} Y_k$. Ne consegue che $\bigcup_n Y_n$ è chiuso sotto $\mathcal{F}$ e quindi $\bigcup_n Y_n \supseteq \mathrm{Cl}_{\mathcal{F}}(Y)$, la chiusura di Y sotto $\mathcal{F}$ definita a pagina 13. Viceversa, è immediato verificare che $\bigcup_n Y_n \subseteq \mathrm{Cl}_{\mathcal{F}}(Y)$. Abbiamo quindi dimostrato che:

Proposizione 7.8. *Se $\mathcal{F}$ è una famiglia di funzioni finitarie su X e $Y\subseteq X$, allora*

$$\mathrm{Cl}_{\mathcal{F}}(Y) = \bigcup_{k\in\mathbb{N}} Y_k\,,$$

dove gli Y_n sono come sopra.

7.B. Alberi. Dato un insieme $\mathcal{F}$ di funzioni finitarie su un qualche insieme X abbiamo visto come descrivere tutte le funzioni finitarie su X ottenibili per composizione di funzioni in $\mathcal{F}$: basta considerare l'insieme delle parole su S dove $S = \mathcal{F}\cup\{\, x_n \mid n\in\omega\,\}$, $a\colon S\to\omega$ la funzione arietà su $\mathcal{F}$ e $a(x_n)=0$, per ogni variabile x_n. Per esempio, usando la Proposizione 7.6, possiamo verificare che se x,y,z,u sono variabili e se $f,g,h\in\mathcal{F}$ sono, rispettivamente, 1-aria, 2-aria e 3-aria, la sequenza

$$hfhxzgfuygxfgzyfhfzhyuxz \tag{31}$$

è una parola di (S,a) che descrive una funzione 4-aria su X. Cerchiamo di descrivere questa funzione, cioè questa parola, a partire dalle funzioni che la compongono, cioè dalle sue sotto-parole. Cominciamo con l'individuare le sotto-parole di altezza 1, cioè quelle individuate da una funzione applicata a variabili...

$$h\,f\,h\,x\,z\,g\,\underbrace{f\,u}\,y\,g\,x\,f\,\underbrace{g\,z\,y}\,f\,h\,\underbrace{f\,z}\,\underbrace{h\,y\,u\,x}\,z$$

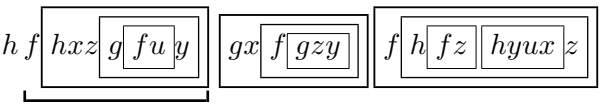
...passiamo poi a quelle di altezza 2...

$$h\,f\,h\,x\,z\,\underbrace{g\,\boxed{f\,u}\,y}\,g\,x\,\underbrace{f\,\boxed{g\,z\,y}}\,f\,\underbrace{h\,\boxed{f\,z}\,\boxed{h\,y\,u\,x}\,z}$$

...poi a quelle di altezza 3...

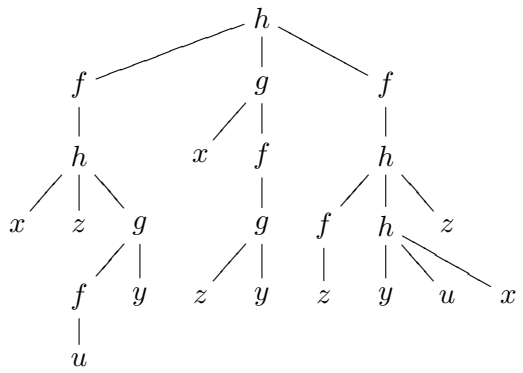
$$\underbrace{h\,f\,h\,x\,z\,\boxed{g\,\boxed{f\,u}\,y}}\,\underbrace{g\,x\,\boxed{f\,\boxed{g\,z\,y}}}\,\underbrace{f\,\boxed{h\,\boxed{f\,z}\,\boxed{h\,y\,u\,x}\,z}}$$

... poi a quella di altezza 4...

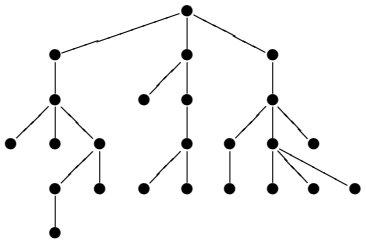


...e a questo punto vediamo che c'è un h seguita da 3 parole (la prima di altezza 4, le altre due di altezza 3) e che quindi la stringa (31) è una parola di altezza 5. Questo algoritmo suggerisce una descrizione più perspicua della stringa:

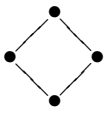
(32)



Questa descrizione della parola (31) si dice ad **albero etichettato**. L'idea è di partire da una struttura del tipo



detta albero, cioè un ordine finito con elemento massimo e tale che i segmenti finali sono linearmente ordinati—in altre parole l'ordinamento non può contenere un sotto-ordinamento a "rombo":



Gli elementi dell'albero si dicono **nodi**, quelli minimali si dicono **nodi terminali**, mentre quello massimo si dice **radice**.[15] Per costruire una parola di (S, a) si parte da un albero e da una funzione dai nodi dell'albero in S. Tale funzione deve soddisfare i seguenti requisiti:

[15]La botanica insiemistica è piuttosto bizzarra, visto che gli alberi crescono all'ingiù. Forse li si dovrebbe chiamare *radici*, ma allora ci sarebbe un problema per denotare il nodo massimo.

- ai nodi terminali si associano $s \in S$ tali che $a(s) = 0$,
- ad un nodo non terminale si associa un $s \in S$ tali che $a(s) =$ il numero di successori del nodo.

Formalmente, l'insieme

$$\mathrm{LTr}(S,a) = \bigcup_n \mathrm{LTr}_n(S,a)$$

degli **alberi etichettati** su (S,a) è definito da

$$\mathrm{LTr}_0 = \{\, \langle s \rangle \mid s \in S \ \wedge\ a(s) = 0 \,\}$$
$$\mathrm{LTr}_{n+1} = \mathrm{LTr}_n \cup \{\, \langle s, t_1, \ldots, t_m \rangle \mid s \in S \ \wedge\ a(s) = m \ \wedge\ t_1, \ldots, t_m \in \mathrm{LTr}_n \,\}.$$

La funzione **altezza** $\mathrm{ht}\colon \mathrm{LTr} \to \omega$ è definita da

$$\mathrm{ht}(t) = \min \{\, n \in \omega \mid t \in \mathrm{LTr}_n \,\}$$

È facile verificare che c'è una bijezione

$$\Phi\colon \mathrm{Words}(S,a) \to \mathrm{LTr}(S,a)$$

che preserva le altezze e che quindi dimostra che $\mathrm{Words}_n(S,a)$ è in bijezione con $\mathrm{LTr}_n(S,a)$ (Esercizio 7.12). Ne segue che tanto Words quanto LTr sono formalizzazioni equivalenti del concetto intuitivo di parola di (S,a).

Esercizi

Se $z, w \in \mathrm{Words}(S,a)$ diremo che

(i) z è una **sotto-parola** di w se $\mathrm{lh}(w) > 0$ e per qualche $n < \mathrm{lh}(w)$

$$\forall m < \mathrm{lh}(z)\, (z(m) = w(m \dot{+} n)).$$

(ii) z è una **sillaba** di w se $\mathrm{lh}(w) > 0$ e $w = \langle s \rangle^\frown w_1{}^\frown \ldots {}^\frown w_m$, con $m = a(s)$ e $z = w_i$ per qualche $i \leq m$.

Esercizio 7.9. Dimostrare che z è una sotto-parola di w se e solo se esistono parole $z_1, \ldots, z_n \in \mathrm{Words}$ tali che $z = z_1$, $w = z_n$ e z_i è una sillaba di z_{i+1}.

Esercizio 7.10. Dimostrare che $\mathrm{ht}(w) = \max \{\, \mathrm{ht}(z) \mid z \text{ è una sillaba di } w \,\}$.

Esercizio 7.11. Dimostrare che $\mathrm{LTr}(S,a)$ è il più piccolo insieme T contenente $\{\, \langle s \rangle \mid s \in S \ \wedge\ a(s) \,\}$ tale che $t_1, \ldots, t_m \in T \wedge s \in S \wedge a(s) = m \Rightarrow \langle s, t_1, \ldots, t_m \rangle \in T$.

Esercizio 7.12. Verificare che $\mathrm{Words}(S,a)$ e $\mathrm{LTr}(S,a)$ sono in bijezione mediante una mappa che preserva le altezze.

8. Aritmetica cardinale (I)

Un insieme X si dice **bene ordinabile** se esiste un buon ordine su X.

Esercizio 8.1. Dimostrare che X è bene ordinabile se e solo se X è immagine suriettiva di un ordinale, cioè

$$\exists \alpha \, \exists f \, (f \colon \alpha \twoheadrightarrow X)$$

se e solo se è iniettabile in un ordinale, cioè

$$\exists \alpha \, \exists f \, (f \colon X \rightarrowtail \alpha) \, .$$

Quindi se X è bene ordinabile e Y è in bijezione con (o anche solo: immagine suriettiva di) X, allora Y è bene ordinabile. Viceversa, se Y è bene ordinabile e X si inietta in Y, allora X è bene ordinabile.

Definizione 8.2. Se X è bene ordinabile la **cardinalità di** X è il più piccolo ordinale $|X|$ in bijezione con X. Quindi, la cardinalità di un insieme è un cardinale.

Vedremo nella sezione 14 che l'Assioma di Scelta AC implica che *ogni* insieme è bene ordinabile e quindi, sotto AC, $|X|$ è definito per tutti gli X.

Esercizio 8.3. Se X e Y sono bene ordinabili, allora $|X| \leq |Y|$ se e solo se $\exists f (f \colon X \rightarrowtail Y)$.

La **somma cardinale** ed il **prodotto cardinale** sono le operazioni binarie Card $\times$ Card $\to$ Card definite da

$$\begin{aligned} \kappa + \lambda &= |\kappa \times \{0\} \cup \lambda \times \{1\}| \\ \kappa \cdot \lambda &= |\kappa \times \lambda| \, . \end{aligned}$$

La definizione è ben posta dato che $\kappa \times \{0\} \cup \lambda \times \{1\}$ e $\kappa \times \lambda$ sono bene ordinabili (Esercizio 3.28). È immediato verificare che la somma e il prodotto cardinale sono operazioni commutative e per (25) e (26) la cardinalità della *somma ordinale* e del *prodotto ordinale* di due ordinali è, rispettivamente, la somma e prodotto *cardinale* delle loro cardinalità, cioè

$$|\alpha \dotplus \beta| = |\alpha| + |\beta| \quad \text{e} \quad |\alpha \cdot \beta| = |\alpha| \cdot |\beta| \, . \tag{33}$$

Esercizio 8.4. Dimostrare che la somma e il prodotto cardinale sono operazioni associative e che vale la proprietà distributiva del prodotto rispetto alla somma.

Se $\kappa, \lambda \geq 2$, la funzione

$$f \colon \kappa \times \{0\} \cup \lambda \times \{1\} \to \kappa \times \lambda$$

data da $f(\alpha, 0) = (\alpha, 0)$ e

$$f(\beta, 1) = \begin{cases} (0, \beta) & \text{se } \beta \neq 0, \\ (1, 1) & \text{se } \beta = 0, \end{cases}$$

è iniettiva e quindi

$$\kappa + \lambda \leq \kappa \cdot \lambda \,. \tag{34}$$

Osserviamo che per la parte (a) della Proposizione 3.22, questa formula vale anche quando uno dei due cardinali è 1 e l'altro è $\geq \omega$. Riassumendo, se κ e λ sono cardinali diversi da 0 e $2 \leq \min(\kappa, \lambda)$ oppure $1 = \min(\kappa, \lambda)$ e $\omega \leq \max(\kappa, \lambda)$, allora

$$\max(\kappa, \lambda) \leq \kappa + \lambda \leq \kappa \cdot \lambda \leq \max(\kappa, \lambda) \cdot \max(\kappa, \lambda) \,. \tag{35}$$

Lemma 8.5. (a) $\forall m, n \in \omega \, (m + n = m \dot{+} n \in \omega)$.
(b) $\forall m, n \in \omega \, (m \cdot n = m \cdot n \in \omega)$.

Dimostrazione. Cominciamo col dimostrare per induzione su n che

$$\forall m \in \omega \, (m \dot{+} n \in \omega) \quad \text{e} \quad \forall m \in \omega \, (m \cdot n \in \omega) \,.$$

Se $n = 0$ allora $m \dot{+} n = n$; se $n = \mathbf{S}(k)$ allora $m \dot{+} n = \mathbf{S}(m \dot{+} k) \in \omega$, per ipotesi induttiva e poiché ω è chiuso per $\mathbf{S}$. Il caso del prodotto è lasciato per esercizio.

Per (33) e il Teorema 3.17 si ha

$$m \dot{+} n = |m \dot{+} n| = |m| + |n| = m + n$$

e, analogamente, $m \cdot n = m \cdot n$. □

Esercizio 8.6. Dimostrare che se $A_1, \ldots, A_n$ sono insiemi finiti, allora anche $A_1 \cup \cdots \cup A_n$ e $A_1 \times \cdots \times A_n$ sono finiti.

Esercizio 8.7. Il **buon ordine di Gödel su** Ord × Ord è

$$(\alpha, \beta) <_{\mathrm{G}} (\gamma, \delta) \Leftrightarrow$$
$$\Big[\max(\alpha, \beta) < \max(\gamma, \delta) \vee \big(\max(\alpha, \beta) = \max(\gamma, \delta) \wedge (\alpha, \beta) <_{\mathrm{lex}} (\gamma, \delta)\big)\Big]$$

Verificare che $<_{\mathrm{G}}$ è un buon-ordine su Ord × Ord e che $\alpha \times \alpha$ è un segmento iniziale, per ogni $\alpha \in \mathrm{Ord}$.

Teorema 8.8. *Sia κ un cardinale infinito. Allora* $\mathrm{ot}(\kappa \times \kappa, <_{\mathrm{G}}) = \kappa$ *e* $|\kappa \times \kappa| = \kappa$.

Dimostrazione. Per induzione su $\kappa \geq \omega$. Sia $\alpha < \kappa$. Se $\alpha < \omega$, allora $|\alpha \times \alpha| = \alpha \cdot \alpha < \omega$ per il Lemma precedente. Se invece $\omega \leq \alpha$, allora $\omega \leq |\alpha| < \kappa$ e quindi, per ipotesi induttiva, $|\alpha| \times |\alpha|$ è di cardinalità $|\alpha|$.

Poiché $|\alpha|\times|\alpha|$ è in bijezione con $\alpha\times\alpha$, otteniamo che $|\alpha\times\alpha|<\kappa$. Abbiamo quindi verificato che

$$\forall\alpha<\kappa\,(|\alpha\times\alpha|<\kappa)\,.$$

Fissiamo $\alpha,\beta<\kappa$. L'insieme dei $<_{\mathrm{G}}$-predecessori di (α,β)

$$X(\alpha,\beta)=\{\,(\alpha',\beta')\in\kappa\times\kappa\mid(\alpha',\beta')<_{\mathrm{G}}(\alpha,\beta)\,\}$$

è contenuto in $\nu\times\nu$, dove $\nu=\max\{\alpha,\beta\}+1$, quindi $|X(\alpha,\beta)|\leq|\nu\times\nu|<\kappa$. Ne segue che il tipo d'ordine di $X(\alpha,\beta)$ è $<|X(\alpha,\beta)|^+\leq\kappa$. Abbiamo quindi dimostrato che

$$\forall\alpha,\beta<\kappa\,(\mathrm{ot}(X(\alpha,\beta),<_{\mathrm{G}})<\kappa)$$

e quindi $\mathrm{ot}(\kappa\times\kappa,<_{\mathrm{G}})\leq\kappa$. D'altra parte la funzione

$$\langle\kappa,<\rangle\to\langle\kappa\times\kappa,<_{\mathrm{G}}\rangle\qquad\alpha\mapsto(\alpha,0)$$

è strettamente crescente e quindi vale la disuguaglianza inversa, da cui $\kappa=\mathrm{ot}(\kappa\times\kappa,<_{\mathrm{G}})$ e $|\kappa\times\kappa|=\kappa$. □

Quindi se κ e λ sono cardinali diversi da 0 e $2\leq\min(\kappa,\lambda)$ oppure $1=\min(\kappa,\lambda)$, la (35) e il Teorema 8.8 implicano

$$\max(\kappa,\lambda)=\kappa+\lambda=\kappa\cdot\lambda\,.$$

In altre parole: la somma ed il prodotto di cardinali sono operazioni banali.

Ricordiamo che per ogni X, l'insieme potenza $\mathscr{P}(X)$ è in bijezione con ${}^X2$: ad ogni $Y\subseteq X$ associamo la sua **funzione caratteristica** $\boldsymbol{\chi}_Y^X=\boldsymbol{\chi}_Y\colon X\to 2$

$$\boldsymbol{\chi}_Y(x)=\begin{cases}1 & \text{se } x\in Y,\\ 0 & \text{altrimenti.}\end{cases}$$

Teorema 8.9 (Cantor)**.** *Non esiste alcuna suriezione da X su $\mathscr{P}(X)$.*

Dimostrazione. Sia $\pi\colon X\twoheadrightarrow\mathscr{P}(X)$ una suriezione e sia

$$Y=\{\,x\in X\mid x\notin\pi(x)\,\}\,.$$

Fissiamo un $\bar{x}\in X$ tale che $\pi(\bar{x})=Y$. Allora $\pi(\bar{x})\in Y\Leftrightarrow\pi(\bar{x})\notin Y$: contraddizione. □

Ricordiamo che due insiemi si dicono equipotenti (pag.12) se sono in bijezione—questa è una relazione d'equivalenza su V le cui classi sono classi proprie (Esercizio 1.26).

Esercizio 8.10. Siano X, Y, Z e W degli insiemi. Dimostrare che:

(i) Se X è equipotente ad Y e Z è equipotente a W, allora $X\times Z$ è equipotente a $Y\times W$.

(ii) Se X è equipotente ad Y, allora $\mathscr{P}(X)$ è equipotente a $\mathscr{P}(Y)$.

(iii) Se X è equipotente ad Y e Z è equipotente a W, allora X^Z è equipotente a Y^W.

(iv) Se $Y \cap Z = \emptyset$, allora $X^{(Y \cup Z)}$ è in bijezione con $X^Y \times X^Z$.

(v) $(X^Y)^Z$ è in bijezione con $X^{Z \times Y}$.

Proposizione 8.11. *Se $2 \leq \kappa \leq \lambda$ e λ è un cardinale infinito, allora gli insiemi*

$$ {}^{\lambda}2, \qquad {}^{\lambda}\kappa, \qquad {}^{\lambda}\lambda $$

sono in bijezione.

Dimostrazione. Poiché ${}^{\lambda}2 \subseteq {}^{\lambda}\kappa \subseteq {}^{\lambda}\lambda$, per il teorema di Shröder-Bernstein è sufficiente dare un'iniezione ${}^{\lambda}\lambda \rightarrowtail {}^{\lambda}2$. Per il Teorema 8.8 e la parte (ii) dell'Esercizio 8.10 $\mathscr{P}(\lambda \times \lambda)$ è in bijezione con $\mathscr{P}(\lambda)$, quindi il risultato discende da ${}^{\lambda}\lambda \subseteq \mathscr{P}(\lambda \times \lambda)$. □

L'esponenziazione cardinale κ^{λ} è definita come $\left|{}^{\lambda}\kappa\right|$, la cardinalità dell'insieme delle $f \colon \lambda \to \kappa$. Tuttavia, se $\lambda \geq \omega$, per garantire che ${}^{\lambda}\kappa$ sia bene ordinabile è necessario usare l'Assioma di Scelta, che introdurremo nel prossimo capitolo. Per questo motivo ci limiteremo al caso $\lambda < \omega$. Sia κ è un cardinale infinito e sia $f \colon \langle \kappa \times \kappa, <_{\mathrm{G}} \rangle \to \langle \kappa, < \rangle$ l'isomorfismo. Definiamo per ricorsione su $n \geq 1$ delle bijezioni $j_n \colon {}^{n}\kappa \to \kappa$ come segue. Poniamo $j_1(\langle \alpha \rangle) = \alpha$ e poiché la funzione ${}^{n+1}\kappa \to {}^{n}\kappa \times \kappa$, $s \mapsto (s \restriction n, s(n))$, è una bijezione, possiamo definire j_{n+1} mediante il diagramma

$$ \begin{array}{ccccccc} & & & \overset{j_{n+1}}{\frown} & & & \\ {}^{n+1}\kappa & \longrightarrow & {}^{n}\kappa \times \kappa & \longrightarrow & \kappa \times \kappa & \longrightarrow & \kappa \\ s & \longmapsto & (s \restriction n, s(n)) & \longmapsto & (j_n(s \restriction n), s(n)) & \longmapsto & f(j_n(s \restriction n), s(n)) \,. \end{array} $$

Quindi, se κ è un cardinale infinito, allora $|{}^{n}\kappa| = \kappa$. Inoltre la funzione $j_{\omega} \colon {}^{<\omega}\kappa \to \omega \times \kappa$

$$ j_{\omega}(s) = \begin{cases} (0,0) & \text{se } s \neq \emptyset, \\ (n, j_n(s)) & \text{se } \mathrm{lh}(s) = n > 0, \end{cases} $$

è iniettiva e quindi $|{}^{<\omega}\kappa| = \kappa$. Abbiamo quindi dimostrato che

Teorema 8.12. *Se X è bene ordinabile e infinito, allora $|{}^{<\omega}X| = |X|$. In particolare, l'insieme delle sequenze finite di naturali ${}^{<\omega}\omega$ è numerabile.*

Esercizi

Esercizio 8.13. Dimostrare che l'esponenziazione ordinale e cardinale coincidono sui naturali,

$$\forall n, m \in \omega \, (n^m = n^{\cdot m} \in \omega) \, .$$

Esercizio 8.14. Dimostrare che un cardinale $\kappa \geq \omega$ è chiuso sotto somma, prodotto ed esponenziazione ordinale, cioè

$$\alpha, \beta < \kappa \quad \Rightarrow \quad \alpha \dot{+} \beta, \ \alpha \cdot \beta, \ \alpha^{\cdot \beta} < \kappa \, .$$

Se $\kappa \leq \lambda$ sono cardinali

$$[\lambda]^\kappa = \{ \, X \subseteq \lambda \mid |X| = \kappa \, \} \tag{36}$$

è la famiglia dei sottoinsiemi di λ di cardinalità κ.

Esercizio 8.15. Dimostrare che:

(i) $[\lambda]^\kappa$ è in bijezione con ${}^\kappa\lambda$,

(ii) $\{ \, f \in {}^\omega\omega \mid f$ è strettamente crescente $\}$ è in bijezione con $[\omega]^\omega$ e quindi con ${}^\omega\omega$.

Esercizio 8.16. Per il Teorema di Cantor 8.9 non esiste nessuna iniezione F dell'insieme delle parti $\mathscr{P}(X)$ in X. In questo esercizio esibiremo esplicitamente dei sottoinsiemi W e Z di X tali che $F(W) = F(Z)$.

Sia $F \colon \mathscr{P}(X) \to X$. Dimostrare che esiste un unico $W \subseteq X$ ed un unico buon ordine $\lhd$ su W tali che

(i) $F(\{ \, z \in W \mid z \lhd w \, \}) = w$, per ogni $w \in W$ e

(ii) $F(W) \in W$.

Concludere che F non è iniettiva, neppure se ristretta a

$$\mathscr{P}_{\mathrm{WO}}(X) = \{ \, Y \subseteq X \mid Y \text{ è bene ordinabile} \, \}$$

l'insieme dei sottoinsiemi bene ordinabili di X.

Capitolo II

Alcuni concetti di base della matematica

9. Il continuo

9.A. Gli assiomi di Dedekind-Peano. Nel capitolo precedente abbiamo costruito l'insieme $\mathbb{N}$ dei numeri naturali e le sue operazioni di somma e prodotto. La struttura $\langle \mathbb{N}, \mathbf{S} \restriction \mathbb{N}, 0\rangle$ soddisfa alcune proprietà che ora andiamo ad esplicitare.

Definizione 9.1. Una struttura $\langle M, S^M, 0^M\rangle$ soddisfa i **postulati** o **assiomi di Dedekind-Peano** se M è un insieme non vuoto, $0^M \in M$, $S^M\colon M \to M$ e valgono le seguenti proprietà:

(DPA.1) $\forall x \big(x \neq 0^M \Rightarrow \exists y \big(S^M(y) = x\big)\big)$,

(DPA.2) $\neg\exists x \big(S^M(x) = 0\big)$,

(DPA.3) $\forall x \forall y \big(x \neq y \Rightarrow S^M(x) \neq S^M(y)\big)$,

(DPA.4) $\forall P \subseteq M \big[\big(0^M \in P \ \wedge\ \forall x \big(x \in P \Rightarrow S^M(x) \in P\big)\big) \Rightarrow P = M\big]$.

Chiaramente $\langle \mathbb{N}, \mathbf{S} \restriction \mathbb{N}, 0\rangle$ soddisfa i postulati di Dedekind-Peano ed è, in un certo senso, l'unica struttura che li soddisfa.

Teorema 9.2. *Se $\langle M, S^M, 0^M\rangle$ soddisfa* (DPA.1)–(DPA.4)*, allora è isomorfo a $\langle \mathbb{N}, \mathbf{S} \restriction \mathbb{N}, 0\rangle$ e l'isomorfismo è unico. In altre parole esiste un'unica bijezione $F\colon \mathbb{N} \to M$ tale che $F(0) = 0^M$ e $F(\mathbf{S}(n)) = S^M(F(n))$.*

Dimostrazione. La $F\colon \mathbb{N} \to M$ è definita mediante la ricorsione $F(0) = 0^M$ e $F(\mathbf{S}(n)) = S^M(F(n))$ quindi esiste ed è unica per il Teorema 4.1. Dobbiamo verificare che F è iniettiva e suriettiva. Per assurdo fissiamo

$n < m \in \mathbb{N}$ tali che $F(n) = F(m)$, con n più piccolo possibile. Sia $m' \in \mathbb{N}$ tale che $m = \mathbf{S}(m')$. Allora $F(m) = S^M(F(m')) \neq 0^M$ per (DPA.2), da cui $F(n) \neq 0^M$ e quindi $n \neq 0$. Sia $n' \in \mathbb{N}$ tale che $\mathbf{S}(n') = n$: allora

$$S^M(F(n')) = F(n) = F(m) = S^M(F(m'))$$

e quindi per (DPA.2) $F(n') = F(m')$, contro la minimalità di n. Questo prova che F è iniettiva. L'insieme $P = \mathrm{ran}(F) \subseteq M$ soddisfa (DPA.4) quindi $\mathrm{ran}(F) = M$, cioè F è suriettiva. □

9.B. Gli interi e i razionali. L'insieme $\mathbb{Z}$ degli interi relativi è definito come $\mathbb{N} \times \mathbb{N}/E_{\mathbb{Z}}$ dove $E_{\mathbb{Z}}$ è la relazione di equivalenza definita da

$$(n, m)\ E_{\mathbb{Z}}\ (h, k) \Leftrightarrow n + k = h + m\,.$$

L'ordinamento $<^{\mathbb{Z}}$ e le operazioni di somma $+^{\mathbb{Z}}$ e prodotto $\cdot^{\mathbb{Z}}$ su $\mathbb{Z}$ sono definite da

$$\begin{aligned}
[(n, m)]_{E_{\mathbb{Z}}} <^{\mathbb{Z}} [(n', m')]_{E_{\mathbb{Z}}} &\ \Leftrightarrow\ n + m' < n' + m\,.\\
[(n, m)]_{E_{\mathbb{Z}}} +^{\mathbb{Z}} [(h, k)]_{E_{\mathbb{Z}}} &= [(n + h, m + k)]_{E_{\mathbb{Z}}}\,,\\
[(n, m)]_{E_{\mathbb{Z}}} \cdot^{\mathbb{Z}} [(h, k)]_{E_{\mathbb{Z}}} &= [(n \cdot h + m \cdot k, n \cdot k + m \cdot h)]_{E_{\mathbb{Z}}}\,.
\end{aligned}$$

La funzione

$$\mathbb{N} \to \mathbb{Z}, \qquad n \mapsto [(n, 0)]_{E_{\mathbb{Z}}}$$

è un morfismo iniettivo rispetto all'ordinamento e alle operazioni di somma e prodotto, quindi, a tutti gli effetti, $\mathbb{N}$ può essere identificato con un sottoinsieme di $\mathbb{Z}$ ed è possibile tralasciare l'apice $^{\mathbb{Z}}$ nella definizione di ordine, somma e prodotto. Gli interi della forma $[(n, 0)]_{E_{\mathbb{Z}}}$ si denotano con n e quelli della forma $[(0, n)]_{E_{\mathbb{Z}}}$ con $-n$. Chiaramente ogni $z \in \mathbb{Z}$ è della forma n oppure $-n$, con $n \in \mathbb{N}$, quindi la funzione $f\colon \mathbb{N} \to \mathbb{Z}$

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

è una bijezione. L'insieme $\mathbb{Q}$ è definito come $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})/E_{\mathbb{Q}}$ dove $E_{\mathbb{Q}}$ è la relazione di equivalenza

$$(x, y)\ E_{\mathbb{Q}}\ (z, w) \Leftrightarrow x \cdot w = y \cdot z\,.$$

L'ordinamento $<^{\mathbb{Q}}$ e le operazioni di somma $+^{\mathbb{Q}}$ e prodotto $\cdot^{\mathbb{Q}}$ su $\mathbb{Q}$ sono date da

$$\begin{aligned}
[(x, y)]_{E_{\mathbb{Q}}} <^{\mathbb{Q}} [(z, w)]_{E_{\mathbb{Q}}} &\ \Leftrightarrow\ x \cdot w < y \cdot z\,,\\
[(x, y)]_{E_{\mathbb{Q}}} +^{\mathbb{Q}} [(z, w)]_{E_{\mathbb{Q}}} &= [(x \cdot w + z \cdot y, y \cdot w)]_{E_{\mathbb{Q}}}\\
[(x, y)]_{E_{\mathbb{Q}}} \cdot^{\mathbb{Q}} [(z, w)]_{E_{\mathbb{Q}}} &= [(x \cdot z, y \cdot w)]_{E_{\mathbb{Q}}}
\end{aligned}$$

La funzione

$$\mathbb{Z} \to \mathbb{Q}, \qquad z \mapsto [(z, 1)]_{E_{\mathbb{Q}}}$$

è un morfismo iniettivo di anelli e preserva l'ordine e quindi $\mathbb{Z}$ viene identificato con un sottoinsieme di $\mathbb{Q}$. Come per gli interi tralasceremo l'apice $^{\mathbb{Q}}$ dai simboli di ordinamento, somma e prodotto. I razionali della forma $[(z,w)]_{E_{\mathbb{Q}}}$ si denotano con z/w e ogni razionale può essere scritto nella forma z/w con z e w relativamente primi. Quindi $\mathbb{Q}$ è in bijezione con un sottoinsieme di $\mathbb{Z}\times\mathbb{Z}$ che è a sua volta in bijezione con $\mathbb{N}\times\mathbb{N}$. Dal Teorema 8.8 ne segue che $\mathbb{Q}$ è in bijezione con un sottoinsieme di $\mathbb{N}$ e poiché $\mathbb{N}\rightarrowtail\mathbb{Z}\rightarrowtail\mathbb{Q}$, per il Teorema di Schröder–Bernstein 2.6 gli insiemi $\mathbb{N}$ e $\mathbb{Q}$ sono in bijezione.

$\langle\mathbb{Q},\leq\rangle$ è un ordine lineare numerabile senza primo o ultimo elemento. Il prossimo teorema ci assicura che (a meno di isomorfismi) è l'unico ordinamento siffatto.

Teorema 9.3 (Cantor)**.** *Se $\langle X,\trianglelefteq\rangle$ e $\langle Y,\leq\rangle$ sono ordini lineari, densi, numerabili, senza primo o ultimo elemento, allora sono isomorfi.*

Dimostrazione. Chiaramente è sufficiente dimostrare questo quando $Y=\mathbb{Q}$. Siano $X=\{\,x_n\mid n\in\omega\,\}$ e $\mathbb{Q}=\{\,q_n\mid n\in\omega\,\}$ enumerazioni senza ripetizioni. Costruiremo induttivamente delle funzioni p_n tali che

(a) $p_0\subseteq p_1\subseteq\dots$,

(b) $x_n\in\operatorname{dom}(p_{2n})\subset X$ e $q_n\in\operatorname{ran}(p_{2n+1})\subset Y$,

(c) $\operatorname{dom}(p_n)$ è finito e $p_n\colon\operatorname{dom}(p_n)\to\operatorname{ran}(p_n)$ è una bijezione che preserva l'ordine, vale a dire

$$\forall x,y\in\operatorname{dom}(p_n)\,(x\trianglelefteq y\Leftrightarrow p_n(x)\leq p_n(y))\,.$$

Una volta ottenuta la successione delle p_n, è possibile definire

$$F=\bigcup_n p_n\,.$$

La condizione (a) ci garantisce che F è una funzione, la (b) che $\operatorname{dom}(F)=X$ e $\operatorname{ran}(F)=\mathbb{Q}$ e la (c) che F preserva l'ordine in quanto per ogni $x_n,x_m\in X$, i valori $F(x_n)$ e $F(x_m)$ sono dati da $p_N(x_n)$ e $p_N(x_m)$, per ogni $N\geq 2\max(n,m)$. Resta soltanto da costruire le p_n.

La funzione $p_0=\{(x_0,q_0)\}$ soddisfa le condizioni (a)–(c). Supponiamo che p_n sia definita e che (a)–(c) siano soddisfatte.

Se $n{+}1=2m$ e se $x_m\in\operatorname{dom}(p_n)$ oppure $n{+}1=2m{+}1$ e se $y_m\in\operatorname{ran}(p_n)$, allora poniamo $p_{n+1}=p_n$: è facile verificare che p_{n+1} soddisfa (a)–(c).

Supponiamo invece che $n+1=2m$ e $x_m\notin\operatorname{dom}(p_n)$. Consideriamo tre casi:

Caso 1: $x_m\lhd\min(\operatorname{dom}(p_n))$. Sia $q=\min(\operatorname{ran}(p_n))-1$ e poniamo $p_{n+1}=p_n\cup\{(x_m,q)\}$.

Caso 2: $\max(\mathrm{dom}(p_n)) \lhd x_m$. Sia $q = \max(\mathrm{ran}(p_n)) + 1$ e poniamo $p_{n+1} = p_n \cup \{(x_m, q)\}$.

Caso 3: esistono $x, x' \in \mathrm{dom}(p_n)$ tali che $x \lhd x_m \lhd x'$, dove x e x' sono elementi consecutivi di $\mathrm{dom}(p_n)$, cioè non esiste alcun $x'' \in \mathrm{dom}(p_n)$ per cui $x \lhd x'' \lhd x'$. Sia $q = \frac{1}{2}(p_n(x') + p_n(x))$ e poniamo $p_{n+1} = p_n \cup \{(x_m, q)\}$.

In tutti e tre i casi è immediato verificare che p_{n+1} soddisfa (a)–(c).

Supponiamo infine che $n + 1 = 2m + 1$ e $q_m \notin \mathrm{dom}(p_n)$. Nuovamente ci sono tre casi da considerare: $q_m < \min(\mathrm{ran}(p_n))$, o $\max(\mathrm{ran}(p_n)) < q_m$, oppure $q < q_m < q'$, per qualche $q, q' \in \mathrm{ran}(p_n)$. In ciascuno dei casi si procede come sopra sfruttando il fatto che X non ha minimo (Caso 1), non ha massimo (Caso 2) ed è denso (Caso 3). □

Quindi, per esempio, gli insiemi ordinati

- $\mathbb{Q}$,
- $\mathbb{Q} \cup \{\sqrt{2}\}$ e
- l'insieme dei numeri algebrici reali[1]

sono isomorfi e tuttavia non è facile definire esplicitamente tale isomorfismo.

La costruzione nella dimostrazione del Teorema 9.3 è nota come metodo del *back and forth*, in quanto dobbiamo assicurarci che la funzione F sia definita su tutti gli x_n (*back*) e che assuma tutti i valori y_n (*forth*). Usando solo una delle due parti della costruzione possiamo dimostrare che ogni ordine lineare numerabile è immergibile in $\mathbb{Q}$.

Teorema 9.4. *Se $\langle X, \trianglelefteq \rangle$ è un ordine lineare numerabile, allora c'è una funzione iniettiva $F\colon X \to \mathbb{Q}$ che preserva l'ordine.*

Dimostrazione. Sia $\{ x_n \mid n \in \omega \}$ un'enumerazione di X. È sufficiente costruire una successione di funzioni p_n tali che

(a) $p_0 \subseteq p_1 \subseteq \dots$,

(b) $\mathrm{dom}(p_n) = \{x_0, \dots, x_n\}$,

(c) $\mathrm{dom}(p_n)$ è finito e $p_n\colon \mathrm{dom}(p_n) \to \mathrm{ran}(p_n)$ è una bijezione che preserva l'ordine, vale a dire

$$\forall i, j < n \, (x_i \lhd x_j \Leftrightarrow p_n(x_i) < p_n(x_j)) \, .$$

$F = \bigcup_n p_n\colon X \to \mathbb{Q}$ è la funzione cercata. La costruzione delle p_n segue la falsariga della dimostrazione del Teorema 9.3. Poniamo $p_0 = \{(x_0, 0)\}$ e supponiamo p_n è data e soddisfa (a)–(c). Consideriamo i tre casi: $x_{n+1} \lhd$

[1] Un numero reale si dice algebrico se è soluzione di un'equazione polinomiale a coefficienti in $\mathbb{Q}$.

$\min\{x_0,\dots,x_n\}$, $\max\{x_0,\dots,x_n\} \lhd x_{n+1}$ e x_{n+1} si trova tra due elementi $\lhd$-consecutivi x_i e x_j di $\{x_0,\dots,x_n\}$. In tutti e tre i casi è possibile trovare un razionale q per cui $p_{n+1} = p_n \cup \{(x_n, q)\}$ soddisfa (a)–(c). □

Sempre utilizzando il metodo del *back and forth* è possibile dimostrare che l'ordine $\mathbb{Q}$ ha molti automorfismi:

Teorema 9.5. *Se $A, B \subset \mathbb{Q}$ sono insiemi finiti di ugual cardinalità, allora c'è un isomorfismo $f\colon \langle \mathbb{Q}, < \rangle \to \langle \mathbb{Q}, < \rangle$ tale che $f[A] = B$.*

Un ordine lineare $\langle L, \leq \rangle$ si dice

- **omogeneo** se due intervalli aperti sono sempre isomorfi, cioè se per ogni $a, a', b, b' \in L$ con $a < b$ e $a' < b'$ c'è un isomorfismo $(a; b) \to (a'; b')$;
- **ultraomogeneo** se per ogni coppia A, B di sottoinsiemi finiti di L di ugual cardinalità, c'è un isomorfismo $f\colon \langle L, \leq \rangle \to \langle L, \leq \rangle$ tale che $f[A] = B$.

Non è difficile verificare che un ordine lineare ultraomogeneo è anche omogeneo. Il Teorema 9.5 mostra quindi che $\mathbb{Q}$ è ultraomogeneo.

9.C. I numeri reali.

Definizione 9.6. Un sottoinsieme $x \subseteq \mathbb{Q}$ è una **sezione di Dedekind** se è un segmento iniziale proprio, privo di massimo, non vuoto di $\mathbb{Q}$, cioè

- $x \neq \emptyset, \mathbb{Q}$,
- $\forall q \in x\, \forall p \in \mathbb{Q}(p < q \Rightarrow p \in x)$,
- $\forall q \in x\, \exists p \in x(q < p)$.

Le sezioni di Dedekind si dicono **numeri reali** e

$$\mathbb{R} = \{\, x \in \mathscr{P}(\mathbb{Q}) \mid x \text{ è una sezione di Dedekind} \,\}.$$

L'ordinamento e la somma su $\mathbb{R}$ sono definiti da

$$x <^{\mathbb{R}} y \;\Leftrightarrow\; x \subset y$$
$$x +^{\mathbb{R}} y = \{\, p + q \mid p \in x \wedge q \in y \,\}.$$

La definizione di moltiplicazione $x \cdot^{\mathbb{R}} y$ è più laboriosa ed è presentata nel Esercizio 9.18.

Esercizio 9.7. (i) Dimostrare che la somma di due numeri reali è ancora un numero reale e che la mappa $\mathbb{Q} \to \mathbb{R}$, $q \mapsto \{\, p \in \mathbb{Q} \mid p < q \,\}$ è un morfismo per l'ordine e la somma.

(ii) Dimostrare che $\mathbb{Q}$ è denso in $\mathbb{R}$.

Un insieme linearmente ordinato $\langle L, \leq \rangle$ si dice **completo** se ogni sottoinsieme non vuoto che ha un maggiorante, ha un estremo superiore e ogni sottoinsieme non vuoto che ha un minorante, ha un estremo inferiore.

Teorema 9.8. *$\langle \mathbb{R}, \leq \rangle$ è completo.*

Dimostrazione. Verifichiamo che ogni sottoinsieme non vuoto e superiormente limitato ammette un estremo superiore—il caso duale degli insiemi limitati inferiormente è lasciato al lettore. Siano $\emptyset \neq X \subseteq \mathbb{R}$ e $M \in \mathbb{R}$ tali che $\forall x \in X\,(x \leq M)$ cioè $\forall x \in X\,(x \subseteq M)$. è facile verificare che $\bar{x} = \bigcup X$ è una sezione di Dedekind e che $\forall x \in X\,(x \leq \bar{x})$. Se y è un maggiorante di X, allora $\forall x \in X\,(x \subseteq y)$, cioè $\bar{x} \leq y$. □

Teorema 9.9 (Cantor)**.** *Ogni ordine lineare, denso, completo ed infinito è più che numerabile. In particolare: $\mathbb{R}$ è più che numerabile.*

Dimostrazione. Per assurdo, sia $\{\, x_n \mid n \in \omega \,\}$ una enumerazione di L, dove $\langle L, \leq \rangle$ è come nell'enunciato. Costruiremo una successione crescente $(a_n)_n$ e una successione decrescente $(b_n)_n$ di elementi di L

$$a_0 < a_1 < a_2 < \ldots \cdots < b_2 < b_1 < b_0$$

tali che non esiste nessun $x \in L$ che maggiora tutti gli a_n e minora tutti i b_n. In particolare L non è completo, contraddicendo la nostra ipotesi. Fissiamo due elementi $a_0 < b_0$: dati $a_0 < \cdots < a_{n-1} < b_{n-1} < \cdots < b_0$, per densità possiamo trovare degli elementi tra a_{n-1} e b_{n-}, sia k_n il minimo k tale che $a_{n-1} < x_k < b_{n-1}$ e sia $a_n = x_{k_n}$. Analogamente sia $b_n = x_{h_n}$ dove h_n è il minimo h tale che $a_n < x_h < b_{n-1}$. Dalla definizione di k_i segue che

$$n < m \Rightarrow k_n < k_m \tag{37}$$

e

$$a_n < x_i < b_{n-1} \Rightarrow k_n < i\,. \tag{38}$$

Quindi se x_i fosse un elemento maggiore degli a_n e minore dei b_n, l'indice i dovrebbe essere maggiore di ogni k_n per (38) e dato che $\sup_n k_n = \omega$ per (37), tale i non può esistere. □

Ricordiamo che ad ogni ordine lineare $\langle L, \leq \rangle$ possiamo associare la **topologia degli intervalli** o **topologia dell'ordine** generata dalle semirette aperte $\{\, x \in L \mid x < b \,\}$ e $\{\, x \in L \mid a < x \,\}$, con $a, b \in L$. Se

$$f \colon \langle L, \leq \rangle \to \langle M, \preceq \rangle$$

è un isomorfismo di ordini lineari, allora f è un omeomorfismo, quando diamo a L ed M la topologia dell'ordine. Osserviamo che $D \subseteq L$ è denso secondo la definizione di pagina 23 se e solo se è un insieme denso in questa topologia.

Se L se contiene un insieme denso e numerabile (cioè se è separabile in questa topologia) diremo che è **separabile**.

Teorema 9.10. *$\langle \mathbb{R}, \leq \rangle$ è, a meno di isomorfismo, l'unico ordine lineare completo, separabile, senza primo o ultimo elemento.*

Dimostrazione. Sia $\langle X, \trianglelefteq \rangle$ un ordine lineare completo, separabile, senza primo o ultimo elemento e sia D il suo sottoinsieme denso e numerabile. Allora $\langle D, \trianglelefteq \rangle$ un ordine lineare numerabile senza primo o ultimo elemento e quindi per il Teorema 9.3 c'è una bijezione strettamente crescente $F\colon \mathbb{Q} \to D$. Per ogni $r \in \mathbb{R}$ possiamo trovare un $p \in \mathbb{Q}$ tale che $r \leq p$ e quindi l'insieme $\{\, F(q) \mid q \in \mathbb{Q} \wedge q \leq r \,\}$ è limitato superiormente da $F(p)$. Possiamo quindi estendere F ad $\mathbb{R}$ ponendo

$$F(r) = \sup \{\, F(q) \mid q \in \mathbb{Q} \wedge q \leq x \,\}$$

dove il sup è calcolato secondo l'ordinamento $\trianglelefteq$. Chiaramente $r \leq s \Rightarrow F(r) \trianglelefteq F(s)$ e se $r < s$ prendiamo $q_1, q_2 \in \mathbb{Q}$, con $r < q_1 < q_2 < s$: allora $F(r) \trianglelefteq F(q_1) \triangleleft F(q_2) \trianglelefteq F(s)$. Quindi F è strettamente crescente. Dobbiamo verificare che F è suriettiva. Se $x \in X$ scelgo $d \in D$ tale che $x \triangleleft d$ e sia $p \in \mathbb{Q}$ tale che $F(q) = d$. L'insieme

$$A = \{\, r \in \mathbb{R} \mid F(r) \trianglelefteq x \,\}$$

è limitato superiormente da p e quindi possiamo calcolare $\bar{r} = \sup A$ secondo l'ordinamento $\trianglelefteq$. Verifichiamo che $F(\bar{r}) = x$. Se $F(\bar{r}) \triangleleft x$ fissiamo un $d' \in D$ con $F(\bar{r}) \triangleleft d' \triangleleft x$. Sia $p' = F^{-1}(d')$: allora $p' \in A$ e quindi $p' \leq \bar{r}$, ma d'altra parte $F(\bar{r}) \triangleleft d'$ implica che $\bar{r} < p$: contraddizione. Il caso in cui $x \triangleleft F(\bar{r})$ porta ugualmente ad una contraddizione ed è lasciato al lettore. □

La costruzione di $\mathbb{R}$ a partire da $\mathbb{Q}$ mediante sezioni di Dedekind può essere generalizzata ad ogni ordine lineare (Esercizio 9.23). Un altro modo per costruire $\mathbb{R}$ a partire da $\mathbb{Q}$ è quello di completare $\mathbb{Q}$ come spazio metrico (Esercizio 9.24).

Per ogni $x \in 2^{\mathbb{N}}$ sia

$$\Phi(x) = \sum_{n=0}^{\infty} \frac{2x(n)}{3^{n+1}}\,. \tag{39}$$

Esercizio 9.11. Dimostrare che:

(i) la serie (39) converge ad un reale in $[0; 1]$;

(ii) se $x \restriction n = y \restriction n$, $x(n) = 0$ e $y(n) = 1$, allora $\Phi(x) < \Phi(y) \leq \Phi(x) + 3^{-n}$.

La funzione $\Phi\colon 2^{\mathbb{N}} \rightarrowtail [0; 1]$ è iniettiva e quindi $\mathscr{P}(\mathbb{N}) \rightarrowtail \mathbb{R}$. Poiché $\mathbb{R} \subseteq \mathscr{P}(\mathbb{Q})$ e $\mathscr{P}(\mathbb{Q})$ è in bijezione con $\mathscr{P}(\mathbb{N})$, ne segue che $\mathbb{R} \rightarrowtail \mathscr{P}(\mathbb{N})$. Per il Teorema di Shröder–Bernstein e per la Proposizione 8.11 segue che:

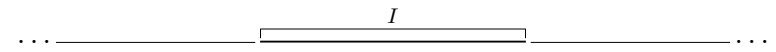
Proposizione 9.12. *Gli insiemi* $\mathbb{R}$, $2^{\mathbb{N}}$ *e* $\mathbb{N}^{\mathbb{N}}$ *sono equipotenti.*

Esercizio 9.13. Dimostrare che ogni intervallo di $\mathbb{R}$ aperto, chiuso o semiaperto non degenere (cioè non vuoto oppure un singoletto) è equipotente ad $\mathbb{R}$.

9.D. L'insieme di Cantor. L'insieme $\mathrm{ran}(\Phi)$ della formula (39) è un insieme ben noto in Analisi. Per descriverlo introduciamo qualche definizione. Fissiamo un intervallo chiuso $I = [a; b]$ non degenere (cioè $a < b$) di $\mathbb{R}$ e fissiamo un $r \in (0; 1)$. Rimuoviamo da I l'intervallo aperto centrato nel punto medio di I di ampiezza $r(b - a)$. Otteniamo così due intervalli chiusi non degeneri

$$\begin{aligned} I_{(0;r)} &= \left[a; a + \frac{1+2r}{2}(b-a)\right] \\ I_{(1;r)} &= \left[b - \frac{1+2r}{2}(b-a); b\right] \end{aligned} \tag{40}$$

Nella figura qui sotto vediamo un esempio con $r = 1/2$: dato un intervallo chiuso $I \subseteq \mathbb{R}$



rimuoviamo la parte centrale di I di lunghezza $1/2$ della lunghezza di I e otteniamo $I_{(0;1/2)}$ e $I_{(1;1/2)}$:

L'**insieme ternario di Cantor** è definito come

$$E_{1/3} = \bigcap_n E^{(n)}_{1/3}\,, \tag{41}$$

dove $E^{(0)}_{1/3}$ è l'intervallo $[0; 1]$, $E^{(n)}_{1/3} \subseteq E^{(n-1)}_{1/3}$ è unione di 2^n intervalli chiusi di lunghezza 3^{-n} ottenuti applicando la costruzione (40) a ciascuno dei 2^{n-1} intervalli di $E^{(n-1)}_{1/3}$. $E_{1/3}$ è un sotto-insieme compatto, non-numerabile di $\mathbb{R}$ con interno vuoto—si veda gli Esercizi 9.26 e 9.27.

Costruiamo la sequenza di intervalli chiusi $\langle I_s \mid s \in 2^{<\mathbb{N}}\rangle$ ponendo

$$\begin{aligned} I_\emptyset &= [0; 1]\,, \\ I_{s^\frown\langle 0\rangle} &= (I_s)_{(0;1/3)}\,, \qquad & I_{s^\frown\langle 1\rangle} &= (I_s)_{(1;1/3)} \end{aligned}$$

definiti come in (40). Per semplicità notazionale poniamo $I_s = [a_s; b_s]$.

Esercizio 9.14. Verificare che

$$E^{(n)}_{1/3} = \bigcup_{s\in{}^n2} I_s$$

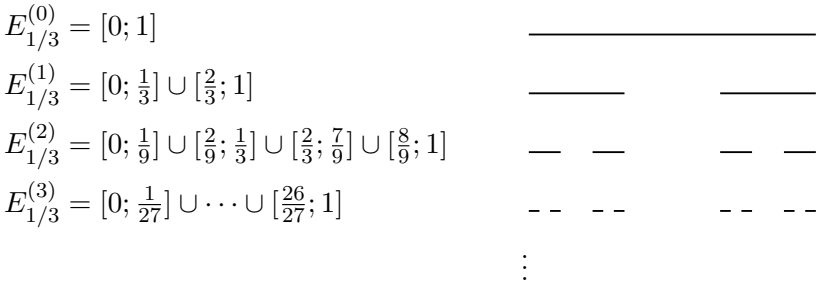


Figura 1. La costruzione dell'insieme di Cantor.

e che

$$a_s = \sum_{i<\mathrm{lh}(s)} \frac{2s(i)}{3^{i+1}} \qquad \text{e} \qquad b_s = a_s + 3^{-\,\mathrm{lh}(s)}\,.$$

È immediato verificare che

$$s \subset t \Rightarrow I_s \supset I_t\,. \tag{42}$$

Supponiamo invece che $s, t \in 2^{<\mathbb{N}}$ siano inconfrontabili, vale a dire $s \not\subseteq t$ e $s \not\supseteq t$. Sia $\bar{n}$ tale che $s \restriction \bar{n} = t \restriction \bar{n}$, ma $s(\bar{n}) \neq t(\bar{n})$. Allora $I_{s\restriction\bar{n}+1} \cap I_{t\restriction\bar{n}+1} = \emptyset$ e quindi $I_s \cap I_t = \emptyset$ per (42). L'ordinamento lessicografico su $2^{\mathbb{N}}$ è definito da

$$x <_{\mathrm{lex}} y \Leftrightarrow \exists n\,(x \restriction n = y \restriction n \ \wedge\ x(n) < y(n)) \tag{43}$$

e la parte (ii) dell'Esercizio 9.11 dice che Φ è strettamente crescente. Dato che per ogni $x \in 2^{\mathbb{N}}$

$$(x \restriction n)^\frown\vec{0} \leq_{\mathrm{lex}} x \leq_{\mathrm{lex}} (x \restriction n)^\frown\vec{1}$$

dove $\vec{1} = \langle 1, 1, \ldots\rangle$, allora

$$\begin{aligned} a_s &= \textstyle\sum_{i<n} \frac{2x(i)}{3^{i+1}} \\ &= \Phi\big((x \restriction n)^\frown\vec{0}\big) \\ &\leq \Phi(x) \\ &\leq \Phi\big((x \restriction n)^\frown\vec{1}\big) \\ &= a_s + \textstyle\sum_{i\geq n} \frac{2}{3^{i+1}} \\ &= b_s \end{aligned}$$

cioè

$$\forall n\,(\Phi(x) \in I_{x\restriction n}) \tag{44}$$

e dato che l'ampiezza di $I_{x\restriction n}$ tende a 0, si ha

$$\{\Phi(x)\} = \bigcup_n I_{x\restriction n} \subseteq \bigcap_n E^n_{1/3} = E_{1/3}\,. \tag{45}$$

In altre parole: $\mathrm{ran}(\Phi) \subseteq E_{1/3}$. Viceversa, fissato un $y \in E_{1/3}$, sia $s_n(y)$ l'unico $s \in {}^n2$ tale che $y \in I_s$. se per qualche $n \leq m$ non valesse $s_n(y) \subseteq s_m(y)$, allora $s_n(y)$ e $s_m(y)$ sarebbero inconfrontabili, e quindi $y \in I_{s_n(y)} \cap I_{s_m(y)} = \emptyset$: una contraddizione. Quindi posto $x \stackrel{\text{def}}{=} \bigcup_n s_n(y)$ si ha che $x \in 2^{\mathbb{N}}$ e $\Phi(x) = y$ per (9.26) e (9.27).

Abbiamo quindi dimostrato il seguente risultato:

Proposizione 9.15. *L'insieme $E_{1/3}$ è* $\mathrm{ran}(\Phi)$*, l'immagine della funzione Φ.*

Se diamo a $2^{\mathbb{N}}$ la topologia dell'ordine, allora Φ è un omeomorfismo tra $2^{\mathbb{N}}$ e $E_{1/3}$. Inoltre la topologia dell'ordine su $2^{\mathbb{N}}$ coincide con la topologia prodotto, dove ciascun fattore $2 = \{0, 1\}$ ha la topologia discreta—vedi l'Esercizio 9.30.

Lo spazio di Cantor $2^{\mathbb{N}}$ non solo si immerge in $[0; 1]$, ma anche in ogni chiuso più che numerabile di $\mathbb{R}$.

Teorema 9.16. *Sia (X, d) uno spazio separabile, metrico completo, privo di punti isolati e non vuoto. Allora c'è una funzione continua e iniettiva $f\colon 2^{\mathbb{N}} \rightarrowtail X$. In particolare: X contiene una copia omeomorfa dell'insieme di Cantor.*

Dimostrazione. Sia $E = \{\, e_n \mid n \in \omega \,\}$ denso in X. Costruiamo induttivamente dei numeri reali r_s e dei punti $x_s \in X$ ($s \in 2^{<\mathbb{N}}$), tali che

(i) $0 < r_s \leq 2^{-\,\mathrm{lh}(s)}$,

(ii) $\mathrm{Cl}(B(x_{s^\frown\langle i\rangle}, r_{s^\frown\langle i\rangle})) \subseteq B(x_s, r_s)$, per $i = 0, 1$,

(iii) $\mathrm{Cl}\big(B(x_{s^\frown\langle 0\rangle}, r_{s^\frown\langle 0\rangle})\big) \cap \mathrm{Cl}\Big(B(x_{s^\frown\langle 1\rangle}, r_{s^\frown\langle 1\rangle})\Big) = \emptyset$.

Poniamo $x_\emptyset \in X$ e $r_\emptyset = 1$. Dato x_s e r_s è facile verificare che $E \cap B(x_s, r_s)$ è infinito, quindi possiamo scegliere due punti distinti $x_{s^\frown\langle 0\rangle}$ e $x_{s^\frown\langle 1\rangle}$ in questo insieme. (Prediamo, per esempio e_k ed e_h, dove k e h sono i primi due indici i tali che $e_i \in E \cap B(x_s, r_s)$.) Prendiamo $r_{s^\frown\langle i\rangle}$ ($i = 0, 1$) sufficientemente piccoli in modo che valgano (i)–(iii).

Per ogni $y \in 2^{\mathbb{N}}$ considero la successione $(x_{y\restriction n})_n$. Poiché $B(x_{y\restriction n}, r_{y\restriction n}) \supseteq B(x_{y\restriction n+1}, r_{y\restriction n+1})$ per (ii),

$$\forall k \geq n\, (x_{y\restriction k} \in B(x_{y\restriction n}, r_{y\restriction n}))\,. \tag{46}$$

Quindi la successione $(x_{y\restriction n})_n$ è di Cauchy e sia

$$f(y) = \lim_n x_{y\restriction n}$$

Per (46) $f(y) \in \mathrm{Cl}\big(B(x_{y\restriction n}, r_{y\restriction n})\big)$ per ogni n e quindi

$$f(y) \in \bigcap_n \mathrm{Cl}\big(B(x_{y\restriction n}, r_{y\restriction n})\big) = \bigcap_n B(x_{y\restriction n}, r_{y\restriction n})\,,$$

dove la seconda uguaglianza segue da (ii). Se $y, z \in 2^{\mathbb{N}}$ sono distinti, sia n tale che $y \restriction n = z \restriction n$ e $y(n) \neq z(n)$. Allora $f(y) \in \mathrm{Cl}\big(B(x_{y\restriction n}, r_{y\restriction n})\big)$ e $f(z) \in \mathrm{Cl}\big(B(x_{z\restriction n}, r_{z\restriction n})\big)$ e quindi $f(y) \neq f(z)$ per (iii). In altre parole, la funzione $f\colon 2^{\mathbb{N}} \to X$ è iniettiva. Resta da dimostrare che è continua. Fissato un $y \in 2^{\mathbb{N}}$ ed un n, basta trovare un k tale che se $z \restriction k = y \restriction k$, allora $d(x_{z\restriction k}, x_{y\restriction k}) < 2^{-n}$. È facile verificare che $k = n$ funziona. □

9.E. Esempi di insiemi equipotenti ad $\mathbb{R}$.

9.E.1. *prodotto di spazi di Cantor.* $2^{\mathbb{N}}$ è equipotente a $(2^{\mathbb{N}})^{\mathbb{N}}$ e a $(2^{\mathbb{N}})^n$, per ogni $n > 0$. Infatti

- $2^{\mathbb{N}} \rightarrowtail (2^{\mathbb{N}})^n$ via $x \mapsto (x, \vec{0}, \dots, \vec{0})$, dove $\vec{0}$ è la successione identicamente 0
- $(2^{\mathbb{N}})^n \rightarrowtail (2^{\mathbb{N}})^{\mathbb{N}}$ via $(x_1, \dots, x_n) \mapsto \langle x_1, \dots, x_n, \vec{0}, \vec{0}, \dots \rangle$
- $(2^{\mathbb{N}})^{\mathbb{N}}$ è equipotente a $2^{\mathbb{N}}$ per le parti (iii) e (v) dell'Esercizio 8.10 e il Teorema 8.8.

Quindi per i Teoremi di Shröder-Bernstein 2.6 e 9.12, $2^{\mathbb{N}}$, $(2^{\mathbb{N}})^n$ e $(2^{\mathbb{N}})^{\mathbb{N}}$ sono equipotenti ad $\mathbb{R}$.

9.E.2. *Il cubo di Hilbert.* Per l'Esercizio 8.10 $\mathbb{R}$, $\mathbb{R}^n$ e $\mathbb{R}^{\mathbb{N}}$ sono equipotenti. In particolare $\mathbb{R}$ è in bijezione con $\mathbb{R}^2$, cioè con $\mathbb{C}$.

Similmente, il cubo n-dimensionale, $[0;1]^n$ e il **cubo di Hilbert** $[0;1]^{\mathbb{N}}$ sono equipotenti a $\mathbb{R}$.

9.E.3. *Lo spazio delle funzioni continue da $\mathbb{R}$ in $\mathbb{R}$.* L'insieme $\mathcal{C}(\mathbb{R}, \mathbb{R})$ delle funzioni continue su $\mathbb{R}$ a valori reali è equipotente ad $\mathbb{R}$. Per vedere questo consideriamo la mappa $\mathcal{C}(\mathbb{R}, \mathbb{R}) \to \mathbb{R}^{\mathbb{Q}}$, $f \mapsto f \restriction \mathbb{Q}$. Se $f, g \in \mathcal{C}(\mathbb{R}, \mathbb{R})$ differiscono in $x_0 \in \mathbb{R}$, allora per continuità esiste un $\varepsilon > 0$ tale che f e g sono sempre distinte sull'intervallo $(x_0 - \varepsilon; x_0 + \varepsilon)$. Sia $q \in \mathbb{Q} \cap (x_0 - \varepsilon; x_0 + \varepsilon)$: allora $f(q) \neq g(q)$ e quindi $f \restriction \mathbb{Q} \neq g \restriction \mathbb{Q}$. Di conseguenza la mappa $f \mapsto f \restriction \mathbb{Q}$ è iniettiva e poiché $\mathbb{Q}$ è in bijezione con $\mathbb{N}$, per l'esempio precedente si ha che $\mathcal{C}(\mathbb{R}, \mathbb{R})$ si inietta in $\mathbb{R}$. Ovviamente $\mathbb{R}$ si inietta in $\mathcal{C}(\mathbb{R}, \mathbb{R})$ e quindi i due insiemi sono equipotenti.

9.E.4. *Spazi metrici separabili.* Sia (X, d) uno spazio metrico separabile e sia $Q = \{\, q_n \mid n \in \mathbb{N} \,\}$ un sotto-insieme denso enumerabile di X. La funzione

$$X \to \mathbb{R}^{\mathbb{N}} \qquad x \mapsto \langle d(x, q_n) \mid n \in \mathbb{N} \rangle \tag{47}$$

è iniettiva, quindi X è iniettabile in $\mathbb{R}$. In particolare questo vale quando X è una varietà topologica (separabile) o uno spazio vettoriale (separabile) e

poiché $\mathbb{R}$ si inietta in un X siffatto, abbiamo un'altra famiglia di esempi di insiemi equipotenti ad $\mathbb{R}$.

9.E.5. *Spazi secondo numerabili.* Se X è uno spazio secondo numerabile, la sua topologia $\mathcal{T}$ (vale a dire: la famiglia degli aperti di X) si inietta in $\mathbb{R}$. Infatti, fissata $\mathcal{B} = \{ V_n \mid n \in \omega \}$ una base numerabile di X, la funzione

$$\mathcal{T} \to \mathscr{P}(\omega) \qquad U \mapsto \{ n \in \omega \mid V_n \subseteq U \}$$

è iniettiva. Passando ai complementi si ha che $\mathcal{C}$, l'insieme dei chiusi di X, si inietta in $\mathbb{R}$. Poiché $\{x\}$ è un chiuso di $\mathbb{R}$, per ogni $x \in \mathbb{R}$, si ha che la famiglia degli aperti (e quindi dei chiusi) di $\mathbb{R}$ è equipotente ad $\mathbb{R}$. Un discorso analogo vale per $\mathbb{R}^n$, $\mathbb{R}^{\mathbb{N}}$, uno **spazio di Banach** separabile, etc.

9.F. $\mathbb{R}$ ed ω_1. Abbiamo visto due esempi di insiemi più che numerabili: l'insieme dei reali $\mathbb{R}$ ed il primo ordinale più che numerabile ω_1 (pag.35). È naturale chiedersi in che relazione siano questi insiemi: sono equipotenti? uno dei due si inietta nell'altro? oppure si surietta?

Proposizione 9.17. *C'è una suriezione* $\mathbb{R} \twoheadrightarrow \omega_1$.

Dimostrazione. Per quanto visto, è sufficiente verificare che $\mathscr{P}(\omega \times \omega)$ si surietta su ω_1. Sia $W \subseteq \mathscr{P}(\omega \times \omega)$ l'insieme dei buoni ordini sul loro campo, cioè

$$W = \{ R \subseteq \omega \times \omega \mid \langle \mathrm{fld}(R), R \rangle \text{ è un buon ordine} \}$$

e sia $F \colon W \to \omega_1$ la funzione che ad ogni R associa il suo tipo d'ordine, cioè $F(R) = \mathrm{ot}(\langle \mathrm{fld}(R), R \rangle)$. È facile verificare che F è suriettiva e quindi possiamo estendere F a $\mathscr{P}(\omega \times \omega)$ ponendo, per esempio, $F(S) = 0$ se $S \notin W$. □

Vediamo cosa si può dire in generale:

- Se $\mathbb{R}$ è bene ordinabile allora è equipotente ad un ordinale più che numerabile e quindi $|\omega_1| \leq |\mathbb{R}|$.
- Se $\mathbb{R} \rightarrowtail \omega_1$, allora $\mathbb{R}$ è bene ordinabile ed essendo ω_1 il primo ordinale più che numerabile, ne segue che ω_1 è equipotente ad $\mathbb{R}$.
- Se $f \colon \omega_1 \twoheadrightarrow \mathbb{R}$ allora $\mathbb{R}$ è bene ordinabile (Esercizio 8.1) e $g \colon \mathbb{R} \to \omega_1$

  $$g(x) = \min \{ \alpha \mid f(\alpha) = x \}$$

  è iniettiva e quindi ω_1 è equipotente ad $\mathbb{R}$.

L'affermazione "$\mathbb{R}$ è bene ordinabile" è conseguenza dell'assioma della scelta AC (sezione 14) ma non è discende dagli assiomi di MK o di ZF e un discorso analogo vale per l'affermazione: $\omega_1 \rightarrowtail \mathbb{R}$. L'affermazione che $\mathbb{R}$ e ω_1 sono equipotenti è nota come **ipotesi del continuo** e verrà esaminata nella sezione 18.

Esercizi

Esercizio 9.18. Se $x, y \in \mathbb{R}$ e $x, y > 0$ definiamo

$$x \cdot y = \{\, p \in \mathbb{Q} \mid \exists q, r \in \mathbb{Q}\, (0 < q \in x \wedge 0 < r \in y \wedge p \leq q \cdot r) \,\}$$

e se x, y non sono entrambi positivi,

$$x \cdot y = \begin{cases} 0 & \text{se } x = 0 \text{ o } y = 0, \\ -\big((-x) \cdot y\big) & \text{se } x < 0 \text{ e } y > 0, \\ -\big(x \cdot (-y)\big) & \text{se } x > 0 \text{ e } y < 0, \\ (-x) \cdot (-y) & \text{se } x < 0 \text{ e } y < 0, \end{cases}$$

dove

$$-x = \{\, p \in \mathbb{Q} \mid \exists s \in \mathbb{Q}\, \forall q \in x\, (p + q < s < 0) \,\}\,.$$

Verificare che l'operazione è ben definita e che $\langle \mathbb{R}, +, \cdot, < \rangle$ è un campo ordinato.

Esercizio 9.19. Dimostrare che, a meno di isomorfismi, gli ordini lineari densi numerabili sono quattro:

$$\mathbb{Q}, \quad [0;1] \cap \mathbb{Q}, \quad [0;1) \cap \mathbb{Q} \quad (0;1] \cap \mathbb{Q}\,.$$

Esercizio 9.20. Dimostrare il Teorema 9.5.

Esercizio 9.21. Sia $\langle L, \leq \rangle$ un ordine lineare tale che per ogni $a, a', b, b' \in L$ con $a < b$ e $a' < b'$ c'è un isomorfismo $f \colon L \to L$ tale che $f(a) = a'$ e $f(b) = b$. (Questo è un rafforzamento della condizione di omogeneità. Dimostrare che $\langle L, \leq \rangle$ è ultraomogeneo.

Esercizio 9.22. Dimostrare che $(0;1)$ e $(0;1) \cup (1;2)$ sono insiemi equipotenti, sono ordini lineari densi senza primo o ultimo elemento, ma non sono isomorfi.

Se $\langle L, \leq \rangle$ e $\langle \hat{L}, \trianglelefteq \rangle$ sono ordini lineari diremo che $\langle \hat{L}, \trianglelefteq \rangle$ è un **completamento** di $\langle L, \leq \rangle$ se

- $\langle \hat{L}, \trianglelefteq \rangle$ è completo e
- $\langle L, \leq \rangle$ si immerge in modo denso in $\langle \hat{L}, \trianglelefteq \rangle$, cioè se esiste una $f \colon \langle L, \leq \rangle \to \langle \hat{L}, \trianglelefteq \rangle$ strettamente crescente tale che $\operatorname{ran}(f)$ è denso in $\hat{L}$.

Esercizio 9.23. Dimostrare che ogni ordine lineare ha un unico completamento, a meno di isomorfismi.

Sia $\hat{\mathbb{Q}}$ il completamento di $\mathbb{Q}$ come spazio metrico—gli elementi di $\hat{\mathbb{Q}}$ sono classi di equivalenza $[(x_n)_n]$ di successioni di Cauchy in $\mathbb{Q}$. Poniamo

$$[(x_n)_n] \lhd [(y_n)_n] \quad \Leftrightarrow \quad \exists N\, \exists q \in \mathbb{Q}\, \forall n \geq N\, (x_n < q < y_n)$$

e $[(x_n)_n] \trianglelefteq [(y_n)_n]$ se e solo se $[(x_n)_n] \lhd [(y_n)_n] \ \vee \ [(x_n)_n] = [(y_n)_n]$.

Esercizio 9.24. Dimostrare che $\langle \hat{\mathbb{Q}}, \trianglelefteq \rangle$ è un completamento di $\langle \mathbb{Q}, \leq \rangle$ come ordine lineare e quindi è isomorfo ad $\langle \mathbb{R}, \leq \rangle$.

Definire le operazioni di somma e prodotto su $\hat{\mathbb{Q}}$ e verificare che coincidono con le operazioni su $\mathbb{R}$ definite nel testo.

Esercizio 9.25. Dimostrare che

(i) gli anelli di polinomi $\mathbb{Z}[X]$ e $\mathbb{Q}[X]$ sono numerabili,

(ii) ogni intervallo aperto $(x; y) \subset \mathbb{R}$ è equipotente a $\mathbb{R}$ e che ogni intervallo aperto razionale $(p; q) \cap \mathbb{Q} = \{\, r \in \mathbb{Q} \mid p < r < q \,\}$ è equipotente a $\mathbb{Q}$. Analogamente per gli intervalli chiusi e semi-aperti.

Esercizio 9.26. Dimostrare che $E_{1/3}$ definito in (41) è un insieme compatto, non-vuoto, privo di interno.

Esercizio 9.27. Fissiamo un numero naturale $b > 1$. L'**espansione di** $x \in [0, 1]$ **in base** b è una sequenza

$$\langle n_0, n_1, n_2, \ldots\ldots \rangle \in {}^{\omega}b$$

tale che

$$x = \sum_{i=0}^{\infty} \frac{n_i}{b^{i+1}}\,.$$

(i) Verificare che se
- $\forall i < k\, (n_i = m_i)$,
- $n_k = m_k + 1$,
- $\forall i > k\, (n_i = 0 \ \wedge \ m_i = b - 1)$,

allora

$$\sum_{i=0}^{\infty} \frac{n_i}{b^{i+1}} = \sum_{i=0}^{\infty} \frac{m_i}{b^{i+1}} \in [0, 1]$$

e quindi l'espansione in base b di un $x \in [0, 1]$ non è unica.

(ii) Dimostrare che se x ammette un'espansione che non è definitivamente uguale a 0 o definitivamente uguale a $b - 1$, allora tale espansione è unica.

(iii) Dimostrare che $E_{1/3}$, l'insieme di Cantor, è l'insieme dei reali in $[0, 1]$ che ammettono un'espansione in base 3 in cui non compare mai la cifra 1 e che $E_{1/3} = \mathrm{ran}(\Phi)$.

Esercizio 9.28. Sia $\mathcal{I}$ l'insieme degli intervalli aperti massimali di $[0;1]$ disgiunti da $E_{1/3}$, cioè

$$\mathcal{I} = \{\, (a;b) \subset [0;1] \mid (a;b) \cap K = \emptyset \ \wedge \ a, b \in K \,\}$$

In altre parole: gli elementi di $\mathcal{I}$ sono gli intervalli aperti che eliminiamo nella costruzione dei $E^n_{1/3}$ (si veda pagina 80). Se $I, J \in \mathcal{I}$, allora $I \cap J \neq \emptyset$ implica che $I = J$, quindi possiamo definire l'ordine stretto $\prec$ su $\mathcal{I}$ ponendo

$$I \prec J \quad \Leftrightarrow \quad \sup I < \inf J\,.$$

Dimostrare che $\langle \mathcal{I}, \prec \rangle$ è isomorfo a $\langle \mathbb{Q}, < \rangle$.

Nel prossimo esercizio dimostreremo che nessun intervallo di $\mathbb{R}$ può essere decomposto in un unione numerabile di intervalli chiusi e disgiunti.

Esercizio 9.29. (i) Sia $(a;b) \subset \mathbb{R}$ e, per assurdo, supponiamo che $\mathcal{I}$ sia una famiglia numerabile di intervalli chiusi a due a due disgiunti tali che $\bigcup \mathcal{I} = (a;b)$. Definiamo l'ordine $\lhd$ su $\mathcal{I}$

$$\forall I < J \in \mathcal{I}\, (I \lhd J \Leftrightarrow \forall x \in I\, \forall y \in J\, (x < y))\,.$$

Dimostrare che $\langle \mathcal{I}, \lhd \rangle$ è isomorfo a $\langle \mathbb{Q}, < \rangle$.

(ii) Sia $F\colon \langle \mathcal{I}, \lhd \rangle \to \langle \mathbb{Q}, < \rangle$ un isomorfismo e sia $z \in \mathbb{R} \setminus \mathbb{Q}$. Allora gli insiemi $\bigcup \{\, I \in \mathcal{I} \mid F(I) < z \,\}$ e $\bigcup \{\, I \in \mathcal{I} \mid F(I) > z \,\}$ mostrano che $(a;b)$ è sconnesso. Concludere che $(a;b)$ non è unione numerabile di intervalli chiusi a due a due disgiunti.

(iii) Generalizzare il risultato precedente ad ogni intervallo chiuso $[a;b]$ o semi-aperto $[a;b)$ e $(a;b]$.

In analogia a quanto fatto in (43), diamo ad $\mathbb{N}^\mathbb{N}$ l'ordine lessicografico

$$x <_{\text{lex}} y \Leftrightarrow \exists n\, (x \restriction n = y \restriction n \wedge x(n) < y(n))\,.$$

Esercizio 9.30. Dimostrare che:

(i) La topologia indotta da $<_{\text{lex}}$ (vale a dire: generata dagli intervalli $(x;y)$ e da $[\vec{0};y)$ dove $\vec{0} = \langle 0, 0, \dots \rangle$) è separabile ed è indotta dalla metrica completa

$$d(x,y) = \begin{cases} 0 & \text{se } x = y, \\ 2^{-n} & \text{se } x \restriction n = y \restriction n \text{ e } x(n) \neq y(n). \end{cases}$$

(ii) La topologia dell'ordine su $\mathbb{N}^\mathbb{N}$ coincide con la topologia prodotto, dove diamo ad $\mathbb{N}$ la topologia discreta.

(iii) Lo spazio $\mathbb{N}^\mathbb{N}$ è **totalmente sconnesso** cioè ammette una base di chiusi-aperti;

(iv) $2^\mathbb{N}$ è un chiuso di $\mathbb{N}^\mathbb{N}$ e la topologia dell'ordine su $2^\mathbb{N}$ coincide con la topologia prodotto.

Nel prossimo esercizio costruiremo una suriezione continua da $2^{\mathbb{N}}$ (e quindi da $E_{1/3}$) su $[0;1]$.

Esercizio 9.31. Dimostrare che la funzione $\Psi\colon 2^{\mathbb{N}} \to [0;1]$

$$\Psi(x) = \sum_{n=0}^{\infty} \frac{2x(n)}{2^{n+1}}$$

- è ben definita (vale a dire: la serie converge),
- è suriettiva,
- $x \leq_{\text{lex}} y \Rightarrow \Psi(x) \leq \Psi(y)$,
- se $x <_{\text{lex}} y$ e $\Psi(x) = \Psi(y)$, allora $x = s^\frown\langle 0, 1, 1, \dots\rangle$ e $y = s^\frown\langle 1, 0, 0, \dots\rangle$.

Concludere che Ψ è continua.

Esercizio 9.32. Dimostrare che esistono suriezioni continue $[0;1] \twoheadrightarrow [0;1]^n$ ($n \in \mathbb{N}$) e $[0;1] \twoheadrightarrow [0;1]^{\mathbb{N}}$. (Nel caso $n = 2$ la funzione si dice **curva di Peano**.)

Esercizio 9.33. Dimostrare che se la funzione in (47) è un omeomorfismo di X sulla sua immagine e che se d è una metrica completa su X, allora l'immagine è un chiuso di $\mathbb{R}^{\mathbb{N}}$. Concludere che, a meno di omeomorfismi, tutti gli spazi separabili, metrici completi sono dei chiusi di $\mathbb{R}^{\mathbb{N}}$.

Esercizio 9.34. Verificare che la dimostrazione del Teorema 9.4 prova che ogni ordinale numerabile è immergibile come sottoinsieme *chiuso* di $\mathbb{R}$. In altre parole, per ogni $\alpha < \omega_1$ c'è una $f\colon \alpha \to \mathbb{Q}$ che preserva l'ordine e tale che $\operatorname{ran}(f)$ è un chiuso di $\mathbb{R}$.

Note e osservazioni

La dimostrazione dell'Esercizio 9.29 è dovuta a Camillo Costantini.

10. Categorie

Il linguaggio delle categorie è molto utile in varie parti della matematica. In questa sezione introdurremo le nozioni di base che verranno usate nel seguito.

Una categoria è una tripla

$$\mathfrak{C} = \langle \mathbf{Obj}^{\mathfrak{C}}, \mathbf{Arw}^{\mathfrak{C}}, \mathbf{dom}^{\mathfrak{C}}, \mathbf{cod}^{\mathfrak{C}}, \circ^{\mathfrak{C}}, \mathbf{1}\rangle$$

dove

- $\mathbf{Obj}^{\mathfrak{C}}$ e $\mathbf{Arw}^{\mathfrak{C}}$ sono classi non vuote, i cui elementi si dicono, rispettivamente, **oggetti** e **frecce** (o **morfismi**) di $\mathfrak{C}$,

- $\mathbf{dom}^{\mathfrak{C}}$ e $\mathbf{cod}^{\mathfrak{C}}$ sono funzioni (o meglio: relazioni funzionali) da $\mathbf{Arw}^{\mathfrak{C}}$ in $\mathbf{Obj}^{\mathfrak{C}}$,
- $\mathbf{1}^{\mathfrak{C}}$ è una funzione (o meglio: relazione funzionale) da $\mathbf{Obj}^{\mathfrak{C}}$ in $\mathbf{Arw}^{\mathfrak{C}}$
- $\circ^{\mathfrak{C}}$ è un'operazione binaria parziale sulle frecce: $g \circ^{\mathfrak{C}} f$ è definita se e solo se $\mathbf{cod}^{\mathfrak{C}} f = \mathbf{dom}^{\mathfrak{C}} g$, in altre parole, il dominio di $\circ^{\mathfrak{C}}$ è

$$\left\{ (g, f) \in \mathbf{Arw}^{\mathfrak{C}} \times \mathbf{Arw}^{\mathfrak{C}} \mid \mathbf{cod}^{\mathfrak{C}} f = \mathbf{dom}^{\mathfrak{C}} g \right\}$$

  Il simbolo $\circ^{\mathfrak{C}}$ si dice **operazione di composizione**.

(Quando non c'è pericolo di confusione lasceremo cadere il suffisso $\mathfrak{C}$ e scriveremo **Obj**, **Arw**, **dom**, etc.) Le seguenti proprietà devono essere soddisfatte:

(i) se f e g sono frecce e $g \circ f$ è definita, allora $\mathbf{dom}\, g \circ f = \mathbf{dom}\, f$ e $\mathbf{cod}\, g \circ f = \mathbf{cod}\, g$.

(ii) se $\mathbf{cod}\, f = \mathbf{dom}\, g$ e $\mathbf{cod}\, g = \mathbf{dom}\, h$, allora

$$h \circ (g \circ f) = (h \circ g) \circ f\,.$$

  (Questa è la proprietà associativa della composizione nelle categorie.)

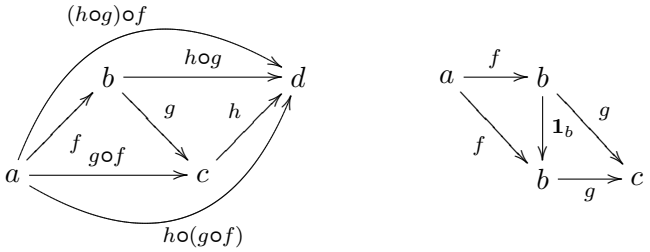
(iii) Per ogni oggetto $a \in \mathbf{Obj}$, la freccia $\mathbf{1}_a$ ha per dominio e codominio a stesso,

$$\mathbf{dom}\, \mathbf{1}_a = a = \mathbf{cod}\, \mathbf{1}_a;$$

(iv) per ogni $a, b, c \in \mathbf{Obj}$ e ogni f e g tali che $\mathbf{dom}\, f = a$, $\mathbf{cod}\, f = b = \mathbf{dom}\, g$ e $\mathbf{cod}\, g = c$, si ha che

$$f = \mathbf{1}_b \circ f \qquad \text{e} \qquad g = g \circ \mathbf{1}_b\,.$$

Una freccia da a in b è una $f \in \mathbf{Arw}^{\mathfrak{C}}$ tale che $\mathbf{dom}\, f = a$ e $\mathbf{cod}\, f = b$ e per brevità questo sarà scritto come $f\colon a \to b$ oppure $a \xrightarrow{f} b$ o ancora $a \underset{f}{\longrightarrow} b$. Le proprietà (ii) e (iv) possono essere formulate dicendo che i diagrammi



commutano.

Definiamo

$$\hom(a, b) = \{\, f \in \mathbf{Arw} \mid \mathbf{dom}(f) = a \wedge \mathbf{cod}(f) = b \,\}\,.$$

Vediamo ora qualche esempio.

10.A. Esempi di categorie.

10.A.1. *La categoria degli insiemi.* La categoria degli insiemi $\mathfrak{Set}$ ha come oggetti gli insiemi e come frecce ha le triple (a, f, b) dove f è una funzione con $\operatorname{dom} f = a$ e $\operatorname{ran} f \subseteq b$. Se poniamo $\mathbf{dom}(a, f, b) = a$, $\mathbf{cod}(a, f, b) = b$, $\circ$ l'usuale composizione di funzioni e $\mathbf{1}_a$ la funzione identità su a, si verifica facilmente che si ottiene una categoria.

La categoria degli ordini parziali $\mathfrak{POrd}$ ha per oggetti gli insiemi parzialmente ordinati $\langle A, \leq\rangle$ e per per frecce le funzioni crescenti tra ordini parziali. Anche in questo caso una freccia è una tripla (A, f, B) con $f\colon A \to B$.

Analogamente possiamo considerare $\mathfrak{Top}$, la categoria degli spazi topologici, dove i morfismi tra due spazi topologici sono funzioni continue. Oppure le categorie $\mathfrak{Grp}$, $\mathfrak{Ring}$,$\mathfrak{Vect}_{\mathbb{k}}$, rispettivamente dei gruppi, degli anelli unitari, degli spazi vettoriali sul campo $\mathbb{k}$, dove la nozione di morfismo è data da una funzione che preserva determinate strutture algebriche.

Negli esempi precedenti la classe degli oggetti era sempre una classe propria e i morfismi erano sempre delle funzioni. Nei prossimi esempi vedremo delle situazioni radicalmente differenti.

10.A.2. *La categoria più semplice.* Consideriamo la categoria più semplice in assoluto, con un unico oggetto $\bullet$ e con un unico morfismo

Questa categoria rappresenta il pre-ordine (non vuoto) più semplice, quello con un solo elemento. (Si veda la sezione 2, pagina 22 per la definizione di pre-ordine.) In effetti ogni pre-ordine $(P, \leq)$ può essere descritto come una categoria ponendo $\mathbf{Obj} = P$ e stabilendo che c'è una (ed una sola) freccia tra p e q se e solo se $p \leq q$.

10.A.3. *Monoidi.* Ogni monoide M può essere considerato come una categoria con un unico oggetto, i cui morfismi sono gli elementi di M, la composizione è l'operazione del monoide ed il morfismo privilegiato è l'identità di M.

Se f è una freccia da a in b diremo che

(1) f è **mono** ovvero che è un **monomorfismo**, in simboli $f\colon a \rightarrowtail b$, se per ogni oggetto c e ogni coppia di frecce $g\colon c \to a$ e $h\colon c \to a$

$$f \circ g = f \circ h \quad \Rightarrow \quad g = h\,.$$

(2) f è **epi** ovvero che è un **epimorfismo**, in simboli $f\colon a \twoheadrightarrow b$, se per ogni oggetto c e ogni coppia di frecce $g\colon b \to c$ e $h\colon b \to c$

$$g \circ f = h \circ f \quad \Rightarrow \quad g = h\,.$$

(3) f è **iso** ovvero che è un **isomorfismo**, in simboli $f\colon a \tilde{\to} b$, se esiste una $g\colon b \to a$ tale che $g \circ f = \mathbf{1}_a$ e $f \circ g = \mathbf{1}_b$.

Osserviamo che la freccia g in 3 è unica, si dice inversa di f e la si denota con f^{-1}: infatti se g_1 e g_2 sono inverse di f, allora

$$\begin{aligned} g_1 &= \mathbf{1}_a \circ g_1 \\ &= (g_2 \circ f) \circ g_1 \\ &= g_2 \circ (f \circ g_1) \\ &= g_2 \circ \mathbf{1}_b \\ &= g_2\,. \end{aligned}$$

Esercizio 10.1. Dimostrare che se una freccia iso è anche mono ed epi e che se $f\colon a \to b$ è iso, anche $f^{-1}\colon b \to a$ è iso.

Due oggetti a e b si dicono **isomorfi** se c'è un isomorfismo tra di loro, in simboli $a \cong b$.

10.B. Funtori. Un **funtore covariante F** dalla categoria $\mathfrak{C}$ alla categoria $\mathfrak{D}$

$$\mathbf{F}\colon \mathfrak{C} \to \mathfrak{D}$$

consiste di una mappa $\mathbf{F}\colon \mathbf{Obj}^{\mathfrak{C}} \to \mathbf{Obj}^{\mathfrak{D}}$ ed un'assegnazione (sempre denotata con $\mathbf{F}$) $\mathbf{Arw}^{\mathfrak{C}} \to \mathbf{Arw}^{\mathfrak{D}}$, tale che

(1) $\mathbf{F}(\mathbf{1}^{\mathfrak{C}}_a) = \mathbf{1}^{\mathfrak{D}}_{\mathbf{F}(a)}$,

(2) se $f\colon a \to b$ allora $\mathbf{F}(f)\colon \mathbf{F}(a) \to \mathbf{F}(b)$ e

(3) $\mathbf{F}(g \circ^{\mathfrak{C}} f) = \mathbf{F}(g) \circ^{\mathfrak{D}} \mathbf{F}(f)$.

Un **funtore controvariante F** dalla categoria $\mathfrak{C}$ alla categoria $\mathfrak{D}$ è una $\mathbf{F}$ come sopra che soddisfa (1) e

(2′) se $f\colon a \to b$ allora $\mathbf{F}(f)\colon \mathbf{F}(b) \to \mathbf{F}(a)$ e

(3′) $\mathbf{F}(g \circ^{\mathfrak{C}} f) = \mathbf{F}(f) \circ^{\mathfrak{D}} \mathbf{F}(g)$.

L'idea di fondo è che un funtore trasforma i diagrammi commutativi di $\mathfrak{C}$ in diagrammi commutativi di $\mathfrak{D}$.

Vediamo qualche esempio di funtore.

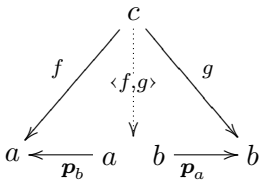
10.B.1. Consideriamo la mappa che associa ad ogni gruppo il suo insieme sostegno: poiché un omomorfismo tra gruppi è in particolare una funzione sugli insiemi sostegno è facile verificare che questo definisce un funtore covariante $\mathfrak{Grp} \to \mathfrak{Set}$ dalla categoria dei gruppi a quella degli insiemi. Un funtore di questo tipo si dice **dimenticante** in quanto dimentica in parte o del tutto la struttura dell'oggetto di partenza. Altri esempi di funtori dimenticanti sono tra la categoria degli anelli nella categoria dei gruppi abeliani, tra la categoria degli spazi topologici e quella degli insiemi, etc.

10.B.2. La costruzione dell'insieme potenza definisce un funtore covariante da $\mathfrak{Set}$ in sé stessa: ad ogni insieme a associamo $\mathscr{P}(a)$ e ad ogni funzione $f\colon a \to b$ associamo la funzione $\mathscr{P}(a) \to \mathscr{P}(b)$ data da $x \mapsto f[x]$.

10.B.3. Ad ogni spazio vettoriale W su un campo $\Bbbk$ associamo il suo duale W^* e ad ogni applicazione lineare $f\colon W \to Z$ associamo l'applicazione duale $f^*\colon Z^* \to W^*$ definita da $f^*(\alpha) = \alpha \circ f$. È immediato verificare che questo definisce un funtore controvariante dalla categoria $\mathfrak{Vect}_\Bbbk$ in sé stessa.

10.B.4. Data una categoria $\mathfrak{C}$, la **categoria opposta** $\mathfrak{C}^{\mathrm{op}}$ ha gli oggetti e le frecce di $\mathfrak{C}$ ma operazioni di **dom** e **cod** scambiate fra di loro e l'operazione di composizione viene eseguita nel verso opposto. Più precisamente: $\mathbf{Obj}^{\mathrm{op}} = \mathbf{Obj}$, $\mathbf{Arw}^{\mathrm{op}} = \mathbf{Arw}$, $\mathbf{dom}(f) = a$ e $\mathbf{cod}(f) = b$ se e solo se $\mathbf{dom}^{\mathrm{op}}(f) = b$ e $\mathbf{cod}(f) = a$ e $f \circ g = h$ se solo se $g \circ^{\mathrm{op}} f = h$. Il funtore identico è controvariante tra $\mathfrak{C}$ e $\mathfrak{C}^{\mathrm{op}}$.

10.C. Prodotti. Se a, b sono oggetti di una categoria $\mathfrak{C}$, un **prodotto** di a e b è un oggetto denotato con $a \quad b$ e due frecce $\boldsymbol{p}_a\colon a \quad b \to a$ e $\boldsymbol{p}_b\colon a \quad b \to b$ tali che per ogni coppia di frecce $f\colon c \to a$ e $g\colon c \to b$ c'è un'unica freccia $\langle f, g\rangle\colon c \to a \quad b$ che rende il diagramma



commutativo. L'esistenza e unicità della funzione $\langle f, g\rangle$ si dice **proprietà di universalità del prodotto**. Se ogni coppia di oggetti ammette un prodotto diremo che la categoria ha prodotti.

Osservazioni 10.2. (a) Abbiamo scritto *un* prodotto e non *il* prodotto in quanto $a \quad b$ è definito a meno di isomorfismi (Esercizio 10.10).

(b) La notazione $a \quad b$ non deve trarre in inganno: in molte categorie l'oggetto prodotto è ottenuto mediante un prodotto cartesiano dei due oggetti, ma ciò non è vero in generale (Esercizio 10.11).

Esercizio 10.3. Verificare che le categorie degli insiemi $\mathfrak{Set}$, dei gruppi $\mathfrak{Grp}$, degli spazi topologici $\mathfrak{Top}$ ammettono prodotti.

10.D. Limiti. Un **sistema diretto superiormente di oggetti e frecce in una categoria $\mathfrak{C}$**

$$(\langle a_i \mid i \in I\rangle, \langle f_{i,j} \mid i \leq j\rangle) \tag{48}$$

è dato da un

- insieme diretto superiormente $\langle I, \leq\rangle$

- degli oggetti di $\mathfrak{C}$, a_i per $i \in I$,
- delle frecce di $\mathfrak{C}$, $f_{i,j} \colon a_i \to a_j$, quando $i, j \in I$ e $i \leq j$ tali che

$$i \leq j \leq k \Rightarrow f_{i,k} = f_{j,k} \circ f_{i,j} \,. \tag{49}$$

Il **limite diretto** o **limite induttivo** di (48)

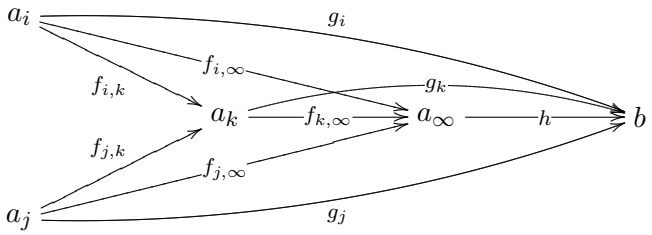
$$(a_\infty, \langle f_{i,\infty} \mid i \in I \rangle)$$

è costituito da:

- un oggetto a_∞ e
- una famiglia di frecce $f_{i,\infty} \colon a_i \to a_\infty$ $(i \in I)$ che commutano con le $f_{i,j}$, cioè

  $$f_{i,\infty} = f_{j,\infty} \circ f_{i,j} \qquad (i \leq j)$$

  e tale che per ogni oggetto b e ogni famiglia di frecce g_i $(i \in I)$ che commutano con le $f_{i,j}$, c'è un'unica freccia $h \colon a_\infty \to b$ che rende commutativo il diagramma



L'esistenza e unicità della freccia h prende il nome di **proprietà universale del limite diretto**. Il limite diretto, se esiste, è definito a meno di isomorfismi: se a_∞ e a'_∞ sono due limiti diretti per lo stesso sistema, siano $h \colon a_\infty \to a'_\infty$ e $h' \colon a'_\infty \to a_\infty$ come da definizione. Se prendiamo $b = a_\infty$ nella definizione di limite diretto, la freccia che rende commutativo il diagramma deve essere $\mathbf{1}_{a_\infty} \colon a_\infty \to a_\infty$. D'altra parte anche $h' \circ h \colon a_\infty \to a_\infty$ è una freccia che commuta, quindi $h' \circ h = \mathbf{1}_{a_\infty}$. Analogamente $h \circ h' = \mathbf{1}_{a'_\infty}$.

Non tutte le categorie ammettono limiti, neppure quando I è finito, ma molte delle categorie familiari si. In particolare le categorie $\mathfrak{Set}$, $\mathfrak{Grp}$, $\mathfrak{POrd}$, $\mathfrak{Top}$ ammettono limiti diretti.

10.D.1. *La categoria* $\mathfrak{Set}$ *degli insiemi.* Fissiamo un sistema diretto

$$(\langle A_i \mid i \in I \rangle, \langle f_{i,j} \mid i \leq j \rangle) \,.$$

Innanzitutto consideriamo un caso particolarmente semplice in cui le frecce sono funzioni di inclusione: in altre parole è data una famiglia A_i $(i \in I)$ di insiemi e la freccia $f_{i,j} \colon A_i \to A_j$ significa che $A_i \subseteq A_j$. Il limite diretto è semplicemente $\bigcup_{i \in I} A_i$.

Se le frecce $f_{i,j}$ sono funzioni iniettive, ma non necessariamente inclusioni, dobbiamo sostituire l'unione con

$$A_\infty = \big(\bigcup_{i\in I}\{i\}\times A_i\big)/\!\sim \tag{50}$$

vale a dire l'unione disgiunta degli A_i modulo la relazione d'equivalenza

$$(i,x)\sim(j,y) \quad \Leftrightarrow \quad \exists k\,(i\le k \ \wedge\ j\le k \ \wedge\ f_{i,k}(x)=f_{j,k}(y))\,.$$

Le funzioni $f_{i,\infty}\colon A_i\to A_\infty$ sono date da

$$f_{i,\infty}(x)=[(i,x)]_\sim\,. \tag{51}$$

Se B è un altro insieme e $g_i\colon A_i\to B$ commutano con le $f_{i,j}$, definiamo $h\colon A_\infty\to B$

$$[(i,x)]_\sim\mapsto g_i(x)\,. \tag{52}$$

Verifichiamo che la definizione non dipende dal rappresentante cioè se $(i,x)\sim(j,y)$ allora $g_i(x)=g_j(y)$. Sia $k\ge i,j$ tale che $f_{i,k}(x)=f_{j,k}(y)$: allora

$$\begin{aligned} g_i(x) &= g_k(f_{i,k}(x))\\ &= g_k(f_{j,k}(y))\\ &= g_j(y)\end{aligned}$$

come richiesto.

Esercizio 10.4. Verificare che la funzione in (52) è l'unica funzione che verifica la proprietà universale del limite diretto.

Osserviamo che l'ipotesi che le $f_{i,j}$ fossero iniettive non è stata usata. Infatti, la costruzione in (50) e (51) funziona per *ogni* sistema diretto di insiemi e funzioni.

10.D.2. *La categoria dei gruppi* $\mathfrak{Grp}$. Il limite di un sistema diretto di gruppi G_i, $(i\in I)$ e omomorfismi $f_{i,j}$ $(i\le j)$ è il gruppo che ha G_∞ il cui insieme supporto è dato da (50). L'operazione su G_∞ è data da

$$[(i,x)]\cdot[(j,y)]=[(k,f_{i,k}(x)\cdot f_{j,k}(y))]$$

dove $k\ge i,j$ e la moltiplicazione $f_{i,k}(x)\cdot f_{j,k}(y)$ è effettuata in G_k. Verifichiamo che la definizione non dipende dalla scelta dei rappresentanti. Supponiamo che $(i,x)\sim(i',x')$ e $(j,y)\sim(j',y')$, $k\ge i,j$ e $k'\ge i',j'$: dobbiamo verificare che

$$(k,f_{i,k}(x)\cdot f_{j,k}(y))\sim(k',f_{i',k'}(x')\cdot f_{j',k'}(y'))\,.$$

Siano $i^* \geq i, i'$ e $j^* \geq j, j'$ tali che $f_{i,i^*}(x) = f_{i',i^*}(x')$ e $f_{j,j^*}(y) = f_{j',j^*}(y')$ e sia $k^* \geq k, k', i^*, j^*$. Allora

$$\begin{aligned} f_{i,k^*}(x) \cdot f_{j,k^*}(y) &= f_{i^*,k^*}\big(f_{i,i^*}(x)\big) \cdot f_{j^*,k^*}\big(f_{j,j^*}(y)\big) \\ &= f_{i^*,k^*}\big(f_{i',i^*}(x')\big) \cdot f_{j^*,k^*}\big(f_{j',j^*}(y')\big) \\ &= f_{i',k^*}(x') \cdot f_{j',k^*}(y')\,, \end{aligned}$$

come dovevasi dimostrare.

L'identità di G_∞ è $[(i, 1_{G_i})]_\sim$, dove 1_{G_i} è l'identità di G_i. I morfismi $f_{i,\infty}\colon G_i \to G_\infty$ sono definiti da (51).

Esercizio 10.5. Verificare che G_∞ verifica la proprietà universale dei limiti diretti.

10.D.3. *La categoria degli ordini parziali* $\mathfrak{POrd}$. Dato un sistema diretto di ordini $\langle A_i, \preccurlyeq_i\rangle$ $(i \in I)$ e funzioni crescenti $f_{i,j}\colon A_i \to A_j$ (con $i \leq j$) il limite diretto è l'insieme ordinato $\langle A_\infty, \preccurlyeq_\infty\rangle$ dove $A\infty$ è l'insieme definito in (50) e $\preccurlyeq_\infty$ è l'ordinamento

$$[(i,x)]_\sim \preccurlyeq_\infty [(j,y)]_\sim \quad \Leftrightarrow \quad \exists k\,(k \geq i, j \ \wedge \ f_{i,k}(x) \preccurlyeq_k f_{j,k}(y))$$

Lasciamo al lettore la verifica che la definizione non dipende dalla scelta dei rappresentanti. Le funzioni $f_{i,\infty}\colon A_i \to A_\infty$ sono come in (51): per la commutatività delle $f_{i,j}$, se $x, y \in A_i$ e $x \preccurlyeq_i y$ allora $f_{i,j}(x) \preccurlyeq_j f_{i,j}(y)$ per ogni $i \leq j$ e quindi $f_{i,\infty}(x) \preccurlyeq_\infty f_{i,\infty}(y)$.

Esercizio 10.6. Dimostrare che se gli $\langle A_i, \preccurlyeq_i\rangle$ sono ordini lineari, allora $\langle A_\infty, \preccurlyeq_\infty\rangle$ è lineare. Dimostrare con un contro-esempio che gli $\langle A_i, \preccurlyeq_i\rangle$ possono essere tutti dei buoni ordini, ma $\langle A_\infty, \preccurlyeq_\infty\rangle$ non è necessariamente un buon ordine.

10.D.4. *La categoria degli spazi topologici* $\mathfrak{Top}$. Dato un sistema diretto di spazi topologici $(X_i, \mathcal{T}_i)$ $(i \in I)$ funzioni continue $f_{i,j}\colon X_i \to X_j$ $(i \leq j)$ è lo spazio $(X_\infty, \mathcal{T}_\infty)$ dove X_∞ è l'insieme limite diretto degli insiemi X_i (50) e la topologia è

$$\mathcal{T}_\infty = \Big\{\, U \subseteq X_\infty \mid \forall i \in I \ f_{i,\infty}^{-1}(U) \in \mathcal{T}_i \,\Big\}\,.$$

Verifichiamo che $\mathcal{T}_\infty$ è una topologia su X_∞. Chiaramente $\emptyset, X_\infty \in \mathcal{T}_\infty$. Se $U, Y \in \mathcal{T}_\infty$, allora $f_{i,\infty}^{-1}(U \cap V) = f_{i,\infty}^{-1}(U) \cap f_{i,\infty}^{-1}(V) \in \mathcal{T}_i$ per ogni $i \in I$, cioè $\mathcal{T}_\infty$ è chiusa per intersezioni finite. Se $\{\, U_j \mid j \in J \,\} \subseteq \mathcal{T}_\infty$, allora $f_{i,\infty}^{-1}\left(\bigcup_{j\in J} U_j\right) = \bigcup_{j\in J} f_{i,\infty}^{-1}(U_j) \in \mathcal{T}_i$, per ogni $i \in I$, da cui $\bigcup_{j\in J} U_j \in \mathcal{T}_\infty$. Quindi $\mathcal{T}_\infty$ è una topologia su X_∞.

Le funzioni $f_{i,\infty}\colon X_i \to X_\infty$ sono continue per definizione di $\mathcal{T}_\infty$. Verifichiamo che vale la proprietà di universalità. $(X', \mathcal{T}')$ uno spazio topologico e $g_i\colon X_i \to X'$ funzioni continue che commutano con le $f_{i,j}$. Poiché la funzione

$h\colon X_\infty \to X'$ definita da (52) è l'unica funzione che rende sia commutativo il diagramma, è sufficiente dimostrare che è continua: se $U' \subseteq X'$ è aperto,

$$f_{i,\infty}^{-1}\big(h^{-1}(U')\big) = g_i^{-1}(U') \in \mathcal{T}_i$$

e quindi $h^{-1}(U') \in \mathcal{T}_\infty$. Quindi $(X_\infty, \mathcal{T}_\infty)$ è il limite diretto del sistema.

10.E. Il teorema di Cantor-Lawvere*. Le categorie che utilizzeremo in questo corso sono sono abbastanza vicine alla teoria degli insiemi, nel senso che le frecce tra oggetti sono funzioni che soddisfano opportune proprietà. Per queste categorie è possibile dimostrare una generalizzazione del Teorema di Cantor 8.9.

Teorema 10.7 (Lawvere)**.** *Sia $\mathfrak{C}$ una categoria in cui le frecce sono funzioni, siano a, b oggetti di $\mathfrak{C}$ e supponiamo $F\colon a \to \hom(a,b)$ sia una suriezione tale che*

$$a \to b \qquad x \mapsto F(x)(x)$$

sia un morfismo di $\mathfrak{C}$. Allora b ha la proprietà del punto fisso, cioè per ogni morfismo $f\colon b \to b$ c'è un $x \in b$ tale che $f(x) = x$.

Dimostrazione. Sia $f\colon b \to b$ un morfismo e sia $g\colon a \to b$ la funzione

$$g(x) = f(F(x)(x))\,. \tag{53}$$

Per l'ipotesi su F, la g è un morfismo di $\mathfrak{C}$ e c'è un $\bar{x} \in a$ tale che $F(\bar{x}) = g$. Sia $\bar{y} = g(\bar{x}) \in b$. Allora

$$\begin{aligned} f(\bar{y}) &= f(g(\bar{x})) \\ &= f\big(F(\bar{x})(\bar{x})\big) && \text{(dato che } g = F(\bar{x})\text{)} \\ &= g(\bar{x}) && \text{(per (53))} \\ &= \bar{y} \end{aligned}$$

vale a dire: $\bar{y}$ è il punto fisso del morfismo g. □

Come corollario otteniamo il Teorema 8.9.

Corollario 10.8 (Cantor)**.** *Se X e Y sono insiemi e Y ha almeno due elementi, non c'è nessuna suriezione $X \twoheadrightarrow Y^X$.*

Analogamente, se X e Y sono spazi topologici e c'è una funzione continua $f\colon Y \to Y$ priva di punti fissi, allora non c'è nessuna suriezione

$$F\colon X \twoheadrightarrow \mathcal{C}(X,Y) \stackrel{\text{def}}{=} \{\, f\colon X \to Y \mid f \text{ è continua} \,\}$$

tale che la mappa $X \to Y$, $x \mapsto F(x)(x)$, sia continua.

Esercizi

Esercizio 10.9. (i) Verificare che nella categoria degli insiemi le frecce mono, epi e iso sono le funzioni iniettive, suriettive e bijettive, rispettivamente.

(ii) Dimostrare che nella categoria degli spazi topologici le frecce mono sono funzioni iniettive; nella categoria degli spazi topologici T_2, una funzione continua $f\colon X \to Y$ è epi se e solo se $\mathrm{ran}(f)$ è denso in Y.

(iii) Considerare il monoide $\langle \mathbb{N}, +, 0\rangle$ come categoria—si veda l'esempio 10.A.3. Dimostrare che tutte le frecce sono mono e epi, ma solo 0 è iso.

Esercizio 10.10. Dimostrare che il prodotto di due oggetti (se esiste) è unico a meno di isomorfismi.

Esercizio 10.11. Consideriamo un insieme parzialmente ordinato $\langle P, \leq\rangle$ come una categoria: gli oggetti sono gli elementi di P e assegniamo una freccia $p \to q$ se e solo se $p \leq q$. Dimostrare che questa categoria ha prodotti se e solo se $\langle P, \leq\rangle$ è un semi-reticolo inferiore e $p \quad q = \inf\{p, q\}$.

Note e osservazioni

La teoria delle categorie è stata inventata nel 1942 da Samuel Eilenberg (1913–1998) e Saunders Mac Lane (1909–2005) nell'ambito della topologia algebrica. La nostra trattazione è molto ridotta—lo studente interessato può consultare i testi [**ML98**] e [**Gol84**].

11. Reticoli e algebre di Boole

11.A. Algebre di Boole. Un **reticolo** è un insieme ordinato $\langle L, \leq\rangle$ in cui ogni coppia di elementi x e y ammette estremo superiore ed inferiore. Nella teoria dei reticoli si usa denotare

- $\sup\{x, y\}$ con $x \vee y$, o $x \curlyvee y$ o $x \sqcup y$ e
- $\inf\{x, y\}$ con $x \wedge y$, o $x \curlywedge y$ o $x \sqcap y$.

Chiaramente, in un reticolo

$$x \leq y \quad \Leftrightarrow \quad x = x \wedge y \quad \Leftrightarrow \quad y = x \vee y\,.$$

Un reticolo $\langle L, \leq\rangle$ si dice:

- **distributivo** se

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z) \tag{54}$$

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z) \tag{55}$$

  per ogni $x, y, z \in L$;
- **complementato** se esistono il massimo $1 = 1_L$ e il minimo $0 = 0_L$ e se per ogni x c'è un y, detto **complemento** di x, tale che

$$x \wedge y = 0 \quad \text{e} \quad x \vee y = 1\,;$$

- **completo** se $\sup X = \bigvee X$ e $\inf X = \bigwedge X$ esistono per ogni $X \subseteq L$.

È facile verificare che le operazioni $\wedge$ e $\vee$ sono commutative e associative e che se $X \subseteq L$ è *finito* esistono sempre $\bigvee X$ e $\bigwedge X$.

Lemma 11.1. *In un reticolo distributivo $\langle L, \leq\rangle$ il complemento di un elemento x è unico e si denota con x^*.*

Dimostrazione. Supponiamo y e z siano complementi di un x:

$$y = 1 \wedge y = (x \vee z) \wedge y = (x \wedge y) \vee (z \wedge y) = 0 \vee (y \wedge z) = y \wedge z\,,$$

da cui $y \leq z$. Analogamente, scambiando y con z, otteniamo che $z \leq y$. □

Quindi, se $\langle B, \leq\rangle$ è un reticolo complementato e distributivo

$$x \vee y = y \vee x \qquad x \wedge y = y \wedge x \tag{56}$$

$$x \vee (y \vee z) = (x \vee y) \vee z \qquad x \wedge (y \wedge z) = (x \wedge y) \wedge z \tag{57}$$

$$(x \vee y) \wedge y = y \qquad (x \wedge y) \vee y = y \tag{58}$$

$$(x \vee y) \wedge z = (x \wedge y) \vee (x \wedge z) \qquad (x \wedge y) \vee z = (x \vee y) \wedge (x \vee z) \tag{59}$$

$$x \vee x^* = 1 \qquad x \wedge x^* = 0 \tag{60}$$

per ogni $x, y, z \in B$. Quindi

$$\langle B, \leq\rangle \mapsto \langle B, \vee, \wedge, ^*, 0, 1\rangle \tag{61}$$

è una corrispondenza tra reticoli distributivi complementati e strutture algebriche dotate di due elementi privilegiati 0 e 1, operazioni binarie $\vee$ e $\wedge$ ed un'operazione unaria * che soddisfano (56)–(60). Viceversa, se B è una struttura come sopra, possiamo definire un ordine $\leq$ su B

$$x \leq y \Leftrightarrow x \wedge y = x\,.$$

Allora $\langle B, \leq\rangle$ è un reticolo distributivo complementato tale che $\inf\{x, y\} = x \wedge y$ e $\sup\{x, y\} = x \vee y$, $\min(B) = 0$ e $\max(B) = 1$. Inoltre la corrispondenza che trasforma strutture algebriche che soddisfano (56)–(60) in reticoli distributivi complementati è l'inversa di (61) (Esercizio 11.27).

I risultati precedenti possono essere formulati convenientemente col linguaggio delle categorie dicendo che la categoria dei reticoli complementati e

distributivi è isomorfa alla categoria delle strutture algebriche che soddisfano (56)–(60).

Definizione 11.2. Un'**algebra di Boole** è un reticolo $\langle B, \leq \rangle$ complementato e distributivo con almeno due elementi o, equivalentemente, è una struttura algebrica $\langle B, \wedge, \vee, ^*, 0, 1 \rangle$ dove 0 e 1 sono distinti, $\wedge$ e $\vee$ sono operazioni binarie su B e * è un'operazione unaria su B che soddisfano (56)–(60).

L'esempio più importante di algebra di Boole è $\langle \mathscr{P}(X), \subseteq \rangle$ con $X \neq \emptyset$, ovvero la struttura algebrica

$$\langle \mathscr{P}(X), \cap, \cup, ', \emptyset, X \rangle ,$$

dove $Y' = X \setminus Y$ è il complementare di Y in X.

Esercizio 11.3. Dimostrare che:

(i) $x \wedge y = 0 \Leftrightarrow x \leq y^*$;

(ii) $(x \wedge y)^* = x^* \vee y^*$ e $(x \vee y)^* = x^* \wedge y^*$ (Leggi di de Morgan);

(iii) $x \leq y \Leftrightarrow y^* \leq x^*$;

(iv) se $x \leq y$ e $z \leq w$, allora $x \wedge z \leq y \wedge w$ e $x \vee z \leq y \vee w$.

Lemma 11.4. *In un'algebra di Boole,*

$$x \wedge y \leq z \quad \Leftrightarrow \quad x \leq z \vee y^* .$$

Dimostrazione. Supponiamo $x \wedge y \leq z$: allora $x = x \wedge (y \vee y^*) = (x \wedge y) \vee (x \wedge y^*) \leq z \vee y^*$. Viceversa, $x \leq z \vee y^*$ implica che $x \wedge y \leq (z \vee y^*) \wedge y = (z \wedge y) \vee (y^* \wedge y) = z \wedge y \leq z$. □

Un'algebra di Boole B si dice **completa** se è completa come reticolo.

Proposizione 11.5. *Un'algebra di Boole B è completa se e solo se esiste $\bigvee X$ per ogni $X \subseteq B$ o, equivalentemente, se esiste $\bigwedge X$ per ogni $X \subseteq B$.*

Dimostrazione. Supponiamo che ogni $X \subseteq B$ ammetta un estremo superiore e sia $Y \subseteq B$. Per ipotesi esiste $b = \bigvee \{ y^* \mid y \in Y \}$ e quindi b^* è un minorante di Y. Se c è un minorante di Y allora c^* è un maggiorante di $\{ y^* \mid y \in Y \}$, quindi $c^* \geq b$, da cui $c \leq b^*$. Segue che $b^* = \bigwedge Y$.

La dimostrazione che se ogni sottoinsieme ammette un estremo inferiore, allora l'algebra è completa è lasciato come esercizio. □

Osservazione 11.6. Le formule (56)–(60) mostrano una *dualità*: se in una formula della colonna di sinistra si scambiano $\wedge$ con $\vee$ e 0 con 1 si ottiene l'analoga formula della colonna di destra. Quindi, se a partire da (56)–(60) si dimostra l'identità

$$\boldsymbol{t}(x_1, \ldots, x_n) = \boldsymbol{s}(x_1, \ldots, x_n)$$

oppure la disuguaglianza

$$\boldsymbol{t}(x_1, \dots, x_n) \leq \boldsymbol{s}(x_1, \dots, x_n)$$

dove $\boldsymbol{t}(x_1, \dots, x_n)$ e $\boldsymbol{s}(x_1, \dots, x_n)$ sono espressioni[2] costruite a partire da $\wedge$, $\vee$, 0 e 1, allora si può dimostrare a partire da (56)–(60) l'identità o la disuguaglianza *duale*

$$\check{\boldsymbol{s}}(x_1, \dots, x_n) = \check{\boldsymbol{t}}(x_1, \dots, x_n)$$
$$\check{\boldsymbol{s}}(x_1, \dots, x_n) \leq \check{\boldsymbol{t}}(x_1, \dots, x_n)\,,$$

dove $\check{\boldsymbol{t}}(x_1, \dots, x_n)$ e $\check{\boldsymbol{s}}(x_1, \dots, x_n)$ sono le espressioni ottenute scambiando $\wedge$ con $\vee$ e 0 con 1.

Lemma 11.7. *Sia B un'algebra di Boole e $X \subseteq B$ un insieme tale che $\bigvee X$ esiste. Allora, per ogni $b \in B$, $\bigvee \{\, b \wedge x \mid x \in X \,\}$ esiste e*

$$b \wedge \bigvee X = \bigvee \{\, b \wedge x \mid x \in X \,\}\,.$$

Analogamente, se $\bigwedge X$ esiste, allora anche $\bigwedge \{\, b \vee x \mid x \in X \,\}$ esiste ed è $b \vee \bigwedge X$.

Dimostrazione. $b \wedge x \leq b \wedge \bigvee X$ per ogni $x \in X$, allora $b \wedge \bigvee X$ è un maggiorante di $\{\, b \vee x \mid x \in X \,\}$. Se c è un altro maggiorante di questo insieme, allora per ogni $x \in X$,

$$b \wedge x \leq c \Rightarrow x \leq b^* \vee c$$

per il Lemma 11.4 e quindi $\bigvee X \leq b^* \vee c$, da cui $b \wedge \bigvee X \leq c$. □

11.B. Morfismi e anelli Booleani.

Definizione 11.8. Un omomorfismo di algebre di Boole $f\colon \langle B, \leq\rangle \to \langle C, \preccurlyeq\rangle$ è una funzione $f\colon B \to C$ tale che $f(0_B) = 0_C$, $f(1_B) = 1_C$ e per ogni $b_1, b_2 \in B$

$$f(b_1 \wedge b_2) = f(b_1) \curlywedge f(b_2) \quad \text{e} \quad f(b_1 \vee b_2) = f(b_1) \curlyvee f(b_2)$$

dove $\curlywedge$ e $\curlyvee$ sono gli operatori di inf e sup di C. Se $f\colon B \to C$ è una bijezione, allora anche f^{-1} è un omomorfismo. Due algebre di Boole si dicono isomorfe se c'è un isomorfismo tra esse.

Esercizio 11.9. Dimostrare che se $f\colon \langle B, \leq\rangle \to \langle C, \preccurlyeq\rangle$ è un omomorfismo di algebre di Boole, allora

$$\forall b \in B\, (f(b^*) = f(b)^\star)$$

dove $c^\star$ è il complemento di c in C.

[2]Come vedremo nella sezione 20.C.4 espressioni siffatte si dicono *termini*.

Una **sub-algebra** di B è un $C \subseteq B$ non-vuoto e chiuso per $\wedge$, $\vee$ e *; equivalentemente, se la funzione identica $C \to B$ è un omomorfismo di algebre.

Esercizio 11.10. Sia B un'algebra di Boole. Dimostrare che:

(i) Se $\emptyset \neq C \subseteq B$, allora C è una sub-algebra di B se e solo se è chiuso per * e $\wedge$ se e solo se è chiuso per * e $\vee$.

(ii) Se $\mathcal{B}$ è una famiglia di sub-algebre di B, allora $\bigcap \mathcal{B}$ è una sub-algebra di B. In particolare, se $\mathcal{B}$ è l'insieme delle sub-algebre che contengono un insieme X, allora $\bigcap \mathcal{B}$ è l'algebra generata da X, cioè la più piccola sub-algebra di B contenente X.

(iii) se $f\colon B \to C$ è un morfismo di algebre di Boole, allora $\mathrm{ran}(f)$ è una sub-algebra di C.

La somma in un'algebra di Boole è l'operazione binaria $+$ definita da

$$x + y \stackrel{\text{def}}{=} (x \wedge y^*) \vee (y \wedge x^*). \tag{62}$$

Osserviamo che se $f\colon B \to C$ è un omomorfismo di algebre di Boole, allora $f(x + y) = f(x) + f(y)$.

Esercizio 11.11. (i) $x = y \Leftrightarrow x + y = 0$;

(ii) $x + y = y + x$;

(iii) $(x + y)^* = (x \wedge y) \vee (x^* \wedge y^*)$;

(iv) $x + (y + z) = (x + y) + z$;

(v) $x \wedge (y + z) = (x \wedge y) + (x \wedge z)$.

Quindi ad ogni algebra di Boole possiamo associare un anello commutativo unitario,

$$\langle B, \vee, \wedge, ^*, 0, 1\rangle \mapsto \langle B, +, \cdot, 0, 1\rangle \tag{63}$$

ponendo $x + y$ come in (62) e

$$x \cdot y \stackrel{\text{def}}{=} x \wedge y\,.$$

In un anello siffatto vale $x^2 = x$, per ogni x, e un anello che gode di questa proprietà si dice **anello Booleano**. Ogni anello Booleano è l'anello costruito a partire da una qualche algebra di Boole (Esercizio 11.31) e ogni omomorfismo $f\colon B \to C$ di algebre di Boole è un omomorfismo di anelli con unità. In altre parole: la corrispondenza (63) è un funtore covariante dalla categoria delle algebre di Boole nella categoria degli anelli Booleani ed è un isomorfismo di categorie. Il **nucleo** di un morfismo di algebre di Boole $f\colon B \to C$ è

$$\ker(f) \stackrel{\text{def}}{=} \{\, b \in B \mid f(b) = 0_C \,\}\,.$$

Quindi f è iniettivo se e solo se il suo nucleo è $\{0_B\}$.

11.C. Atomi. Un **atomo** di un'algebra di Boole B è un elemento minimale di $B \setminus \{0\}$ cioè un $a \in B \setminus \{0\}$ per cui non esistono $0 < b < a$. L'insieme degli atomi di B si indica con $\mathrm{At}(B)$. Un'algebra si dice **atomica** se per ogni $b \in B \setminus \{0\}$ c'è un atomo $a \leq b$.

Esercizio 11.12. Se B è un'algebra di Boole finita, allora è atomica e completa.

Proposizione 11.13. *Se B è un'algebra di Boole e $a \in B$, le seguenti condizioni sono equivalenti:*

(a) $a \in \mathrm{At}(B)$*;*

(b) $a \neq 0$ *e per ogni $b, c \in B$, $a \leq b \vee c$ se e solo se $a \leq b$ oppure $a \leq c$;*

(c) *per ogni $b \in B$, $a \leq b$ oppure $a \leq b^*$, ma non entrambi.*

Dimostrazione. (a) $\Rightarrow$ (b). Se $a \leq b$ oppure $a \leq c$ allora, chiaramente, $a \leq b \vee c$. Viceversa, se $a \not\leq b$ e $a \not\leq c$, allora $a \wedge b^* \neq 0$ e $a \wedge c^* \neq 0$ per la parte (i) dell'Esercizio 11.3. Poiché a è un atomo, $a \wedge b^* = a$ e $a \wedge c^* = a$, cioè $a \leq b^*$ e $a \leq c^*$, da cui $a \leq b^* \wedge c^* = (b \vee c)^*$. Se $a \leq b \vee c$ allora $a \leq (b \vee c)^* \wedge (b \vee c) = 0$: una contraddizione. Quindi $a \not\leq b \vee c$.

(b) $\Rightarrow$ (c). Fissato $b \in B$, si ha che $a \leq 1 = b \vee b^*$ e quindi $a \leq b$ oppure $a \leq b^*$. Tuttavia, non è possibile che $a \leq b$ e $a \leq b^*$ valgano entrambe poiché ciò implicherebbe $a \leq 0 = b \wedge b^*$.

(c) $\Rightarrow$ (a). Osserviamo che (c) implica banalmente che $a \neq 0$. Se esistesse $0 < b < a$, allora $a \not\leq b$ implica che $a \leq b^*$, da cui $0 = a \wedge b^{**} = a \wedge b = b$, contraddizione. □

Teorema 11.14. (a) *Per ogni algebra di Boole B tale che $\mathrm{At}(B) \neq \emptyset$, la funzione $F\colon B \to \mathscr{P}(\mathrm{At}(B))$*

$$F(b) = \{\, a \in \mathrm{At}(B) \mid a \leq b \,\}$$

è un omomorfismo.

(b) *B è atomica se e solo se F è iniettivo.*

(c) *Se B è completa, o anche solo: se $\bigvee X$ esiste per ogni $X \subseteq \mathrm{At}(B)$, allora F è suriettivo.*

Dimostrazione. (a) Sia $a \in \mathrm{At}(B)$. Allora $a \leq b \wedge c$ se e solo se $a \leq b$ e $a \leq c$ e per la Proposizione 11.13, $a \leq b \vee c$ se e solo se $a \leq b$ oppure $a \leq c$. Quindi $F(b \wedge c) = F(b) \cap F(c)$ e $F(b \vee c) = F(b) \cup F(c)$, cioè F è un omomorfismo.

(b) È immediato verificare che F è atomica se e solo se $\ker(F) = \{0\}$ se e solo se F è iniettivo.

(c) Se $X \subseteq \mathrm{At}(B)$, sia $b = \bigvee X$. Allora $X \subseteq F(b)$. Vogliamo dimostrare che $X = F(b)$: se per assurdo esistesse $a \in F(b) \setminus X$, allora, trattandosi di atomi, $\forall x \in X\,(a \wedge x = 0)$, quindi per la Proposizione 11.7

$$a = a \wedge b = a \wedge \bigvee X = \bigvee \{\, a \wedge x \mid x \in X \,\} = 0\,,$$

contraddizione. □

Corollario 11.15. *Ogni algebra di Boole atomica è isomorfa ad una sub-algebra di $\mathscr{P}(I)$, per qualche insieme I. Ogni algebra di Boole atomica e completa (o anche solo: tale che $\bigvee X$ esiste per ogni X insieme di atomi) è isomorfa a $\mathscr{P}(I)$, per qualche insieme I.*

11.D. Esempi di algebre di Boole.

11.D.1. $\langle \mathscr{P}(X), \subseteq \rangle$ è un'algebra di Boole (se $X \neq \emptyset$) ed è atomica e completa. Le operazioni di reticolo sono $\cap$ e $\cup$, il complemento di A è $X \setminus A$. Una sub-algebra di $\mathscr{P}(X)$ è un $\emptyset \neq \mathcal{F} \subseteq \mathscr{P}(X)$ chiuso per unioni, intersezioni e complementi. Per il Teorema di Stone 14.12 ogni algebra di Boole è isomorfa ad una sub-algebra $\mathcal{F}$ di qualche $\mathscr{P}(X)$. L'operazione di somma $+$ in $\mathscr{P}(X)$ (o in una sua sub-algebra) è la differenza simmetrica $\triangle$.

11.D.2. Su ogni insieme di due elementi, per esempio $\{0, 1\}$ possiamo dare una struttura di algebra di Boole ponendo $0 < 1$. è banalmente completa ed atomica. Poiché tutte le algebre di questo tipo sono isomorfe, l'unica algebra di Boole con due elementi si dice **algebra minimale** ed è (isomorfa ad) una sub-algebra di ogni algebra di Boole. L'operazione di somma è l'addizione modulo 2.

11.D.3. Se X è un insieme,

$$\{\, Y \subseteq X \mid |Y| < \aleph_0 \ \vee\ |X \setminus Y| < \aleph_0 \,\}$$

è una sub-algebra di $\mathscr{P}(X)$. Chiaramente, se X è finito, coincide con $\mathscr{P}(X)$.

Più in generale, se $\lambda \leq \kappa$ sono cardinali infiniti,

$$\{\, Y \subseteq \kappa \mid |Y| < \lambda \ \vee\ |\kappa \setminus Y| < \lambda \,\}$$

è una sub-algebra di $\mathscr{P}(\kappa)$.

11.D.4. Se X è uno spazio topologico, un insieme U si dice **chiuso-aperto**[3] se è simultaneamente chiuso ed aperto.

$$\mathrm{CLOP}(X) = \{\, U \subseteq X \mid U \text{ è chiuso-aperto in } X \,\}$$

è una sub-algebra di $\mathscr{P}(X)$ che si chiama **algebra dei chiusi-aperti** Se X è connesso $\mathrm{CLOP}(X)$ è l'algebra minimale. In generale $\mathrm{CLOP}(X)$ non è completa. Contiene atomi se X ha punti isolati.

[3] In inglese *clopen*.

11.D.5. Un aperto U di uno spazio topologico X si dice **regolare** se

$$r(U) \stackrel{\text{def}}{=} \operatorname{Int}(\operatorname{Cl}(U)) = U\,.$$

Esercizio 11.16. Dimostrare che se U, V sono aperti di X:

(i) $r(U)$ è il più piccolo aperto regolare contenete U,

(ii) $U \subseteq V \Rightarrow r(U) \subseteq r(V)$;

(iii) $r(r(U)) = r(U)$;

(iv) se U è regolare, allora $\operatorname{Int}(X \setminus U)$ è regolare.

Se U, V sono aperti regolari, allora $r(U \cap V) \subseteq r(U) = U$ e $r(U \cap V) \subseteq r(V) = V$, da cui $r(U \cap V) \subseteq U \cap V$. Quindi l'intersezione di due aperti regolari è un aperto regolare.

Esercizio 11.17. Dimostrare con un esempio che l'unione di aperti regolari non è necessariamente regolare.

Se U è aperto (non necessariamente regolare) e Y arbitrario, allora $U \cap \operatorname{Cl}(Y) \subseteq \operatorname{Cl}(U \cap Y)$, quindi, tenendo presente che l'interno di un'intersezione è l'intersezione degli interni,

$$\begin{aligned} U \cap \operatorname{Int}(\operatorname{Cl}(Y)) &= \operatorname{Int}(U) \cap \operatorname{Int}(\operatorname{Cl}(Y)) \\ &= \operatorname{Int}(U \cap \operatorname{Cl}(Y)) \\ &\subseteq \operatorname{Int}(\operatorname{Cl}(U \cap Y))\,. \end{aligned}$$

In particolare, se V è aperto

$$U \cap r(V) \subseteq r(U \cap V)\,. \tag{64}$$

Definiamo una struttura di algebra di Boole su

$$\operatorname{RO}(X) = \{\, U \subseteq X \mid U \text{ è regolare} \,\}$$

ponendo $U \wedge V = U \cap V$, $U \vee V = r(U \cup V)$ e $U^* = \operatorname{Int}(X \setminus U)$. Verifichiamo, per esempio, la proprietà distributiva. Siano $U, V, W \in \operatorname{RO}(X)$:

$$\begin{aligned} U \wedge (V \vee W) &= U \cap r(V \cup W) \\ &\subseteq r(U \cap (V \cup W)) && \text{(per (64))} \\ &= r((U \cap V) \cup (U \cap W)) \\ &= (U \wedge V) \vee (U \wedge W)\,. \end{aligned}$$

$\operatorname{RO}(X)$ è l'**algebra degli aperti regolari** di X. Se $\mathcal{A}$ è una famiglia di aperti regolari, $\bigvee \mathcal{A} = r(\bigcup \mathcal{A})$; quindi $\operatorname{RO}(X)$ è un'algebra completa.

$\operatorname{CLOP}(X)$ è una sub-algebra di $\operatorname{RO}(X)$, ma, in generale, $\operatorname{RO}(X)$ non è una sub-algebra di $\mathscr{P}(X)$.

11.D.6. Sia $\langle L, \leq\rangle$ linearmente ordinato e sia $\mathfrak{I}$ l'insieme di tutti gli intervalli della forma $(a; b]$ e delle semirette della forma

$$\{\, x \in L \mid x \leq b \,\} \quad \text{e} \quad \{\, x \in L \mid a < x \,\}\,.$$

Sia B l'insieme delle unioni finite di elementi di $\mathfrak{I}$:

$$B \stackrel{\text{def}}{=} \Big\{ \bigcup \mathcal{J} \mid \mathcal{J} \subseteq \mathfrak{I}, |\mathcal{J}| < \omega \Big\}\,.$$

B è una sub-algebra di $\mathscr{P}(L)$ e si dice l'**algebra degli intervalli** di $\langle L, \leq\rangle$.

Esercizio 11.18. Dimostrare che se $\langle L, \leq\rangle$ è denso allora l'algebra degli intervalli è priva di atomi.

11.E. Algebre finitamente generate. Il Lemma 11.7 implica che

$$x \wedge \bigvee_{i\in I} y_i = \bigvee_{i\in I} (x \wedge y_i) \quad \text{e} \quad x \vee \bigwedge_{i\in I} y_i = \bigwedge_{i\in I} (x \vee y_i)\,,$$

dove I è un insieme arbitrario. È possibile generalizzare questa formula a patto di considerare insiemi finiti di indici finiti.

Lemma 11.19. *Sia B un'algebra di Boole e siano I e J_i ($i \in I$) degli insiemi finiti e non vuoti. Allora, per ogni $x_{i,j} \in B$ ($i \in I$ e $j \in J_i$)*

$$\bigwedge_{i\in I} \bigvee_{j\in J_i} x_{i,j} = \bigvee_{f\in \mathsf{X}_{i\in I} J_i} \bigwedge_{i\in I} x_{i,f(i)} \quad e \quad \bigvee_{i\in I} \bigwedge_{j\in J_i} x_{i,j} = \bigwedge_{f\in \mathsf{X}_{i\in I} J_i} \bigvee_{i\in I} x_{i,f(i)}\,. \tag{65}$$

Dimostrazione. Per dualità è sufficiente dimostrare la prima delle due formule. La dimostrazione procede per induzione su $|I| \geq 1$. Se $|I| = 1$ il risultato è banale, quindi possiamo assumere che il risultato valga per ogni insieme I di cardinalità $n \geq 1$ e dimostrarlo per insiemi di cardinalità $n+1$. Supponiamo $|I| = n+1$ e chiaramente possiamo supporre che $I = n+1 = \{0, \ldots, n\}$. Allora:

$$\begin{aligned}
\bigwedge_{i\leq n} \bigvee_{j\in J_i} x_{i,j} &= \Big(\bigvee_{j\in J_0} x_{0,j}\Big) \wedge \Big(\bigwedge_{1\leq i\leq n} \bigvee_{j\in J_i} x_{i,j}\Big) \\
&= \Big(\bigvee_{j\in J_0} x_{0,j}\Big) \wedge \Big(\bigvee_{f\in J_1\times\cdots\times J_n} \bigwedge_{1\leq i\leq n} x_{i,f(i)}\Big) \\
&= \bigvee_{j\in J_0} \Big(x_{0,j} \wedge \Big(\bigvee_{f\in J_1\times\cdots\times J_n} \bigwedge_{1\leq i\leq n} x_{i,f(i)}\Big)\Big) \\
&= \bigvee_{j\in J_0} \bigvee_{f\in J_1\times\cdots\times J_n} \Big(x_{0,j} \wedge \Big(\bigwedge_{1\leq i\leq n} x_{i,f(i)}\Big)\Big) \\
&= \bigvee_{f\in \mathsf{X}_{i\leq n} J_i} \bigwedge_{i\leq n} x_{i,f(i)}\,,
\end{aligned}$$

dove nella seconda riga abbiamo usato l'ipotesi induttiva e nella terza riga abbiamo usato il Lemma 11.7. □

Definiamo, per $X \subseteq B$,

$$X^{\wedge} = \{\, x_1 \wedge \cdots \wedge x_n \mid x_1, \ldots, x_n \in X \text{ e } n \geq 1 \,\}$$
$$X^{\vee} = \{\, x_1 \vee \cdots \vee x_n \mid x_1, \ldots, x_n \in X \text{ e } n \geq 1 \,\}.$$

Teorema 11.20. *Se B è un'algebra di Boole e $X \subseteq B$, l'algebra generata da X è*

$$C \stackrel{\text{def}}{=} \left((X \cup \{\, x^* \mid x \in X \,\} \cup \{0,1\})^{\wedge} \right)^{\vee}.$$

Dimostrazione. C è contenuto nell'algebra generata da X ed è chiaramente non vuoto e chiuso per $\vee$. Quindi per l'Esercizio 11.10 è sufficiente dimostrare che è chiuso per complementi: un generico elemento di C è della forma

$$\bigvee_{i \in I} \bigwedge_{j \in J_i} y_{i,j}$$

dove $y_{i,j} \in X \cup \{\, x^* \mid x \in X \,\} \cup \{0,1\}$ e I e J_i sono insiemi finiti, quindi il suo complemento è

$$\bigwedge_{i \in I} \bigvee_{j \in J_i} y^*_{i,j} = \bigvee_{f \in \bigtimes_{i \in I} J_i} \bigwedge_{i \in I} y^*_{i,j} \in C.$$

□

Osservazione 11.21. Il motivo della presenza di 0 e 1 nella formula che definisce C è per il caso in cui $X = \emptyset$. Se $X \neq \emptyset$, allora $0 \in (X \cup \{\, x^* \mid x \in X \,\})^{\wedge}$ e $1 \in \left((X \cup \{\, x^* \mid x \in X \,\})^{\wedge} \right)^{\vee}$, quindi l'algebra generata da X è

$$C \stackrel{\text{def}}{=} \left((X \cup \{\, x^* \mid x \in X \,\})^{\wedge} \right)^{\vee}.$$

Corollario 11.22. *Sia A un'algebra di Boole, $B \subseteq A$ e $x \in A \setminus B$. La sub-algebra di A generata da $B \cup \{x\}$ è*

$$\{\, (b_1 wedge x) \vee ({}_2b \wedge x^*) \mid b_1, b_2 \in B \,\}.$$

Un'algebra di Boole si dice **finitamente generata** se esiste un $X \subseteq B$ finito tale che B è l'algebra generata da X.

Corollario 11.23. *Ogni algebra di Boole finitamente generata è finita.*

Esercizi

Esercizio 11.24. Sia $\langle L, \leq \rangle$ un ordine in cui ogni $X \subseteq L$ ha un estremo superiore (oppure ogni $X \subseteq L$ ha un estremo inferiore). Allora è un reticolo completo.

Esercizio 11.25. Dimostrare che l'equivalenza (54) $\Leftrightarrow$ (55) vale in ogni reticolo.

Esercizio 11.26. Dimostrare che

$$L = \{\, V \subseteq \mathbb{R}^n \mid V \text{ sottospazio vettoriale di } \mathbb{R}^n \,\},$$

ordinato per inclusione è uno reticolo completo e complementato, ma se $n > 1$ non distributivo.

Esercizio 11.27. Sia B un insieme dotato di due elementi privilegiati 0 e 1, di due operazioni binarie $\wedge$ e $\vee$ e di un'operazione 1-aria * che soddisfano (56)–(60). Dimostrare che:

(i) $1 \wedge x = x$ e $0 \vee x = x$,

(ii) $x \wedge x = x \vee x = x$,

(iii) $x \wedge y = x \Leftrightarrow x \vee y = y$,

(iv) la relazione $x \leq y \Leftrightarrow x \wedge y = x$ è un ordine su B tale che $\inf\{x, y\} = x \wedge y$ e $\sup\{x, y\} = x \vee y$,

(v) $0 \leq x \leq 1$.

Concludere che $\langle B, \leq \rangle$ è un reticolo distributivo complementato e che $\wedge$, $\vee$ e * sono, rispettivamente, le operazioni di inf, sup e complemento. Verificare che la corrispondenza

$$\langle B, \vee, \wedge, ^*, 0, 1 \rangle \mapsto \langle B, \leq \rangle$$

tra strutture algebriche che soddisfano (56)–(60) e reticoli distributivi complementati è l'inversa della corrispondenza (61).

Esercizio 11.28. Sia B un'algebra di Boole. Definiamo due nuove operazioni binarie su B: il **tratto di Sheffer** $\mid$ e la **freccia di Pierce** $\uparrow$

$$x \mid y = x^* \wedge y^*$$
$$x \uparrow y = x^* \vee y^*\,.$$

Dimostrare che $\vee$, $\wedge$, *, 0 e 1 sono definibili mediante equazioni usando l'operazione $\mid$ oppure l'operazione $\uparrow$.

Esercizio 11.29. Verificare che se $\langle B, \leq \rangle$ e $\langle C, \preceq \rangle$ sono algebre di Boole, allora $B \times C$ con l'ordinamento prodotto

$$(b_1, c_1) \trianglelefteq (b_2, c_2) \quad \Leftrightarrow \quad b_1 \leq b_2 \text{ e } c_1 \preceq c_2$$

è un'algebra di Boole. Come sono definite le operazioni $\wedge$, $\vee$ e * su $B \times C$?

Esercizio 11.30. Dare un esempio di algebra di Boole che non è atomica, ma che ha atomi.

Esercizio 11.31. Sia $\langle B, +, \cdot, 0, 1 \rangle$ un anello Booleano, cioè un anello con unità in cui $x^2 = x$ per ogni x. Definiamo

$$\begin{aligned} x \wedge y &= x \cdot y \\ x \vee y &= x + y + x \cdot y \\ x^* &= 1 + x \,. \end{aligned}$$

Dimostrare che

(i) $x + x = 0$, cioè ogni elemento del gruppo additivo $\langle B, + \rangle$ ha ordine 2;

(ii) $x \cdot y = y \cdot x$ e quindi B è un anello commutativo;

(iii) B con le operazioni $\wedge$, $\vee$ e * è un'algebra di Boole.

Verificare che la corrispondenza

$$\langle B, +, \cdot, 0, 1 \rangle \mapsto \langle B, \vee, \wedge, ^*, 0, 1 \rangle$$

tra anelli Booleani e algebre di Boole è l'inversa della corrispondenza (63).

Esercizio 11.32. Sia $\langle R, +, \cdot, 0, 1 \rangle$ un anello unitario (non necessariamente commutativo) e sia

$$\bar{R} = \left\{ x \in R \mid x^2 = x \text{ e } \forall y \in R \, (x \cdot y = y \cdot x) \right\}.$$

(Un elemento di un anello R per cui vale $x^2 = x$ si dice idempotente.) Definiamo

$$x \oplus y = x + y - 2x \cdot y \,.$$

Dimostrare che $\langle \bar{R}, \oplus, \cdot, 0, 1 \rangle$ è un anello Booleano.

Esercizio 11.33. Sia $\langle X, \leq \rangle$ un insieme linearmente ordinato e dotato di minimo. Una semiretta chiusa a sinistra di $\langle X, \leq \rangle$ è un insieme della forma

$$\{ x \in X \mid a \leq x \},$$

per qualche $a \in X$. Un intervallo semi-chiuso a sinistra di $\langle X, \leq \rangle$ è un insieme della forma $[a; b)$, con $a, b \in X$ e $a < b$. Sia H l'insieme di tutte le semirette chiuse a sinistra e tutti gli intervalli semi-chiusi a sinistra e sia B l'insieme di tutte le unioni finite di elementi di H. Dimostrare che B con l'unione, l'intersezione e l'operazione di complemento rispetto ad X è un'algebra di Boole.

Esercizio 11.34. Verificare che se B è un'algebra di Boole e $\emptyset \neq X \subseteq X$, allora l'algebra generata da X è $((X \cup \{ x^* \mid x \in X \})^\wedge)^\vee$.

Note e osservazioni

Le algebre di Boole sono state inventate dal matematico inglese George Boole (1815–1864) nel 1847. Per una trattazione enciclopedica sulle algebre di Boole si vedano i tre volumi dell'Handbook of Boolean Algebras [**Kop89, MB89a, MB89b**]. In particolare, l'articolo di S. Koppelberg nel primo volume è un'ottima introduzione all'argomento.

12. Ideali e filtri

Definizione 12.1. Un **ideale** di un algebra di Boole B è un sottoinsieme non-vuoto $I \subseteq B$ chiuso per l'operazione $\vee$ e $\leq$-segmento iniziale di B. Un ideale si dice proprio se $I \neq B$. Se X è un insieme, un **ideale su** X è un ideale di $\mathscr{P}(X)$.

Ricordiamo che ogni algebra di Boole è un anello Booleano.

Esercizio 12.2. Verificare che se B è un'algebra di Boole, allora I è un ideale secondo la Definizione 12.3 se e solo se è un ideale nel senso degli anelli.

Quindi

Teorema 12.3. *Sia B un'algebra di Boole. $I \subset B$ è un ideale se e solo se $I = \ker(f)$, per qualche omomorfismo f di dominio B.*

La nozione duale di ideale è quella di filtro.

Definizione 12.4. Un **filtro** di un algebra di Boole B è un sottoinsieme non-vuoto $F \subseteq B$ chiuso per l'operazione $\wedge$ e $\leq$-segmento finale di B. Un filtro si dice proprio se $F \neq B$. Se X è un insieme, un **filtro su** X è un filtro di $\mathscr{P}(X)$.

L'operazione di complementazione applicata a sottoinsiemi manda ideali in filtri e viceversa, cioè se $I \subseteq B$ è un ideale (proprio)

$$\check{I} = \{ x^* \mid x \in I \}$$

è il filtro (proprio) duale di I; se $F \subseteq B$ è un filtro (proprio)

$$\check{F} = \{ x^* \mid x \in F \}$$

è l'ideale (proprio) duale di F. Una **base** di un filtro F di B è un $X \subseteq F$ chiuso sotto $\wedge$ e tale che

$$F = \{\, b \in B \mid \exists x \in X\, (x \leq b) \,\}\,.$$

Se $X^\wedge$ è una base di F, diremo che X è una **sotto-base** di F. Se X è una base o sotto-base di F, diremo che F è il **filtro generato** da X. Un filtro F generato da un singoletto $\{a\}$ si dice **filtro principale** e a si dice **generatore** di F; con abuso di linguaggio, diremo che F è generato da a.

Esercizio 12.5. (i) F è il filtro di B generato da a se e solo se $F = \{\, b \in B \mid a \leq b \,\}$.

(ii) Un ideale che sia il duale di un filtro principale generato da a si dice **ideale principale generato da** a^* ed è della forma $\{\, b \mid b \leq a^* \,\}$. Dimostrare che un ideale è principale nel senso delle algebre di Boole se e solo se è un ideale principale nel senso degli anelli.

Un filtro/ideale si dice massimale se è proprio e se è massimale tra i filtri/ideali propri. I filtri massimali si dicono **ultrafiltri**.

Esercizio 12.6. (i) Se $\mathcal{F}$ è una famiglia di filtri di un'algebra di Boole B, allora $\bigcap \mathcal{F}$ è un filtro di B.

(ii) Il filtro D generato da $X \subseteq B$ è

$$D = \bigcap \{\, F \mid F \supseteq X \text{ e } F \text{ è un filtro} \,\}$$

è il più piccolo filtro contenente X.

(iii) Se F è il filtro generato dalla sottobase X allora F è proprio se e solo se $0 \notin X^\wedge$.

(iv) Se $f\colon B \to C$ è un omomorfismo suriettivo di algebre di Boole, allora $\ker(f)$ è massimale se e solo se C è l'algebra minimale $\{0, 1\}$.

Proposizione 12.7. *Se F è un filtro proprio di B, le seguenti condizioni sono equivalenti:*

(a) *F è un ultrafiltro,*

(b) $\forall x \in B\, (x \in F \Leftrightarrow x^* \notin F)$,

(c) $\forall x, y \in B\, (x \vee y \in F \Rightarrow (x \in F$ *oppure* $y \in F))$.

Dimostrazione. (a) $\Rightarrow$ (b): Se F è un ultrafiltro e $x \notin F$ allora $F \cup \{x\}$ genera il filtro banale. Poiché F è chiuso sotto $\wedge$, questo implica che $x \wedge y = 0$ per qualche $y \in F$, cioè $y \leq x^*$ e quindi $x^* \in F$. Analogamente $x^* \notin F$ implica $x = x^{**} \in F$.

(b) $\Rightarrow$ (c): Se $x \vee y \in F$ e $x \notin F$ allora $x^* \in F$ e quindi $(x \vee y) \wedge x^* \in F$. Ma

$$(x \vee y) \wedge x^* = (x \wedge x^*) \vee (y \wedge x^*) = y \wedge x^*\,,$$

quindi $y \in F$.

(c) $\Rightarrow$ (a): Se $D \supset F$ è un filtro e $x \in D \setminus F$, allora $1 = x \vee x^* \in F$ e $x^* \in F \subset D$ per la nostra assunzione. Ma allora $x \wedge x^* \in D$, cioè D è improprio. Quindi F è un ultrafiltro. □

12.A. Esempi di ideali e filtri.

12.A.1. *L'ideale degli insiemi finiti.* Se $\lambda \leq \kappa$ sono cardinali infiniti,

$$\{\, X \subseteq \kappa \mid |X| < \lambda \,\}$$

è un ideale proprio non-principale. Quando $\kappa = \lambda = \omega$ otteniamo Fin, l'ideale dei sottoinsiemi finiti di $\mathbb{N}$. L'algebra quoziente $\mathscr{P}(\mathbb{N})/\mathrm{Fin}$ è quella dell'Esempio 2.B.5.

12.A.2. *Insiemi di densità nulla.* Un sottoinsieme X di $\mathbb{N}$ ha densità 0 se

$$\lim_{n\to\infty} \frac{|X \cap n|}{n} = 0\,.$$

I sottoinsiemi di densità 0 formano un ideale proprio non principale.

12.A.3. *Il filtro degli intorni di un punto.* Se X è uno spazio topologico, la famiglia degli intorni di un punto $\bar{x} \in X$ è un filtro proprio. Se X è T_2, è un ultrafiltro se e solo se è principale se e solo se $\bar{x}$ è un punto isolato di X.

12.A.4. *Il filtro di Fréchet.* Il **filtro di Fréchet** su $\mathbb{N}$ è

$$\{\, X \subseteq \mathbb{N} \mid \mathbb{N} \setminus X \text{ è finito.} \,\}$$

Chiaramente questo filtro è il duale di Fin.

Esercizi

Esercizio 12.8. Dimostrare che se F è proprio e generato da a, allora F è un ultrafiltro se e solo se a è un atomo.

Esercizio 12.9. Dimostrare che se D è un ultrafiltro su un insieme X e $\{X_0, \ldots, X_k\}$ è una partizione di X, allora c'è un unico $i < k$ tale che $X_i \in D$.

Esercizio 12.10. Un ideale proprio I di un'algebra di Boole B si dice **primo** se $x \wedge y \in I$ implica che $x \in I$ oppure $y \in I$. Dimostrare che I è primo se e solo se è un ideale primo nel senso degli anelli, se e solo se è massimale.

Esercizio 12.11. Dimostrare che ogni ultrafiltro non principale su $\mathbb{N}$ estende il filtro di Fréchet.

Esercizio 12.12. Dimostrare che se B è un'algebra di Boole numerabile e F è un filtro proprio di B, allora F può essere esteso ad un ultrafiltro.

Esercizio 12.13. Sia B un'algebra di Boole e sia $b \in B \setminus \{0\}$ un elemento al di sotto del quale non ci sono atomi.

(1) Costruire una funzione $\langle b_s \mid s \in 2^{<\mathbb{N}} \rangle$ tale che
- $b_\emptyset = b$,
- $0 < b_{s^\frown\langle i\rangle} < b_s$ e
- $b_{s^\frown\langle 0\rangle} \wedge b_{s^\frown\langle 1\rangle} = 0$.

(2) Dimostrare che $2^{\mathbb{N}}$ si inietta in $\{ F \mid F$ è un filtro di B e $b \in F \}$.

(3) Usare l'Esercizio 12.12 per concludere che se B è numerabile e priva di atomi, allora l'insieme degli ultrafiltri di B è equipotente ad $\mathbb{R}$.

13. Il calcolo proposizionale

13.A. Le proposizioni. Fissiamo un insieme non vuoto

$$L = \{A, B, C, \dots\}$$

i cui elementi vengono detti **lettere proposizionali** ed un altro insieme

$$\{\boldsymbol{\neg}, \boldsymbol{\vee}, \boldsymbol{\wedge}, \boldsymbol{\Rightarrow}, \boldsymbol{\Leftrightarrow}\}$$

i cui elementi vengono detti **simboli di connettivi logici**. Le **proposizioni sull'alfabeto** L sono definite induttivamente da:

- ogni lettera proposizionale è una proposizione,
- se $\boldsymbol{p}$ e $\boldsymbol{q}$ sono proposizioni, anche $(\boldsymbol{\neg p})$, $(\boldsymbol{p \vee q})$, $(\boldsymbol{p \wedge q})$, $(\boldsymbol{p \Rightarrow q})$ e $(\boldsymbol{p \Leftrightarrow q})$ sono proposizioni.[4]

Il simbolo di connettivo $\boldsymbol{\neg}$ si dice unario, mentre gli altri simboli di connettivi si dicono binari. Formalmente l'insieme delle proposizioni $\mathrm{Prop} = \mathrm{Prop}(L)$, è l'insieme delle parole su (S, a) dove

$$S = \{\boldsymbol{\neg}, \boldsymbol{\vee}, \boldsymbol{\wedge}, \boldsymbol{\Rightarrow}, \boldsymbol{\Leftrightarrow}\} \cup L\,,$$

$a(\boldsymbol{\neg}) = 1$, $a(\square) = 2$, per ogni $\square \in \{\boldsymbol{\vee}, \boldsymbol{\wedge}, \boldsymbol{\Rightarrow}, \boldsymbol{\Leftrightarrow}\}$ e $a(A) = 0$, per ogni $A \in L$. L'insieme $\mathrm{Prop}(L)$ si dice anche **calcolo proposizionale** sull'insieme L.

Osservazione 13.1. La natura degli elementi di L e dei connettivi è irrilevante: l'unica richiesta è che i connettivi siano oggetti (cioè: insiemi) che non appartengano ad L. Per esempio, potremmo rimpiazzare L con $\{0\} \times L$ e stabilire che $\boldsymbol{\neg}, \boldsymbol{\vee}, \boldsymbol{\wedge}, \boldsymbol{\Rightarrow}, \boldsymbol{\Leftrightarrow}$ sono—rispettivamente—le coppie ordinate

$$(1,0), \dots, (1,4)\,.$$

Dal Corollario 7.7 otteniamo:

Proposizione 13.2. *Sia* $\boldsymbol{p} \in \mathrm{Prop}(L)$. *Allora:*

[4] Usiamo i simboli $\boldsymbol{\neg}, \boldsymbol{\vee}, \dots$ in neretto per distinguerli dai connettivi $\neg, \vee, \dots$ del linguaggio matematico informale.

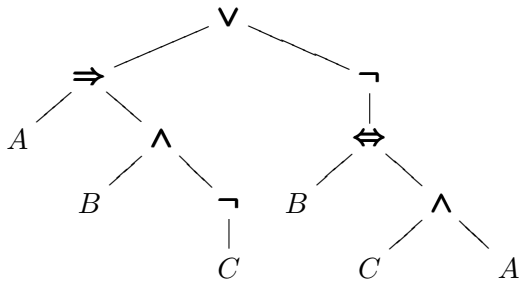
- *se* $\mathrm{lh}(\boldsymbol{p}) = 1$, *allora* $\boldsymbol{p} = \langle A \rangle$, *per una ed una sola* $A \in L$,
- *se* $\mathrm{lh}(\boldsymbol{p}) > 1$ *e la stringa* $\boldsymbol{p}$ *comincia con* $\boldsymbol{\neg}$, *allora esiste ed è unica* $\boldsymbol{q} \in \mathrm{Prop}(L)$ *tale che* $\boldsymbol{p} = \langle \boldsymbol{\neg} \rangle^\frown \boldsymbol{q}$,
- *se* $\mathrm{lh}(\boldsymbol{p}) > 1$ *e la stringa* $\boldsymbol{p}$ *comincia con un simbolo* $\square$ *di connettivo binario, allora esistono e sono uniche* $\boldsymbol{q}, \boldsymbol{r} \in \mathrm{Prop}(L)$ *tali che* $\boldsymbol{p} = \langle \square \rangle^\frown \boldsymbol{q}^\frown \boldsymbol{r}$.

Per semplicità notazionale scriveremo $\boldsymbol{\neg p}$ e $\boldsymbol{p} \,\square\, \boldsymbol{r}$ invece di $\langle \boldsymbol{\neg} \rangle^\frown \boldsymbol{p}$ e $\langle \square \rangle^\frown \boldsymbol{p}^\frown \boldsymbol{r}$. Inoltre useremo la convenzione che il connettivo $\boldsymbol{\neg}$ lega più strettamente degli altri connettivi binari e quindi potremo risparmiarci l'uso di qualche parentesi.

La notazione mediante alberi etichettati (§77.B) è particolarmente utile qui. Per esempio la proposizione

$$(A \boldsymbol{\Rightarrow} (B \boldsymbol{\wedge} \boldsymbol{\neg} C)) \boldsymbol{\vee} \boldsymbol{\neg} (B \boldsymbol{\Leftrightarrow} (C \boldsymbol{\wedge} A))$$

può essere scritta come



Il vantaggio di questo tipo di scrittura è che risulta immediata la struttura della proposizione.

13.B. Valutazioni. Una **valutazione in un'algebra di Boole** $\langle B, \wedge, \vee, ^*, \rangle$ o B-valutazione è una funzione $\mathcal{V}\colon \mathrm{Prop}(L) \to B$ tale che

$$\begin{aligned}
\mathcal{V}(\boldsymbol{\neg p}) &= \mathcal{V}(\boldsymbol{p})^* \\
\mathcal{V}(\boldsymbol{p} \boldsymbol{\wedge} \boldsymbol{q}) &= \mathcal{V}(\boldsymbol{p}) \wedge \mathcal{V}(\boldsymbol{q}) \\
\mathcal{V}(\boldsymbol{p} \boldsymbol{\vee} \boldsymbol{q}) &= \mathcal{V}(\boldsymbol{p}) \vee \mathcal{V}(\boldsymbol{q}) \\
\mathcal{V}(\boldsymbol{p} \boldsymbol{\Rightarrow} \boldsymbol{q}) &= \mathcal{V}(\boldsymbol{p})^* \vee \mathcal{V}(\boldsymbol{q}) \\
\mathcal{V}(\boldsymbol{p} \boldsymbol{\Leftrightarrow} \boldsymbol{q}) &= \big(\mathcal{V}(\boldsymbol{p})^* \vee \mathcal{V}(\boldsymbol{q})\big) \wedge \big(\mathcal{V}(\boldsymbol{p}) \vee \mathcal{V}(\boldsymbol{q})^*\big).
\end{aligned}$$

Lemma 13.3. *Ogni funzione* $F\colon L \to B$ *può essere estesa ad un'unica* B*-valutazione.*

Dimostrazione. Sia $\mathrm{Prop}_n = \{\, \boldsymbol{p} \in \mathrm{Prop}(L) \mid \mathrm{ht}(\boldsymbol{p}) \leq n \,\}$. Definiamo induttivamente $F_n \colon \mathrm{Prop}_n \to B$ ponendo $F_0(\langle A \rangle) = F(A)$ e

$$F_{n+1}(\boldsymbol{p}) = \begin{cases} F_n(\boldsymbol{p}) & \text{se } \boldsymbol{p} \in \mathrm{Prop}_0, \\ F_n(\boldsymbol{q})^* & \text{se } \boldsymbol{p} = \boldsymbol{\neg q}, \\ F_n(\boldsymbol{q}) \vee F_n(\boldsymbol{r}) & \text{se } \boldsymbol{p} = \boldsymbol{q \vee r}, \\ F_n(\boldsymbol{q}) \wedge F_n(\boldsymbol{r}) & \text{se } \boldsymbol{p} = \boldsymbol{q \wedge r}, \\ F_n(\boldsymbol{q})^* \vee F_n(\boldsymbol{r}) & \text{se } \boldsymbol{p} = \boldsymbol{q \Rightarrow r}, \\ (F_n(\boldsymbol{q}) + F_n(\boldsymbol{r}))^* & \text{se } \boldsymbol{p} = \boldsymbol{q \Leftrightarrow r}, \end{cases}$$

dove $+$ è l'operazione di somma in B definita in (62). Poiché $F_0 \subseteq F_1 \subseteq \ldots$, la funzione $\mathcal{V} \stackrel{\text{def}}{=} \bigcup_n F_n \colon \mathrm{Prop} \to B$ è una funzione ed è la B-valutazione cercata. □

Esercizio 13.4. Dimostrare che se $\mathcal{V}$ è una B-valutazione, $\mathcal{V}(\boldsymbol{p \Rightarrow q}) = 1$ se e solo se $\mathcal{V}(\boldsymbol{p}) \leq \mathcal{V}(\boldsymbol{q})$.

In particolare, ogni funzione

$$\mathcal{V} \colon L \to \{0, 1\}$$

che associa ad ogni lettera un valore di verità: vero (1) o falso (0), può essere estesa in modo canonico ad una funzione (che indicheremo ancora con $\mathcal{V}$)

$$\mathcal{V} \colon \mathrm{Prop}(L) \to \{0, 1\}$$

che assegna un valore di verità ad ogni proposizione.

Definizione 13.5. Una $\mathcal{V} \in {}^{L}2$ **soddisfa** $\Gamma \subseteq \mathrm{Prop}(L)$ ovvero $\mathcal{V}$ è un **modello** di Γ se

$$\forall \boldsymbol{p} \in \Gamma \, (\mathcal{V}(\boldsymbol{p}) = 1) \,.$$

Se $\Gamma, \Delta \subseteq \mathrm{Prop}(L)$, diremo che Δ è **conseguenza tautologica** o più semplicemente **conseguenza logica** di Γ, in simboli

$$\Gamma \models \Delta \,,$$

se e solo se ogni modello di Γ è un modello di Δ. Quando Γ o Δ sono dei un singoletti $\{\boldsymbol{p}\}$ e $\{\boldsymbol{q}\}$ scriveremo che $\mathcal{V}$ soddisfa (è un modello di) $\boldsymbol{p}$ e $\boldsymbol{p} \models \boldsymbol{q}$ invece di $\mathcal{V}$ soddisfa Γ e $\Gamma \models \Delta$.

Una $\boldsymbol{p}$ che è soddisfatta da ogni $\mathcal{V}$ si dice **tautologia proposizionale**; una $\boldsymbol{p}$ che non ha nessun modello (cioè che non è soddisfatta da alcuna $\mathcal{V}$) si dice **contraddizione proposizionale**.

Se $\boldsymbol{p} \models \boldsymbol{q}$ e $\boldsymbol{q} \models \boldsymbol{p}$, allora diremo che $\boldsymbol{p}$ e $\boldsymbol{q}$ sono **tautologicamente equivalenti**, in simboli

$$\boldsymbol{p} \equiv \boldsymbol{q} \,.$$

Equivalentemente, $\boldsymbol{p} \equiv \boldsymbol{q}$ se e solo se $\mathcal{V}(\boldsymbol{p}) = \mathcal{V}(\boldsymbol{q})$, per ogni valutazione $\mathcal{V}$. La $\equiv$ è una relazione di equivalenza su $\mathrm{Prop}(L)$. Le tautologie proposizionali sono tutte $\equiv$-equivalenti e formano una classe d'equivalenza che si indica con $\top$. Analogamente le contraddizioni proposizionali formano una classe d'equivalenza che si indica con $\bot$. Se $[\boldsymbol{p}], [\boldsymbol{q}] \in \mathrm{Prop}(L)/\equiv$ poniamo

$$[\boldsymbol{p}] \vee [\boldsymbol{q}] = [\boldsymbol{p} \boldsymbol{\vee} \boldsymbol{q}]$$
$$[\boldsymbol{p}] \wedge [\boldsymbol{q}] = [\boldsymbol{p} \boldsymbol{\wedge} \boldsymbol{q}]$$
$$[\boldsymbol{p}]^* = [\boldsymbol{\neg p}]\,.$$

Esercizio 13.6. Dimostrare che:

(i) con queste operazioni $\mathrm{Prop}(L)/\equiv$ è un'algebra di Boole, con $\bot$ minimo e $\top$ massimo,

(ii) se $\boldsymbol{p} \in \mathrm{Prop}(L)$ e $\mathcal{V}$, $\mathcal{W}$ sono valutazioni tali che $\mathcal{V}(A) = \mathcal{W}(A)$ per ogni lettera A che compare in $\boldsymbol{p}$, allora $\mathcal{V}(\boldsymbol{p}) = \mathcal{W}(\boldsymbol{p})$,

(iii) le seguenti affermazioni sono equivalenti
  (a) $[\boldsymbol{p}] \leq [\boldsymbol{q}]$
  (b) $\boldsymbol{p} \boldsymbol{\Rightarrow} \boldsymbol{q}$ è una tautologia proposizionale,
  (c) $\mathcal{V}(\boldsymbol{p}) \leq \mathcal{V}(\boldsymbol{q})$, per ogni valutazione $\mathcal{V}$.

Teorema 13.7. *Sia* $B = \mathrm{Prop}(L)/\equiv$.

(a) *Se* L *è finito,* $L = \{A_0, \ldots, A_{n-1}\}$*, allora* B *è atomica e gli atomi sono le classi d'equivalenza delle proposizioni della forma*

$$\boldsymbol{q}^s = A_0^{s(0)} \boldsymbol{\wedge} \ldots \boldsymbol{\wedge} A_{n-1}^{s(n-1)}$$

dove $s \in {}^n2$ *e*

$$A_k^i = \begin{cases} A_k & \text{se } i = 1, \\ \boldsymbol{\neg} A_k & \text{se } i = 0. \end{cases}$$

Quindi $|\mathrm{At}(B)| = 2^n$ *e* $|B| = 2^{2^n}$.

(b) *Se* L *è infinito, allora* B *è priva di atomi.*

Dimostrazione. (a) Osserviamo che $\mathcal{V}(\boldsymbol{q}^s) = 1$ se e solo se $\mathcal{V}(A_k) = s(k)$. In altre parole, $\boldsymbol{q}^s$ è soddisfatta da un'unica valutazione che indichiamo con $\mathcal{V}_s$. Questo implica che $\boldsymbol{q}^s \not\equiv \boldsymbol{q}^t$ quando $s \neq t$. Se $[\boldsymbol{p}] < [\boldsymbol{q}^s]$ allora per l'Esercizio 13.6 $\mathcal{V}(\boldsymbol{p}) \leq \mathcal{V}(\boldsymbol{q}^s)$ per ogni $\mathcal{V}$ e

$$0 = \mathcal{W}(\boldsymbol{p}) < \mathcal{W}(\boldsymbol{q}^s) = 1$$

per una qualche $\mathcal{W}$. Ma $\mathcal{W}(\boldsymbol{q}^s) = 1$ se e solo se $\mathcal{W} = \mathcal{V}_s$, quindi $\mathcal{V}(\boldsymbol{p}) = 0$ per ogni valutazione, cioè $\boldsymbol{p}$ è una contraddizione proposizionale, ovvero $[\boldsymbol{p}] = 1$. Segue che i $[\boldsymbol{q}^s]$ sono atomi. Infine mostriamo che se $[\boldsymbol{p}] > \bot$, allora $[\boldsymbol{p}] \geq [\boldsymbol{q}^s]$ per qualche s: sia $\mathcal{W}$ una valutazione tale che $\mathcal{W}(\boldsymbol{p}) = 1$ e sia $s \in {}^n2$ tale che $\mathcal{W} = \mathcal{V}_s$, vale a dire $s(k) = \mathcal{W}(A_k)$ per $k = 0, \ldots, n-1$. Se $\mathcal{V} = \mathcal{W}$,

allora $1 = \mathcal{W}(\boldsymbol{q}^s) \leq \mathcal{W}(\boldsymbol{p}) = 1$. Se $\mathcal{V} \neq \mathcal{W}$, allora $0 = \mathcal{V}(\boldsymbol{q}^s) \leq \mathcal{V}(\boldsymbol{p})$. Quindi $[\boldsymbol{q}^s] \leq [\boldsymbol{p}]$.

(b) Sia $\boldsymbol{p} \in \mathrm{Prop}(L) \setminus \bot$ e sia A una lettera che non occorre in $\boldsymbol{p}$. Dimostriamo che $\bot < [A \boldsymbol{\wedge} \boldsymbol{p}] < [\boldsymbol{p}]$. Chiaramente $\mathcal{W}(A \boldsymbol{\wedge} \boldsymbol{p}) \leq \mathcal{W}(\boldsymbol{p})$ per ogni valutazione $\mathcal{W}$ e poiché $\boldsymbol{p}$ non è una contraddizione proposizionale, c'è una valutazione $\mathcal{V}$ tale che $\mathcal{V}(\boldsymbol{p}) = 1$. Siano $\mathcal{V}_0$ e $\mathcal{V}_1$ le valutazioni

$$\mathcal{V}_i(B) = \begin{cases} \mathcal{V}(B) & \text{se } B \neq A, \\ i & \text{se } B = A. \end{cases}$$

Per l'Esercizio 13.6 $\mathcal{V}_0$ e $\mathcal{V}_1$ testimoniano, rispettivamente, che $[A \boldsymbol{\wedge} \boldsymbol{p}] < [\boldsymbol{p}]$ e $\bot < [A \boldsymbol{\wedge} \boldsymbol{p}]$.

Per l'arbitrarietà di $\boldsymbol{p}$ e A, questo prova che B è priva di atomi. □

13.C. Soddisfacibilità e tavole di verità.

Definizione 13.8. Un insieme Γ di proposizioni si dice **soddisfacibile** se esiste una valutazione $\mathcal{V}$ tale che $\forall \boldsymbol{p} \in \Gamma\, (\mathcal{V}(\boldsymbol{p}) = 1)$. Si dice **finitamente soddisfacibile** se ogni sottoinsieme finito di Γ è soddisfacibile.

Chiaramente se Γ è soddisfacibile è anche finitamente soddisfacibile e, banalmente, se L è finito vale anche l'implicazione inversa per il Teorema 13.7. Nella prossima sezione dimostreremo che l'implicazione vale per tutti gli L (Teorema 14.8).

Una **tavola di verità** n-aria per L è semplicemente una funzione

$$T \colon {}^n2 \to 2\,.$$

Più concretamente, è una tabella

A_1	A_2	$\dots$	A_n	$T(A_1, \dots, A_n)$
0	0	$\dots$	0	i_1
0	0	$\dots$	1	i_2
$\vdots$	$\vdots$		$\vdots$	$\vdots$
1	1	$\dots$	1	i_{2^n}

con $n+1$ colonne, indicizzate da A_1, $A_2, \dots, A_n$ e $T(A_1, \dots, A_n)$ e con 2^n righe: nella sotto-matrice di sinistra scriviamo le possibili valutazioni di $A_1, \dots, A_n$ (ovvero gli elementi di ${}^n2$ e nell'ultima colonna i valori di T. I

connettivi $\neg, \vee, \wedge, \Rightarrow, \Leftrightarrow$ definiscono delle tavole di verità

A	$\neg A$
0	1
1	0

A	B	$A \vee B$
0	0	0
1	0	1
0	1	1
1	1	1

A	B	$A \wedge B$
0	0	0
1	0	0
0	1	0
1	1	1

A	B	$A \Rightarrow B$
0	0	1
1	0	1
0	1	1
1	1	1

A	B	$A \Leftrightarrow B$
0	0	1
1	0	0
0	1	0
1	1	1

Ogni proposizione $\boldsymbol{p}$ contenente n lettere proposizionali $A_1, \ldots, A_n$ definisce una tavola di verità n-aria: ad ognuna delle 2^n valutazioni $\mathcal{V}$ di $A_1, \ldots, A_n$ associamo il valore $\mathcal{V}(\boldsymbol{p})$. Il seguente risultato dimostra il converso.

Proposizione 13.9. *Ogni tavola di verità n-aria è la tavola di verità di una proposizione $\boldsymbol{p}$ contenente le lettere $A_1, \ldots, A_n$. Inoltre possiamo supporre che $\boldsymbol{p}$ contenga soltanto i connettivi $\neg$ e $\wedge$, oppure soltanto i connettivi $\neg$ e $\vee$*

Dimostrazione. Poiché $A \vee B$ e $\neg(\neg A \wedge \neg B)$ hanno la stessa tavola di verità e così pure $A \wedge B$ e $\neg(\neg A \vee \neg B)$, i connettivi $\wedge$ e $\vee$ sono definibili l'uno a partire dall'altro mediante $\neg$. È quindi sufficiente dimostrare che la proposizione $\boldsymbol{p}$ è costruita a partire da $\neg$, $\wedge$ e $\vee$. Fissiamo una tavola di verità T. Data una valutazione $\mathcal{V}$ di $A_1, \ldots, A_n$, vale a dire una riga della tavola di verità, definiamo $A_i^{\mathcal{V}} = A_i$ se $\mathcal{V}(A_i) = 1$ e $A_i^{\mathcal{V}} = \neg A_i$ altrimenti. Sia $\boldsymbol{p}_{\mathcal{V}}$ la proposizione ottenuta prendendo la congiunzione

$$A_1^{\mathcal{V}} \wedge \cdots \wedge A_n^{\mathcal{V}}$$

se nell'ultima colonna il valore corrispondente è 1 e

$$\neg \left(A_1^{\mathcal{V}} \wedge \cdots \wedge A_n^{\mathcal{V}} \right)$$

altrimenti. Sia $\boldsymbol{p}$ la disgiunzione delle 2^n proposizioni $\boldsymbol{p}_{\mathcal{V}}$: è immediato verificare che la tavola di verità di $\boldsymbol{p}$ è T. □

Esercizi

Esercizio 13.10. Un insieme S di connettivi si dice **adeguato** se ogni tavola di verità può essere ottenuta da una proposizione contenente solo connettivi in S. Quindi $\{\neg, \wedge\}$ e $\{\neg, \vee\}$ sono adeguati. Siano $\mid$ e $\uparrow$ i connettivi definiti da

A	B	$A \mid B$
0	0	1
1	0	0
0	1	0
1	1	0

A	B	$A \uparrow B$
0	0	1
1	0	1
0	1	1
1	1	0

Dimostrare che

- $\{\neg, \Rightarrow\}$, $\{\mid\}$ e $\{\uparrow\}$ sono adeguati, mentre
- $\{\neg, \Leftrightarrow\}$, $\{\vee, \wedge\}$, $\{\vee, \Rightarrow\}$, $\{\wedge, \Rightarrow\}$, $\{\vee, \Rightarrow\}$ non sono adeguati.

Esercizio 13.11. Siano $A_1, \dots, A_n$ le lettere che compaiono in una proposizione $\boldsymbol{p}$ e siano $\boldsymbol{q}_1, \dots, \boldsymbol{q}_n \in \mathrm{Prop}(L)$, dove L è un insieme arbitrario. Sia

$$\boldsymbol{p}[\boldsymbol{q}_1/A_1, \dots, \boldsymbol{q}_n/A_n]$$

la proposizione ottenuta sostituendo $\boldsymbol{q}_i$ al posto di A_i. Dimostrare che $\boldsymbol{p}$ è una tautologia/contraddizione se e solo se $\boldsymbol{p}[\boldsymbol{q}_1/A_1, \dots, \boldsymbol{q}_n/A_n]$ è una tautologia/contraddizione.

14. L'Assioma di Scelta

La notazione con "insiemi indicizzati" è molto comoda in matematica e spesso una famiglia $\mathcal{A}$ di insiemi viene descritta come $\{ A_i \mid i \in I \}$. Ciò può essere sempre fatto—basta porre $I = \mathcal{A}$ e prendere come $i \mapsto A_i$ la funzione identica. Tuttavia l'uso indiscriminato di lettere indicizzate può nascondere alcuni aspetti delicati. Per esempio, supponiamo di avere una famiglia non vuota $\{ A_i \mid i \in I \}$ di insiemi non vuoti, vale a dire: $I \neq \emptyset$ e $\forall i \in I\, (A_i \neq \emptyset)$. Viene spontaneo riformulare la seconda condizione come "esiste $a_i \in A_i$". Tuttavia la scrittura "a_i" sottintende l'esistenza di una funzione f che ad $i \in I$ associa $f(i) = a_i \in A_i$. In altre parole, siamo passati dall'ipotesi originale "$\forall i \in I\, \exists x \in A_i$" a

$$\exists f\, \forall i \in I\, (f(i) \in A_i)$$

scambiando l'ordine dei quantificatori. L'Assioma di Scelta, in simboli AC, asserisce che questo scambio di quantificatori è lecito:

Assioma di Scelta. *Se $\mathcal{A}$ è un insieme non-vuoto e se $\forall A \in \mathcal{A}\,(A \neq \emptyset)$, allora esiste $f\colon \mathcal{A} \to \bigcup \mathcal{A}$ tale che $\forall A \in \mathcal{A}\,(f(A) \in A)$.*

Esercizio 14.1. Dimostrare che l'Assioma di scelta è equivalente all'affermazione: Se I è un insieme non vuoto e gli insiemi A_i $(i \in I)$ sono non vuoti, allora anche $\bigtimes_{i\in I} A_i \neq \emptyset$.

L'Assioma di Scelta è indipendente dagli altri assiomi della teoria degli insiemi, vale a dire: non è possibile dimostrare (Cohen, 1963) o refutare (Gödel, 1938) AC a partire da ZF o da MK.

14.A. Il principio del buon ordinamento e il Lemma di Zorn. In questa sezione dimostreremo che AC è equivalente all'affermazione che ogni insieme è bene ordinabile. Innanzi tutto osserviamo che, anche senza scelta, dato un insieme X c'è sempre un ordinale che non si inietta in X. Se $X = \emptyset$ il risultato è banale quindi possiamo supporre che $X \neq \emptyset$. Sia

$$\mathcal{W} = \{\, R \subseteq X \times X \mid R \text{ è un buon ordine su un sottoinsieme di } X \,\}.$$

Per il rimpiazzamento $\{\, \mathrm{ot}(R) \mid R \in \mathcal{W} \,\}$ è un insieme e coincide con l'insieme $\{\, \alpha \mid \exists f\colon \alpha \rightarrowtail X \,\}$. Quindi possiamo definire l'ordinale

$$\mathrm{Hrtg}(X) = \sup \{\, \alpha \dot{+} 1 \mid \exists f\colon \alpha \rightarrowtail X \,\}. \tag{66}$$

detto il **numero di Hartogs** dell'insieme X.

Esercizio 14.2. Dimostrare che $\mathrm{Hrtg}(X)$ è il più piccolo ordinale che non si inietta in X e che $\mathrm{Hrtg}(X)$ è un cardinale.

Teorema 14.3. *Assumiamo* AC. *Ogni insieme è in bijezione con un ordinale. Equivalentemente, ogni insieme è bene ordinabile.*

Dimostrazione. Sia X un insieme. Se $X = \emptyset$ allora, banalmente, X è bene ordinabile, quindi possiamo supporre $X \neq \emptyset$. Fissiamo $C\colon \mathscr{P}(X) \setminus \{\emptyset\} \to X$ una funzione di scelta, vale a dire $C(Y) \in Y$ per tutti gli $\emptyset \neq Y \subseteq X$. Diamo innanzi tutto un'idea informale della dimostrazione: sia x_0 un elemento di X, per esempio $x_0 = C(X)$ e supponiamo di aver costruito $x_0, x_1, \ldots, x_\beta, \ldots$ elementi distinti di X, con $\beta < \alpha$. Se $X = \{\, x_\beta \mid \beta < \alpha \,\}$ allora $\alpha \to X$, $\beta \mapsto x_\beta$ è la bijezione cercata. Altrimenti scegliamo un nuovo elemento $x_\alpha \in X$ distinto dai precedenti, per esempio $x_\alpha = C(X \setminus \{\, x_\beta \mid \beta < \alpha \,\})$. Se la funzione $\alpha \mapsto x_\alpha$ fosse definita per tutti gli $\alpha < \mathrm{Hrtg}(X)$, allora avremmo un'iniezione $\mathrm{Hrtg}(X) \rightarrowtail X$, contro l'Esercizio 14.2. Quindi esiste un $\bar\alpha < \mathrm{Hrtg}(X)$ tale che $X = \{\, x_\beta \mid \beta < \bar\alpha \,\}$.

Vediamo ora la dimostrazione nei suoi dettagli tecnici. Sia $F\colon \mathrm{V} \to \mathrm{V}$

$$F(h) = \begin{cases} C(X \setminus \mathrm{ran}(h)) & \text{se } h \text{ è una funzione e } \mathrm{ran}(h) \subset X, \\ X & \text{altrimenti.} \end{cases}$$

Per il Teorema 4.2 c'è una $G\colon \mathrm{Ord} \to \mathrm{V}$ tale che $\forall \alpha \in \mathrm{Ord}\,(G(\alpha) = F(G \restriction \alpha))$.

Fatto 14.3.1. *Se $G(\alpha) = X$ e $\alpha < \beta$ allora $G(\beta) = X$.*

Dimostrazione. $X = G(\alpha) \in \mathrm{ran}(G \restriction \beta)$, quindi $\mathrm{ran}(G \restriction \beta) \not\subset X$. Ne segue che $F(G \restriction \beta) = X$ e quindi $G(\beta) = X$. □

Fatto 14.3.2. *Se $G(\beta) \neq X$ e $\alpha < \beta$, allora $G(\alpha) \neq G(\beta)$.*

Dimostrazione. $G(\alpha) \in \mathrm{ran}(G \restriction \beta) \subseteq X$, quindi $G(\alpha)$ è distinto da $G(\beta) \in X \setminus \mathrm{ran}(G \restriction \beta)$. □

Ne segue che $G(\alpha) = X$ per qualche $\alpha < \mathrm{Hrtg}(X)$, altrimenti si avrebbe una funzione iniettiva $\mathrm{Hrtg}(X) \rightarrowtail X$. Sia $\bar{\alpha}$ minimo tale che $G(\bar{\alpha}) = X$. Allora $g = G \restriction \bar{\alpha}$ è una funzione iniettiva in X. Se $\mathrm{ran}(g) \neq X$, allora

$$X = G(\bar{\alpha}) = F(g) = C(X \setminus \mathrm{ran}(g)) \in X$$

contraddizione. Quindi $g\colon \bar{\alpha} \to X$ è una bijezione. □

Quindi, assumendo AC, la Definizione 8.2 di cardinalità può essere estesa ad ogni insieme.

Esercizio 14.4. Sia $\mathcal{A}$ una famiglia non vuota di sottoinsiemi non vuoti di un insieme I. Supponiamo I sia bene ordinabile. Dimostrare che esiste una funzione di scelta per $\mathcal{A}$. Concludere che l'enunciato del Teorema 14.3 "Ogni insieme è bene ordinabile" implica AC.

Quindi, assumendo AC, il Teorema 8.12 può essere riformulato in generale.

Teorema 14.5 (AC)**.** *Se X è infinito, allora $|X| = |{}^{<\omega}X|$.*

Il prossimo risultato stabilisce un'importante equivalenza tra AC e un principio molto usato in matematica: il Lemma di Zorn.

Teorema 14.6. *Sono equivalenti:*

(a) AC,

(b) **Principio di massimalità di Hausdorff:** *Ogni insieme parzialmente ordinato contiene una catena massimale.*

(c) **Lemma di Zorn:** *Ogni insieme parzialmente ordinato in cui ogni catena ha un estremo superiore, contiene un elemento massimale.*

Dimostrazione. (a) ⇒ (b). Per assurdo, sia X un insieme parzialmente ordinato da $\leq$ privo di catene massimali. Se $C \subseteq X$ è una catena, l'insieme

$$K(C) = \{\, x \in X \setminus C \mid C \cup \{x\} \text{ è una catena} \,\}$$

è non vuoto. Fissiamo una funzione di scelta $F\colon \mathscr{P}(X) \setminus \{\emptyset\} \to X$. La funzione $g\colon \mathrm{Hrtg}(X) \to X$ definita da

$$g(\alpha) = F\left(K\left(\{\, g(\beta) \mid \beta < \alpha \,\}\right)\right).$$

è iniettiva e questo contraddice l'Esercizio 14.2.

(b) $\Rightarrow$ (c). Sia X un insieme parzialmente ordinato i cui ogni catena ha un maggiorante. Se $C \subseteq X$ è una catena massimale, allora il maggiorante di C deve appartenere a C e quindi è un elemento massimale di X.

(c) $\Rightarrow$ (a). Sia $\{\, A_i \mid i \in I \,\}$ una famiglia non vuota di insiemi non vuoti. L'insieme

$$X = \{\, p \mid p \text{ è una funzione, } \mathrm{dom}\, p \subseteq I \text{ e } \forall i \in \mathrm{dom}(p)\,(p(i) \in A_i) \,\}$$

ordinato per inclusione soddisfa le ipotesi del Lemma di Zorn, quindi c'è una $f \in X$ massimale. Se esistesse un $i_0 \in I \setminus \mathrm{dom}(f)$, allora $f \cup \{(i_0, \bar{a})\} \in X$, per un qualsiasi $\bar{a} \in A_i$, contro la massimalità di f. Quindi f è una funzione di scelta per $\{\, A_i \mid i \in I \,\}$. □

14.B. Ultrafiltri e il Teorema di Stone.

Teorema 14.7. *Assumiamo* AC. *Ogni filtro proprio in un'algebra di Boole può essere esteso ad un ultrafiltro.*

Dimostrazione. Sia B è un'algebra di Boole ed $F \subseteq B$ un filtro proprio. Allora

$$\mathcal{F} = \{\, D \subseteq B \mid D \text{ è un filtro proprio e } F \subseteq D \,\}$$

con la relazione di inclusione soddisfa alle ipotesi del Lemma di Zorn: se $\mathcal{C} \subseteq \mathcal{F}$, è facile verificare che $\bigcup \mathcal{C}$ è un filtro contenete F. Se $0 \in \bigcup \mathcal{C}$, allora $0 \in D \in \mathcal{F}$, contraddicendo il fatto che D è proprio. Sia $U \in \mathcal{F}$ un elemento massimale: è immediato verificare che U è un ultrafiltro e che $F \subseteq U$. □

L'Assioma di Scelta non è necessario quando l'algebra di Boole è numerabile—si veda l'Esercizio 12.12.

Il seguente risultato è noto come **Teorema di Compattezza per il calcolo proposizionale**.

Teorema 14.8. *Assumiamo* AC. *Sia* $\Gamma \subseteq \mathrm{Prop}(L)$ *un insieme finitamente soddisfacibile. Allora* Γ *è soddisfacibile.*

Dimostrazione. L'ipotesi su Γ equivale a dire che $\bot \neq [\boldsymbol{p}_1 \wedge \ldots \wedge \boldsymbol{p}_n]$ per ogni $\boldsymbol{p}_1 \ldots, \boldsymbol{p}_n \in \Gamma$, cioè che il filtro generato da $\{\, [\boldsymbol{p}] \mid \boldsymbol{p} \in \Gamma \,\}$ è proprio. Sia D un ultrafiltro che estende questo filtro e sia $\mathcal{V}\colon L \to 2$

$$\mathcal{V}(A) = 1 \qquad \text{se e solo se} \qquad [A] \in D\,.$$

È facile verificare che

$$\mathcal{V}(\boldsymbol{p}) = 1 \qquad \text{se e solo se} \qquad [\boldsymbol{p}] \in D\,. \tag{67}$$

Quindi $\boldsymbol{p} \in \Gamma$ implica che $[\boldsymbol{p}] \in F \subseteq D$, da cui $\mathcal{V}(\boldsymbol{p}) = 1$. Abbiamo quindi dimostrato che Γ è soddisfacibile. □

Esercizio 14.9. Completare i dettagli della dimostrazione precedente dimostrando, per induzione sulla lunghezza di $\boldsymbol{p}$, che vale (67).

Corollario 14.10. *Se* $\Gamma \models \boldsymbol{p}$ *allora* $\Delta \models \boldsymbol{p}$ *per qualche* $\Delta \subseteq \Gamma$ *finito.*

Dimostrazione. Supponiamo, per assurdo, che $\Delta \not\models \boldsymbol{p}$, per ogni $\Delta \subseteq \Gamma$ finito e sia $\mathcal{V}_\Delta$ una valutazione che soddisfa Δ ma tale che $\mathcal{V}_\Delta(\boldsymbol{p}) = 0$. Allora $\mathcal{V}_\Delta$ soddisfa $\Delta \cup \{\boldsymbol{p}\}$. Ne segue che

$$\forall \Delta \subseteq \Gamma\,(\Delta \text{ finito } \Rightarrow \Delta \cup \{\boldsymbol{\neg p}\} \text{ è soddisfacibile})$$

e quindi per il Teorema di Compattezza $\Gamma \cup \{\boldsymbol{p}\}$ è soddisfacibile. Sia $\mathcal{V}$ una valutazione che soddisfa Γ e $\boldsymbol{\neg p}$. Ma, per ipotesi, ogni valutazione che soddisfa Γ deve soddisfare anche $\boldsymbol{p}$: contraddizione. □

Vediamo un'interessante applicazione del Teorema di Compattezza del calcolo proposizionale.

Teorema 14.11. *Ogni ordine parziale stretto* $\prec$ *su un insieme* X *può essere esteso ad un ordine totale stretto* $\lhd$ *su* X*, vale a dire* $\langle X, \lhd\rangle$ *è lineare e*

$$\forall x, y \in X\,(x \prec y \Rightarrow x \lhd y)\,.$$

Dimostrazione. Sia $\langle X, \prec\rangle$ un ordine parziale stretto: per la Proposizione 4.8 possiamo supporre che X sia infinito. Sia $L = X \times X$ e consideriamo il calcolo proposizionale $\mathrm{Prop}(L)$ in cui le lettere proposizionali sono le coppie ordinate (x, y), con $x, y \in X$. Sia $\Gamma \subseteq \mathrm{Prop}(L)$ l'insieme

$$\{\,\boldsymbol{\neg}(x,x) \mid x \in X\,\} \cup \{\,(x,y)\,\boldsymbol{\vee}(y,x) \mid x, y \in X, x \neq y\,\}$$
$$\cup \left\{\,\big((x,y)\,\boldsymbol{\wedge}(y,z)\big)\,\boldsymbol{\Rightarrow}(x,z) \mid x, y, z \in X\,\right\}.$$

L'idea è che una lettera proposizionale (x, y) asserisce che x precede y in un ordine stretto su X. L'insieme Γ è costituito da tre insiemi: il primo insieme equivale alla proprietà irriflessiva, il secondo alla connessione, il terzo alla transitività. Per ogni $\mathcal{V}\colon L \to 2$ definiamo una relazione binaria $\lhd = \lhd_{\mathcal{V}}$ su X

$$x \lhd y \quad \Leftrightarrow \quad \mathcal{V}(A) = 1, \text{ dove } A = (x, y) \in L$$

e, viceversa, ogni relazione binaria $\lhd$ definisce una valutazione $\mathcal{V} = \mathcal{V}_\lhd$. Allora $\mathcal{V}$ soddisfa Γ se e solo se $\lhd$ è un ordine lineare stretto su X. Inoltre se $\mathcal{V}$ soddisfa $\Gamma \cup \Delta$, dove

$$\Delta = \{\,(x, y) \mid x \prec y\,\}\,,$$

allora l'ordinamento indotto $\lhd$ estende $\prec$. Quindi, per il Teorema di Compattezza, è sufficiente dimostrare che $\Gamma \cup \Delta$ è finitamente soddisfacibile.

Sia $\Gamma_0 \cup \Delta_0$ finito, con $\Gamma_0 \subseteq \Gamma$ e $\Delta_0 \subseteq \Delta$. Sia X_0 l'insieme degli $x \in X$ che occorrono in una qualche lettera proposizionale di Δ_0. Allora X_0 è finito e per la Proposizione 4.8 c'è un ordine totale stretto $\lhd$ su X_0 che estende $\prec$ su X_0. È possibile estendere $\lhd$ ad ordine totale stretto su X, che continuiamo a indicare con $\lhd$. Per fare questo basta fissare un ordine lineare di $X \setminus X_0$ (che esiste sempre per il Teorema 14.3) e porre tutti gli elementi di X_0 prima degli elementi di $X \setminus X_0$. Allora la valutazione $\mathcal{V}\colon L \to 2$ indotta da $\lhd$ soddisfa $\Gamma \cup \Delta_0$ e quindi, a maggior ragione, soddisfa $\Gamma_0 \cup \Delta_0$. Per l'arbitrarietà di $\Gamma_0 \cup \Delta_0$ si ha che $\Gamma \cup \Delta$ è finitamente soddisfacibile, come richiesto. □

Dimostriamo infine che ogni algebra di Boole è isomorfa ad una subalgebra di qualche $\mathscr{P}(X)$.

Teorema 14.12 (Stone)**.** *Assumiamo* AC*. Sia B un'algebra di Boole e sia $\mathcal{U}$ l'insieme di tutti gli ultrafiltri di B. La funzione $f\colon B \to \mathscr{P}(\mathcal{U})$*

$$f(b) = \{\, D \in \mathcal{U} \mid b \in D \,\}$$

è un morfismo iniettivo di algebre di Boole.

Dimostrazione. $f(0_B) = \emptyset$ e $f(1_B) = \mathcal{U}$, poiché nessun ultrafiltro contiene 0_B e tutti contengono 1_B. Supponiamo $D \in f(b) \cup f(c)$: allora $b \in D$ o $c \in D$ e poiché $b, c \leq b \vee c$ otteniamo in ogni caso $b \vee c \in D$, cioè $D \in f(b \vee c)$. Viceversa, se $D \in f(b \vee c)$, cioè $b \vee c \in D$, allora per la Proposizione 12.7 $b \in D$ o $c \in D$, da cui $D \in f(b) \cup f(c)$. Quindi

$$\forall b, c \in B\, (f(b \vee c) = f(b) \cup f(c))\,.$$

Nessun ultrafiltro può contenere b e b^*, per qualunque $b \in B$, quindi $f(b) \cap f(b^*) = \emptyset$. Viceversa se $D \notin f(b)$, cioè $b \notin D$, allora $b^* \in D$ per la Proposizione 12.7 e quindi $D \in f(b^*)$. Cioè

$$\forall b \in B\, (f(b^*) = \mathcal{U} \setminus f(b))\,.$$

Per ogni $b \neq 0_B$, l'insieme $\{\, c \in B \mid b \leq c \,\}$ è un filtro che quindi può essere esteso ad un ultrafiltro. In altre parole

$$\forall b \in B \setminus \{0_B\}\ f(b) \neq \emptyset\,.$$

Quindi $\ker f = \{0_B\}$, cioè f è un morfismo iniettivo. □

Esercizi

Esercizio 14.13. Dimostrare—senza assumere AC—che le seguenti affermazioni sono equivalenti:

(i) AC.

(ii) Se $\mathcal{A}$ è una partizione di un insieme non vuoto X, allora esiste $f\colon \mathcal{A} \to \bigcup A = X$ tale che $f(A) \in A$, per ogni $A \in \mathcal{A}$.

(iii) Se $\mathcal{A}$ è una partizione di un insieme non vuoto X, allora esiste $T \subseteq \bigcup \mathcal{A}$ tale che $T \cap A$ è un singoletto, per ogni $A \in \mathcal{A}$.

(iv) Se $f\colon X \twoheadrightarrow Y$ allora esiste un'inversa sinistra per f, cioè esiste $g\colon Y \rightarrowtail X$ tale che $\forall y \in Y\ (f \circ g(y) = y)$.

(v) Se R è una relazione ed è un insieme, allora c'è una funzione f tale che $\mathrm{dom}(f) = \mathrm{dom}(R)$ e $\forall x \in \mathrm{dom}(R)\ (x, f(x)) \in R$.

Nel Teorema 8.8 abbiamo visto che $|\kappa \times \kappa| = \kappa$, per ogni cardinale infinito κ. Quindi, assumendo AC, se X e Y sono insiemi non vuoti e X è infinito, allora

$$|X \times X| = |X|\,,$$
$$|X \cup Y| = |X \times Y|\,.$$

Nel prossimo esercizio vedremo che queste due conseguenze di AC sono entrambe equivalenti ad AC stesso.

Esercizio 14.14. (i) Sia X è un insieme infinito e sia $f\colon X \times \mathrm{Hrtg}(X) \rightarrowtail X \cup \mathrm{Hrtg}(X)$. Dimostrare che

$$\forall x \in X\ \exists \alpha \in \mathrm{Hrtg}(X)\ f(x, \alpha) \in \mathrm{Hrtg}(X)\,.$$

Concludere che se $|X \cup Y| = |X \times Y|$ per ogni coppia di insiemi infiniti non vuoti X e Y, allora AC vale.

(ii) Dimostrare che se $|X \cup \mathrm{Hrtg}(X)| = |(X \cup \mathrm{Hrtg}(X)) \times (X \cup \mathrm{Hrtg}(X))|$, allora $X \rightarrowtail \mathrm{Hrtg}(X)$. Concludere che se X è equipotente a $X \times X$, per ogni insieme infinito X, allora AC vale.

Esercizio 14.15. Dimostrare che:

(i) Se V_α è bene ordinabile per ogni α, allora AC vale.

(ii) Se $\mathscr{P}(\alpha)$ è bene ordinabile per ogni α, allora AC vale.

Note e osservazioni

La letteratura sull'assioma di scelta è vastissima. A parte i classici libri [**Jec73, RR85**] e il monumentale [**HR98**] segnaliamo tra le più recenti pubblicazioni [**Her06**]. L'Esercizio 14.15 è dovuto a Sierpiński.

15. Applicazioni dell'Assioma di Scelta*

L'Assioma di Scelta ha molte importanti applicazioni in matematica.

15.A. Algebra.

Teorema 15.1 (AC)**.** *Ogni spazio vettoriale V su un campo $\Bbbk$ ha una base. Due basi di V su $\Bbbk$ sono in bijezione.*

In particolare $\mathbb{R}$ ha una base su $\mathbb{Q}$; una base siffatta si dice **base di Hamel**.

Un campo $\Bbbk$ si dice algebricamente chiuso se ogni polinomio a coefficienti in $\Bbbk$ ha una soluzione in $\Bbbk$. Un campo $\overline{\Bbbk}$ si dice **chiusura algebrica** di un campo $\Bbbk$ se è algebricamente chiuso, $\overline{\Bbbk} \supseteq \Bbbk$ e non esistono campi algebricamente chiusi $\Bbbk'$ tali che $\Bbbk \subset \Bbbk' \subset \overline{\Bbbk}$.

Teorema 15.2 (AC)**.** *Per ogni campo $\Bbbk$, la chiusura algebrica esiste ed è unica a meno di isomorfismi.*

Teorema 15.3 (AC)**.** *In un anello con unità, ogni ideale proprio può essere esteso ad un ideale massimale.*

15.B. Topologia. Ricordiamo che la **topologia prodotto** o **topologia di Tychonoff** è generata dagli aperti di base

$$\begin{aligned} \boldsymbol{N}(U_{i_0}, \dots, U_{i_n}) &= \{\, f \in \bigtimes_{i\in I} X_i \mid f(i_k) \in U_{i_k},\ k = 0, \dots, n \,\} \\ &= \bigtimes_{j\in\{i_0,\dots,i_n\}} U_j \times \bigtimes_{i\in I\setminus\{i_0,\dots,i_n\}} X_i \end{aligned}$$

dove $\{i_0, \dots, i_n\} \subseteq I$ e U_{i_k} è aperto in X_{i_k}.

Teorema 15.4 (Tychonoff)**.** *Assumiamo* AC*. Allora il prodotto di spazi compatti è compatto.*

Infatti questo risultato è *equivalente* all'Assioma di Scelta—Esercizio 15.8. Poiché AC è l'affermazione che il prodotto di insiemi non vuoti è non vuoto, il Teorema di Tychonoff deve essere inteso come segue: Dati degli spazi compatti X_i $(i \in I)$, se l'*insieme* $\bigtimes_{i\in I} X_i$ è non-vuoto, allora è compatto come spazio topologico. Osserviamo che se $\bigtimes_{i\in I} X_i = \emptyset$, allora è banalmente uno spazio compatto.

15.C. Analisi.

Teorema 15.5 (Hahn-Banach)**.** *Assumiamo* AC*. Siano X uno spazio vettoriale su $\mathbb{R}$, $X_0 \subseteq X$ un sottospazio e $\lambda_0 \colon X_0 \to \mathbb{R}$ un'applicazione lineare. Supponiamo $p \colon X \to \mathbb{R}$ sia un'applicazione sub-lineare, cioè*

$$p(x+y) \leq p(x) + p(y)$$

tale che $\forall x \in X_0\, (\lambda_0(x) \leq p(x))$. Allora c'è un'estensione lineare $\lambda \colon X \to \mathbb{R}$ di λ_0 tale che $\forall x \in X\, (\lambda(x) \leq p(x))$.

15.D. Insiemi patologici. Tuttavia AC alcune conseguenze indesiderabili, per esempio l'esistenza di insieme patologici. Per esempio:

Teorema 15.6 (Vitali)**.** *Assumiamo* AC*, o anche solo che $\mathbb{R}$ sia bene ordinabile. Esiste un sottoinsieme di $[0;1]$ non Lebesgue misurabile.*[5]

Il risultato seguente, noto come **Paradosso di Banach-Tarski** è probabilmente la più contro-intuitiva conseguenza dell'Assioma di Scelta.

Teorema 15.7 (Banach-Tarski)**.** *Assumiamo* AC*, o anche solo che $\mathbb{R}$ sia bene ordinabile e sia*

$$B = \left\{ (x,y,z) \in \mathbb{R}^3 \mid x^2 + y^2 + z^2 \leq 1 \right\}$$

la palla unitaria dello spazio euclideo. Esiste una partizione

$$\{X_1, \ldots, X_n, Y_1, \ldots, Y_m\}$$

di B ed esistono $\sigma_1, \ldots, \sigma_n, \tau_1, \ldots, \tau_m$ isometrie di $\mathbb{R}^3$ tali che

$$\{\sigma_1[X_1], \ldots, \sigma_n[X_n]\} \quad e \quad \{\tau_1[Y_1], \ldots, \tau_m[Y_m]\}$$

sono partizioni di B.

In altre parole: è possibile suddividere B in un numero finito di pezzi che opportunamente traslati e ruotati formano due copie di B.

[5] La misura di Lebesgue è richiamata nella sezione 1616.A.

Esercizi

Nel prossimo esercizio dimostreremo che il Teorema di Tychonoff implica AC.

Esercizio 15.8. Sia $\langle X_i \mid i \in I\rangle$ una famiglia di insiemi non vuoti e sia y un insieme che non appartiene a $\bigcup_{i\in I} X_i$. Diamo a $Y_i = X_i \cup \{y\}$ la topologia i cui aperti sono $\emptyset$, $\{y\}$ e Y_i. Dimostrare che:

(i) Y_i è compatto (ma, in generale, non T_0) e tale che $\prod_{i\in I} Y_i$ è compatto e non vuoto.

(ii) $\bigtimes_{i\in I} X_i$ è l'intersezione di una famiglia con la proprietà dell'intersezione finita di chiusi di $\bigtimes_{i\in I} Y_i$,

(iii) $\bigtimes_{i\in I} X_i \neq \emptyset$.

Note ed osservazioni

L'assioma di scelta ha uno *status* particolare in matematica in quanto ha molte conseguenze utili e interessanti e alcune altre contro-intuitive e bizzarre. Dato che le prime sono di gran lunga più numerose delle seconde, AC viene considerato dalla maggioranza dei matematici un principio insiemisticamente valido. Inoltre nel 1937 Kurt Gödel ha dimostrato che se mai una contraddizione in matematica fosse ottenibile mediante l'assioma di scelta, allora si potrebbe ottenere una contraddizione anche senza usare AC. In altre parole: non possiamo refutare AC a partire dagli assiomi di MK o di ZF, a meno che queste teorie non siano contraddittorie, nel qual caso ogni affermazione sarebbe dimostrabile. Nel 1963, Paul J. Cohen dimostrò un risultato analogo per la negazione di AC, e quindi non possiamo dimostrare AC a partire dagli assiomi di MK o di ZF, a meno che queste teorie non siano contraddittorie. Per una panoramica dei vari "disastri" che possono capitare in matematica se si assume o se non si assume AC rimandiamo al libro di Herrlich [**Her06**]. La monografia [**Wag93**] contiene un'esposizione dettagliata del paradosso di Banach-Tarski (Teorema 15.7).

16. Forme deboli dell'Assioma di Scelta

L'Assioma di Scelta è utile in molte parti della Matematica, ma ancora più utili sono alcuni suoi indebolimenti. L'**Assioma delle Scelte Numerabili** è l'enunciato: per ogni insieme X, vale $\mathsf{AC}_\omega(X)$, dove $\mathsf{AC}_\omega(X)$ è:

> Per ogni successione $\langle A_n \mid n \in \omega \rangle$ di sotto-insiemi non vuoti di X, esiste una f tale che $f(n) \in A_n$ per ogni $n \in \omega$, cioè:
>
> $$\forall A \in (\mathscr{P}(X) \setminus \{\emptyset\})^\omega \, \exists f \in X^\omega \, \forall n \in \omega \, (f(n) \in A_n) \, .$$

Se X è bene ordinabile allora $\mathsf{AC}_\omega(X)$ è vero in quanto possiamo sempre scegliere l'elemento minimo di A_n, ma se X non è bene ordinabile questo $\mathsf{AC}_\omega(X)$ non è dimostrabile in MK o in ZF.

Esercizio 16.1. Dimostrare che se X si surietta su Y, allora $\mathsf{AC}_\omega(X) \Rightarrow \mathsf{AC}_\omega(Y)$.

In particolare, $\mathsf{AC}_\omega(\mathbb{R})$ dice che per ogni successione numerabile di insiemi non vuoti di reali $A_0, A_1, \ldots$ c'è un successione di reali $a_0, a_1, \ldots$ tali che $a_n \in A_n$.

Esercizio 16.2. Assumere $\mathsf{AC}_\omega(\mathbb{R})$. Dimostrare che:

(68) Per ogni $f \colon \mathbb{R} \to \mathbb{R}$, se f è sequenzialmente continua in un punto $\bar{x}$, vale a dire $f(x_n) \to f(\bar{x})$ per ogni successione $x_n \to \bar{x}$, allora f è continua in $\bar{x}$.

Infatti l'enunciato (68) è *equivalente* ad $\mathsf{AC}_\omega(\mathbb{R})$—si veda l'Esercizio 16.28. Tuttavia la sua versione globale:

> Per ogni $f \colon \mathbb{R} \to \mathbb{R}$, se f è sequenzialmente continua in *ogni* punto $\bar{x}$, allora f è continua su $\mathbb{R}$.

è dimostrabile senza l'Assioma di Scelta [**Her06**, pag. 30].

Teorema 16.3. *Assumiamo* AC_ω. *Ogni insieme infinito* X *contiene una successione di elementi distinti, cioè esiste* $f \colon \omega \rightarrowtail X$.

Dimostrazione. Sia $\mathcal{G}_n = \{ \, g \mid g \colon n \rightarrowtail X \, \}$. Poiché X è infinito, $\mathcal{G}_n \neq \emptyset$ per tutti gli $n \in \omega$. Infatti se, per assurdo, $\bar{n}$ fosse il minimo naturale tale che $\mathcal{G}_{\bar{n}} = \emptyset$, allora $\bar{n} \neq 0$, dato che $\emptyset \in \mathcal{G}_0 = \emptyset$, e quindi $\bar{n} = \bar{m} + 1$. Sia $p \in \mathcal{G}_{\bar{m}}$ e sia x un elemento di $A_{\bar{m}}$: allora $p \cup \{(\bar{m}, x)\} \in \mathcal{G}_{\bar{m}+1} = \mathcal{G}_{\bar{n}}$, contro la nostra ipotesi. Per ricorsione definiamo $f \colon \omega \to X$

$$f(0) = g_1(0)$$
$$f(n+1) = g_{n+2}(i)$$

dove $i = \min \{ \, k \leq n+1 \mid g_{n+2}(k) \notin \{f(0), \ldots, f(n)\} \, \}$. Poiché $\operatorname{ran}(g_{n+2})$ ha $n+2$ elementi, almeno uno di questi non appartiene all'insieme $\{f(0), \ldots, f(n)\}$ e quindi f è ben definita. Una facile induzione mostra che f è iniettiva. □

Teorema 16.4. AC_ω *implica che l'unione numerabile di insiemi numerabili è numerabile.*

Dimostrazione. Siano X_n insiemi tali che $|X_n| \leq \omega$ e dimostriamo che $|\bigcup_n X_n| \leq \omega$. Sia $N\colon \bigcup_n X_n \to \omega$

$$N(x) = \min\{\, n \in \omega \mid x \in X_n \,\}.$$

Per AC_ω possiamo scegliere delle funzioni iniettive $f_n\colon X_n \rightarrowtail \omega$ e quindi definire l'iniezione

$$F\colon \bigcup_n X_n \rightarrowtail \omega \times \omega\,, \qquad F(x) = (N(x), f_{N(x)}(x))\,.$$

□

Se $\alpha_n < \omega_1$, allora $\sup\{\, \alpha_n \mid n < \omega \,\} = \bigcup_n \alpha_n < \omega_1$ per il Teorema 16.4 e analizzando la dimostrazione si vede che è sufficiente assumere $\mathsf{AC}_\omega(\mathbb{R})$: per ogni n scegliamo[6] un $R_n \subseteq \omega \times \omega$ tale che $\langle \mathrm{fld}(R_n), R_n\rangle$ è un buon ordine di tipo α_n. Da R_n possiamo ricostruire la funzione $f_n\colon \alpha_n \rightarrowtail \omega$ e la dimostrazione procede come prima. Abbiamo quindi dimostrato:

Teorema 16.5. $\mathsf{AC}_\omega(\mathbb{R})$ *implica che ogni successione* $\langle \alpha_n \mid n < \omega\rangle$ *in* ω_1 *è superiormente limitata in* ω_1.

Esercizio 16.6. Sia κ è un cardinale infinito e siano X_α tali che $|X_\alpha| \leq \kappa$ per ogni $\alpha < \kappa$. Dimostrare che AC implica che $\left|\bigcup_{\alpha<\kappa} X_\alpha\right| \leq \kappa$.

Un'altra forma debole dell'Assioma di Scelta è data dall'**Assioma delle Scelte Dipendenti**. Per ogni insieme $X \neq \emptyset$, $\mathsf{DC}(X)$ asserisce che:

> Se R è una relazione su X è tale che $\forall x\, \exists y\, (x\ R\ y)$, allora per ogni $x_0 \in X$ c'è una $f \in {}^{\omega}X$ tale che $f(0) = x_0$ e $\forall n\, (f(n)\ R\ f(n+1))$.

Come per l'Assioma delle Scelte numerabili, $\mathsf{DC}(X)$ è dimostrabile quando X è bene ordinabile, ma non in generale.

Esercizio 16.7. Dimostrare che se X si surietta su Y, allora $\mathsf{DC}(X) \Rightarrow \mathsf{DC}(Y)$.

Proposizione 16.8. $\mathsf{AC} \Rightarrow \mathsf{DC} \Rightarrow \mathsf{AC}_\omega$.

Dimostrazione. Cominciamo col dimostrare che DC è conseguenza dell'Assioma di Scelta. Sia X un insieme e $R \subseteq X \times X$ tale che $\forall x\, \exists y\, (x\ R\ y)$. Fissiamo un $x_0 \in X$ e una funzione di scelta $C\colon \mathscr{P}(X) \setminus \{\emptyset\} \to X$. Per ricorsione definiamo la funzione $f\colon \omega \to X$ ponendo $f(0) = x_0$ e

$$f(n+1) = C\,(\{\, y \in X \mid f(n)\ R\ y \,\})\,.$$

È immediato verificare che la funzione f soddisfa DC.

[6] $R_n \in \mathscr{P}(\omega \times \omega)$ e $\omega \times \omega$ è in bijezione con ω, per cui $\mathsf{AC}_\omega(\mathbb{R})$ è sufficiente.

Per verificare che $\mathsf{DC} \Rightarrow \mathsf{AC}_\omega$ fissiamo una famiglia $\{ A_n \mid n \in \omega \}$ di insiemi non vuoti. Sia $X = \bigcup_n A_n \times \{n\}$ e sia $R \subseteq X \times X$ la relazione

$$(a, n)\ R\ (b, m) \quad \Leftrightarrow \quad m = n + 1\,.$$

Fissiamo un elemento $a_0 \in A_0$: per DC c'è una funzione $f\colon \omega \to X$ tale che $f(0) = (a_0, 0)$ e $f(n)\ R\ f(n+1)$ per tutti gli n. La funzione

$$g(n) = \text{la prima componente della coppia ordinata } f(n)$$

è la funzione cercata. □

È stato dimostrato che le implicazioni nella Proposizione 16.8 non possono essere rovesciate.

Esercizio 16.9. Assumiamo DC. Dimostrare che una relazione irriflessiva R su un insieme X è ben-fondata se e solo se non esistono sequenze $\langle x_n \mid n < \omega \rangle$ tali che $x_{n+1}\ R\ x_n$, per tutti gli n.

16.A. La misura di Lebesgue. Una famiglia di insiemi $\mathcal{S} \subseteq \mathscr{P}(X)$ è una **σ-algebra** se è una sub-algebra di Boole di $\mathscr{P}(X)$ e se è numerabilmente completa, cioè per ogni $\mathcal{A} \subseteq \mathcal{S}$ numerabile, $\bigcup \mathcal{A} \in \mathcal{S}$.

Esercizio 16.10. Se $\Sigma \neq \emptyset$ è una famiglia di σ-algebre su X ciascuna delle quali contiene $\mathcal{A} \subseteq \mathscr{P}(X)$, cioè

$$\forall \mathcal{S} \in \Sigma\, (\mathcal{A} \subseteq \mathcal{S})$$

allora $\bigcap \Sigma$ è una σ-algebra contenete $\mathcal{A}$.

Per ogni $\mathcal{A} \subseteq \mathscr{P}(X)$ possiamo quindi definire la σ-algebra generata da $\mathcal{A}$ come la più piccola σ-algebra contenente $\mathcal{A}$,

$$\bigcap \{\, \mathcal{S} \subseteq \mathscr{P}(X) \mid \mathcal{S} \text{ è una } \sigma\text{-algebra e } \mathcal{A} \subseteq \mathcal{S} \,\}$$

Se assumiamo $\mathsf{AC}_\omega(\mathbb{R})$, è possibile dare una descrizione alternativa di questa σ-algebra:

$$\begin{aligned} \mathcal{S}_0 &= \mathcal{A} \cup \breve{\mathcal{A}} \cup \{\emptyset, X\} \\ \mathcal{S}_{\alpha+1} &= \{ \bigcup_{n\in\omega} A_n \mid A_n \in \mathcal{S}_\alpha \cup \breve{\mathcal{S}}_\alpha \} \\ \mathcal{S}_\lambda &= \bigcup_{\alpha<\lambda} \mathcal{S}_\alpha \qquad\qquad \lambda \text{ limite,} \end{aligned}$$

dove $\breve{\mathcal{B}} \stackrel{\text{def}}{=} \{\, X \setminus B \mid B \in \mathcal{B} \,\}$, per ogni $\mathcal{B} \subseteq \mathscr{P}(X)$. È facile verificare per induzione su α che

- $\beta < \alpha \Rightarrow \mathcal{S}_\beta \cup \breve{\mathcal{S}}_\beta \subseteq \mathcal{S}_\alpha$ e
- $\mathcal{S}_\alpha$ è contenuto nella σ-algebra generata da $\mathcal{A}$.

Per costruzione $\mathcal{S}_{\omega_1}$ è non vuoto, contiene $\mathcal{A}$ ed è chiuso per complementi: se $A \in \mathcal{S}_{\omega_1}$ allora $A \in \mathcal{S}_\alpha$, quindi $X \setminus A \in \breve{\mathcal{S}}_\alpha \subseteq \mathcal{S}_{\alpha+1}$. Inoltre, data una successione di insiemi $A_n \in \mathcal{S}_{\omega_1}$, $(n \in \omega)$, scegliamo degli ordinali $\alpha_n \in \omega_1$ tali che $A_n \in \mathcal{S}_{\alpha_n}$: per il Teorema 16.5 esiste $\alpha < \omega_1$ tale che $\{ A_n \mid n \in \omega \} \subseteq \mathcal{S}_\alpha$ e quindi $\bigcup_n A_n \in \mathcal{S}_{\alpha+1}$. Quindi $\mathcal{S}_{\omega_1}$ è una σ-algebra ed è la σ-algebra generata da $\mathcal{A}$.

Se X è uno spazio topologico con topologia $\mathcal{T}$, la σ-algebra dei **Boreliani**

$$\mathbf{Bor}(X, \mathcal{T})$$

è la più piccola σ-algebra su X contenente $\mathcal{T}$. Quando la topologia $\mathcal{T}$ è chiara dal contesto scriveremo semplicemente $\mathbf{Bor}(X)$.

Uno **spazio di misura** è una tripla $\langle X, \mathcal{S}, \mu \rangle$ tale che

- $\mathcal{S}$ è una σ-algebra su X
- $\mu \colon \mathcal{S} \to [0; +\infty]$ soddisfa
  (a) $\mu(\emptyset) = 0$,
  (b) se $A_n \in \mathcal{S}$ sono a due a due disgiunti, allora

$$\mu\left(\bigcup_n A_n\right) = \sum_{n=0}^{\infty} \mu(A_n)\,. \tag{69}$$

La serie (69) è a termini positivi, quindi la sua somma è ben definita. Gli insiemi in $\mathcal{S}$ si dicono **$\mathcal{S}$-misurabili**, o misurabili secondo $\mathcal{S}$, mentre la funzione μ si dice **misura**. La proprietà (69) si dice **σ-additività**.

Esercizio 16.11. Dimostrare che per ogni misura μ,

$$A \subseteq B \Rightarrow \mu(A) \leq \mu(B)$$
$$\mu(A \cup B) = \mu(A) + \mu(B) - \mu(A \cap B)$$

Osserviamo che la nozione di spazio di misura è ridondante, dato che dalla misura μ possiamo ricavare la σ-algebra $\mathcal{S} = \mathrm{dom}(\mu)$ e da questa si ricava l'insieme $X = \bigcup \mathcal{S}$. Tuttavia spesso non si distingue tra una misura μ ed una sua restrizione ad una sotto-σ-algebra, per cui la nozione di spazio di misura risulta molto comoda. Uno spazio di misura $\langle X, \mathcal{S}, \mu \rangle$ si dice:

spazio di misura completo se

$$\forall A \in \mathcal{S}\, \forall B \subseteq X\, (\mu(A) = 0 \Rightarrow B \in \mathcal{S} \wedge \mu(B) = 0)\,;$$

spazio di probabilità se $\mu(X) = 1$;

spazio di misura finito se $\mu(X) < \infty$;

spazio di misura σ-finito se esistono $X_n \in \mathcal{S}$ tali che $X = \bigcup_n X_n$ e $\mu(X_n) < \infty$.

La misura μ si dirà, rispettivamente, **misura completa**, **misura di probabilità**, **misura finita**, **misura σ-finita**. Una **misura esterna** su X è una funzione

$$F\colon \mathscr{P}(X) \to [0;+\infty]$$

che soddisfa

(1) $F(\emptyset) = 0$,

(2) $A \subseteq B \Rightarrow F(A) \leq F(B)$,

(3) $F(\bigcup_n X_n) \leq \sum_{n=0}^{\infty} F(X_n)$, per ogni successione $X_n \in \mathcal{S}$, $(n \in \omega)$.

La proprietà (3) si dice **σ-sub-additività**. A dispetto del nome, una misura esterna non è necessariamente una misura. Tuttavia ogni misura esterna induce una misura.

Teorema 16.12 (Carathéodory)**.** *Se F è una misura esterna su X, allora*

$$\mathcal{S} = \{\, A \subseteq X \mid \forall B \subseteq X\, (F(B \cap A) + F(B \setminus A) \leq F(B)) \,\}$$

è una σ-algebra, $\mu = F \restriction \mathcal{S}$ è una misura e lo spazio $\langle X, \mathcal{S}, \mu\rangle$ è completo.

Per una dimostrazione si veda un qualsiasi testo di teoria della misura, per esempio [**Fre01**, Theorem 113C].

Diamo ora un cenno su come si definisce la misura di Lebesgue su $\mathbb{R}$. Definiamo $F\colon \mathscr{P}(\mathbb{R}) \to [0;\infty]$

$$F(A) = \inf\left\{ \sum_n (b_n - a_n) \mid A \subseteq \bigcup_{n<\omega} [a_n; b_n) \right\},$$

dove tacitamente assumiamo che quando si considera l'intervallo semiaperto $[a;b)$ si ha che $b \geq a$. È facile verificare che F verifica le proprietà (1) e (2) della definizione di misura esterna. Per dimostrare la sub-additività, fissiamo un $\varepsilon > 0$ e facciamo vedere che $F(\bigcup_n X_n) \leq \sum_{n=0}^{\infty} F(X_n) + \varepsilon$. Per ogni n scegliamo una famiglia di intervalli semiaperti che ricopre X_n e che approssima $F(X_n)$ a meno di $\varepsilon/2^{n+1}$, cioè

$$X_n \subseteq \bigcup_{i\in\omega} [a_i^{(n)}; b_i^{(n)}) \qquad \text{e} \qquad \sum_{i=0}^{\infty} (b_i^{(n)} - a_i^{(n)}) < F(X_n) + \varepsilon/2^{n+1}\,. \tag{70}$$

Per far questo dobbiamo effettuare ω scelte elementi di $(\mathbb{R}^2)^\omega$ e dato che quest'insieme è equipotente ad $\mathbb{R}$ (vedi 9.E.2 a pagina 83) è sufficiente usare $\mathsf{AC}_\omega(\mathbb{R})$. Scelti gli $[a_i^{(n)}; b_i^{(n)})$ possiamo concludere osservando che $\bigcup_n X_n \subseteq \bigcup_n \bigcup_i [a_i^{(n)}; b_i^{(n)})$ e

$$\sum_{n=0}^{\infty}\sum_{i=0}^{\infty} (b_i^{(n)} - a_i^{(n)}) \leq \sum_{n=0}^{\infty} (F(X_n) + \varepsilon/2^{n+1}) = \sum_{n=0}^{\infty} F(X_n) + \varepsilon\,.$$

Quindi F è una misura esterna su $\mathbb{R}$. La misura indotta da questa F si dice **misura di Lebesgue** su $\mathbb{R}$ e la si indica con λ, e la σ-algebra data dal teorema di Carathéodory viene denotato è la famiglia degli **insiemi Lebesgue misurabili** e la si denota con $\mathrm{Meas}(\mathbb{R}, \lambda)$ o semplicemente $\mathrm{Meas}(\lambda)$. Questa σ-algebra è più grande di $\mathbf{Bor}(\mathbb{R})$, la σ-algebra dei Boreliani di $\mathbb{R}$.

La costruzione della misura di Lebesgue può essere ripetuta per $\mathbb{R}^n$, usando invece degli intervalli $[a; b)$ gli insiemi

$$[\boldsymbol{a}; \boldsymbol{b}) \stackrel{\text{def}}{=} \{\, \boldsymbol{c} \in \mathbb{R}^n \mid a_i \leq c_i < b_i \,\}$$

dove $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{R}^n$. Analogamente, al posto della lunghezza $(b - a)$ si considera il volume $\prod_{i=1}^{n}(b_i - a_i)$. La misura e la σ-algebra corrispondenti si denotano con λ^n e $\mathrm{Meas}(\mathbb{R}^n, \lambda^n)$ o $\mathrm{Meas}(\lambda^n)$.

La misura λ^n gode della seguente proprietà: per ogni $A \subseteq \mathbb{R}^n$ Lebesgue-misurabile,

$$\begin{aligned} \lambda^n(A) &= \sup \{\, \lambda^n(K) \mid K \subseteq A \ \wedge\ K \text{ compatto} \,\} \\ &= \inf \{\, \lambda^n(U) \mid U \supseteq A \ \wedge\ U \text{ aperto} \,\} \end{aligned} \tag{71}$$

Un sotto-insieme di uno spazio topologico si dice $\mathbf{G}_\delta$ se è intersezione numerabile di aperti e $\mathbf{F}_\sigma$ se è unione numerabile di chiusi. Un insieme che sia unione numerabile di compatti si dice $\mathbf{K}_\sigma$.

$$\begin{aligned} \forall A \subseteq \mathbb{R}^n \big[& A \in \mathrm{Meas}(\lambda^n) \Leftrightarrow \\ & \exists F \in \mathbf{K}_\sigma\, \exists G \in \mathbf{G}_\delta\, (F \subseteq A \subseteq G \ \wedge \lambda^n(F) = \lambda^n(G)) \big]. \end{aligned} \tag{72}$$

Un'altra importante caratteristica della misura di Lebesgue è che è invariante per isometrie, cioè se $\sigma\colon \mathbb{R}^n \to \mathbb{R}^n$ è un'isometria e $A \in \mathrm{Meas}(\lambda^n)$, allora $\sigma[A] \in \mathrm{Meas}(\lambda^n)$ e $\lambda^n(\sigma[A]) = \lambda^n(A)$.

La misura di Lebesgue sugli intervalli coincide con la lunghezza, cioè se I è un intervallo (aperto, chiuso, semiaperto) di estremi $a < b$, allora $\lambda(I) = b - a$. Ricordiamo che l'insieme $E_{1/3}$ di Cantor (vedi pagina 80) è ottenuto rimuovendo dall'intervallo $[0; 1]$ una famiglia numerabile di aperti. La misura del suo complementare in $[0; 1]$ è

$$\sum_{n=1}^{\infty} \frac{1}{3^n} = 1$$

quindi $\lambda(E_{1/3}) = 0$. Quindi l'insieme $E_{1/3}$ di Cantor è un esempio di insieme chiuso, più che numerabile, privo di interno e di misura 0.

Argomentando come per la misura di Lebesgue, si dimostra che la funzione $F\colon \mathscr{P}(2^{\mathbb{N}}) \to [0; 1]$

$$F(A) = \inf \left\{ \sum_{s \in \mathcal{A}} 2^{-\mathrm{lh}(s)} \mid \mathcal{A} \subseteq 2^{<\mathbb{N}} \ \wedge\ \bigcup \mathcal{A} \supseteq A \right\}$$

è una misura esterna e quindi risulta definita uno spazio di misura $\langle 2^{\mathbb{N}}, \mathrm{Meas}, \mu\rangle$. Per verificare la sub-additività di F, in analogia con quanto fatto in (70), dati $X_n \subseteq 2^{\mathbb{N}}$ si scelgono $\mathcal{A}_n \subseteq 2^{<\mathbb{N}}$ tali che $F(X_n) \leq \sum_{s\in\mathcal{A}_n} 2^{-\mathrm{lh}(s)} + \varepsilon/2^{n+1}$ e poiché $\mathcal{A}_n$ è un elemento di $\mathscr{P}(2^{<\mathbb{N}})$ che è equipotente ad $\mathbb{R}$, tale scelta è lecita per $\mathsf{AC}_\omega(\mathbb{R})$. È facile verificare che è di probabilità e che $\mu(\boldsymbol{N}_s) = 2^{-\mathrm{lh}(s)}$.

Osservazione 16.13. La misura μ si dice **misura di Cantor** o anche **misura di Lebesgue sull'insieme di Cantor**. La scelta di chiamare μ misura di Lebesgue può apparire per lo meno bizzarra, visto che $2^{\mathbb{N}}$ viene spesso identificato con $E_{1/3}$ e $\mu(2^{\mathbb{N}}) = 1$, mentre $\lambda(E_{1/3}) = 0$. Tuttavia $2^{\mathbb{N}}$ è anche identificabile con (cioè omeomorfo a) un sotto-insieme di $[0;2]$ che ha λ-misura uguale ad 1 (Esercizio 16.26). Un sottoinsieme di $\mathbb{R}$ omeomorfo a $2^{\mathbb{N}}$ può essere ottenuto generalizzando la costruzione di $E_{1/3}$ in più direzioni. Per esempio possiamo rimpiazzare l'intervallo $[0;1]$ con un generico intervallo chiuso J e scegliere un coefficiente $r_n \in (0;1)$ da utilizzare al passo n della costruzione, cioè definiamo

$$\mathrm{Cantor}(J;(r_m)_m) = \bigcap_n \mathrm{Cantor}^{(n)}(J;(r_m)_m) \tag{73}$$

dove $\mathrm{Cantor}^{(0)}(J;(r_m)_m) = J$, $\mathrm{Cantor}^{(n)}(J;(r_m)_m)$ è unione di 2^n intervalli chiusi disgiunti e $\mathrm{Cantor}^{(n+1)}(J;(r_m)_m)$ è ottenuto rimpiazzando ciascuno intervallo I di $\mathrm{Cantor}^{(n)}(J;(r_m)_m)$ con $I_{(0;r_n)}$ e $I_{(1;r_n)}$, definiti in (40). Gli insiemi $\mathrm{Cantor}(J;(r_m)_m)$ si dicono **insiemi di Cantor generalizzati**. Quando la successione $(r_n)_n$ è costantemente uguale a r scriveremo $\mathrm{Cantor}(J,r)$. Quindi $E^{(n)}_{1/3} = \mathrm{Cantor}^{(n)}([0;1],1/3)$ e

$$E_{1/3} = \mathrm{Cantor}([0;1],1/3)\,.$$

16.B. La categoria di Baire. Sia $\langle P,\leq\rangle$ un insieme pre-ordinato e consideriamo la topologia $\mathcal{T}$ su P generata dagli insiemi

$$\boldsymbol{N}(p) \stackrel{\mathrm{def}}{=} \{\, q\in P \mid q\leq p\,\} \qquad (p\in P)\,.$$

$\boldsymbol{N}(p)$ è un intorno di base del punto p. Questa topologia, che non deve essere confusa con la topologia degli intervalli (si veda pagina 58), in generale non è neppure T_0. Un insieme $D\subseteq P$ è denso in questa topologia se

$$\forall p\in P\,\exists q\in D\,(q\leq p)\,.$$

Per evitare confusioni con l'altra nozione di densità, se vale la proprietà introdotta qui sopra diremo che D è **denso nel senso del *forcing***[7]. Vediamo un paio di esempi.

[7] Il nome *forcing* si riferisce ad un'importante tecnica usata in teoria degli insiemi.

16.B.1. Se X è uno spazio topologico sia P l'insieme degli aperti non-vuoti di X con l'ordinamento

$$p \leq q \quad \Leftrightarrow \quad p \subseteq q\,.$$

Se $U \subseteq X$ è un aperto denso, allora

$$\{\, p \in P \mid p \subseteq U \,\}$$

è un insieme denso (nel senso del *forcing*) in P. Se X è metrico, anche l'insieme

$$\left\{\, p \in P \mid \operatorname{diam}(p) \leq 2^{-n} \,\right\}$$

è denso.

16.B.2. Sia $P = \{\, p \mid p \text{ è una funzione, } p \subseteq \omega \times \omega,\ |p| < \omega \,\}$ con l'ordinamento

$$p \leq q \quad \Leftrightarrow \quad p \supseteq q\,.$$

A prima vista l'ordinamento di P sembra contro-intuitivo, ma se identifichiamo ogni $p \in P$ con l'aperto $\boldsymbol{N}(p) = \{\, x \in {}^{\omega}\omega \mid p \subset x \,\}$ dello spazio di Baire ${}^{\omega}\omega$, vediamo che $p \leq q$ se e solo se $\boldsymbol{N}(p) \subseteq \boldsymbol{N}(q)$, come nell'esempio precedente.

Esercizio 16.14. Verificare che per ogni $n \in \omega$ gli insiemi

$$A_n = \{\, p \mid n \in \operatorname{dom}(p) \,\} \qquad \text{e} \qquad B_n = \{\, p \mid n \in \operatorname{ran}(p) \,\}$$

sono densi in P.

Il seguente risultato, benché semplice, è di grande utilità.

Teorema 16.15. *Assumiamo* DC. *Sia* $(P, \leq)$ *un insieme pre-ordinato e siano* $D_n \subseteq P$ $(n \in \omega)$ *degli insiemi densi nel senso del* forcing. *Allora per ogni* $\bar{p} \in P$ *c'è una successione* $\bar{p} \geq p_0 \geq p_1 \geq \ldots$ *di elementi di* P *tale che* $\forall n \in \omega\,(p_n \in D_n)$.

Dimostrazione. Fissiamo $\bar{p} \in P$ e consideriamo la relazione R su $\bigcup_{n\in\omega}\{n\}\times D_n$,

$$(n, q)\ R\ (m, r) \quad \Leftrightarrow \quad m = n + 1\ \wedge\ q \geq r\,.$$

Per la densità di D_0 troviamo un $p_0 \in D_0$ tale che $\bar{p} \geq p_0$. La densità dei D_n assicura che possiamo applicare DC e ottenere una successione

$$(0, p_0)\ R\ (1, p_1)\ R\ (2, p_2)\ R \ldots$$

e quindi la successione $\bar{p} \geq p_0 \geq p_1 \geq \ldots$ è come richiesto. □

Osservazione 16.16. Nella dimostrazione precedente DC è stata applicata all'insieme $\omega \times P$. Quindi per l'Esercizio 16.7, se P è numerabile, il risultato vale senza ipotesi aggiuntive.

Il prossimo risultato, noto come **Teorema di Categoria di Baire**, asserisce che in molti spazi topologici, l'intersezione numerabile di aperti densi è non vuota. Ricordiamo che uno spazio topologico X si dice localmente compatto se è T_2 e ogni punto ha un intorno la cui chiusura è compatta. Ne segue che se $x \in U$ esiste $V \subseteq U$ intorno compatto di x.

Teorema 16.17. *Assumiamo* DC. *Sia $X \neq \emptyset$ uno spazio localmente compatto, oppure metrico completo. Se gli U_n sono aperti densi e se U è un aperto non vuoto, allora*

$$\bigcap_{n\in\omega} U_n \cap U \neq \emptyset\,.$$

Dimostrazione. Supponiamo che X sia metrico completo. Sia

$$P = \{\, p \subseteq X \mid p \text{ è una palla aperta} \,\}$$

con l'ordinamento $p \leq q \Leftrightarrow p \subseteq q$. Sia

$$D_n = \left\{\, p \mid \operatorname{diam}(p) \leq 2^{-n} \ \wedge\ \operatorname{Cl}(p) \subseteq U_n \,\right\}.$$

Come osservato nell'Esempio 16.B.1, l'insieme D_n è denso in P. Sia $\bar{p} \in P$ tale che $\bar{p} \subseteq U$. Possiamo quindi trovare una successione $(p_n)_n$ come nel Teorema 16.15. Sia $x_n \in X$ il centro di p_n. Per costruzione, $x_i, x_j \in p_N$ e quindi $d(x_i, x_j) < 2^{-N}$, per ogni $i, j \geq N$ e quindi $(x_n)_n$ è una successione di Cauchy rispetto alla metrica completa d. Quindi c'è un $\bar{x} \in X$ che è limite della successione $(x_n)_n$. Per ogni $n \in \mathbb{N}$, $d(\bar{x}, x_n) \leq 2^{-n}$ e quindi $\bar{x} \in \operatorname{Cl}(p_n) \subseteq U_n$. In altre parole: $\bar{x} \in \bigcap_n U_n$. Dato che $\bar{x} \in p_0 \subseteq U$, abbiamo provato che $\bigcap_{n\in\omega} U_n \cap U \neq \emptyset$, come richiesto.

Supponiamo ora X localmente compatto: il pre-ordine è

$$P = \{\, p \subseteq X \mid p \neq \emptyset \text{ è un aperto con chiusura compatta} \,\}$$

con l'ordinamento $p \leq q \Leftrightarrow \operatorname{Cl}(p) = \operatorname{Cl}(q)$ e sia

$$D_n = \{\, p \in P \mid p \subseteq U_n \,\}\,.$$

Sia $\bar{p} \in P$ tale che $\bar{p} \subseteq U$. Fissata la successione $(p_n)_n$ come dal Teorema 16.15, osserviamo che

$$\{\, \operatorname{Cl}(p_n) \mid n \in \omega \,\}$$

è una famiglia decrescente di compatti non vuoti e quindi, per la proprietà dell'intersezione finita, $\bigcap_n \operatorname{Cl}(p_n)$ contiene un elemento $\bar{x}$. Quindi $\bar{x} \in \bigcap_n U_n$ e dato che $\bar{x} \in p_0 \subseteq \bar{p} \subseteq U$, il teorema è dimostrato. □

Osservazioni 16.18. (a) Se X è *separabile* metrico completo, oppure *secondo numerabile* localmente compatto, allora l'ordine P può essere preso numerabile e quindi, per l'Osservazione 16.16, il ricorso a DC può essere evitato. (Nel caso degli spazi metrici si prendono palle aperte centrate nei punti dell'insieme numerabile e di raggio razionale; nel caso degli spazi localmente compatti si prendono gli aperti di base con

chiusura compatta.) In particolare, il Teorema 16.17 per $\mathbb{R}^n$ o per uno spazio di Banach separabile è dimostrabile senza scelta.

(b) Il Teorema 16.17 per X metrico completo arbitrario implica DC.

(c) Se X soddisfa le ipotesi del Teorema 16.17 e non ha punti isolati, allora $X \setminus \{x\}$ è un aperto denso di X e quindi X non è numerabile.

Un sotto-insieme M di uno spazio topologico X si dice **magro** o di **prima categoria** se esistono chiusi C_n con interno vuoto tali che $M \subseteq \bigcup_n C_n$. Quindi il teorema di Categoria di Baire dice che in uno spazio localmente compatto, oppure metrico completo, nessun aperto non vuoto è magro.

Il Teorema di Categoria di Baire viene spesso usato per dimostrare risultati di *esistenza*: se vogliamo un $x \in X$ che soddisfa la proprietà P (e se X è metrico completo oppure localmente compatto) è sufficiente dimostrare che $\{\, x \in X \mid P(x) \,\}$ è non magro e quindi non vuoto. (In molti casi si dimostra che questo insieme è comagro e quindi non magro.) Per esempio l'insieme

$$\mathscr{D} = \{\, \mathscr{C}([0;1]) \mid \exists x \in [0;1] \ f \text{ non è differenziabile in } x \,\}$$

è magro e quindi $\mathscr{C}([0;1]) \setminus \mathscr{D}$ è comagro [**Fol99**, pag.??]. In particolare, la generica funzione continua su $[0;1]$ non è differenziabile in alcun punto. Vediamo ora un'applicazione alle algebre di Boole del Teorema 16.15.

Teorema 16.19. *Due algebre di Boole numerabili e prive di atomi sono isomorfe.*

Per dimostrare questo risultato introduciamo la seguente

Definizione 16.20. Siano A e B due algebre di Boole. Un **isomorfismo parziale** di A in B è un isomorfismo $p\colon A' \to B'$ dove A' e B' sono subalgebre finite di A e B, rispettivamente.

Lemma 16.21. *Siano A e B algebre di Boole e sia $p\colon A' \to B'$ un isomorfismo parziale di A in B. Supponiamo B sia priva di atomi. Allora $\forall x \in A \setminus A' \exists y \in B \setminus B'$ tale che p si estende ad un isomorfismo parziale $q\colon A'' \to B''$, dove A'' e B'' sono le algebre di Boole generate da $A' \cup \{x\}$ e $B' \cup \{y\}$.*

Dimostrazione. Per il Corollario 11.22 $A'' = \{\, (u \wedge x) \vee (v \wedge x^*) \mid u, v \in A' \,\}$, quindi gli atomi di A'' sono gli elementi non nulli della forma

$$\left\{\, a \wedge x \mid a \in \mathrm{At}(A') \,\right\} \cup \left\{\, a \wedge x^* \mid a \in \mathrm{At}(A') \,\right\}.$$

Definiamo

$$\mathcal{A}_1 = \left\{\, a \in \mathrm{At}(A') \mid 0_A < a \wedge x < a \,\right\}$$
$$\mathcal{A}_2 = \left\{\, a \in \mathrm{At}(A') \mid a < x \,\right\}.$$

Per ogni $a \in \mathcal{A}_1$, poiché B non ha atomi possiamo scegliere un $0_B < y_a < p(a)$ e per $a \in \mathcal{A}_2$ sia $y_a = p(a)$. (AC non è necessario in quanto B è numerabile.) Sia

$$y = \bigvee_{a \in \mathcal{A}_1 \cup \mathcal{A}_2} y_a$$

e sia $\mathcal{B}''$ l'algebra generata da $\mathcal{B}' \cup \{y\}$. (L'operazione di sup è legittima in quanto $\mathcal{A}_1 \cup \mathcal{A}_2$ è finito.) Dato che $p(a) \wedge y = y_a$, si ha che

$$0_A < a \wedge x < a \Rightarrow 0_B < p(a) \wedge y < p(a)$$

Supponiamo $a < x$: allora deve esistere un atomo $a' \neq a$ tale che $a' \wedge x \neq 0_A$ e quindi

$$p(a) < p(a) \vee y_{a'} = y_a \vee y_{a'} \leq y$$

da cui otteniamo

$$a < x \Rightarrow p(a) < y\,.$$

Infine, se $a \wedge x = 0_A$, allora $p(a) \wedge y = 0_B$. Lasciamo come esercizio al lettore verificare che gli atomi di B'' sono gli elementi non nulli di

$$\big\{\, p(a) \wedge y \mid a \in \mathrm{At}(A') \,\big\} \cup \big\{\, p(a) \wedge y^* \mid a \in \mathrm{At}(A') \,\big\}$$
$$\big\{\, b \wedge y \mid b \in \mathrm{At}(B') \,\big\} \cup \big\{\, b \wedge y^* \mid b \in \mathrm{At}(B') \,\big\}\,.$$

e che la funzione $\mathrm{At}(A'') \to \mathrm{At}(B'')$ data da

$$a \wedge x \mapsto p(a) \wedge y, \qquad a \wedge x^* \mapsto p(a) \wedge y^*$$

è una bijezione e si estende ad un isomorfismo di A'' su B''. □

Siamo ora in grado di dimostrare il Teorema 16.19.

Dimostrazione. Siano $A = \{\, a_n \mid n \in \omega \,\}$ e $B = \{\, b_n \mid n \in \omega \,\}$ due algebre di Boole come nell'enunciato del teorema. Un isomorfismo parziale di A in B è un isomorfismo $p\colon A' \to B'$ dove A' e B' sono subalgebre finite di A e B, rispettivamente.

Il Lemma ci assicura che ogni isomorfismo parziale da A in B può essere esteso in modo da contenere nel dominio un qualsiasi $x \in A$. Poiché l'inverso di un isomorfismo parziale da A in B è un isomorfismo parziale da B in A, quindi il Lemma dimostra che ogni isomorfismo parziale può essere esteso in modo da contenere nell'immagine un qualsiasi $y \in B$. Sia

$$P = \{\, p \mid p \text{ è un isomorfismo parziale di } A \text{ in } B \,\}$$

ordinato mediante il converso dell'inclusione, cioè $p \leq q \Leftrightarrow q \subseteq p$. Il Lemma 16.21 ci assicura che gli insiemi $D_{2n} = \{\, p \in P \mid a_n \in \mathrm{dom}(p) \,\}$ sono densi e dato che l'inverso di un isomorfismo parziale di A in B è un isomorfismo parziale di B in A, abbiamo che anche gli $D_{2n+1} = \{\, p \in P \mid b_n \in \mathrm{ran}(p) \,\}$

sono densi. Possiamo quindi trovare una successione $p_0 \geq p_1 \geq p_2 \geq \dots$ tale che $p_i \in D_i$. Per costruzione la funzione

$$f \stackrel{\text{def}}{=} \bigcup_n p_n \colon A \to B$$

è una bijezione tra A e B. È quindi sufficiente dimostrare che f è un omomorfismo. Se $x, y \in A$, fissiamo indici $m, n, h, k \in \omega$ tali che $x = a_m$, $y = a_n$, $x^* = a_h$ e $x \wedge y = a_k$. Allora $x, y, x^*, x \wedge y \in \mathrm{dom}(p_{2N})$ dove $N = \max\{n, m, h, k\}$ e poiché p_{2N} è un isomorfismo parziale, $p_{2N}(x^*) = p_{2N}(x)^*$ e $p_{2N}(x \wedge y) = p_{2N}(x) \wedge p_{2N}(y)$. Dal momento che f estende p_{2N} si ha che $f(x^*) = f(x)^*$ e $f(x \wedge y) = f(x) \wedge f(y)$. Essendo x e y arbitrari in A, otteniamo che f è un morfismo. □

Corollario 16.22. *Le algebre di Boole* $\mathrm{Prop}(L)$*, dove* L *è un insieme numerabile e l'algebra degli intervalli di* $\mathbb{Q}$ *sono isomorfe.*

16.C. σ-ideali. Un ideale I su un insieme X è un **σ-ideale** se è chiuso per unioni numerabili, vale a dire se $A_n \in I$, allora

$$\bigcup_n A_n \in I\,.$$

Per il Teorema 16.4 la famiglia dei sottoinsiemi numerabili di X

$$\{\, A \subseteq X \mid |A| \leq \aleph_0 \,\} \tag{74}$$

è un σ-ideale. È un ideale proprio se e solo se X non è numerabile. Conviene introdurre la seguente notazione: per ogni cardinale κ (finito o infinito) e ogni insieme X definiamo

$$[X]^{\kappa} = \{\, A \subseteq X \mid |A| = \kappa \,\} \tag{75}$$

$$[X]^{<\kappa} = \{\, A \subseteq X \mid |A| < \kappa \,\} \tag{76}$$

$$[X]^{\leq\kappa} = \{\, A \subseteq X \mid |A| \leq \kappa \,\} \tag{77}$$

sono, rispettivamente, la famiglia dei sottoinsiemi di X di cardinalità κ, minore di κ, al più κ. Osserviamo che la formula (75) è la generalizzazione ad un insieme X arbitrario della formula (36). Il σ-ideale (74) è

$$[X]^{\leq\aleph_0}\,,$$

mentre l'ideale dei sottoinsiemi finiti è

$$[X]^{<\aleph_0}\,.$$

Se μ è una misura completa sull'insieme X,

$$\mathrm{Null}(\mu) \stackrel{\text{def}}{=} \{\, A \subseteq X \mid \mu(A) = 0 \,\}$$

è il σ-ideale dei sottoinsiemi di μ misura 0; se X è uno spazio localmente compatto, oppure metrico completo,

$$\mathrm{Mgr}(X) \stackrel{\text{def}}{=} \{\, A \subseteq X \mid A \text{ è magro in } X \,\}$$

è il σ-ideale dei sottoinsiemi magri di X. Chiaramente ogni sottoinsieme numerabile di $\mathbb{R}$ è di misura (di Lebesgue) nulla e di prima categoria, cioè

$$[\mathbb{R}]^{\leq\omega} \subseteq \mathrm{Null}(\lambda) \cap \mathrm{Mgr}(\mathbb{R})\,.$$

I σ-ideali su $\mathbb{R}$ sono nozioni di "trascurabilità": in molte dimostrazioni è sufficiente argomentare che una certa proprietà φ vale per tutti i numeri reali *eccetto che per una quantità trascurabile di eccezioni*, vale a dire

$$\{\, x \in \mathbb{R} \mid \varphi \text{ non vale in } x \,\}$$

è in un qualche σ-ideale proprio, quale $[\mathbb{R}]^{\leq\omega}$, $\mathrm{Null}(\lambda)$, o $\mathrm{Mgr}(\mathbb{R})$. Osserviamo che gli ideali $\mathrm{Null}(\lambda)$ e $\mathrm{Mgr}(\mathbb{R})$ sono distinti, anzi ortogonali: infatti c'è un sottoinsieme $\mathbb{R}$ di misura 0 il cui complemento è magro (Esercizio 16.32).

Esercizi

Un insieme si dice **Dedekind-infinito** o, più brevemente, **D-infinito**, se è in bijezione con un suo sottoinsieme proprio. Altrimenti si dice **Dedekind-finito**, ovvero **D-finito**.

Esercizio 16.23. Dimostrare che per ogni insieme X le seguenti condizioni sono equivalenti:

(i) X è D-infinito,

(ii) X e $X \setminus \{x\}$ sono equipotenti, per ogni $x \in X$,

(iii) c'è una funzione $f\colon \omega \rightarrowtail X$.

Concludere che da AC_ω segue che un insieme è D-finito se e solo se è finito.

Esercizio 16.24. Supponiamo che esista un $A \subseteq \mathbb{R}$ infinito ma D-finito. (Naturalmente non possiamo assumere AC_ω.) Dimostrare che A può essere preso contenuto in $(0;1)$ e tale che $0 = \inf A$. Verificare che la funzione caratteristica $\boldsymbol{\chi}_A$ è discontinua in 0, ma è sequenzialmente continua in 0.

Esercizio 16.25. (i) Dimostrare che $\mathsf{DC}(X)$ è equivalente al seguente enunciato, apparentemente più debole, in cui non si fissa il primo elemento della successione f:

> Se R è una relazione su X è tale che $\forall x\, \exists y\, (x\ R\ y)$, allora c'è una $f \in {}^{\omega}X$ tale che $\forall n\, (f(n)\ R\ f(n+1))$.

(ii) Dimostrare che DC implica la sua versione per classi proprie:

> Per ogni classe $X \neq \emptyset$ (propria o meno), per ogni $x_0 \in X$ e ogni relazione R su X tale che $\forall x\, \exists y\, (x\ R\ y)$, c'è una $f \in {}^{\omega}X$ tale che $f(0) = x_0$ e $\forall n\, (f(n)\ R\ f(n+1))$.

Esercizio 16.26. Dimostrare che:

(i) Per ogni $a < b$ e ogni successione $(r_n)_n$ di reali in $(0; 1)$, gli insiemi $2^{\mathbb{N}}$ e $\mathrm{Cantor}([a; b], (r_n)_n)$ sono omeomorfi, vale a dire, tutti gli insiemi di Cantor generalizzati (vedi (73)) sono tra loro omeomorfi.

(ii) $\lambda\,(\mathrm{Cantor}([a; b], r)) = 0$,

(iii) Per ogni $0 \leq s < b - a$ c'è una successione $(r_n)_n$ tale che

$$\lambda\,(\mathrm{Cantor}([a; b], (r_n)_n)) = 0\,.$$

Esercizio 16.27. Se $\emptyset \neq A_n \subseteq \mathbb{R}$ poniamo $B_n = A_0 \times \cdots \times B_n \subseteq \mathbb{R}^n$. Dimostrare che se c'è una successione strettamente crescente di naturali $(n_i)_i$ ed una successione di reali $(b_i)_i$ tali che $b_i \in B_{n_i}$, allora c'è una successione di reali $(a_n)_n$ tale che $a_n \in A_n$, per ogni n. Concludere che $\mathsf{AC}_\omega(\mathbb{R})$ è equivalente all'enunciato (apparentemente più debole):

> Se $\emptyset \neq A_n \subseteq \mathbb{R}$, allora c'è una successione strettamente crescente di naturali $(n_i)_i$ e una una successione di reali $(b_i)_i$ tale che $b_i \in A_{n_i}$.

Esercizio 16.28. Sia $\emptyset \neq A_n \subseteq (2^{-n-1}; 2^{-n})$ e sia $f\colon \mathbb{R} \to \mathbb{R}$ la funzione caratteristica di $\bigcup_n A_n$,

$$f(x) = \sum_{i=0}^{\infty} \boldsymbol{\chi}_{A_n}(x)\,.$$

Dimostrare che f è discontinua in 0 e che se $x_i \to 0$ è tale che $f(x_i) \not\to 0$, allora c'è una successione crescente $(n_i)_i$ ed una successione di reali $(b_i)_i$ tali che $b_i \in A_{n_i}$.

Usare l'Esercizio 16.27 per concludere che (68) implica $\mathsf{AC}_\omega(\mathbb{R})$.

Esercizio 16.29. Verificare che il Teorema 16.17 per $X = \mathbb{R}$ vale senza ipotesi addizionali.

Esercizio 16.30. Assumere $\mathsf{AC}_\omega(\mathbb{R})$ e verificare che $\mathrm{Null}(\lambda)$ e $\mathrm{Mgr}(\mathbb{R})$ sono σ-ideali su $\mathbb{R}$.

Esercizio 16.31. Dimostrare che se vale AC_ω, allora uno spazio secondo numerabile è separabile.

Esercizio 16.32. Dimostrare che per ogni $\varepsilon > 0$ ci sono aperti densi $U_n^\varepsilon \mathbb{R}$ tali che $\lambda(U_n^\varepsilon) \leq \varepsilon$.

Concludere che c'è un $F \subseteq \mathbb{R}$ che è $F = \bigcup_n C_n$, C_n è chiuso e privo di interno, $\mathbb{R} \setminus F$ ha misura di Lebesgue nulla.

Esercizio 16.33. Dimostrare che se $A, B \subseteq \mathbb{R}$ sono bene-ordinati sotto l'usuale ordinamento di $\mathbb{R}$, allora $A + B = \{ a + b \mid a \in A, b \in B \}$ è bene ordinato.

(Suggerimento: Per assurdo, considerare una successione strettamente decrescente $a_n + b_n$ e usare l'Esercizio 4.29.)

Esercizio 16.34. Dimostrare che se A è un'algebra di Boole numerabile e B è un'algebra di Boole priva di atomi, allora ogni isomorfismo parziale $p\colon A' \to B'$ si estende ad un monomorfismo $f\colon A \to B$.

Esercizio 16.35. Dimostrare che un'algebra di Boole numerabile priva di atomi B è **ultraomogenea** cioè ogni isomorfismo parziale $p\colon B' \to B''$ con $B, B'' \subseteq B$ si estende ad un automorfismo $f\colon B \to B$.

Il prossimo esercizio richiede qualche nozione di analisi funzionale. Uno **spazio di Fréchet** è uno spazio vettoriale su $\mathbb{R}$ dotato di una metrica completa d tale che le operazioni di somma $F \times F \to F$ e di prodotto per scalare $\mathbb{R} \times F \to F$ sono continue. In particolare ogni spazio di Banach è uno spazio di Fréchet (ma non viceversa).

Esercizio 16.36. Sia F uno spazio di Fréchet di dimensione infinita. Dimostrare che ogni suo sotto-spazio di dimensione finita è un chiuso privo di interno. Concludere che la dimensione di F è maggiore di $\aleph_0$.

Note e osservazioni

Gli assiomi assiomi delle scelte numerabili AC_ω e delle scelte dipendenti DC, sono usati comunemente in matematica, per esempio per verificare che una funzione è continua (Esercizio 16.2), o per costruire la misura di Lebesgue (si veda pag.132), o per dimostrare il Teorema di Baire 16.17. Il libro [**Oxt80**] è un ottima introduzione alle tecniche di misura e categoria. Per una trattazione enciclopedica della teoria della misura il riferimento d'obbligo è Measure Theory, il trattato in cinque volumi di D.H. Fremlin (quattro già pubblicati) [**Fre01, Fre02, Fre03, Fre04**]. Inoltre, se non assumiamo questi principi, varie patologie possono manifestarsi: sottoinsiemi di $\mathbb{R}$ infiniti ma Dedekind-finiti, funzioni discontinue in un punto $\bar{x}$, ma sequenzialmente continue in $\bar{x}$, etc (si veda gli Esercizi 16.23 e 16.24). Per una panoramica dei vari "disastri" che possono capitare se non si assume AC_ω oppure DC rimandiamo al libro di Herrlich [**Her06**]. Viceversa i vari "disastri" in analisi (insiemi non Lebesgue misurabili, decomposizioni paradossali della sfera—si veda la sezione 15.D) costruiti mediante AC, l'assioma di scelta vero e proprio, non sono ottenibile mediante DC, come afferma un celebre risultato di

Robert M. Solovay del 1965 (vedi [**Jec03**, pag.??]). Rimandiamo il lettore interessato al libro [**Sch97**], una vera enciclopedia per quanto riguarda gli aspetti fondazionali dell'analisi matematica. Per un'introduzione all'analisi funzionale si veda il libro di Walter Rudin [**Rud91**].

17. Il Teorema di Ramsey*

Gli ultrafiltri su ω hanno importanti applicazioni in vari settori della matematica, per esempio la topologia generale, l'analisi funzionale, etc. Come esempio vedremo un'interessante applicazione alla combinatorica: il Teorema di Ramsey. Ricordiamo che per ogni numero naturale $r > 0$

$$[X]^r = \{\, Y \subseteq X \mid |Y| = r \,\}\,.$$

è l'insieme dei sottoinsiemi di X di cardinalità r (vedi (75)). Quando X ha un ordine lineare canonico, come nel caso degli ordinali, gli elementi di $[X]^r$ possono essere identificati con *successioni crescenti* di lunghezza r di elementi di X. In particolare, se $\bar{x} \in [X]^r$, allora $x_0, x_1, \ldots, x_{r-1}$ sono gli elementi di $\bar{x}$ enumerati in ordine crescente.

Un **grafo** è un insieme di punti detti **vertici** e di archi o **spigoli** tra questi: formalmente un grafo è una coppia $\langle V, E\rangle$ dove $V \neq \emptyset$ è l'insieme dei vertici ed $E \subseteq [V]^2$ è l'insieme degli spigoli. Diremo che $\langle V, E\rangle$ è **completo** se $E = [V]^2$. Dato un grafo $\langle V, E\rangle$ (non necessariamente completo) e un numero naturale $k > 0$, una funzione $f\colon E \to k$ si dice **colorazione** del grafo con k colori: il colore dello spigolo $\{x, y\}$ è $f(\{x, y\}) \in \{0, 1, \ldots, k-1\}$. Se f è una k-colorazione, otteniamo degli insiemi $C_i \stackrel{\text{def}}{=} f^{-1}\text{“}\{i\} \subseteq [V]^2$ tali che

$$[V]^2 = C_0 \cup \cdots \cup C_{k-1}\,.$$

Viceversa, dati $C_0, \ldots, C_{k-1} \subseteq [V]^2$ tali che $[V]^2 = C_0 \cup \cdots \cup C_{k-1}$, possiamo definire una k-colorazione f ponendo

$$f(\{x, y\}) = \text{il minimo } i \text{ tale che } \{x, y\} \in C_i\,.$$

Un sottoinsieme $H \subseteq V$ si dice **monocromatico** ovvero **omogeneo** per la colorazione f se $f \restriction E \cap [H]^2$ è costante, vale a dire

$$\exists i \in k\, \forall x, y \in H\, (\{x, y\} \in E \Rightarrow f(\{x, y\}) = i)\,.$$

Equivalentemente, se $[V]^2 = C_0 \cup \cdots \cup C_{k-1}$, allora $[H]^2 \subseteq C_i$, per qualche i. Il Teorema di Ramsey dice che se $[\mathbb{N}]^2$ è colorato con k-colori, allora c'è un sottoinsieme *infinito* H monocromatico. In effetti il teorema di Ramsey dice molto di più.

Teorema 17.1 (Teorema di Ramsey nel caso infinito)**.** *Supponiamo V sia un insieme numerabile e*

$$[V]^r = C_0 \cup \cdots \cup C_{k-1}$$

dove $k, r \in \omega \setminus \{0\}$ e $C_i \subseteq [V]^r$, allora esiste un $H \subseteq V$ infinito tale che $[H]^r \subseteq C_i$, per qualche $i < k$.

Dimostrazione. Cominciamo con due semplici osservazioni. Innanzi tutto possiamo supporre che i C_i siano a due a due disgiunti: in caso contrario si considerano gli insiemi

$$C'_0 = C_0 \quad \text{e} \quad C'_{i+1} = C_{i+1} \setminus \left(C'_0 \cup \ldots C'_i\right).$$

La seconda osservazione è che basta dimostrare il Teorema per $k = 2$. Infatti il caso $k = 1$ è banale e per $k > 2$ si procede per induzione: supponiamo vero il risultato per $k \geq 2$ e dimostriamolo per $k+1$. Per il Teorema nel caso $k = 2$, esiste $H \subseteq V$ infinito tale che $[H]^r \subseteq C_0$ oppure $[H]^r \subseteq C_1 \cup \cdots \cup C_k$. Se vale la prima possibilità abbiamo dimostrato il teorema, quindi possiamo supporre

$$[H]^r \subseteq (C_1 \cap [H]^r) \cup \cdots \cup (C_k \cap [H]^r).$$

Per ipotesi induttiva c'è un $H' \subseteq H$ infinito tale che $[H]^r \subseteq C_i$ per qualche $1 \leq i \leq k$, come richiesto.

Dimostriamo quindi il teorema per $k = 2$. La dimostrazione procede per induzione su $r \geq 1$.

Supponiamo $r = 1$: l'insieme $[V]^1$ è identificabile con V per cui il risultato diventa:

$$\text{Se } V = C_0 \cup C_1, \text{ allora almeno uno tra } C_0 \text{ e } C_1 \text{ è infinito,}$$

e questo discende immediatamente dall'Esercizio 8.6.

Assumiamo il risultato vero per r e dimostriamolo per $r + 1$. Per semplicità notazionale possiamo supporre che $V = \omega$. Sia

$$f \colon [\omega]^{r+1} \to 2$$

la colorazione associata alla partizione $\{C_0, C_1\}$, vale a dire

$$f(\bar{x}) = i \;\Leftrightarrow\; \bar{x} \in C_i\,.$$

Se C_i è finito, allora

$$H = \{\, n \in \omega \mid \neg\exists \bar{x} \in [\omega]^r \,(n \in \bar{x} \wedge \bar{x} \in C_i)\,\}$$

è infinito e $[H]^r \subseteq C_{1-i}$, quindi possiamo supporre che C_0 e C_1 siano entrambi infiniti. Costruiremo un insieme $K \subseteq \omega$ tale che

$$\forall \bar{x}, \bar{y} \in [K]^{r+1} \,(x_0 = y_0 \wedge \cdots \wedge x_{r-1} = y_{r-1} \Rightarrow f(\bar{x}) = f(\bar{y})) \tag{78}$$

vale a dire: il valore di $f(\bar{x})$ dipende solo dai primi r elementi di $\bar{x}$. Possiamo quindi definire una funzione $g \colon [K]^r \to 2$ ponendo

$$g(\bar{x}) = f(\bar{x} \cup \{n\})$$

per qualche (equivalentemente: per ogni) $n \in K$ con $n > \max(\bar{x})$. Per ipotesi induttiva c'è un $H \subseteq K$ infinito ed omogeneo per g. Fissiamo $\bar{x}, \bar{y} \in [H]^{r+1}$. Poiché K soddisfa (78) e $H \subseteq K$, se $\bar{x}, \bar{y} \in [H]^{r+1}$ allora

$$\begin{aligned} f(\bar{x}) &= g(\{x_0, \dots, x_{r-1}\}) \\ &= g(\{y_0, \dots, y_{r-1}\}) \\ &= f(\bar{y})\,, \end{aligned}$$

cioè H è l'insieme omogeneo cercato. Quindi è sufficiente dimostrare l'esistenza di un insieme K che soddisfa (78).

Fissiamo un ultrafiltro non principale U su ω. Per ogni $\bar{x} \in [\omega]^r$ sia

$$D_i(\bar{x}) = \{\, n \in \omega \mid n > \max \bar{x} \ \wedge\ f(\bar{x} \cup \{n\}) = i \,\}\,.$$

Poiché

$$D_0(\bar{x}) \cup D_1(\bar{x}) = \omega \setminus (\max \bar{x} + 1) \in U$$

sia

$$i(\bar{x}) = \text{l'unico } i \in 2 \text{ tale che } D_i(\bar{x}) \in U.$$

Costruiamo induttivamente una successione di naturali y_n come segue:

- poiché $r = \{0, 1, \dots, r-1\} \in [\omega]^r$, allora
$$Y_0 = D_{i(r)}(r)$$
è ben definito; sia
$$y_0 = \min Y_0\,.$$
Osserviamo che $y_0 > r$.
- Supponiamo di aver definito $y_0, \dots, y_n$. L'insieme
$$\mathcal{X}_n = [r \cup \{y_0, \dots, y_n\}]^r$$
è finito (ha esattamente $\binom{r+n+1}{r}$ elementi) e poiché U è chiuso per intersezioni finite,
$$Y_{n+1} = \bigcap_{\bar{x} \in \mathcal{X}_n} D_{i(\bar{x})}(\bar{x}) \in U\,.$$
Dato che $\emptyset \notin U$, ne segue che $Y_{n+1} \neq \emptyset$. Sia
$$y_{n+1} = \min Y_{n+1}\,.$$

È facile verificare che $r \leq y_0 < y_1 < \dots$ e che $Y_0 \supset Y_1 \supset \dots$. Sia

$$K = \{\, y_n \mid n \in \omega \,\}\,.$$

Fissiamo un $\bar{x} \in [K]^r$ e sia $y_n = \max \bar{x}$, per cui $\bar{x} \in \mathcal{X}_n$. Se $n < m, h$, allora $y_m, y_h \in Y_{n+1} \subseteq D_{i(\bar{x})}(\bar{x})$ per cui $f(\bar{x} \cup \{y_m\}) = f(\bar{x} \cup \{y_h\})$. Quindi K soddisfa (78). □

Osservazione 17.2. La dimostrazione data del Teorema di Ramsey usa AC. Tuttavia il teorema è dimostrabile in ZF o in MK mediante un argomento più delicato—si veda l'Esercizio 17.4.

Corollario 17.3. *Se $<$ e $\prec$ sono due ordini totali su un insieme infinito X, allora c'è un sottoinsieme infinito $H \subseteq X$ su cui $<$ coincide con $\prec$ oppure con l'ordinamento inverso $\succ$, vale a dire*

$$\forall x, y \in H\,(x < y \Leftrightarrow x \prec y) \;\vee\; \forall x, y \in H\,(x < y \Leftrightarrow y \prec x)\,.$$

Esercizi

Esercizio 17.4. Costruire esplicitamente, senza usare l'esistenza di ultrafiltri, gli insiemi Y_n della dimostrazione del Teorema 17.1 e concludere che il Teorema di Ramsey è dimostrabile senza AC.

Esercizio 17.5. Due elementi x, y di un insieme ordinato $\langle X, \leq\rangle$ si dicono **incomparabili** se

$$x \not\leq y \quad \wedge \quad y \not\leq x\,.$$

Un sottoinsieme di X costituito da elementi a due a due incomparabili si dice **indipendente**.

Dimostrare che per ogni successione $\langle x_n \mid n \in \omega\rangle$ di elementi distinti di di X ammette una sottosuccessione $\langle x_{n_k} \mid k \in \omega\rangle$ strettamente crescente, oppure strettamente decrescente, oppure tale che $\{\, x_{n_k} \mid k \in \omega \,\}$ è un insieme indipendente di $\langle X, \leq\rangle$.

In particolare AC_ω implica che ogni insieme ordinato infinito contiene una catena infinita, oppure insieme indipendente infinito.

18. Aritmetica cardinale (II)

L'Assioma di Scelta, che assumeremo d'ora in poi, ci consente di sviluppare l'aritmetica cardinale.

Definizione 18.1. Per κ, λ cardinali definiamo l'**esponenziazione cardinale**

$$\kappa^\lambda = \left|{}^\lambda\kappa\right|\,.$$

Chiaramente, se $\kappa \leq \nu$ e $\lambda \leq \mu$ sono cardinali, allora $\kappa^\lambda \leq \nu^\mu$.

Esercizio 18.2. Siano κ, λ, μ cardinali. Dimostrare che

$$\left(\kappa^{\lambda}\right)^{\mu} = \kappa^{\lambda\cdot\mu}$$
$$\kappa^{\lambda+\mu} = \kappa^{\lambda}\cdot\kappa^{\mu}$$
$$(\kappa\cdot\lambda)^{\mu} = \kappa^{\mu}\cdot\lambda^{\mu}\,.$$

Il Teorema di Cantor 8.9 può essere riformulato come

$$\forall I\left(|I| < 2^{|I|}\right). \tag{79}$$

L'**ipotesi del continuo**, in simboli CH, è l'enunciato

$$2^{\aleph_0} = \aleph_1\,,$$

o equivalentemente:

$$\forall X \subseteq \mathbb{R}\,(|X| \leq \aleph_0 \vee |X| = |\mathbb{R}|)\,.$$

L'**ipotesi generalizzata del continuo** (GCH) è la naturale generalizzazione di CH a tutti i cardinali infiniti:

$$\forall\alpha \in \mathrm{Ord}\left(2^{\aleph_\alpha} = \aleph_{\alpha+1}\right),$$

o equivalentemente:

$$\forall X \subseteq \mathscr{P}(\aleph_\alpha)\,(|X| \leq \aleph_\alpha \vee |X| = |\mathscr{P}(\aleph_\alpha)|)\,.$$

CH e GCH sono indipendenti da $\mathsf{ZF}+\mathsf{AC}$ e da $\mathsf{MK}+\mathsf{AC}$, nel senso che né $\mathsf{ZF}+\mathsf{AC}$ né $\mathsf{MK}+\mathsf{AC}$ sono in grado di dimostrare (Cohen, 1963) o refutare (Gödel, 1938) queste affermazioni.

18.A. Somme e prodotti generalizzati.

Definizione 18.3. Data una successione $\langle k_i \mid i \in I\rangle$ di cardinali, la **somma generalizzata** dei κ_i è

$$\sum_{i\in I}\kappa_i = \left|\bigcup_{i\in I}\{i\}\times\kappa_i\right|,$$

il **prodotto generalizzato** dei κ_i è

$$\prod_{i\in I}\kappa_i = |\mathsf{X}_{i\in I}\kappa_i|\,.$$

Dalla definizione si ottiene subito che

- $\kappa = \sum_{i\in\kappa} 1 = \sum_{i\in\kappa}\kappa_i$, con $\kappa_i = 1$,
- $2^{\kappa} = \prod_{i\in\kappa} 2 = \prod_{i\in\kappa}\kappa_i$, con $\kappa_i = 2$.

Proposizione 18.4. *Se I è un insieme infinito e $1 \leq \kappa_i$, per ogni $i \in I$,*

$$\sum_{i\in I} \kappa_i = |I| \cdot \sup_{i\in I} \kappa_i \,.$$

Dimostrazione. Per ogni $\alpha \in \sup_{i\in I} \kappa_i$ scegliamo un $i(\alpha) \in I$ tale che $\alpha \in \kappa_{i(\alpha)}$: la funzione $\sup_{i\in I} \kappa_i \to \bigcup_{i\in I}\{i\} \times \kappa_i$, $\alpha \mapsto (i(\alpha), \alpha)$ è iniettiva e prova che $\sup_{i\in I} \kappa_i \leq \sum_{i\in I} \kappa_i$. Chiaramente

$$|I| = \sum_{i\in I} 1 \leq \sup_{i\in I} \kappa_i$$

e quindi per (35) $|I| \cdot \sup_{i\in I} \kappa_i \leq \sum_{i\in I} \kappa_i$. L'inclusione $\bigcup_{i\in I}\{i\} \times \kappa_i \subseteq I \times \sup_{i\in I} \kappa_i$ prova l'altra disuguaglianza. □

Teorema 18.5. *Per ogni famiglia di insiemi $\{ X_i \mid i \in I \}$*

$$\left|\bigcup_{i\in I} X_i\right| \leq |I| \cdot \sup_{i\in I} |X_i| \,.$$

Dimostrazione. Per ogni $i \in I$ fissiamo una bijezione $f_i \colon X_i \to |X_i|$ e per ogni $x \in \bigcup_{i\in I} X_i$ fissiamo un $i(x) \in I$ tale che $x \in X_{i(x)}$. La funzione

$$\bigcup_{i\in I} X_i \to \bigcup_{i\in I}\{i\} \times |X_i| \quad x \mapsto (i(x), f_{i(x)}(x))$$

è iniettiva e quindi $\left|\bigcup_{i\in I} X_i\right| \leq \sum_{i\in I} |X_i|$. Il risultato segue immediatamente dalla Proposizione 18.4. □

Teorema 18.6. *Sia κ un cardinale infinito ed $\mathcal{F} = \{ f_\alpha \mid \alpha < \lambda \}$ una famiglia di cardinalità $\lambda \leq \kappa$ di funzioni finitarie su un insieme X di cardinalità κ. Allora*

$$|\mathrm{Cl}_{\mathcal{F}}(Y)| \leq \max\{\omega, \lambda, |Y|\}$$

per ogni $Y \subseteq X$.

Dimostrazione. Posso supporre $X = \kappa$. Per la Proposizione 7.8, $\mathrm{Cl}_{\mathcal{F}}(Y) = \bigcup_n Y_n$, dove $Y_0 = Y$ e $Y_{n+1} = Y_n \cup \{ f(\bar{y}) \mid \bar{y} \in Y^{<\omega} \}$. Per il Teorema 18.5 è sufficiente dimostrare che per ogni $n \in \omega$

$$|Y_n| \leq \nu \,,$$

dove $\nu = \max(\omega, \lambda, |Y|)$. Questo certamente vero se $n = 0$. Supposto vero per un certo $\bar{n}$, allora $|Y_{\bar{n}}^{<\omega}| \leq \nu$ per il Teorema 14.5, e dato che $Y_{\bar{n}+1}$ è immagine suriettiva di $\mathcal{F} \times Y_{\bar{n}}^{<\omega}$, si ha che $|Y_{\bar{n}+1}| \leq \lambda \cdot \nu = \nu$. □

Esercizio 18.7. Dimostrare che se $|I| \geq 3$ e $2 \leq \kappa_i \leq \lambda_i$ $(i \in I)$, allora la funzione $F\colon \bigcup_{i\in I}\{i\}\times\kappa_i \to \bigtimes_{i\in I}\lambda_i$ che ad (i,α) associa la funzione $F(i,\alpha) \in \bigtimes_{i\in I}\lambda_i$ definita da

$$F(i,\alpha)(j) = \begin{cases} \alpha & \text{se } i = j, \\ 0 & \text{se } i \neq j \text{ e } \alpha > 0, \\ 1 & \text{se } i \neq j \text{ e } \alpha = 0, \end{cases}$$

è iniettiva.

Dalla formula (34) (se $|I| = 2$) e dall'Esercizio 18.7 (se $|I| > 2$) ricaviamo che se $I \neq \emptyset$

$$2 \leq \kappa_i \leq \lambda_i \Rightarrow \sum_{i\in I} \kappa_i \leq \prod_{i\in I} \lambda_i\,.$$

Teorema 18.8 (J. König)**.** *Se $\kappa_i < \lambda_i$ per ogni $i \in I$, allora*

$$\sum_{i\in I} \kappa_i < \prod_{i\in I} \lambda_i\,.$$

Dimostrazione. È sufficiente dimostrare che $\sum_{i\in I}\kappa_i \not\geq \prod_{i\in I}\lambda_i$, cioè che nessuna funzione $F\colon \bigcup_i\{i\}\times\kappa_i \to \bigtimes_{i\in I}\lambda_i$ può essere suriettiva. Fissiamo una F come sopra: per ogni $i \in I$, l'insieme

$$\{\, F(i,\alpha)(i) \mid \alpha \in \kappa_i \,\}$$

ha cardinalità $< \lambda_i$, per cui possiamo definire la funzione $f \in \bigtimes_{i\in I}\lambda_i$

$$f(i) = \min\left(\lambda_i \setminus \{\, F(i,\alpha)(i) \mid \alpha \in \kappa_i \,\}\right).$$

Verifichiamo che $f \notin \operatorname{ran}(F)$: se, per assurdo, $f = F(i_0,\alpha_0)$, allora per definizione di f,

$$f(i_0) \notin \{\, F(i_0,\alpha)(i_0) \mid \alpha \in \kappa_{i_0} \,\},$$

una contraddizione. □

In particolare, se prendiamo $\kappa_i = 1$ e $\lambda_i = 2$ ri-otteniamo la (79).

18.B. Cardinali regolari e singolari.

Definizione 18.9. Una funzione $f\colon \beta \to \alpha$ si dice **cofinale (in α)** se $\operatorname{ran}(f)$ è illimitato in α, cioè

$$\forall \alpha' < \alpha\, \exists \beta' < \beta\, \big(\alpha' \leq f(\beta')\big)$$

La **cofinalità** di un ordinale α è il più piccolo β per cui esiste una $f\colon \beta \to \alpha$ cofinale. Questo β lo si denota $\operatorname{cof}(\alpha)$.

Vediamo qualche esempio.

18.B.1. Dato che la funzione identica è cofinale, $\operatorname{cof}(\alpha) \leq \alpha$, per ogni α. In particolare $\operatorname{cof}(0) = 0$.

18.B.2. La cofinalità di un ordinale successore $\gamma+1$ è 1, come testimoniato dalla funzione $0 \mapsto \gamma$. Viceversa, se λ è limite, $\mathrm{cof}(\lambda)$ è limite.

18.B.3. $\mathrm{cof}(\omega) = \omega$ e, per il Teorema 16.5, $\mathrm{cof}(\omega_1) = \omega_1$. Invece, $\mathrm{cof}(\aleph_\omega) = \omega$, dato che $n \mapsto \aleph_n$ è cofinale.

Lemma 18.10. *C'è una funzione $f\colon \mathrm{cof}(\alpha) \to \alpha$ cofinale e crescente.*

Dimostrazione. Sia α limite e $g\colon \mathrm{cof}(\alpha) \to \alpha$ cofinale. Definiamo per $\beta < \mathrm{cof}(\alpha)$

$$\begin{aligned} f(0) &= g(0) \\ f(\beta) &= \min\left(\alpha \setminus \sup\{\, \max(g(\gamma), f(\gamma)) \mid \gamma < \beta \,\}\right). \end{aligned}$$

Verifichiamo che la f è definita su $\mathrm{cof}(\alpha)$ e cioè che

$$\alpha \setminus \sup\{\, \max(g(\gamma), f(\gamma)) \mid \gamma < \beta \,\} \neq \emptyset\,,$$

per ogni $\beta < \mathrm{cof}(\alpha)$. Sia $\bar\beta \leq \mathrm{cof}(\alpha)$ minimo tale che

$$\alpha = \bigcup \{\, \max(g(\gamma), f(\gamma)) \mid \gamma < \beta \,\}\,.$$

La funzione $f\colon \bar\beta \to \alpha$ è strettamente crescente e maggiora $g \restriction \bar\beta$, dato che

$$\gamma_1 < \gamma_2 < \bar\beta \quad \Rightarrow \quad f(\gamma_2) > \sup\{\, \max(g(\gamma), f(\gamma)) \mid \gamma < \gamma_2 \,\} \geq f(\gamma_1), g(\gamma_1)\,.$$

Quindi

$$\alpha = \sup\{\, f(\gamma) \mid \gamma < \bar\beta \,\}$$

e $f\colon \bar\beta \to \alpha$ è cofinale e quindi $\bar\beta = \mathrm{cof}(\alpha)$. Abbiamo quindi dimostrato che $f\colon \mathrm{cof}(\alpha) \to \alpha$ è cofinale e crescente. □

Lemma 18.11. *Se $f\colon \beta \to \alpha$ e $g\colon \gamma \to \beta$ sono cofinali e crescenti, allora $f \circ g\colon \gamma \to \alpha$ è cofinale e crescente.*

Dimostrazione. La funzione $f \circ g\colon \gamma \to \alpha$ è chiaramente crescente. Se $\alpha' < \alpha$ sia $\beta' < \beta$ tale che $f(\beta') \geq \alpha'$ e sia $\gamma' < \gamma$ tale che $g(\gamma') \geq \beta'$. Allora $g(f(\gamma')) \geq \alpha'$. □

Corollario 18.12. $\mathrm{cof}(\mathrm{cof}(\alpha)) = \mathrm{cof}(\alpha)$.

Definizione 18.13. Un ordinale limite λ si dice **regolare** se $\mathrm{cof}(\lambda) = \lambda$. Altrimenti si dice **singolare**.

Se λ è un cardinale infinito, parleremo di **cardinale regolare** o **singolare**.

Se $f\colon |\lambda| \to \lambda$ è una bijezione, allora f è cofinale e quindi un ordinale regolare è sempre un cardinale regolare. Viceversa, gli ordinali limite che non sono cardinali sono ordinali singolari.

Teorema 18.14. *Ogni cardinale successore infinito κ^+ è regolare.*

Dimostrazione. Sia κ un cardinale $\geq \omega$ e supponiamo, per assurdo, che $\mathrm{cof}(\kappa^+) < \kappa^+$. Sia $f\colon \mathrm{cof}(\kappa^+) \to \kappa^+$ cofinale. Allora

$$\kappa^+ = \bigcup_{i<\mathrm{cof}(\kappa^+)} f(i)$$

e quindi per il Teorema 18.5

$$\kappa^+ = \left|\kappa^+\right| \leq \sum_{i<\mathrm{cof}(\kappa^+)} |f(i)| \leq \mathrm{cof}(\kappa) \cdot \sup_{i<\mathrm{cof}(\kappa)} |f(i)| \leq \kappa\,,$$

assurdo. □

Teorema 18.15. *Se κ è un cardinale singolare allora esiste una successione crescente $\langle \kappa_i \mid i < \mathrm{cof}(\kappa)\rangle$ di cardinali regolari tale che*

$$\kappa = \sup_{i<\mathrm{cof}(\kappa)} \kappa_i = \sum_{i<\mathrm{cof}(\kappa)} \kappa_i\,.$$

Dimostrazione. Sia $f\colon \mathrm{cof}(\kappa) \to \kappa$ cofinale e crescente. La funzione

$$g(\alpha) = \min\{\,\lambda \in \kappa \mid \lambda \text{ è regolare, } \lambda \geq f(\alpha) \text{ e } \forall \beta < \alpha\,(g(\beta) < \lambda)\,\}$$

è definita per ogni $\alpha < \mathrm{cof}(\kappa)$ dato che i cardinali regolari sono illimitati al di sotto di κ e quindi se $\bar\alpha < \mathrm{cof}(\kappa)$ fosse il più piccolo ordinale tale che $g(\bar\alpha)$ non è definita, allora vorrebbe dire che $\kappa = \sup_{\beta<\bar\alpha} g(\beta)$, cioè $g\colon \bar\alpha \to \kappa$ sarebbe cofinale, contro il fatto che $\bar\alpha < \mathrm{cof}(\kappa)$. Posto $\kappa_i = g(i)$, si ha che

$$\kappa = \sup_{i<\mathrm{cof}(\kappa)} \kappa_i \leq \sum_{i<\mathrm{cof}(\kappa)} \kappa_i \leq \kappa \cdot \mathrm{cof}(\kappa) = \kappa$$

come richiesto. □

Teorema 18.16. *Se κ è un cardinale infinito*

$$\kappa^{\mathrm{cof}(\kappa)} > \kappa\,.$$

Dimostrazione. Se κ è regolare l'enunciato diventa $\kappa^\kappa = 2^\kappa > \kappa$, che è vero per (79). Suppongo quindi che $\mathrm{cof}(\kappa) < \kappa$. Per il Teorema 18.15 possiamo trovare cardinali κ_i tali che $\kappa = \sup_{i<\mathrm{cof}(\kappa)} \kappa_i$ e quindi per il Teorema di König 18.8

$$\kappa = \sum_{i<\mathrm{cof}(\kappa)} \kappa_i < \prod_{i<\mathrm{cof}(\kappa)} \kappa = \kappa^{\mathrm{cof}(\kappa)}\,.$$

□

Corollario 18.17. $\mathrm{cof}(2^\kappa) > \kappa$.

Dimostrazione. Se $\lambda = \mathrm{cof}(2^\kappa) \leq \kappa$, allora $2^\kappa < (2^\kappa)^\lambda = 2^{\kappa\cdot\lambda} = 2^\kappa$, contraddizione. □

In particolare, $\mathrm{cof}(2^{\aleph_0}) > \aleph_0$ e quindi $2^{\aleph_0}$ non può essere $\aleph_\omega$, $\aleph_{\omega+\omega}$ (o, più in generale, $\aleph_\lambda$ con $\lambda < \omega_1$ ordinale limite) né può essere il primo punto fisso della funzione $\aleph$ (vedi pag.46). Il seguente risultato è noto come **formula di Hausdorff**.

Teorema 18.18 (Hausdorff)**.** $\aleph_{\alpha+1}^{\aleph_\beta} = \max\left(\aleph_{\alpha+1}, \aleph_\alpha^{\aleph_\beta}\right)$.

Dimostrazione. Se $\aleph_{\alpha+1} \leq \aleph_\beta$ allora per la Proposizione 8.11

$$2^{\aleph_\beta} = \aleph_\alpha^{\aleph_\beta} = \aleph_{\alpha+1}^{\aleph_\beta} > \aleph_\beta \geq \aleph_{\alpha+1}$$

e quindi il teorema è dimostrato.

Supponiamo invece che $\aleph_\beta < \aleph_{\alpha+1}$. Se $f\colon \aleph_\beta \to \aleph_{\alpha+1}$, allora per la regolarità di $\aleph_{\alpha+1}$ (Teorema 18.14) c'è un $\gamma < \aleph_{\alpha+1}$ tale che $\operatorname{ran} f \subseteq \gamma$. Quindi ${}^{\aleph_\beta}\aleph_{\alpha+1} = \bigcup_{\gamma<\aleph_{\alpha+1}} {}^{\aleph_\beta}\gamma$ e per il Teorema 18.5

$$\aleph_{\alpha+1}^{\aleph_\beta} = \left|\bigcup_{\gamma<\aleph_{\alpha+1}} {}^{\aleph_\beta}\gamma\right| \leq \aleph_{\alpha+1} \cdot \aleph_\alpha^{\aleph_\beta}.$$

L'altra disuguaglianza è immediata. □

18.C. Ulteriori risultati di aritmetica cardinale. Come abbiamo visto, la funzione esponenziale

$$\kappa \mapsto 2^\kappa$$

dove κ è un cardinale infinito, deve soddisfare

(i) $\kappa \leq \lambda \Rightarrow 2^\kappa \leq 2^\lambda$,

(ii) $\mathrm{cof}(2^\kappa) > \kappa$.

Un teorema di Easton asserisce che (i) e (ii) sono le uniche restrizioni per quanto riguarda i cardinali *regolari*. Per esempio, è possibile che $2^\kappa = \kappa^{++}$ per ogni κ regolare. Oppure è possibile che l'ipotesi generalizzata del continuo fallisca per la prima volta ad un qualsiasi cardinale regolare, vale a dire: è possibile che $2^\kappa > \kappa^+$ e che $\forall\lambda < \kappa\left(2^\lambda = \lambda^+\right)$, con κ cardinale regolare arbitrario. La situazione per i cardinali *singolari* è drasticamente differente. Jack Silver dimostrò nel 1974 che l'ipotesi generalizzata del continuo non può fallire per la prima volta a un cardinale singolare di *cofinalità più che numerabile*. Per esempio, se $\forall\alpha < \omega_1\left(2^{\aleph_\alpha} = \aleph_{\alpha+1}\right)$, allora $2^{\aleph_{\omega_1}} = \aleph_{\omega_1}+1$. Il caso dei cardinali singolari di cofinalità numerabile è ancora diverso: Menachem Magidor dimostrò nel 1978 che è possibile che l'ipotesi generalizzata del continuo fallisca per la prima volta ad $\aleph_\omega$, cioè che $\forall n < \omega\left(2^{\aleph_n} = \aleph_{n+1}\right)$ e $2^{\aleph_\omega} > \aleph_{\omega+1}$. Tuttavia il valore di $2^{\aleph_\omega}$ non può essere arbitrariamente grande. Infatti nel 1989 Saharon Shelah dimostrò che se $\forall n\left(2^{\aleph_n} < \aleph_\omega\right)$, allora

$$2^{\aleph_\omega} < \aleph_{\min(\omega_4,(2^{\aleph_0})^+)}.$$

Esercizi

Esercizio 18.19. Sia V uno spazio vettoriale su un campo $\Bbbk$ e sia B una base di V. Dimostrare che $\bigcup \{ V^X \mid X \subset B, |X| < \omega \}$ si surietta su V. Concludere che se V è di dimensione infinita, cioè $|B| \geq \aleph_0$, allora $|V| = \max(|\Bbbk|, |B|)$.

Esercizio 18.20. Supponiamo che $f_i \colon \kappa_i \to \alpha$ sia cofinale e crescente e che κ_i sia regolare $(i = 0, 1)$. Allora $\kappa_0 = \kappa_1 = \operatorname{cof}(\alpha)$.

Esercizio 18.21. Sia $\mathcal{T}$ una topologia secondo numerabile su un insieme X. Dimostrare che $\mathbf{Bor}(X, \mathcal{T}) = \bigcup_{\alpha<\omega_1} \mathcal{S}_\alpha$ e che $|\mathcal{S}_\alpha| \leq 2^{\aleph_0}$. Concludere che $|\mathbf{Bor}(X, \mathcal{T})|$, la cardinalità della famiglia dei Boreliani di X, è $\leq 2^{\aleph_0}$. In particolare $|\mathbf{Bor}(\mathbb{R})| = 2^{\aleph_0}$.

Note e osservazioni

I risultati di consistenza relativa dell'ipotesi (generalizzata) del continuo e della sua negazione sono stati ottenuti da Kurt Gödel nel 1937 e Paul Cohen nel 1963. Per un'esposizione moderna si vedano i libri di Kunen **[Kun80]** e di Jech **[Jec03]**. In particolare, nel secondo libro si trovano tutte le dimostrazioni dei risultati menzionati nella sezione §18.C.

Capitolo III

Strutture e linguaggi

19. Strutture

Una **struttura** $\mathcal{A}$ consiste di un *insieme* non-vuoto A dotato di una famiglia di relazioni $R_i \subseteq A^{n_i}$ ($i \in I$ e $n_i \geq 1$), di funzioni $f_j \colon A^{m_j} \to A$ ($j \in J$ e $m_j \geq 1$) e di elementi privilegiati $c_k \in A$ ($k \in K$). Non escludiamo che uno o più tra gli insiemi I, J e K siano vuoti.

19.A. Esempi.

19.A.1. Un semigruppo è (o meglio: può essere costruito come) una struttura

$$\langle S, * \rangle$$

con un'operazione binaria associativa $* \colon S \times S \to S$, nessuna relazione e nessuna costante. Un gruppo può essere identificato con una struttura con un'operazione binaria $*$ (il prodotto), un'operazione unaria $'$ (l'inverso) ed una costante e (l'identità). La struttura risultante sarà

$$\langle G, *, ', e \rangle \,.$$

19.A.2. Ricordiamo che un grafo è un insieme $V \neq \emptyset$ di vertici e un insieme $E \subseteq [V]^2$ di spigoli (pagina 143). Ogni grafo può essere identificato con la struttura $\langle V, \tilde{E} \rangle$ dove $\tilde{E} = \{\, (x, y) \mid \{x, y\} \in E \,\}$.

19.A.3. Un (pre-)ordine $\langle A, \leq \rangle$ è una struttura con un'unica relazione binaria $\leq$ su A che soddisfa le usuali proprietà dei pre-ordini, cioè riflessiva (antisimmetrica) e transitiva.

19.A.4. Un **anello** è una struttura $\langle R, +, \cdot, 0 \rangle$, dove $+$ e $\cdot$ soddisfano alle usuali proprietà e 0 è una costante. Un **anello unitario** è una struttura $\langle R, +, \cdot, 0, 1 \rangle$.

19.A.5. Uno spazio vettoriale su $\mathbb{R}$ è una struttura $\langle V, +, \langle \lambda_x \mid x \in \mathbb{R}\rangle, \mathbf{0}\rangle$ dove $+\colon V \times V \to V$ è l'operazione di somma di vettori, $\mathbf{0} \in V$ è l'elemento neutro e $\lambda_x\colon V \to V$, $\mathbf{v} \mapsto x\mathbf{v}$ è il prodotto per scalare. Questa è una struttura con nessuna relazione, un'operazione binaria $(+)$, $2^{\aleph_0}$ operazioni unarie, $(\lambda_x,\ x \in \mathbb{R})$ e una costante.

Più in generale, un R-modulo sinistro (dove R è un anello) può essere visto come una struttura $\langle M, +, \langle \lambda_x \mid x \in R\rangle, \mathbf{0}\rangle$, dove $\lambda_x\colon M \to M$, $m \mapsto xm$, è il prodotto per l'elemento $x \in R$.

19.B. Definizioni. Un **tipo di similarità** o **segnatura** è una 4-upla $\tau = \langle I, J, K, \mathrm{ar}\rangle$, con I, J, K insiemi disgiunti e $\mathrm{ar}\colon I \cup J \to \omega \setminus \{0\}$. Una segnatura τ si dice

- **relazionale** se $J = K = \emptyset$,
- **funzionale** se $I = K = \emptyset$,
- **finita** se la sua cardinalità è finita, dove la cardinalità di τ è il numero cardinale
$$\mathrm{card}(\tau) = |I| + |J| + |K| \,.$$

Una τ-struttura è una 4-upla
$$\mathcal{A} = \langle A, \langle R_i^{\mathcal{A}} \mid i \in I\rangle, \langle f_j^{\mathcal{A}} \mid j \in J\rangle, \langle c_k^{\mathcal{A}} \mid k \in K\rangle\rangle$$
tale che

- $A = \|\mathcal{A}\|$ è un insieme non-vuoto detto l'**universo** di $\mathcal{A}$,
- $R_i^{\mathcal{A}} \subseteq A^{\mathrm{ar}(i)}$, per ogni $i \in I$,
- $f_j^{\mathcal{A}}\colon A^{\mathrm{ar}(j)} \to A$, per ogni $j \in J$,
- $c_k^{\mathcal{A}} \in A$, per ogni $k \in K$.

Le relazioni $R_i^{\mathcal{A}}$, le funzioni $f_j^{\mathcal{A}}$ e gli elementi $c_k^{\mathcal{A}}$ si dicono, rispettivamente, **relazioni**, **funzioni** e **costanti** della τ-struttura $\mathcal{A}$. Una τ-struttura si dice relazionale (funzionale) se τ è relazionale (rispettivamente: funzionale). La classe delle τ-strutture si indica con
$$\mathfrak{Str}(\tau)\,.$$

Esercizio 19.1. Dimostrare che $\mathfrak{Str}(\tau)$ è una classe propria.

Diremo che due segnature $\tau = \langle I, J, K, \mathrm{ar}\rangle$ e $\tau' = \langle I', J', K', \mathrm{ar}'\rangle$ sono isomorfe se esiste una bijezione $\varphi\colon I \cup J \cup K \to I' \cup J' \cup K'$ tale che $\varphi[I] = I'$, $\varphi[J] = J'$, $\varphi[K] = K$ e per ogni $x \in I \cup J$
$$\mathrm{ar}'(\varphi(x)) = \mathrm{ar}(x)\,.$$
è evidente che φ induce una classe-funzione bijettiva
$$\Phi\colon \mathfrak{Str}(\tau) \to \mathfrak{Str}(\tau')\,.$$

Inoltre, con abuso di notazione, scriveremo

$$\tau \subseteq \tau'$$

se $I \subseteq I'$, $J \subseteq J'$, $K \subseteq K'$ e $\mathrm{ar} = \mathrm{ar}' \restriction I \cup J$.

Se $\mathcal{A}, \mathcal{B} \in \mathfrak{Str}(\tau)$, un **morfismo** da $\mathcal{A}$ in $\mathcal{B}$ è una funzione $\pi\colon \|\mathcal{A}\| \to \|\mathcal{B}\|$

- $\forall \bar{a} \in A^{\mathrm{ar}(i)} \left(\bar{a} \in R_i^{\mathcal{A}} \Leftrightarrow \pi(\bar{a}) \in R_i^{\mathcal{B}}\right)$, per ogni $i \in I$,
- $\forall \bar{a} \in A^{\mathrm{ar}(j)} \big(\pi(f_j^{\mathcal{A}}(\bar{a})) = f_j^{\mathcal{B}}(\pi(\bar{a}))\big)$, per ogni $j \in J$,
- $\pi(c_k^{\mathcal{A}}) = c_k^{\mathcal{B}}$, per ogni $k \in K$.

Esercizio 19.2. Verificare che $\mathfrak{Str}(\tau)$ è una categoria.

Notazione. Per semplicità di notazione se π è una funzione di dominio A, scriveremo $\bar{a} \in A$ e $\pi(\bar{a})$ invece di $(a_1, \dots, a_n) \in A^{<\omega}$ e $(\pi(a_1), \dots, \pi(a_n))$.

È importante che un morfismo preservi tutte le costanti. Per esempio $F\colon \mathbb{Z} \to \mathbb{Z}$, $k \mapsto 0$, è un morfismo della struttura $\langle \mathbb{Z}, +, \cdot, 0\rangle$ in sé stessa (cioè è un morfismo di anelli), ma non è un morfismo di $\langle \mathbb{Z}, +, \cdot, 0, 1\rangle$ in sé stessa (cioè non è un morfismo di anelli unitari). Un'**immersione** di $\mathcal{A}$ in $\mathcal{B}$ è un morfismo iniettivo di $\mathcal{A}$ in $\mathcal{B}$; un **isomorfismo** è un morfismo bijettivo. Diremo che $\mathcal{A}$ e $\mathcal{B}$ sono isomorfe

$$\mathcal{A} \cong \mathcal{B}$$

se c'è un isomorfismo tra le due strutture—chiaramente $\cong$ è una relazione di equivalenza su $\mathfrak{Str}(\tau)$. Un **automorfismo** è un isomorfismo di una struttura in se stessa e

$$\mathrm{Aut}(\mathcal{A})$$

è il gruppo degli automorfismi di $\mathcal{A}$. Diremo che $\mathcal{A}$ **si immerge in** $\mathcal{B}$, in simboli

$$\mathcal{A} \Subset \mathcal{B}\,.$$

se c'è un'immersione di $\mathcal{A}$ in $\mathcal{B}$. Nel caso in cui l'universo di $\mathcal{A}$ è fisicamente contenuto nell'universo di $\mathcal{B}$ e le relazioni, funzioni, costanti di $\mathcal{A}$ coincidono con l restrizioni di quelli di $\mathcal{B}$, cioè se $\|\mathcal{A}\| \subseteq \|\mathcal{B}\|$ e la funzione identica $\mathcal{A} \hookrightarrow \mathcal{B}$ è un'immersione, allora diremo che $\mathcal{A}$ è una **sotto-struttura** di $\mathcal{B}$

$$\mathcal{A} \subseteq \mathcal{B}\,.$$

Se inoltre $\mathcal{A} \neq \mathcal{B}$ (o, equivalentemente, $\|\mathcal{A}\| \neq \|\mathcal{B}\|$) diremo che $\mathcal{A}$ è una **sotto-struttura propria** di $\mathcal{B}$, in simboli

$$\mathcal{A} \subset \mathcal{B}\,.$$

L'espressione $\mathcal{A} \Subset \mathcal{B}$ significa che $\mathcal{A}$ è (isomorfo a) una sotto-struttura di $\mathcal{B}$; analogamente $\mathcal{A} \subset \mathcal{B}$ significa che $\mathcal{A}$ è (isomorfo a) una sotto-struttura *propria* di $\mathcal{B}$ La **cardinalità** di $\mathcal{A}$

$$\mathrm{card}(\mathcal{A})$$

è la cardinalità $|A|$ dell'universo $A = \|\mathcal{A}\|$.

Se $\mathcal{B} \subseteq \mathcal{A}$, allora $B = \|\mathcal{B}\|$ è un sottoinsieme dell'universo di $\mathcal{A}$. Il viceversa non è vero: cioè se $B \subseteq \|\mathcal{A}\|$, non è detto che B sia l'universo di una $\mathcal{B}$ sotto-struttura di $\mathcal{A}$. Quando ciò accade la struttura $\mathcal{B}$ è unica e quindi, con abuso di linguaggio, diremo che B è una sotto-struttura di $\mathcal{A}$.

Esercizio 19.3. (i) Se $\mathcal{A}$ è una struttura relazionale allora ogni $\emptyset \neq B \subseteq \|\mathcal{A}\|$ è l'universo di una sotto-struttura. Se $\mathcal{A}$ è priva di funzioni (cioè $J_\tau = \emptyset$) e $\emptyset \neq B \supseteq \{\, c_k^{\mathcal{A}} \mid k \in K \,\}$, allora B è l'universo di una sotto-struttura.

(ii) Se $\emptyset \neq X \subseteq \|\mathcal{A}\|$ e

$$\Sigma = \{\, \|\mathcal{B}\| \mid X \subseteq \|\mathcal{B}\| \wedge \mathcal{B} \subseteq \mathcal{A} \,\} .$$

Allora $S = \bigcap \Sigma$ è l'universo di una sotto-struttura $\mathcal{S} \subseteq \mathcal{A}$, la **sotto-struttura generata da** X. Dimostrare che S è la chiusura di $X \cup \{\, c_k^{\mathcal{A}} \mid k \in K \,\}$ sotto le funzioni $\left\{\, f_j^{\mathcal{A}} \mid j \in J \,\right\}$ e quindi

$$|S| \leq \max(|J|, |K|, |X|, \aleph_0) .$$

Se $\tau = \langle I, J, K, \mathrm{ar}\rangle$ e $\tau' = \langle I', J', K', \mathrm{ar}'\rangle$ sono tipi di similarità, con un abuso di linguaggio poniamo $\tau \subseteq \tau'$ se e solo se

$$I \subseteq I', \quad J \subseteq J', \quad K \subseteq K', \quad \mathrm{ar}' \restriction I \cup J = \mathrm{ar} .$$

Se $\mathcal{A}'$ è una τ'-struttura e $\tau \subseteq \tau'$, la **contrazione** di $\mathcal{A}'$ a τ è la τ-struttura

$$\mathcal{A}' \restriction \tau = \langle \|\mathcal{A}'\|, \langle R_i^{\mathcal{A}'} \mid i \in I\rangle, \langle f_j^{\mathcal{A}'} \mid j \in J\rangle, \langle c_k^{\mathcal{A}'} \mid k \in K\rangle\rangle$$

Esercizio 19.4. Dimostrare che la mappa $\mathfrak{Str}(\tau') \to \mathfrak{Str}(\tau)$ è un funtore dimenticante.

Viceversa, se $\mathcal{A}$ è una τ-struttura e $\mathcal{A}'$ è una τ'-struttura la cui contrazione a τ è $\mathcal{A}$, allora diremo che $\mathcal{A}'$ è un'**espansione** di $\mathcal{A}$ a τ'. Ogni τ-struttura ammette una τ'-espansione, ma, in generale, ad una stessa τ-struttura corrispondono più τ'-espansioni. In altre parole il funtore contrazione $\mathfrak{Str}(\tau') \twoheadrightarrow \mathfrak{Str}(\tau)$ è suriettivo.

19.C. Ultraprodotti. Sia X è un insieme non-vuoto. Il **prodotto** di una famiglia di τ-strutture $\{\, \mathcal{A}_x \mid x \in X \,\}$ è la τ-struttura $\prod_x \mathcal{A}_x$ di universo $\bigtimes_{x\in X} \|\mathcal{A}_x\|$ dove le relazioni, funzioni e costanti sono definite nel modo ovvio: se, per esempio, $\mathrm{ar}(i) = 2$ e $\mathrm{ar}(j) = 1$, allora per ogni $g, h \in \bigtimes_{x\in X} \|\mathcal{A}_x\|$:

$$(g,h) \in R_i^{\prod_x \mathcal{A}_x} \Leftrightarrow \forall x \in X \big((g(x), h(x)) \in R_i^{\mathcal{A}_x}\big),$$
$$f_j^{\prod_x \mathcal{A}_x}(g) = \langle f_j^{\mathcal{A}_x}(g(x)) \mid x \in X\rangle$$

e per le costanti:

$$c_k^{\prod_x \mathcal{A}_x} = \langle c_k^{\mathcal{A}_x} \mid x \in X \rangle.$$

Se F è un filtro su X, consideriamo la relazione d'equivalenza $\sim$ su $\bigtimes_{x\in X} \|\mathcal{A}_x\|$

$$g \sim h \Leftrightarrow \{\, x \in X \mid g(x) = h(x) \,\} \in F$$

e sia

$$A_F = \{\, [g] \mid g \in \bigtimes_{x\in X} \|\mathcal{A}_x\| \,\}.$$

Il **prodotto ridotto rispetto ad** F è la τ-struttura $\prod_x \mathcal{A}_x/F = \prod_F \mathcal{A}_x$ di universo A_F dove

- se $\mathrm{ar}(i) = n$ e $[g_1], \dots, [g_n] \in A_F$, allora

$$([g_1], \dots, [g_n]) \in R_i^{\prod_F \mathcal{A}_x} \Leftrightarrow \left\{ x \in X \mid (g_1(x), \dots, g_n(x)) \in R_i^{\mathcal{A}_x} \right\} \in F$$

- se $\mathrm{ar}(j) = n$ e $[g_1], \dots, [g_n] \in A_F$, allora

$$f_j^{\prod_F \mathcal{A}_x}([g_1], \dots, [g_n]) = [\langle f_j^{\mathcal{A}_x}(g_1(x), \dots, g_n(x)) \mid x \in X \rangle]$$

- $c_k^{\prod_F \mathcal{A}_x} = [\langle c_k^{\mathcal{A}_x} \mid x \in X \rangle]$.

Esercizio 19.5. Verificare che la definizione del prodotto ridotto di strutture è ben posta. Dimostrare che il prodotto di strutture è un caso particolare di prodotto ridotto.

Se $\mathcal{A}_x = \mathcal{A}$ per ogni $x \in X$, diremo che

$$\prod_F \mathcal{A}_x = \mathcal{A}^X/F$$

è una **potenza ridotta**. Se F è un ultrafiltro, diremo che $\prod_F \mathcal{A}_x$ è un **ultraprodotto**; se $\mathcal{A}_x = \mathcal{A}$ per ogni $x \in X$, parleremo di **ultrapotenza**.

Esercizio 19.6. Dimostrare che se U è l'ultrafiltro principale su X generato da $\{x_0\}$, allora $\prod_U \mathcal{A}_x \cong \mathcal{A}_{x_0}$.

19.D. Limiti diretti. La categoria $\mathfrak{Str}(\boldsymbol{L})$ delle $\boldsymbol{L}$-strutture ammette limiti diretti—la verifica è una generalizzazione del fatto che $\mathfrak{Grp}$, la categoria dei gruppi (§10.D.2) e $\mathfrak{POrd}$, la categoria degli ordini (§10.D.3) ammettono limiti diretti.

Fissiamo un insieme diretto superiormente $\langle X, \leq \rangle$ di indici[1] e un **sistema diretto superiormente di τ-strutture e morfismi** $\mathcal{A}_x$ $(x \in X)$ e $\pi_{x,y} \colon \mathcal{A}_x \to \mathcal{A}_y$ $(x \leq y)$. Il limite diretto $\lim_{x\in X} \mathcal{A}_x$ è la struttura $\mathcal{A}_\infty$ il cui universo è l'insieme A_∞ definito in (50). Vediamo ora come definire le

[1]Usiamo le lettere X e x per gli indici dato che le lettere I e i sono già impegnate per enumerare le relazioni delle strutture.

relazioni $R_i^{\mathcal{A}_\infty}$ $(i \in I)$, le funzioni $f_j^{\mathcal{A}_\infty}$ $(j \in J)$ e le costanti $c_k^{\mathcal{A}_\infty}$ $(k \in K)$. Se $\mathrm{ar}(i) = n$ definiamo $R_i^{\mathcal{A}_\infty} \subseteq A_\infty^n$

$$([(x_1, a_1)]_\sim, \dots, [(x_n, a_n)]_\sim) \in R_i^{\mathcal{A}_\infty} \quad \Leftrightarrow$$
$$\exists y \geq x_1, \dots, x_n \left((\pi_{x_1,y}(a_1), \dots, \pi_{x_n,y}(a_n)) \in R_i^{\mathcal{A}_y} \right).$$

Se $\mathrm{ar}(j) = n$ definiamo $f_j^{\mathcal{A}_\infty} \colon A_\infty^n \to A_\infty$.

$$f_j^{\mathcal{A}_\infty}\big([(x_1, a_1)], \dots, [(x_n, a_n)]\big) = [f_j^{\mathcal{A}_y}(\pi_{x_1,y}(a_1), \dots, \pi_{x_n,y}(a_n))]$$

per qualche $y \geq x_1, \dots, x_n$. La verifica che la definizione di $R_i^{\mathcal{A}_\infty}$ e di $f_j^{\mathcal{A}_\infty}$ non dipende dalla scelta dei rappresentanti è analoga alle verifiche nel caso degli ordini (§10.D.3) e nel caso dei gruppi (§10.D.2). Infine se $k \in K$ definiamo $c_k^{\mathcal{A}_\infty} \in A_\infty$

$$c_k^{\mathcal{A}_\infty} \in A_\infty = [(x, c_k^{\mathcal{A}_x})]$$

per un qualche $x \in X$. Se $y \in X$ è un altro elemento di X, sia $z \geq x, y$: dato che

$$\pi_{x,z}\big(c_k^{\mathcal{A}_x}\big) = c_k^{\mathcal{A}_z} = \pi_{y,z}\big(c_k^{\mathcal{A}_y}\big)$$

si deduce che $(x, c_k^{\mathcal{A}_x}) \sim (y, c_k^{\mathcal{A}_y})$ e quindi $c_k^{\mathcal{A}_\infty}$ è ben definito.

Infine, i morfismi $\pi_{x,\infty} \colon \mathcal{A}_x \to \mathcal{A}_\infty$ sono dati dalle funzioni

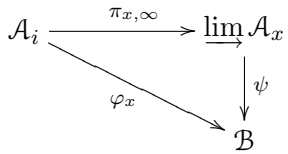
$$\pi_{x,\infty}(a) = [(x, a)].$$

Esercizi

Esercizio 19.7. (i) Verificare che le $\pi_{x,\infty}$ sono davvero dei morfismi, che

$$x \leq y \Rightarrow \pi_{y,\infty} \circ \pi_{x,y} = \pi_{x,\infty}$$

e che vale la seguente proprietà di universalità: per ogni $\mathcal{B} \in \mathfrak{Stt}(\tau)$ e per ogni famiglia di morfismi $\varphi_x \colon \mathcal{A}_x \to \mathcal{B}$ tali che $x \leq y \Rightarrow \varphi_y \circ \pi_{x,y} = \varphi_x$ esiste un unico morfismo $\psi \colon \varinjlim \mathcal{A}_x \rightarrowtail \mathcal{B}$ che rende il diagramma



commutativo.

(ii) Verificare che se i φ_x sono immersioni anche ψ è un'immersione.

(iii) Verificare che l'unione di strutture è un caso particolare di limite diretto.

Esercizio 19.8. Una struttura si dice **finitamente generata** se è generata da un insieme finito. Per ogni τ-struttura $\mathcal{A}$ sia

$$\mathfrak{FG}(\mathcal{A}) = \{\, \mathcal{B} \mid \mathcal{B} \subseteq \mathcal{A} \text{ e } \mathcal{B} \text{ è finitamente generata} \,\}\,.$$

Per $\mathcal{B} \subseteq \mathcal{C}$ sotto-strutture finitamente generate di $\mathcal{A}$ sia $\pi_{\mathcal{B},\mathcal{C}}\colon \mathcal{B} \hookrightarrow \mathcal{C}$ la mappa di inclusione. Dimostrare che $\langle \mathfrak{FG}(\mathcal{A}), \subseteq \rangle$ è diretto superiormente e che $\mathfrak{FG}(\mathcal{A})$ con le funzioni $\pi_{\mathcal{B},\mathcal{C}}$ forma un sistema diretto superiormente di τ-strutture e morfismi e che

$$\mathcal{A} \;\cong\; \varinjlim \langle \mathcal{B} \mid \mathcal{B} \in \mathfrak{FG}(\mathcal{A}) \rangle\,.$$

20. Linguaggi

Le strutture si distinguono in base alle proprietà che soddisfano. La controparte matematica del concetto intuitivo di proprietà è quello di formula di un linguaggio formale. Per ogni segnatura τ costruiremo un linguaggio $\boldsymbol{L}$ e a partire da esso costruiremo le sue formule $\boldsymbol{\varphi}$. (Tanto gli $\boldsymbol{L}$ quanto le $\boldsymbol{\varphi}$ saranno insiemi.) Vedremo poi come definire la nozione "la formula $\boldsymbol{\varphi}$ è vera nella struttura $\mathcal{A}$". Le formule di $\boldsymbol{L}$ sono la codifica insiemistica delle usuali espressioni matematiche riguardanti le τ-strutture e quindi avremo bisogno di una controparte insiemistica dei vari simboli logici: $\exists, \forall, \neg, \vee, \ldots$. Al fine di evitare confusioni, in questa sezione (ma solo in questa) distingueremo tipograficamente tra i simboli del linguaggio oggetto (che sono insiemi) e quelli del linguaggio informale in cui vengono esposti i risultati.

20.A. Simboli. Un **linguaggio del prim'ordine $\boldsymbol{L}$** è costituito da

- una lista infinita di oggetti che chiamiamo **variabili**

$$\boldsymbol{v}_0, \boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n, \ldots$$

- cinque oggetti distinti che chiamiamo **connettivi $\boldsymbol{\neg}$**, **$\boldsymbol{\vee}$**, **$\boldsymbol{\wedge}$**, **$\boldsymbol{\Rightarrow}$** e **$\boldsymbol{\Leftrightarrow}$**,
- due oggetti distinti **$\boldsymbol{\exists}$** e **$\boldsymbol{\forall}$** che chiamiamo, rispettivamente **quantificatore esistenziale** e **quantificatore universale**,
- un oggetto che chiamiamo **simbolo di uguaglianza** $\equiv$,
- tre famiglie disgiunte di oggetti che chiamiamo, rispettivamente, **simboli di relazione** $\{\, \boldsymbol{R}_i \mid i \in I \,\}$, **simboli di funzione** o **di operazione** $\{\, \boldsymbol{f}_j \mid j \in J \,\}$, **simboli di costante** $\{\, \boldsymbol{c}_k \mid k \in K \,\}$,
- una funzione $\mathrm{ar}\colon \{\, \boldsymbol{R}_i \mid i \in I \,\} \cup \{\, \boldsymbol{f}_j \mid j \in J \,\} \to \omega \setminus \{0\}$, detta **arietà**.

Spesso i simboli di relazione sono detti **predicati**. La natura di questi oggetti è irrilevante: per esempio possiamo stipulare che

$$\boldsymbol{v}_n = (0, n)\,,$$

che i simboli

$$\neg \quad \vee \quad \wedge \quad \Rightarrow \quad \Leftrightarrow \quad \exists \quad \forall \quad \equiv$$

siano, rispettivamente, le coppie $(1,0),(1,1),\dots,(1,7)$ e che

$$\boldsymbol{R}_i \quad \boldsymbol{f}_j \quad \boldsymbol{c}_k$$

siano, rispettivamente, $(2,i)$, $(3,j)$ e $(4,k)$. Diremo che $\boldsymbol{R}_i$ è un simbolo di relazione m-ario se $m = \mathrm{ar}(\boldsymbol{R}_i)$ e, analogamente, $\boldsymbol{f}_j$ è un simbolo di funzione n-ario se $n = \mathrm{ar}(\boldsymbol{f}_j)$. Quindi

Definizione 20.1. Un linguaggio $\boldsymbol{L}$ è una coppia $(\mathcal{S}, \mathrm{ar})$ dove $\mathcal{S}$ è un insieme di coppie ordinate e

$$\begin{aligned}(a,b) \in \mathcal{S} \Leftrightarrow (a = 0 \wedge b \in \omega) \vee (a = 1 \wedge b \in \{0,1,\dots,7\}) \\ \vee (a = 2 \wedge b \in I) \vee (a = 3 \wedge b \in J) \vee (a = 4 \wedge b \in K)\end{aligned}$$

e $\mathrm{ar}\colon (\{2\} \times I) \cup (\{3\} \times J) \to \omega \setminus \{0\}$. Gli insiemi $\mathrm{Vbl}, \mathrm{Rel}, \mathrm{Func}, \mathrm{Const} \subseteq \mathcal{S}$ sono definiti da:

$$\begin{aligned}\mathrm{Vbl} &= \{0\} \times \omega \\ \mathrm{Rel} &= \{\, s \in \mathcal{S} \mid \exists i \in I\, (s = (2,i)) \,\} \\ \mathrm{Func} &= \{\, s \in \mathcal{S} \mid \exists j \in J\, (s = (3,j)) \,\} \\ \mathrm{Const} &= \{\, s \in \mathcal{S} \mid \exists k \in K\, (s = (4,k)) \,\}\end{aligned}$$

e quindi

$$\mathcal{S} = \mathrm{Vbl} \cup \mathrm{Rel} \cup \mathrm{Func} \cup \mathrm{Const} \cup \{\neg, \vee, \wedge, \Rightarrow, \Leftrightarrow, \exists, \forall, \equiv\}.$$

Ogni tipo di similarità τ genera un linguaggio $\boldsymbol{L}_\tau$ e, viceversa, ogni linguaggio $\boldsymbol{L}$ genera un tipo di similarità $\tau_{\boldsymbol{L}}$. Una $\boldsymbol{L}$-struttura è, per definizione, una $\tau_{\boldsymbol{L}}$-struttura e $\mathfrak{Str}(\boldsymbol{L}) = \mathfrak{Str}(\tau_{\boldsymbol{L}})$. La **cardinalità** di $\boldsymbol{L}$ è

$$\begin{aligned}\mathrm{card}(\boldsymbol{L}) &= \max(\aleph_0, |I|, |J|, |K|) \\ &= \max(\aleph_0, \mathrm{card}(\tau_{\boldsymbol{L}})) \\ &= |\mathcal{S}|\ .\end{aligned}$$

Diremo che $\boldsymbol{L}$ è un **sotto-linguaggio** di $\boldsymbol{L}'$ ovvero che $\boldsymbol{L}'$ è un'**estensione** di $\boldsymbol{L}$ se e solo se $\tau_{\boldsymbol{L}} \subseteq \tau_{\boldsymbol{L}'}$ e, con abuso di notazione, scriveremo

$$\boldsymbol{L} \subseteq \boldsymbol{L}'\,.$$

Definizione 20.2. Se $\tau_{\boldsymbol{L}} = \langle I, J, K, \mathrm{ar}\rangle$, $\mathcal{A} \in \mathfrak{Str}(\boldsymbol{L})$ e $B \subseteq \|\mathcal{A}\|$, l'espansione $\mathcal{A}'$ di $\mathcal{A}$ in cui ogni elemento $b \in B$ è una costante si dice **espansione canonica di $\mathcal{A}$ mediante gli elementi di** B. Formalmente si pone $\tau' = \langle I, J, K \cup \{\, b' \mid b \in B \,\}, \mathrm{ar}\rangle$ con i b' distinti e tali che $b' \notin I \cup J \cup K$ e

(per esempio $b' = (b, I \cup J \cup K)$). Per semplicità notazionale useremo $\mathring{b}$ a posto di $\boldsymbol{c}_{b'}$ e useremo $\boldsymbol{L} \cup \left\{ \mathring{b} \mid b \in B \right\}$ per indicare il linguaggio $\boldsymbol{L}_{\tau'}$ e

$$\langle \mathcal{A}, b \rangle_{b \in B}$$

per l'espansione canonica di $\mathcal{A}$ mediante gli elementi di B.

Analogamente, se R_x è una relazione su $\|\mathcal{A}\|$ e f_y è una funzione finitaria su $\|\mathcal{A}\|$, dove x e y variano negli insiemi X e Y, possiamo definire l'espansione canonica di $\mathcal{A}$ mediante le relazioni R_x e le funzioni f_y

$$\langle \mathcal{A}, R_x, f_y \rangle_{x \in X, y \in Y} .$$

Il linguaggio per questa struttura è $\boldsymbol{L} \cup \left\{ \mathring{R}_x \mid x \in X \right\} \cup \left\{ \mathring{f}_y \mid y \in Y \right\}$.

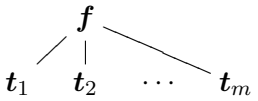
20.B. Termini. I **termini** di $\boldsymbol{L}$ sono le variabili, le costanti e le espressioni $\boldsymbol{f}_j(\boldsymbol{t}_1, \ldots, \boldsymbol{t}_m)$, dove $\boldsymbol{t}_1, \ldots, \boldsymbol{t}_m$ sono termini. Formalmente l'insieme

$$\mathrm{Term} = \mathrm{Term}(\boldsymbol{L})$$

dei termini è $\mathrm{Words}(\mathrm{Vbl} \cup \mathrm{Func} \cup \mathrm{Const}, a)$, l'insieme delle parole sull'insieme di simboli $\mathrm{Vbl} \cup \mathrm{Func} \cup \mathrm{Const}$, dove $a(s) = 0$ se $s \in \mathrm{Vbl} \cup \mathrm{Const}$ e $a(s) = \mathrm{ar}(s)$, se $s \in \mathrm{Func}$. $\mathrm{Term}_n = \mathrm{Words}_n$ è l'insieme dei termini di altezza $\leq n$, quindi Term_0 è identificabile con $\mathrm{Vbl} \cup \mathrm{Const}$ e

$$\mathrm{Term}_{n+1} = \left\{ \langle \boldsymbol{f}_j \rangle^\frown \boldsymbol{t}_1 {}^\frown \ldots {}^\frown \boldsymbol{t}_m \mid j \in J, m = \mathrm{ar}(\boldsymbol{f}_j), \boldsymbol{t}_1, \ldots, \boldsymbol{t}_m \in \mathrm{Term}_n \right\} \cup \mathrm{Term}_n \ .$$

Scriveremo $\boldsymbol{f}_j(\boldsymbol{t}_1, \ldots, \boldsymbol{t}_m)$ al posto di $\langle \boldsymbol{f}_j \rangle^\frown \boldsymbol{t}_1 {}^\frown \ldots {}^\frown \boldsymbol{t}_m$ e spesso utilizzeremo la notazione ad albero



Il Corollario 7.7 garantisce che un termine che non sia una variabile o una costante è della forma $\boldsymbol{f}_j(\boldsymbol{t}_1, \ldots, \boldsymbol{t}_m)$ per un'unica m-upla $\boldsymbol{t}_1, \ldots, \boldsymbol{t}_m$. L'insieme $\boldsymbol{V}(\boldsymbol{t})$ delle **variabili di un termine** $\boldsymbol{t}$ è definito per ricorsione su $\mathrm{ht}(\boldsymbol{t})$:

- $\boldsymbol{V}(\boldsymbol{c}_k) = \emptyset$ e $\boldsymbol{V}(\boldsymbol{v}_n) = \{\boldsymbol{v}_n\}$,
- $\boldsymbol{V}(\boldsymbol{f}_j(\boldsymbol{t}_1, \ldots, \boldsymbol{t}_n)) = \boldsymbol{V}(\boldsymbol{t}_1) \cup \cdots \cup \boldsymbol{V}(\boldsymbol{t}_n)$.

L'insieme dei **termini chiusi**

$$\mathrm{ClTerm} = \{ \boldsymbol{t} \in \mathrm{Term} \mid \boldsymbol{V}(\boldsymbol{t}) = \emptyset \}$$

è la collezione dei termini costruiti a partire dalle costanti.

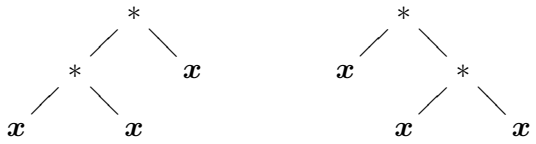
20.C. Esempi di linguaggi e termini.

20.C.1. *Il linguaggio minimale.* Consideriamo il linguaggio più semplice in assoluto, $\boldsymbol{L}_\emptyset$, quello che non contiene alcun simbolo di relazione, di funzione o di costante. I termini sono le variabili e nessun termine è chiuso. Più in generale, in ogni linguaggio $\boldsymbol{L}$ privo di simboli di funzione e di simboli di costanti $\mathrm{Term}(\boldsymbol{L}) = \mathrm{Vbl}$ e $\mathrm{ClTerm}(\boldsymbol{L}) = \emptyset$.

20.C.2. *Il linguaggio dei semigruppi.* Il linguaggio dei semigruppi $\boldsymbol{L}_{\mathrm{sgrp}}$ contiene solo un simbolo di funzione 2-aria $*$. Ogni semigruppo può essere visto come $\boldsymbol{L}$-struttura, ma, ovviamente, non vale il viceversa. Per ogni variabile $\boldsymbol{x}$ possiamo costruire il termine

$$\boldsymbol{x}^n \stackrel{\mathrm{def}}{=} (\cdots(\boldsymbol{x} * \boldsymbol{x}) * \boldsymbol{x} \cdots \boldsymbol{x}) * \boldsymbol{x} \qquad (n \geq 1)\,.$$

Poichè $(\boldsymbol{x}*\boldsymbol{x})*\boldsymbol{x}$ e $\boldsymbol{x}*(\boldsymbol{x}*\boldsymbol{x})$ sono termini distinti, rappresentati dagli alberi



c'è una certa arbitrarietà nella definizione di $\boldsymbol{x}^n$; per esempio potevamo definirlo così che $\boldsymbol{x}^{n+1} = \boldsymbol{x} * \boldsymbol{x}^n$. Le possibili definizioni di $\boldsymbol{x}^3$ sono 2, per $\boldsymbol{x}^4$ sono 5 e per $\boldsymbol{x}^5$ sono 14. Il numero di termini distinti contenenti $n+1$ variabili è una quantità ben noto in Combinatorica: è $\binom{2n}{n} - \binom{2n}{n-1}$ il *numero di Catalan di ordine* n.

20.C.3. *Il linguaggio degli anelli unitari.* Il linguaggio degli anelli unitari $\boldsymbol{L}_{\mathrm{ring}}$ ha due operazioni binarie: $+$ e $\cdot$, una operazione 1 aria: $-$, e due costanti: $\mathbf{0}$ e $\mathbf{1}$. Ogni anello unitario è una $\boldsymbol{L}_{\mathrm{ring}}$-struttura, ma non viceversa. Possiamo quindi costruire dei termini chiusi $\boldsymbol{t}_n$ dove n varia in $\mathbb{Z}$: basta porre $\boldsymbol{t}_0 = \mathbf{0}$, $\boldsymbol{t}_1 = \mathbf{1}$, $\boldsymbol{t}_{n+1} = \boldsymbol{t}_n + \mathbf{1}$ e per $n < 0$ porre $\boldsymbol{t}_n = -\boldsymbol{t}_{-n}$.

20.C.4. *Il linguaggio delle algebre di Boole.* Il linguaggio $\boldsymbol{L}_{\mathrm{Boole}}$ delle algebre di Boole ha un simbolo di relazione binaria $\leq$, due simboli di funzione $\wedge$ e $\vee$ binarie, un simbolo di funzione unaria * e due costanti: 0 e 1. Ad ogni termine $\boldsymbol{t}$ possiamo associare il termine duale $\breve{\boldsymbol{t}}$ ottenuto scambiando $\vee$ con $\wedge$ e 0 con 1. Ad ogni espressione del tipo[2]

$$\begin{aligned} \boldsymbol{t}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n) &\leq \boldsymbol{s}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n) \\ \boldsymbol{t}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n) &= \boldsymbol{s}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n) \end{aligned} \tag{80}$$

possiamo associare le espressioni duali

$$\begin{aligned} \breve{\boldsymbol{s}}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n) &\leq \breve{\boldsymbol{t}}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n) \\ \breve{\boldsymbol{s}}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n) &= \breve{\boldsymbol{t}}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n) \end{aligned} \tag{81}$$

[2]Come vedremo in §20.D, espressioni siffatte si dicono formule atomiche.

Quindi il principio di dualità formulato nell'Osservazione 11.6 dice che un'espressione come in (80) vale in ogni algebra di Boole se e solo se l'espressione duale (81) vale in ogni algebra di Boole.

20.C.5. *Il linguaggio numerabile massimale.* Sia

$$\boldsymbol{L}_\infty = \langle \{\, \boldsymbol{R}_{n,m} \mid n, m \in \omega, n \neq 0 \,\}, \{\, \boldsymbol{f}_{n,m} \mid n, m \in \omega, n \neq 0 \,\}, \{\, \boldsymbol{c}_m \mid m \in \omega \,\} \rangle$$

dove, per ogni $m \in \omega$,

- $\boldsymbol{R}_{n,m}$ è un simbolo di relazione n-aria,
- $\boldsymbol{f}_{n,m}$ è un simbolo di funzione n-aria,
- $\boldsymbol{c}_m$ è un simbolo di costante.

Ogni linguaggio numerabile $\boldsymbol{L}$ è un sottolinguaggio di $\boldsymbol{L}_\infty$, quindi ogni struttura numerabile è una contrazione di una $\boldsymbol{L}_\infty$-struttura.

20.D. Formule. Una **formula atomica** di $\boldsymbol{L}$ è una stringa

$$\langle \boldsymbol{R}_i \rangle^\frown \boldsymbol{t}_1{}^\frown \ldots {}^\frown \boldsymbol{t}_m$$

dove $\boldsymbol{R}_i$ è m-ario e $\boldsymbol{t}_1, \ldots, \boldsymbol{t}_m$ sono termini, oppure è una stringa

$$\langle \equiv \rangle^\frown \boldsymbol{t}_1{}^\frown \boldsymbol{t}_2$$

con $\boldsymbol{t}_1$ e $\boldsymbol{t}_2$ termini. Scriveremo AtFml = AtFml($\boldsymbol{L}$) per indicare l'insieme delle formule atomiche.

L'insieme Fml = Fml($\boldsymbol{L}$) delle **formule** di $\boldsymbol{L}$ è il più piccolo insieme di stringhe contenente AtFml e chiuso sotto le seguenti operazioni:

- $\boldsymbol{\varphi} \mapsto \boldsymbol{\neg\varphi}$,
- $(\boldsymbol{\varphi}, \boldsymbol{\psi}) \mapsto \langle \square \rangle^\frown \boldsymbol{\varphi}^\frown \boldsymbol{\psi}$, dove $\square \in \{\boldsymbol{\vee}, \boldsymbol{\wedge}, \boldsymbol{\Rightarrow}, \boldsymbol{\Leftrightarrow}\}$,
- $\boldsymbol{\varphi} \mapsto \boldsymbol{\exists v}_n\, \boldsymbol{\varphi}$ e
- $\boldsymbol{\varphi} \mapsto \boldsymbol{\forall v}_n\, \boldsymbol{\varphi}$.

Notazione. (a) Le lettere greche $\boldsymbol{\varphi}, \boldsymbol{\psi}, \boldsymbol{\chi}, \ldots$ variamente decorate variano su Fml.

(b) Il simbolo $\square$ verrà usato per designare un generico simbolo di connettivo binario, vale a dire un elemento di $\{\boldsymbol{\vee}, \boldsymbol{\wedge}, \boldsymbol{\Rightarrow}, \boldsymbol{\Leftrightarrow}\}$.

(c) Scriveremo $\boldsymbol{x} \not\equiv \boldsymbol{t}$ invece di $\boldsymbol{\neg}\,(\boldsymbol{s} \equiv \boldsymbol{t})$.

Formalmente Fml è l'insieme delle parole su (S, a) dove

$$S = \{\boldsymbol{\neg}, \boldsymbol{\vee}, \boldsymbol{\wedge}, \boldsymbol{\Rightarrow}, \boldsymbol{\Leftrightarrow}\} \cup \{\, \boldsymbol{\exists v}_n, \boldsymbol{\forall v}_n \mid n \in \omega \,\} \cup \text{AtFml}$$

e

- $a(\boldsymbol{\varphi}) = 0$, per ogni n e ogni $\boldsymbol{\varphi} \in$ AtFml,
- $a(\boldsymbol{\neg}) = 1$ e $a(\square) = 2$,

- $a(\exists \boldsymbol{v}_n) = a(\forall \boldsymbol{v}_n) = 1$, per ogni $n \in \omega$.

Osserviamo che le espressioni "$\exists \boldsymbol{v}_n$" e "$\forall \boldsymbol{v}_n$" sono da considerarsi come simboli di base, da cui poi costruire le parole e quindi, a rigor di logica, dovremmo scrivere $\langle \exists, \boldsymbol{v}_n \rangle \in S$ e $\langle \forall, \boldsymbol{v}_n \rangle \in S$. Al fine di alleggerire la notazione utilizzeremo le seguenti convenzioni:

- Scriveremo
$$\boldsymbol{R}_i(\boldsymbol{t}_1, \dots, \boldsymbol{t}_n) \qquad \text{e} \qquad \boldsymbol{t}_1 \equiv \boldsymbol{t}_2$$
invece di $\langle \boldsymbol{R}_i, \boldsymbol{t}_1, \dots, \boldsymbol{t}_n \rangle$ e $\langle \equiv, \boldsymbol{t}_1, \boldsymbol{t}_2 \rangle$ per le formule atomiche e
$$\neg \boldsymbol{\varphi}, \quad \boldsymbol{\varphi} \vee \boldsymbol{\psi}, \quad \boldsymbol{\varphi} \wedge \boldsymbol{\psi}, \quad \boldsymbol{\varphi} \Rightarrow \boldsymbol{\psi}, \quad \boldsymbol{\varphi} \Leftrightarrow \boldsymbol{\psi}, \quad \exists \boldsymbol{v_n}\, \boldsymbol{\varphi}, \quad \forall \boldsymbol{v_n}\, \boldsymbol{\varphi}$$
invece di $\langle \neg \rangle^\frown \boldsymbol{\varphi}$, $\langle \vee \rangle^\frown \boldsymbol{\varphi}^\frown \boldsymbol{\psi}$, $\langle \wedge \rangle^\frown \boldsymbol{\varphi}^\frown \boldsymbol{\psi}$, $\langle \Rightarrow \rangle^\frown \boldsymbol{\varphi}^\frown \boldsymbol{\psi}$, $\langle \Leftrightarrow \rangle^\frown \boldsymbol{\varphi}^\frown \boldsymbol{\psi}$.
- Per evitare un eccessivo uso di parentesi, useremo la convenzione per cui $\neg$ lega più fortemente di $\vee$, $\wedge$, $\Rightarrow$ o $\Leftrightarrow$,
- Le lettere $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}, \boldsymbol{w}$ variamente decorate variano su Vbl.

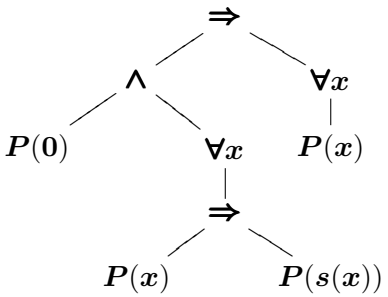
Per esempio, nel linguaggio $\boldsymbol{L}$ contenente una simbolo costante $\mathbf{0}$, un simbolo di relazione 1-aria $\boldsymbol{s}$, e un simbolo di predicato 1-ario $\boldsymbol{P}$, la formula

$$\boldsymbol{P}(\mathbf{0}) \wedge \forall \boldsymbol{x}\, (\boldsymbol{P}(\boldsymbol{x}) \Rightarrow \boldsymbol{P}(\boldsymbol{s}(\boldsymbol{x}))) \Rightarrow \forall \boldsymbol{x} \boldsymbol{P}(\boldsymbol{x}) \tag{82}$$

è la scrittura informale della parola (cioè della stringa)

$$\boxed{\Rightarrow}\boxed{\wedge}\boxed{\boldsymbol{P}\mathbf{0}}\boxed{\forall \boldsymbol{x}}\boxed{\boldsymbol{P}\boldsymbol{x}}\boxed{\Rightarrow}\boxed{\boldsymbol{P}\boldsymbol{s}\boldsymbol{x}}\boxed{\forall \boldsymbol{x}}\boxed{\boldsymbol{P}\boldsymbol{x}}$$

dove abbiamo evidenziato ciascun simbolo di S e il simbolo $\boldsymbol{x}$ sta per un qualche elemento di Vbl, per esempio $\boldsymbol{v}_3$, oppure $\boldsymbol{v}_{258}$. Naturalmente, una formula può essere vista come un albero etichettato in cui i nodi terminali sono formule atomiche e gli altri nodi sono connettivi, oppure quantificatori seguiti da una variabile. La formula qui sopra può essere scritta come:



L'altezza $\mathrm{ht}(\boldsymbol{\varphi})$ di una formula è l'altezza di $\boldsymbol{\varphi}$ come parola. Quindi è definita da

- $\mathrm{ht}(\boldsymbol{\varphi}) = 0$ se $\boldsymbol{\varphi} \in \mathrm{AtFml}$,
- $\mathrm{ht}(\neg \boldsymbol{\psi}) = \mathrm{ht}(\boldsymbol{\psi}) + 1$,
- $\mathrm{ht}(\boldsymbol{\psi} \,\square\, \boldsymbol{\chi}) = \max\big(\mathrm{ht}(\boldsymbol{\psi}), \mathrm{ht}(\boldsymbol{\chi})\big) + 1$,

- $\mathrm{ht}(\exists \boldsymbol{v}_n\, \psi) = \mathrm{ht}(\forall \boldsymbol{v}_n\, \psi) = \mathrm{ht}(\psi) + 1$.

Per esempio, l'altezza della formula (82) è 4.

L'insieme $\mathrm{Sub}(\varphi)$ delle **sotto-formule** di φ è definito da

$$\mathrm{Sub}(\varphi) = \begin{cases} \emptyset & \text{se } \varphi \in \mathrm{AtFml}, \\ \{\psi\} \cup \mathrm{Sub}(\psi) & \text{se } \varphi \in \{\neg\psi, \exists \boldsymbol{x}\, \psi, \forall \boldsymbol{x}\, \psi\}, \\ \{\psi, \chi\} \cup \mathrm{Sub}(\psi) \cup \mathrm{Sub}(\chi) & \text{se } \varphi = \psi \sqcap \chi\,. \end{cases}$$

Per esempio, le sotto-formule di (82) sono:

$$\begin{array}{rr} \boldsymbol{P}(\boldsymbol{0}) & \boldsymbol{P}(\boldsymbol{x}) \\ \boldsymbol{P}(\boldsymbol{s}(\boldsymbol{x})) & \boldsymbol{P}(\boldsymbol{x}) \Rightarrow \boldsymbol{P}(\boldsymbol{s}(\boldsymbol{x})) \\ \forall \boldsymbol{x} \boldsymbol{P}(\boldsymbol{x}) & \forall \boldsymbol{x}\, (\boldsymbol{P}(\boldsymbol{x}) \Rightarrow \boldsymbol{P}(\boldsymbol{s}(\boldsymbol{x})))\,. \end{array}$$

Esercizio 20.3. Verificare che se $\boldsymbol{L} \subseteq \boldsymbol{L}'$ allora $\mathrm{Term}(\boldsymbol{L}) \subseteq \mathrm{Term}(\boldsymbol{L}')$ e $\mathrm{Fml}(\boldsymbol{L}) \subseteq \mathrm{Fml}(\boldsymbol{L}')$.

20.E. Occorrenze libere e vincolate. Come abbiamo visto nella sezione 20.D, una formula di un linguaggio $\boldsymbol{L}$ è una parola su un certo (Σ, a), cioè una stringa finita i cui elementi sono formule atomiche, connettivi, o quantificatori con variabili. Dato che anche le formule atomiche sono a loro volta delle stringhe, è possibile vedere una formula come una stringa di elementi di $\mathcal{S}$, dove $\mathcal{S}$ è come nella Definizione 20.1. In particolare la formula (82) può essere vista come una stringa di lunghezza 16

$$\boxed{\Rightarrow}\boxed{\wedge}\boxed{\boldsymbol{P}}\boxed{\boldsymbol{0}}\boxed{\forall}\boxed{\boldsymbol{x}}\boxed{\boldsymbol{P}}\boxed{\boldsymbol{x}}\boxed{\Rightarrow}\boxed{\boldsymbol{P}}\boxed{\boldsymbol{s}}\boxed{\boldsymbol{x}}\boxed{\forall}\boxed{\boldsymbol{x}}\boxed{\boldsymbol{P}}\boxed{\boldsymbol{x}}$$

dove abbiamo evidenziato ciascun simbolo. (La lunghezza della stessa formula, vista come parola su Σ è 9.) Un'**occorrenza** di una variabile $\boldsymbol{x}$ in una formula φ è un $n \in \mathrm{lh}(\varphi)$ per cui $\boldsymbol{x}$ è l'oggetto al posto n-esimo nella sequenza φ, cioè $\varphi(n) = \boldsymbol{x}$. Per esempio, se φ è la formula

$$\exists \boldsymbol{y}\, (\boldsymbol{R}(\boldsymbol{y}, \boldsymbol{x}) \wedge \boldsymbol{f}(\boldsymbol{z}) \equiv \boldsymbol{x})$$

vale a dire φ è la stringa

$$\langle \exists, \boldsymbol{y}, \wedge, \boldsymbol{R}, \boldsymbol{y}, \boldsymbol{x}, \equiv, \boldsymbol{f}, \boldsymbol{z}, \boldsymbol{x} \rangle$$

allora le occorrenze di $\boldsymbol{x}$ sono 5 e 9, quelle di $\boldsymbol{y}$ sono 1 e 4, quella di $\boldsymbol{z}$ è 8. $\boldsymbol{O}(\boldsymbol{x}; \varphi)$ è l'insieme delle **occorrenze di $\boldsymbol{x}$ in φ**. Chiaramente $\boldsymbol{O}(\boldsymbol{x}; \varphi) = \emptyset$ se e solo se $\boldsymbol{x}$ non compare in φ. Una variabile $\boldsymbol{x}$ **occorre** in φ se e solo se $\boldsymbol{O}(\boldsymbol{x}; \varphi) \neq \emptyset$.

Un'occorrenza di una variabile $\boldsymbol{x}$ in una formula può essere **libera** oppure **vincolata** ma non entrambe: le occorrenze di $\boldsymbol{x}$ in una parte della formula del tipo $\exists \boldsymbol{x}\, \varphi$ o $\forall \boldsymbol{x}\, \varphi$ sono tutte vincolate. Formalmente, l'insieme

$$\boldsymbol{FO}(\boldsymbol{x}; \varphi) \subseteq \boldsymbol{O}(\boldsymbol{x}; \varphi)$$

delle occorrenze libere di $\boldsymbol{x}$ in $\boldsymbol{\varphi}$ è definito induttivamente come segue:

- se $\boldsymbol{\varphi} \in \mathrm{AtFml}$, allora $\boldsymbol{FO}(\boldsymbol{x}; \boldsymbol{\varphi}) = \boldsymbol{O}(\boldsymbol{x}; \boldsymbol{\varphi})$
- se $\boldsymbol{\varphi} = \boldsymbol{\psi} \mathbin{\square} \boldsymbol{\chi}$, allora

$$\boldsymbol{FO}(\boldsymbol{x}; \boldsymbol{\varphi}) = \{\, 1 + n \mid n \in \boldsymbol{FO}(\boldsymbol{x}; \boldsymbol{\psi}) \,\} \cup \{\, 1 + \mathrm{lh}(\boldsymbol{\psi}) + n \mid n \in \boldsymbol{FO}(\boldsymbol{x}; \boldsymbol{\chi}) \,\}$$

- se $\boldsymbol{\varphi} = \boldsymbol{\neg\psi}$, allora

$$\boldsymbol{FO}(\boldsymbol{x}; \boldsymbol{\varphi}) = \{\, 1 + n \mid n \in \boldsymbol{FO}(\boldsymbol{x}; \boldsymbol{\psi}) \,\}$$

- se $\boldsymbol{\varphi} = \boldsymbol{\exists y\, \psi}$ o $\boldsymbol{\varphi} = \boldsymbol{\forall y\, \psi}$, e $\boldsymbol{y} \neq \boldsymbol{x}$, allora

$$\boldsymbol{FO}(\boldsymbol{x}; \boldsymbol{\varphi}) = \{\, 2 + n \mid n \in \boldsymbol{FO}(\boldsymbol{x}; \boldsymbol{\psi}) \,\}$$

- se $\boldsymbol{\varphi} = \boldsymbol{\exists x\, \psi}$ oppure $\boldsymbol{\varphi} = \boldsymbol{\forall x\, \psi}$, allora $\boldsymbol{FO}(\boldsymbol{x}; \boldsymbol{\varphi}) = \emptyset$.

Una variabile $\boldsymbol{x}$ occorre libera in $\boldsymbol{\varphi}$ se $\boldsymbol{FO}(\boldsymbol{x}; \boldsymbol{\varphi}) \neq \emptyset$. L'insieme

$$\boldsymbol{O}(\boldsymbol{x}; \boldsymbol{\varphi}) \setminus \boldsymbol{FO}(\boldsymbol{x}; \boldsymbol{\varphi})$$

è l'insieme delle occorrenze vincolate di $\boldsymbol{x}$ in $\boldsymbol{\varphi}$.

Esercizio 20.4. Dare un esempio di una formula $\boldsymbol{\varphi}$ in cui una variabile $\boldsymbol{x}$ occorre libera e vincolata.

L'insieme delle variabili che occorrono libere in $\boldsymbol{\varphi}$ è indicato con

$$\boldsymbol{Fv}(\boldsymbol{\varphi}) \stackrel{\mathrm{def}}{=} \{\, \boldsymbol{x} \in \mathrm{Vbl} \mid \boldsymbol{FO}(\boldsymbol{x}; \boldsymbol{\varphi}) \neq \emptyset \,\}.$$

La notazione

$$\boldsymbol{\varphi}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)$$

significa che le variabili che occorrono libere in $\boldsymbol{\varphi}$ sono tra $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$, vale a dire $\boldsymbol{Fv}(\boldsymbol{\varphi}) \subseteq \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\}$. Un **enunciato** è una formula priva di variabili libere; l'insieme degli $\boldsymbol{L}$-enunciati si indica con

$$\mathrm{Sent}(\boldsymbol{L})$$

e di solito le lettere $\boldsymbol{\sigma}, \boldsymbol{\tau}, \ldots$ variamente decorate denotano un enunciato.

20.F. Sostituzione di termini. Se $\boldsymbol{t}, \boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ sono termini e $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ sono variabili distinte

$$\boldsymbol{t}[\boldsymbol{u}_1/\boldsymbol{x}_1, \ldots, \boldsymbol{u}_n/\boldsymbol{x}_n]$$

è il termine ottenuto da $\boldsymbol{t}$ sostituendo $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ al posto di $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$. La definizione formale di $\boldsymbol{t}[\boldsymbol{u}_1/\boldsymbol{x}_1, \ldots, \boldsymbol{u}_n/\boldsymbol{x}_n]$ è per induzione sull'altezza di $\boldsymbol{t}$:

$$\boldsymbol{t}[\boldsymbol{u}_1/\boldsymbol{x}_1, \ldots, \boldsymbol{u}_n/\boldsymbol{x}_n] = \begin{cases} \boldsymbol{t} & \text{se } \boldsymbol{V}(\boldsymbol{t}) \cap \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\} = \emptyset, \\ \boldsymbol{u}_m & \text{se } \boldsymbol{t} = \boldsymbol{x}_m, \text{ per qualche } 1 \leq m \leq n, \\ \boldsymbol{f}_j(\boldsymbol{t}_1[\boldsymbol{u}_1/\boldsymbol{x}_1, \ldots, \boldsymbol{u}_n/\boldsymbol{x}_n], \ldots, \boldsymbol{t}_m[\boldsymbol{u}_1/\boldsymbol{x}_1, \ldots, \boldsymbol{u}_n/\boldsymbol{x}_n]) & \\ \qquad \text{se } \boldsymbol{t} = \boldsymbol{f}_j(\boldsymbol{t}_1, \ldots, \boldsymbol{t}_m). \end{cases}$$

Osservazioni 20.5. (a) Mentre le variabili $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ devono essere necessariamente distinte, non si richiede questo per i termini $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$.

(b) I termini $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ devono essere sostituiti a $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ *simultaneamente*, vale a dire *non* è possibile prima sostituire $\boldsymbol{x}_1$ con $\boldsymbol{u}_1$, nel termine così risultante sostituire $\boldsymbol{x}_2$ con $\boldsymbol{u}_2$, etc. In altre parole, in generale il termine $\boldsymbol{t}[\boldsymbol{u}_1/\boldsymbol{x}_1, \ldots, \boldsymbol{u}_n/\boldsymbol{x}_n]$ è differente da $\boldsymbol{t}_n$, dove $\boldsymbol{t}_0 = \boldsymbol{t}$ e $\boldsymbol{t}_{k+1} = \boldsymbol{t}_k[\boldsymbol{u}_{k+1}/\boldsymbol{x}_{k+1}]$ (Esercizio 20.6).

Se $\boldsymbol{\varphi}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)$ è una formula e $\boldsymbol{t}_1, \ldots, \boldsymbol{t}_n$ sono termini, allora

$$\boldsymbol{\varphi}[\boldsymbol{t}_1/\boldsymbol{x}_1, \ldots, \boldsymbol{t}_n/\boldsymbol{x}_n] \tag{83}$$

è la formula ottenuta da $\boldsymbol{\varphi}$ sostituendo le occorrenze libere di $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ con $\boldsymbol{t}_1, \ldots, \boldsymbol{t}_n$:

$$\boldsymbol{\varphi}[\boldsymbol{t}_1/\boldsymbol{x}_1, \ldots, \boldsymbol{t}_n/\boldsymbol{x}_n] = \begin{cases} \boldsymbol{t}_h \equiv \boldsymbol{t}_k & \text{se } \boldsymbol{\varphi} \text{ è } \boldsymbol{x}_h \equiv \boldsymbol{x}_k, \\ \boldsymbol{R}_i(\boldsymbol{t}_{k_1}, \ldots, \boldsymbol{t}_{k_n}) & \text{se } \boldsymbol{\varphi} \text{ è } \boldsymbol{R}_i(\boldsymbol{x}_{k_1}, \ldots, \boldsymbol{x}_{k_n}), \\ \neg(\psi[\boldsymbol{t}_1/\boldsymbol{x}_1, \ldots, \boldsymbol{t}_n/\boldsymbol{x}_n]) & \text{se } \boldsymbol{\varphi} \text{ è } \neg\psi, \\ \psi[\boldsymbol{t}_1/\boldsymbol{x}_1, \ldots, \boldsymbol{t}_n/\boldsymbol{x}_n] \,\square\, \chi[\boldsymbol{t}_1/\boldsymbol{x}_1, \ldots, \boldsymbol{t}_n/\boldsymbol{x}_n] & \\ \qquad\qquad \text{se } \boldsymbol{\varphi} \text{ è } \psi \,\square\, \chi, & \\ \boldsymbol{Q}\boldsymbol{y}\,\psi[\boldsymbol{t}_1/\boldsymbol{x}_1, \ldots, \boldsymbol{t}_n/\boldsymbol{x}_n] & \text{se } \boldsymbol{\varphi} \text{ è } \boldsymbol{Q}\boldsymbol{y}\,\psi \text{ e} \\ & \qquad \boldsymbol{y} \notin \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\} \\ \boldsymbol{Q}\boldsymbol{y}\,\psi[\boldsymbol{t}_1/\boldsymbol{x}_1, \ldots, \boldsymbol{t}_{k-1}/\boldsymbol{x}_{k-1}, \boldsymbol{t}_{k+1}/\boldsymbol{x}_{k+1}, \ldots, \boldsymbol{t}_n/\boldsymbol{x}_n] & \\ \qquad\qquad \text{se } \boldsymbol{\varphi} \text{ è } \boldsymbol{Q}\boldsymbol{y}\,\psi \text{ e } \boldsymbol{y} = \boldsymbol{x}_k, & \end{cases}$$

dove $\boldsymbol{Q}$ è $\exists$ oppure $\forall$.

Esercizi

Esercizio 20.6. Dimostrare che se $\boldsymbol{x}_2 \notin \boldsymbol{V}(\boldsymbol{u}_1)$ e $\boldsymbol{x}_1 \notin \boldsymbol{V}(\boldsymbol{u}_2)$, allora

$$(\boldsymbol{t}[\boldsymbol{u}_1/\boldsymbol{x}_1])\,[\boldsymbol{u}_2/\boldsymbol{x}_2] = (\boldsymbol{t}[\boldsymbol{u}_2/\boldsymbol{x}_2])\,[\boldsymbol{u}_1/\boldsymbol{x}_1] = \boldsymbol{t}[\boldsymbol{u}_1/\boldsymbol{x}_1, \boldsymbol{u}_2/\boldsymbol{x}_2]\,.$$

dimostrare con un controesempio che l'ipotesi $\boldsymbol{x}_2 \notin \boldsymbol{V}(\boldsymbol{u}_1) \wedge \boldsymbol{x}_1 \notin \boldsymbol{V}(\boldsymbol{u}_2)$ è necessaria.

21. La relazione di soddisfazione

21.A. Interpretazione di termini in strutture. Se $\boldsymbol{t}$ è un termine chiuso di $\boldsymbol{L}$ e $\mathcal{A}$ è una $\boldsymbol{L}$-struttura, possiamo far corrispondere a $\boldsymbol{t}$ un unico elemento

$\boldsymbol{t}^{\mathcal{A}} \in \|\mathcal{A}\|$, l'**interpretazione di $\boldsymbol{t}$ in $\mathcal{A}$**:

$$\boldsymbol{t}^{\mathcal{A}} = \begin{cases} \boldsymbol{c}_k^{\mathcal{A}} & \text{se } \boldsymbol{t} = \boldsymbol{c}_k, \\ \boldsymbol{f}_j^{\mathcal{A}}(\boldsymbol{t}_1^{\mathcal{A}}, \dots, \boldsymbol{t}_n^{\mathcal{A}}) & \text{se } \boldsymbol{t} = \boldsymbol{f}_j(\boldsymbol{t}_1, \dots, \boldsymbol{t}_n)\,. \end{cases}$$

Per esempio, il termine $\mathbf{1} + \mathbf{1} + \mathbf{1}$ nel linguaggio $\boldsymbol{L}_{\text{ring}}$ degli anelli con unità, interpretato in $\mathbb{Z}$ è il numero 3, interpretato in $\mathbb{Z}/3\mathbb{Z}$ è lo 0 dell'anello. Osserviamo che se $\mathcal{A}'$ è un'espansione di $\mathcal{A}$ e $\mathcal{A} \subseteq \mathcal{B}$, allora

$$\boldsymbol{t}^{\mathcal{A}} = \boldsymbol{t}^{\mathcal{A}'} = \boldsymbol{t}^{\mathcal{B}}\,. \tag{84}$$

Se $\boldsymbol{t}$ è un termine non chiuso, non possiamo associargli un'interpretazione in $\mathcal{A}$ se prima non assegniamo un valore alle variabili. Fissiamo una

$$g\colon \text{Vbl} \to \|\mathcal{A}\|\,.$$

Una funzione siffatta si dice **assegnazione** in $\mathcal{A}$. Ad ogni termine $\boldsymbol{t}$ possiamo associare un elemento di $\|\mathcal{A}\|$,

$$\boldsymbol{t}^{\mathcal{A}}[g]$$

detto l'**interpretazione di $\boldsymbol{t}$ mediante** g ponendo

$$\boldsymbol{t}^{\mathcal{A}}[g] = \begin{cases} \boldsymbol{c}^{\mathcal{A}} & \text{se } \boldsymbol{t} \text{ è } \boldsymbol{c}, \\ g(\boldsymbol{x}) & \text{se } \boldsymbol{t} \text{ è } \boldsymbol{x}, \\ \boldsymbol{f}^{\mathcal{A}}(\boldsymbol{u}_1^{\mathcal{A}}[g], \dots, \boldsymbol{u}_n^{\mathcal{A}}[g]) & \text{se } \boldsymbol{t} \text{ è } \boldsymbol{f}(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n). \end{cases}$$

Per esempio, nel linguaggio $\boldsymbol{L}_{\text{ring}}$ se $\boldsymbol{t}$ è $(\boldsymbol{x} + \boldsymbol{y})\cdot(\boldsymbol{x} + \boldsymbol{y})$ e g è un'assegnazione in $\mathcal{A}$ tale che $g(\boldsymbol{x}) = a$ e $g(\boldsymbol{y}) = b$, allora $\boldsymbol{t}^{\mathcal{A}}[g]$ è l'elemento $(a+b)^2 \in \|\mathcal{A}\|$. Il prossimo risultato dice che $\boldsymbol{t}^{\mathcal{A}}[g]$ dipende solo dai valori di $g(\boldsymbol{x})$, con $\boldsymbol{x}$ variabile di $\boldsymbol{t}$.

Lemma 21.1. *Se $g, h\colon \text{Vbl} \to \|\mathcal{A}\|$ sono assegnazioni tali che $g \restriction \boldsymbol{V}(\boldsymbol{t}) = h \restriction \boldsymbol{V}(\boldsymbol{t})$, allora $\boldsymbol{t}^{\mathcal{A}}[g] = \boldsymbol{t}^{\mathcal{A}}[h]$.*

Dimostrazione. Se $\boldsymbol{t} = \boldsymbol{c}$ con $\boldsymbol{c} \in \text{Const}$ oppure $\boldsymbol{t} = \boldsymbol{x}$ con $\boldsymbol{x} \in \text{Vbl}$, il risultato è immediato. Supponiamo che $\boldsymbol{t} = \boldsymbol{f}(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)$. Allora $\boldsymbol{V}(\boldsymbol{t}) = \boldsymbol{V}(\boldsymbol{u}_1) \cup \dots \cup \boldsymbol{V}(\boldsymbol{u}_1)$ e quindi, per ipotesi induttiva, $\boldsymbol{u}_i^{\mathcal{A}}[g] = \boldsymbol{u}_i^{\mathcal{A}}[h]$, per $i = 1, \dots, n$, quindi

$$\boldsymbol{t}^{\mathcal{A}}[g] = \boldsymbol{f}^{\mathcal{A}}(\boldsymbol{u}_i^{\mathcal{A}}[g], \dots, \boldsymbol{u}_i^{\mathcal{A}}[g]) = \boldsymbol{f}^{\mathcal{A}}(\boldsymbol{u}_i^{\mathcal{A}}[h], \dots, \boldsymbol{u}_i^{\mathcal{A}}[h]) = \boldsymbol{t}^{\mathcal{A}}[h]\,.$$

□

Supponiamo che le variabili di un termine $\boldsymbol{t}$ di $\boldsymbol{L}$ siano comprese tra $\boldsymbol{x}_1, \dots, \boldsymbol{x}_n$, vale a dire $\boldsymbol{V}(\boldsymbol{t}) \subseteq \{\boldsymbol{x}_1, \dots, \boldsymbol{x}_n\}$. Siano $a_1, \dots, a_n$ elementi di $\|\mathcal{A}\|$ non necessariamente distinti. Se g e h sono assegnazioni in $\mathcal{A}$ tali che $g(\boldsymbol{x}_i) = h(\boldsymbol{x}_i) = a_i$, per $1 \leq i \leq n$, allora, per il Lemma 21.1, $\boldsymbol{t}^{\mathcal{A}}[g] = \boldsymbol{t}^{\mathcal{A}}[h]$. Quest'elemento lo si denota con

$$\boldsymbol{t}^{\mathcal{A}}[a_1, \dots, a_n]\,.$$

Un modo equivalente per definire $\boldsymbol{t}^{\mathcal{A}}[a_1, \dots, a_n]$ si ottiene considerando

$$\mathcal{A}' \stackrel{\text{def}}{=} \langle \mathcal{A}, a_1, \dots, a_n \rangle$$

l'espansione di $\mathcal{A}$ al linguaggio $\boldsymbol{L}' = \boldsymbol{L} \cup \{\mathring{a}_1, \dots, \mathring{a}_n\}$. In altre parole: introduciamo n nuovi simboli di costante $\mathring{a}_1, \dots, \mathring{a}_n$ che devono essere interpretati come $a_1, \dots, a_n$ —si noti che gli $\mathring{a}_i$ sono tutti distinti, mentre gli a_i non lo sono necessariamente. Il termine chiuso di $\boldsymbol{L}'$

$$\boldsymbol{t}[\mathring{a}_1/\boldsymbol{x}_1, \dots, \mathring{a}_n/\boldsymbol{x}_n]$$

ottenuto sostituendo $\mathring{a}_1, \dots, \mathring{a}_n$ a $\boldsymbol{x}_1, \dots, \boldsymbol{x}_n$ ha come interpretazione in $\mathcal{A}'$ proprio $\boldsymbol{t}^{\mathcal{A}}[a_1, \dots, a_n]$.

Lemma 21.2. *Se $\boldsymbol{t}$ è un termine le cui variabili sono tra $\boldsymbol{x}_1, \dots, \boldsymbol{x}_n$ e se $\pi \colon \mathcal{A} \to \mathcal{B}$ è un morfismo, allora*

$$\forall a_1, \dots, a_n \in \|\mathcal{A}\| \big(\pi\big(\boldsymbol{t}^{\mathcal{A}}[a_1, \dots, a_n]\big) = \boldsymbol{t}^{\mathcal{B}}[\pi(a_1), \dots, \pi(a_n)]\big).$$

Dimostrazione. Per induzione su $\mathrm{lh}(\boldsymbol{t})$. Se $\boldsymbol{t} = \boldsymbol{c}_k$, allora $\boldsymbol{t}^{\mathcal{A}} = \boldsymbol{c}_k^{\mathcal{A}}$ e $\boldsymbol{t}^{\mathcal{B}} = \boldsymbol{c}_k^{\mathcal{B}}$ e quindi $\pi(\boldsymbol{t}^{\mathcal{A}}) = \boldsymbol{t}^{\mathcal{B}}$ per definizione di morfismo. Se $\boldsymbol{t} = \boldsymbol{x}_k$ allora $\boldsymbol{t}^{\mathcal{A}}[a_1, \dots, a_n] = a_k$ e $\boldsymbol{t}^{\mathcal{B}}(\pi(a_1), \dots, \pi(a_n)) = \pi(a_k)$ e quindi il risultato segue. Se $\boldsymbol{t} = \boldsymbol{f}_j(\boldsymbol{t}_1, \dots, \boldsymbol{t}_m)$ allora

$$\begin{aligned}
\pi(\boldsymbol{t}^{\mathcal{A}}[\bar{a}]) &= \pi\big(\boldsymbol{f}_j^{\mathcal{A}}\big(\boldsymbol{t}^{\mathcal{A}}[\bar{a}], \dots, \boldsymbol{t}^{\mathcal{A}}[\bar{a}]\big)\big) \\
&= \boldsymbol{f}_j^{\mathcal{B}}\big(\pi\big(\boldsymbol{t}_1^{\mathcal{A}}[\bar{a}]\big), \dots, \pi\big(\boldsymbol{t}^{\mathcal{A}}[\bar{a}]\big)\big) \quad \text{(per definizione di morfismo)} \\
&= \boldsymbol{f}_j^{\mathcal{B}}\big(\boldsymbol{t}_1^{\mathcal{B}}\big[\pi(\bar{a})\big], \dots, \boldsymbol{t}^{\mathcal{B}}\big[\pi(\bar{a})\big]\big) \quad \text{(per ipotesi induttiva)} \\
&= \boldsymbol{t}^{\mathcal{B}}\big[\pi(\bar{a})\big] \quad \text{(per definizione di sostituzione).}
\end{aligned}$$

□

21.B. La verità di una formula in una struttura. Le formula di un linguaggio $\boldsymbol{L}$ sono oggetti che codificano delle proprietà delle $\boldsymbol{L}$-strutture. Per esempio, nel linguaggio $\boldsymbol{L}$ contenente un'unica operazione binaria $*$, la formula

$$\boldsymbol{x} * \boldsymbol{y} = \boldsymbol{z} \tag{85}$$

è vera nella $\boldsymbol{L}$-struttura $\mathcal{A} = \langle A, \cdot \rangle$ se e solo se alle variabili $\boldsymbol{x}$, $\boldsymbol{y}$ e $\boldsymbol{z}$ associamo degli elementi a, b e c tali che $a \cdot b = c$. Quindi la verità di (85) in $\mathcal{A}$ dipende da come valutiamo le variabili, cioè da un'assegnazione in $\mathcal{A}$. Per un altro esempio consideriamo il linguaggio per gli ordini $\boldsymbol{L} = \{\lhd\}$: la formula

$$\boldsymbol{x} \lhd \boldsymbol{y} \tag{86}$$

è vera in un ordine stretto $\langle A, < \rangle$ relativamente ad un'assegnazione g se e solo se $g(\boldsymbol{x}) < g(\boldsymbol{y})$. Osserviamo che la formula $\boldsymbol{x} \lhd \boldsymbol{x}$ non è mai vera in un ordine un ordine stretto, qualsiasi sia la valutazione. Quindi, se $\boldsymbol{\varphi}$ è una formula atomica, per ogni $\boldsymbol{L}$-struttura $\mathcal{A}$ e ogni assegnazione g in $\mathcal{A}$ siamo in

grado di dire quando $\boldsymbol{\varphi}$ è vera in $\mathcal{A}$ relativamente ad g. Fissati $\mathcal{A}$ e g siamo in grado di stabilire la verità di una qualsiasi formula priva di quantificatori $\boldsymbol{\varphi}$: se $\boldsymbol{\varphi}$ è $\boldsymbol{\neg\psi}$ allora $\boldsymbol{\varphi}$ è vera in $\mathcal{A}$ se e solo $\boldsymbol{\psi}$ non è vera in $\mathcal{A}$, se $\boldsymbol{\varphi}$ è $\boldsymbol{\neg\psi \wedge \chi}$ allora $\boldsymbol{\varphi}$ è vera in $\mathcal{A}$ se e solo tanto $\boldsymbol{\psi}$ quanto $\boldsymbol{\chi}$ sono vere in $\mathcal{A}$, etc. Infine, per stabilire la verità di una formula contenete quantificatori ci basiamo sul significato intuitivo di $\boldsymbol{\exists}$ e $\boldsymbol{\forall}$. Per esempio la formula (anzi: l'enunciato) $\boldsymbol{\forall x \forall y}\,(\boldsymbol{x} * \boldsymbol{y} = \boldsymbol{y} * \boldsymbol{x})$ è vera in $\mathcal{A} = \langle A, \cdot \rangle$ se e solo se per ogni scelta di elementi $a, b \in A$ si ha che $a \cdot b = b \cdot a$, cioè se $\cdot$ è un'operazione commutativa. Analogamente una formula del tipo $\boldsymbol{\exists z\, \varphi}$ con variabili libere $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ è vera $\mathcal{A}$ secondo l'assegnazione $\boldsymbol{x}_i \mapsto a_i$ se c'è un elemento $b \in A$ per cui assegnando b a $\boldsymbol{z}$ la formula $\boldsymbol{\varphi}$ risulta vera in $\mathcal{A}$. Per esempio, la formula

$$\boldsymbol{x} \lhd \boldsymbol{y} \boldsymbol{\Rightarrow} \boldsymbol{\exists z}\,(\boldsymbol{x} \lhd \boldsymbol{z} \lhd \boldsymbol{y}) \tag{87}$$

è sempre vera in $\langle \mathbb{Q}, < \rangle$ (o più in generale: in qualsiasi ordine denso) indipendentemente dall'assegnazione g: se $g(\boldsymbol{x}) < g(\boldsymbol{y})$ basta prendere per $\boldsymbol{z}$ un elemento in mezzo, se invece $g(\boldsymbol{y}) \leq g(\boldsymbol{x})$, la formula $\boldsymbol{x} \lhd \boldsymbol{y}$ risulta essere non vera e quindi la (87) è vera, indipendentemente dalla verità o meno di $\boldsymbol{\exists z}\,(\boldsymbol{x} \lhd \boldsymbol{z} \lhd \boldsymbol{y})$. Viceversa la verità di (87) in $\langle \mathbb{Z}, < \rangle$ dipende dall'assegnazione g: la formula è vera se e solo se $g(\boldsymbol{x}) \geq g(\boldsymbol{y})$ oppure $g(\boldsymbol{x}) + 1 < g(\boldsymbol{y})$, cioè se e solo se

$$g(\boldsymbol{x}) < g(\boldsymbol{y}) \Rightarrow g(\boldsymbol{x}) + 1 < g(\boldsymbol{y}).$$

(Osserviamo che $\Rightarrow$ è l'usuale simbolo di implicazione che si utilizza in matematica, mentre $\boldsymbol{\Rightarrow}$ è il simbolo del nostro linguaggio $\boldsymbol{L}$.) Diamo ora la trattazione formale delle idee esposte fin qui.

Fissiamo un linguaggio $\boldsymbol{L}$ ed una $\boldsymbol{L}$-struttura $\mathcal{A}$. Definiamo quando una $\boldsymbol{L}$-formula $\boldsymbol{\varphi}$ è **vera in** $\mathcal{A}$ secondo un'assegnazione g in $\mathcal{A}$, in simboli

$$\mathcal{A} \models \boldsymbol{\varphi}[g]\,. \tag{88}$$

L'espressione qui sopra si legge anche: $\mathcal{A}$ **soddisfa** $\boldsymbol{\varphi}$ con l'assegnazione g, ovvero $\mathcal{A}$ è un **modello** di $\boldsymbol{\varphi}$ per l'assegnazione g. Nel caso in cui la (88) non valga, scriveremo $\mathcal{A} \not\models \boldsymbol{\varphi}[g]$ e diremo che $\boldsymbol{\varphi}$ è **falsa** in $\mathcal{A}$ per l'assegnazione g. Equivalentemente: che $\mathcal{A}$ non soddisfa $\boldsymbol{\varphi}$ con l'assegnazione g; che $\mathcal{A}$ non è un modello di $\boldsymbol{\varphi}$ per l'assegnazione g. Se $\mathcal{A}$ soddisfa $\boldsymbol{\varphi}$ per *ogni* assegnazione g, diremo semplicemente che $\boldsymbol{\varphi}$ è vera in $\mathcal{A}$. Analogamente, se $\mathcal{A}$ non soddisfa $\boldsymbol{\varphi}$ per *ogni* assegnazione g, diremo che $\boldsymbol{\varphi}$ è falsa in $\mathcal{A}$.

Se $\boldsymbol{\varphi}$ è atomica, la definizione di (88) è immediata:

- se $\boldsymbol{\varphi}$ è $\boldsymbol{t}_1 \equiv \boldsymbol{t}_2$, allora (88) diventa

  $$\boldsymbol{t}_1^{\mathcal{A}}[g] = \boldsymbol{t}_2^{\mathcal{A}}[g]\,,$$

  cioè i termini $\boldsymbol{t}_1$ e $\boldsymbol{t}_2$ interpretati in $\mathcal{A}$ via g individuano lo stesso elemento di $\mathcal{A}$.

- se $\boldsymbol{\varphi}$ è $\boldsymbol{R}_i(\boldsymbol{t}_1, \ldots, \boldsymbol{t}_m)$, allora (88) diventa

$$\left(\boldsymbol{t}_1^{\mathcal{A}}[g], \ldots, \boldsymbol{t}_m^{\mathcal{A}}[g]\right) \in \boldsymbol{R}_i^{\mathcal{A}},$$

  cioè se la n-upla dei termini interpretati appartiene all'interpretazione del simbolo di relazione.

Osserviamo che le formule (85) e (86) sono vere in $\mathcal{A} = \langle A, \cdot, < \ldots \rangle$ per l'assegnazione g se e solo se $g(\boldsymbol{x}) \cdot g(\boldsymbol{y}) = g(\boldsymbol{z})$ e $g(\boldsymbol{x}) < g(\boldsymbol{y})$.

Supponiamo ora che la formula $\boldsymbol{\varphi}$ sia ottenuta da $\boldsymbol{\psi}$ e $\boldsymbol{\chi}$ mediante connettivi logici e supponiamo di aver già definito $\mathcal{A} \models \boldsymbol{\psi}[g]$ e $\mathcal{A} \models \boldsymbol{\chi}[g]$.

Se $\boldsymbol{\varphi}$ è $\boldsymbol{\neg\psi}$, allora $\mathcal{A} \models \boldsymbol{\varphi}[g]$ se e solo se $\mathcal{A} \not\models \boldsymbol{\psi}[g]$, cioè se e solo se $\boldsymbol{\psi}$ è falsa in $\mathcal{A}$ per l'assegnazione g.

Se $\boldsymbol{\varphi}$ è $\boldsymbol{\psi \vee \chi}$, allora

$$\mathcal{A} \models (\boldsymbol{\psi \vee \chi})\,[g] \quad \Leftrightarrow \quad (\mathcal{A} \models \boldsymbol{\psi}[g]) \vee (\mathcal{A} \models \boldsymbol{\chi}[g])\,,$$

cioè $\boldsymbol{\psi \vee \chi}$ è vera in $\mathcal{A}$ per l'assegnazione g se e solo se $\boldsymbol{\psi}$ o $\boldsymbol{\chi}$ sono vere in $\mathcal{A}$ per l'assegnazione g. Analogamente, stabiliremo che le formule

$$\mathcal{A} \models (\boldsymbol{\psi \wedge \chi})\,[g], \quad \mathcal{A} \models (\boldsymbol{\psi \Rightarrow \chi})\,[g], \quad \mathcal{A} \models (\boldsymbol{\psi \Leftrightarrow \chi})\,[g]$$

significano, rispettivamente, che:

- $\mathcal{A} \models \boldsymbol{\psi}[g]$ e $\mathcal{A} \models \boldsymbol{\chi}[g]$,
- se $\mathcal{A} \models \boldsymbol{\psi}[g]$ allora $\mathcal{A} \models \boldsymbol{\chi}[g]$,
- $\mathcal{A} \models \boldsymbol{\psi}[g]$ se e solo se $\mathcal{A} \models \boldsymbol{\chi}[g]$.

Fino a questo punto la definizione della relazione di soddisfazione sembra una semplice operazione di riscrittura: la si definisce in modo ovvio per le formule atomiche e poi si procede per induzione sulla complessità della formula. Il vero problema sorge quando si incontrano formule contenti quantificatori. Introduciamo la seguente notazione: se $g\colon \mathrm{Vbl} \to \mathcal{A}$ è un'assegnazione, $\boldsymbol{x} \in \mathrm{Vbl}$ e $a \in \|\mathcal{A}\|$, definiamo l'assegnazione $g_{a/\boldsymbol{x}}\colon \mathrm{Vbl} \to \|\mathcal{A}\|$

$$g_{a/\boldsymbol{x}}(\boldsymbol{v}_n) = \begin{cases} a & \text{se } \boldsymbol{x} = \boldsymbol{v}_n, \\ g(\boldsymbol{v}_n) & \text{altrimenti.} \end{cases}$$

Quindi la funzione $g_{a/\boldsymbol{x}}$ differisce da g in al più un punto, la variabile $\boldsymbol{x}$, e se $a = g(\boldsymbol{x})$ allora $g = g_{a/\boldsymbol{x}}$.

Esercizio 21.3. Se $\boldsymbol{x}$ e $\boldsymbol{y}$ sono variabili distinte, allora

$$\left(g_{a/\boldsymbol{x}}\right)_{b/\boldsymbol{y}} = \left(g_{b/\boldsymbol{y}}\right)_{a/\boldsymbol{x}}$$

per ogni assegnazione $g\colon \mathrm{Vbl} \to \|\mathcal{A}\|$ e ogni $a, b \in \|\mathcal{A}\|$.

Definiamo ora la relazione di soddisfazione per formule contenenti quantificatori:

$$\mathcal{A} \models \exists \boldsymbol{x}\, \boldsymbol{\varphi}[g] \quad \Leftrightarrow \quad \exists a \in \|\mathcal{A}\| \left(\mathcal{A} \models \boldsymbol{\varphi}[g_{a/\boldsymbol{x}}]\right)$$
$$\mathcal{A} \models \forall \boldsymbol{x}\, \boldsymbol{\varphi}[g] \quad \Leftrightarrow \quad \forall a \in \|\mathcal{A}\| \left(\mathcal{A} \models \boldsymbol{\varphi}[g_{a/\boldsymbol{x}}]\right).$$

In altre parole, $\exists \boldsymbol{x}\, \boldsymbol{\varphi}$ è vera in $\mathcal{A}$ per l'assegnazione g se e solo se *esiste* un a tale che, assegnando questo a ad $\boldsymbol{x}$ e mantenendo l'assegnazione g per le altre variabili, la formula $\boldsymbol{\varphi}$ è vera in $\mathcal{A}$. Analogamente, $\forall \boldsymbol{x}\, \boldsymbol{\varphi}$ è vera in $\mathcal{A}$ per l'assegnazione g se e solo se *per ogni* a, assegnando a ad $\boldsymbol{x}$ e mantenendo l'assegnazione g per le altre variabili, la formula $\boldsymbol{\varphi}$ è vera in $\mathcal{A}$.

21.C. Qualche risultato sulla relazione di soddisfazione. Nelle pagine che seguono dovremo spesso dimostrare risultati del tipo:

(89) $$\ldots \text{se } \mathcal{A} \models \boldsymbol{\varphi}[g], \text{ allora } \mathcal{B} \models \boldsymbol{\varphi}[g] \ldots$$

La verifica di ciò avviene per induzione sulla complessità di $\boldsymbol{\varphi}$, e considerando che ci sono quattro simboli dei connettivi binari ($\vee$, $\wedge$, $\Rightarrow$, $\Leftrightarrow$) e due simboli di quantificatore ($\exists$, $\forall$) i conti possono risultare un po' lunghi. Tuttavia per come è stata definita $\models$, possiamo ridurre il numero di casi da verificare.

Esercizio 21.4. Dimostrare che:

(i) $\mathcal{A} \models \neg\neg\boldsymbol{\varphi}[g]$ se e solo se $\mathcal{A} \models \boldsymbol{\varphi}[g]$;
(ii) $\mathcal{A} \models (\boldsymbol{\varphi} \wedge \boldsymbol{\psi})[g]$ se e solo se $\mathcal{A} \models \neg\left(\neg\boldsymbol{\varphi} \vee \boldsymbol{\psi}\right)[g]$;
(iii) $\mathcal{A} \models (\boldsymbol{\varphi} \vee \boldsymbol{\psi})[g]$ se e solo se $\mathcal{A} \models \neg\left(\neg\boldsymbol{\varphi} \wedge \neg\boldsymbol{\psi}\right)[g]$;
(iv) $\mathcal{A} \models (\boldsymbol{\varphi} \Rightarrow \boldsymbol{\psi})\,[g]$ se e solo se $\mathcal{A} \models (\neg\boldsymbol{\varphi} \vee \boldsymbol{\psi})\,[g]$;
(v) $\mathcal{A} \models (\boldsymbol{\varphi} \Leftrightarrow \boldsymbol{\psi})\,[g]$ se e solo se $\mathcal{A} \models ((\neg\boldsymbol{\varphi} \vee \boldsymbol{\psi}) \wedge (\boldsymbol{\varphi} \vee \neg\boldsymbol{\psi}))\,[g]$;
(vi) $\mathcal{A} \models \forall \boldsymbol{x}\, \boldsymbol{\varphi}[g]$ se e solo se $\mathcal{A} \models \neg\exists \boldsymbol{x}\, \neg\boldsymbol{\varphi}[g]$;
(vii) $\mathcal{A} \models \exists \boldsymbol{x}\, \boldsymbol{\varphi}[g]$ se e solo se $\mathcal{A} \models \neg\forall \boldsymbol{x}\, \neg\boldsymbol{\varphi}[g]$.

Quindi per verificare la (89) è sufficiente restringerci alla collezione delle formule generate dalle formule atomiche, da un insieme adeguato di connettivi (Esercizio 13.10), per esempio $\{\neg, \vee\}$, e da uno dei due quantificatori.

Lemma 21.5. *Sia* $\boldsymbol{\varphi}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)$ *una* $\boldsymbol{L}$*-formula. Se* $g, h\colon \mathrm{Vbl} \to \|\mathcal{A}\|$ *sono assegnazioni tali che* $g \restriction \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\} = h \restriction \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\}$,

$$\mathcal{A} \models \boldsymbol{\varphi}[g] \quad \Leftrightarrow \quad \mathcal{A} \models \boldsymbol{\varphi}[h]\,.$$

Dimostrazione. La verifica è per induzione su $\mathrm{ht}(\boldsymbol{\varphi})$. Se $\boldsymbol{\varphi}$ è $\neg\boldsymbol{\psi}$ oppure $\boldsymbol{\psi} \vee \boldsymbol{\chi}$, il risultato è banale. Supponiamo quindi $\boldsymbol{\varphi}$ sia della forma $\exists \boldsymbol{y}\, \boldsymbol{\psi}$. Se $\mathcal{A} \models \exists \boldsymbol{y}\, \boldsymbol{\psi}[g]$, allora c'è un $a \in \mathcal{A}$ tale che $\mathcal{A} \models \boldsymbol{\psi}[g_{a/\boldsymbol{y}}]$. Per ipotesi induttiva $\mathcal{A} \models \boldsymbol{\psi}[g_{a/\boldsymbol{y}}]$ se e solo se $\mathcal{A} \models \boldsymbol{\psi}[h_{a/\boldsymbol{y}}]$ e quindi $\mathcal{A} \models \exists \boldsymbol{y}\, \boldsymbol{\psi}[h]$. Analogamente $\mathcal{A} \models \exists \boldsymbol{y}\, \boldsymbol{\psi}[h]$ implica $\mathcal{A} \models \exists \boldsymbol{y}\, \boldsymbol{\psi}[g]$. □

Per quanto dimostrato, data una formula $\boldsymbol{\varphi}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)$ ed elementi non necessariamente distinti $a_1, \ldots, a_n \in \|\mathcal{A}\|$ definiamo

$$\mathcal{A} \models \boldsymbol{\varphi}[a_1, \ldots, a_n]$$

se e solo se $\mathcal{A} \models \boldsymbol{\varphi}[g]$ per qualche (equivalentemente: per ogni) assegnazione g tale che $g(\boldsymbol{x}_i) = a_i$, $(1 \leq i \leq n)$. Se $\boldsymbol{\sigma}$ è un enunciato, allora le assegnazioni diventano irrilevanti, per cui poniamo

$$\mathcal{A} \models \boldsymbol{\sigma}$$

se vale $\mathcal{A} \models \boldsymbol{\sigma}[g]$ per una (equivalentemente: per tutte) le assegnazioni.

Esercizio 21.6. Sia $\boldsymbol{L}' \subseteq \boldsymbol{L}$ e $\boldsymbol{\varphi} \in \mathrm{Fml}(\boldsymbol{L}')$. Verificare per induzione su $\mathrm{ht}(\boldsymbol{\varphi})$ che per ogni $\mathcal{A} \in \mathfrak{Str}(\boldsymbol{L})$ e ogni $g\colon \mathrm{Vbl} \to \|\mathcal{A}\|$,

$$\mathcal{A} \models \boldsymbol{\varphi}[g] \quad \Leftrightarrow \quad (\mathcal{A} \restriction \boldsymbol{L}') \models \boldsymbol{\varphi}[g]\,.$$

Proposizione 21.7. *Sia $\boldsymbol{\varphi}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)$ una $\boldsymbol{L}$-formula, $\mathcal{A}$ una $\boldsymbol{L}$-struttura e $a_1, \ldots, a_n \in \|\mathcal{A}\|$.*

(a) *Se $\boldsymbol{y} \notin \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\}$, allora*

$$\begin{aligned} \mathcal{A} \models \boldsymbol{\exists y}\, \boldsymbol{\varphi}[a_1, \ldots, a_n] \quad &\Leftrightarrow \quad \mathcal{A} \models \boldsymbol{\forall y}\, \boldsymbol{\varphi}[a_1, \ldots, a_n] \\ &\Leftrightarrow \quad \mathcal{A} \models \boldsymbol{\varphi}[a_1, \ldots, a_n]\,. \end{aligned}$$

(b) *Se $\boldsymbol{y} = \boldsymbol{x}_m$ per qualche $1 \leq m \leq n$, allora*

$$\begin{aligned} &\mathcal{A} \models \big(\boldsymbol{\exists x}_m\, \boldsymbol{\varphi}\big)[a_1, \ldots, a_n] \;\Leftrightarrow \\ &\qquad\qquad \exists a \in \|\mathcal{A}\|\, (\mathcal{A} \models \boldsymbol{\varphi}[a_1, \ldots, a_{m-1}, a, a_{m+1}, \ldots, a_n])\,, \\ &\mathcal{A} \models \big(\boldsymbol{\forall x}_m\, \boldsymbol{\varphi}\big)[a_1, \ldots, a_n] \;\Leftrightarrow \\ &\qquad\qquad \forall a \in \|\mathcal{A}\|\, (\mathcal{A} \models \boldsymbol{\varphi}[a_1, \ldots, a_{m-1}, a, a_{m+1}, \ldots, a_n])\,. \end{aligned}$$

Dimostrazione. (a) Supponiamo che $\mathcal{A} \models \boldsymbol{\exists y}\, \boldsymbol{\varphi}[a_1, \ldots, a_n]$, vale a dire che $\mathcal{A} \models \boldsymbol{\exists y}\, \boldsymbol{\varphi}[g]$ per una (equivalentemente: per ogni) assegnazione g tale che $g(\boldsymbol{x}_i) = a_i$ $(1 \leq i \leq n)$. Allora $\mathcal{A} \models \boldsymbol{\varphi}[g_{a/\boldsymbol{y}}]$ per qualche $a \in \|\mathcal{A}\|$. Per l'ipotesi su $\boldsymbol{y}$, $g_{a/\boldsymbol{y}}(\boldsymbol{x}_i) = a_i$ e quindi $\mathcal{A} \models \boldsymbol{\varphi}[a_1, \ldots, a_n]$. L'implicazione $\big(\mathcal{A} \models \boldsymbol{\varphi}[a_1, \ldots, a_n]\big) \Rightarrow \big(\mathcal{A} \models \boldsymbol{\exists y}\, \boldsymbol{\varphi}[a_1, \ldots, a_n]\big)$ è immediata, quindi

$$\mathcal{A} \models \boldsymbol{\varphi}[a_1, \ldots, a_n] \quad \Leftrightarrow \quad \mathcal{A} \models \boldsymbol{\exists y}\, \boldsymbol{\varphi}[a_1, \ldots, a_n] \tag{90}$$

Dato che le variabili libere di $\boldsymbol{\neg\varphi}$ sono esattamente le stesse di $\boldsymbol{\varphi}$, abbiamo che

$$\begin{aligned} \mathcal{A} \models \boldsymbol{\forall y}\, \boldsymbol{\varphi}[a_1, \ldots, a_n] &\Leftrightarrow \mathcal{A} \not\models \boldsymbol{\exists y}\, \boldsymbol{\neg\varphi}[a_1, \ldots, a_n] \\ &\Leftrightarrow \mathcal{A} \not\models \boldsymbol{\neg\varphi}[a_1, \ldots, a_n] \\ &\Leftrightarrow \mathcal{A} \models \boldsymbol{\varphi}[a_1, \ldots, a_n]\,, \end{aligned}$$

dove nella seconda riga abbiamo usato l'equivalenza (90) per $\boldsymbol{\neg\varphi}$.

La parte (b) è una semplice riformulazione della definizione di $\models$ nel caso del quantificatore esistenziale—i dettagli sono lasciati al lettore. □

Esercizio 21.8. Generalizzare la Proposizione 21.7 al caso di formule con più quantificatori dello stesso tipo (per esempio $\exists \boldsymbol{y}_1 \exists \boldsymbol{y}_2 \dots \exists \boldsymbol{y}_m \, \boldsymbol{\varphi}$, oppure $\forall \boldsymbol{y}_1 \forall \boldsymbol{y}_2 \dots \forall \boldsymbol{y}_m \, \boldsymbol{\varphi}$).

La **chiusura universale** di una formula $\boldsymbol{\varphi}$ è l'enunciato $\forall \boldsymbol{v}_{k_1} \dots \forall \boldsymbol{v}_{k_n} \boldsymbol{\varphi}$ dove $\{\boldsymbol{v}_{k_1}, \dots, \boldsymbol{v}_{k_n}\}$ sono le variabili libere di $\boldsymbol{\varphi}$. Diremo che una $\boldsymbol{L}$-struttura $\mathcal{A}$ soddisfa una formula (con eventualmente variabili libere) $\boldsymbol{\varphi}$ se e solo se $\mathcal{A}$ soddisfa la sua chiusura universale di $\boldsymbol{\varphi}$.

21.D. Formule logicamente valide. Una $\boldsymbol{L}$-formula $\boldsymbol{\varphi}$ è **logicamente valida** se è vera in ogni $\boldsymbol{L}$-struttura, cioè se

$$\mathcal{A} \models \boldsymbol{\varphi}[g]$$

per ogni $\mathcal{A} \in \mathfrak{Str}(\boldsymbol{L})$ e ogni assegnazione g. Vediamo qualche esempio di formula logicamente valida.

21.D.1. *Assiomi dell'identità.* Per ogni scelta variabili $\boldsymbol{x}$, $\boldsymbol{y}$ e $\boldsymbol{z}$ e di termini $\boldsymbol{s}$, $\boldsymbol{t}$ ed $\boldsymbol{u}$, le seguenti formule sono logicamente valide:

$$\boldsymbol{t} \equiv \boldsymbol{t} \tag{91}$$

$$\boldsymbol{s} \equiv \boldsymbol{t} \Rightarrow \boldsymbol{t} \equiv \boldsymbol{s} \tag{92}$$

$$(\boldsymbol{s} \equiv \boldsymbol{t} \wedge \boldsymbol{t} \equiv \boldsymbol{u}) \Rightarrow \boldsymbol{s} \equiv \boldsymbol{u} \tag{93}$$

$$\boldsymbol{x} \equiv \boldsymbol{y} \Rightarrow \boldsymbol{t}[\boldsymbol{x}/\boldsymbol{z}] \equiv \boldsymbol{t}[\boldsymbol{y}/\boldsymbol{z}]\,, \tag{94}$$

dove $\boldsymbol{t}[\boldsymbol{x}/\boldsymbol{z}]$ e $\boldsymbol{t}[\boldsymbol{y}/\boldsymbol{z}]$ sono i termini ottenuti da $\boldsymbol{t}$ sostituendo rispettivamente $\boldsymbol{x}$ e $\boldsymbol{y}$ a $\boldsymbol{z}$. Le formule (91)–(94).

21.D.2. *Tautologie.* Una formula si dice **elementare** se è atomica oppure della forma $\exists \boldsymbol{x} \, \boldsymbol{\psi}$ o della forma $\forall \boldsymbol{x} \, \boldsymbol{\psi}$. Ad ogni $\boldsymbol{\varphi}$ possiamo associare un insieme $\mathcal{E}(\boldsymbol{\varphi})$ di formule elementari come segue:

- se $\boldsymbol{\varphi}$ è elementare, allora $\mathcal{E}(\boldsymbol{\varphi}) = \{\boldsymbol{\varphi}\}$,
- se $\boldsymbol{\varphi} = \neg \boldsymbol{\psi}$, allora $\mathcal{E}(\boldsymbol{\varphi}) = \mathcal{E}(\boldsymbol{\psi})$,
- se $\boldsymbol{\varphi} = \boldsymbol{\psi} \,\square\, \boldsymbol{\chi}$, allora $\mathcal{E}(\boldsymbol{\varphi}) = \mathcal{E}(\boldsymbol{\psi}) \cup \mathcal{E}(\boldsymbol{\chi})$.

Ad ogni $\boldsymbol{\varphi} \in \mathrm{Fml}(\boldsymbol{L})$ possiamo associare una proposizione $\boldsymbol{p}_{\boldsymbol{\varphi}}$ del calcolo proposizionale sulle lettere $\{\boldsymbol{\psi}_1, \dots, \boldsymbol{\psi}_n\} = \mathcal{E}(\boldsymbol{\varphi})$:

$$\boldsymbol{p}_{\boldsymbol{\varphi}} = \begin{cases} \boldsymbol{\varphi} & \text{se } \boldsymbol{\varphi} \text{ è elementare,} \\ \neg \boldsymbol{p}_{\boldsymbol{\psi}} & \text{se } \boldsymbol{\varphi} = \neg \boldsymbol{\psi}, \\ \boldsymbol{p}_{\boldsymbol{\psi}} \,\square\, \boldsymbol{p}_{\boldsymbol{\chi}} & \text{se } \boldsymbol{\varphi} = \boldsymbol{\psi} \,\square\, \boldsymbol{\chi}. \end{cases}$$

Lemma 21.9. *Siano* $\boldsymbol{\varphi}$, $\boldsymbol{p}_{\boldsymbol{\varphi}}$ *e* $\boldsymbol{\psi}_1, \dots, \boldsymbol{\psi}_n$ *come sopra. Sia* $g\colon \mathrm{Vbl} \to \|\mathcal{A}\|$ *un'assegnazione e sia* $\mathcal{V}$ *la valutazione definita da*

$$\mathcal{V}(\boldsymbol{\psi}_i) = 1 \;\Leftrightarrow\; \mathcal{A} \models \boldsymbol{\psi}_i[g]\,.$$

Allora

$$\mathcal{V}(\boldsymbol{p}_{\boldsymbol{\varphi}}) = 1 \;\Leftrightarrow\; \mathcal{A} \models \boldsymbol{\varphi}[g]\,.$$

Dimostrazione. Per induzione sull'altezza della proposizione $\boldsymbol{p}_{\boldsymbol{\varphi}}$. Se $\mathrm{ht}(\boldsymbol{p}_{\boldsymbol{\varphi}}) = 0$ allora $\boldsymbol{\varphi}$ è elementare e il risultato segue immediatamente. Se $\mathrm{ht}(\boldsymbol{p}_{\boldsymbol{\varphi}}) > 0$ allora $\boldsymbol{\varphi} = \boldsymbol{\neg\psi}$ oppure $\boldsymbol{\varphi} = \boldsymbol{\psi} \,\square\, \boldsymbol{\chi}$, cioè $\boldsymbol{p}_{\boldsymbol{\varphi}} = \boldsymbol{\neg p}_{\boldsymbol{\psi}}$ oppure $\boldsymbol{p}_{\boldsymbol{\varphi}} = \boldsymbol{p}_{\boldsymbol{\psi}} \,\square\, \boldsymbol{p}_{\boldsymbol{\chi}}$ e il risultato segue dalla definizione di $\models$. □

Diremo che una formula $\boldsymbol{\varphi} \in \mathrm{Fml}(\boldsymbol{L})$ è una **tautologia** se e solo se la formula proposizionale $\boldsymbol{p}_{\boldsymbol{\varphi}}$ è una tautologia proposizionale (Definizione 13.5).

Corollario 21.10. *Se* $\boldsymbol{\varphi} \in \mathrm{Fml}(\boldsymbol{L})$ *è una tautologia, allora* $\boldsymbol{\varphi}$ *è logicamente valida.*

21.D.3. *Quantificatori e connettivi.* Le formule

$$\boldsymbol{\exists x}\,(\boldsymbol{\varphi} \boldsymbol{\vee} \boldsymbol{\psi}) \boldsymbol{\Leftrightarrow} (\boldsymbol{\exists x \varphi} \boldsymbol{\vee} \boldsymbol{\exists x}\,\boldsymbol{\psi}) \tag{95}$$

$$\boldsymbol{\forall x}\,(\boldsymbol{\varphi} \boldsymbol{\wedge} \boldsymbol{\psi}) \boldsymbol{\Leftrightarrow} (\boldsymbol{\forall x}\,\boldsymbol{\varphi} \boldsymbol{\wedge} \boldsymbol{\forall x}\,\boldsymbol{\psi}) \tag{96}$$

$$\boldsymbol{\exists x}\,(\boldsymbol{\varphi} \boldsymbol{\wedge} \boldsymbol{\psi}) \boldsymbol{\Rightarrow} (\boldsymbol{\exists x}\,\boldsymbol{\varphi} \boldsymbol{\wedge} \boldsymbol{\exists x}\,\boldsymbol{\psi}) \tag{97}$$

$$(\boldsymbol{\forall x}\,\boldsymbol{\varphi} \boldsymbol{\vee} \boldsymbol{\forall x}\,\boldsymbol{\psi}) \boldsymbol{\Rightarrow} \boldsymbol{\forall x}\,(\boldsymbol{\varphi} \boldsymbol{\vee} \boldsymbol{\psi}) \tag{98}$$

sono logicamente valide.

Per verificare (95)–(98) fissiamo una $\boldsymbol{L}$-struttura $\mathcal{A}$ e un'assegnazione g.

Se $\mathcal{A} \models \boldsymbol{\exists x}\,(\boldsymbol{\varphi} \boldsymbol{\vee} \boldsymbol{\psi})\,[g]$ fissiamo un $a \in \|\mathcal{A}\|$ tale che $\mathcal{A} \models (\boldsymbol{\varphi} \boldsymbol{\vee} \boldsymbol{\psi})\,[g_{a/\boldsymbol{x}}]$. Ciò equivale a dire che $\mathcal{A} \models \boldsymbol{\varphi}[g_{a/\boldsymbol{x}}]$ o $\mathcal{A} \models \boldsymbol{\psi}[g_{a/\boldsymbol{x}}]$, da cui $\mathcal{A} \models \boldsymbol{\exists x}\,\boldsymbol{\varphi}[g]$ o $\mathcal{A} \models \boldsymbol{\exists x}\,\boldsymbol{\psi}[g]$. Segue che

$$\mathcal{A} \models (\boldsymbol{\exists x}\,\boldsymbol{\varphi} \boldsymbol{\vee} \boldsymbol{\exists x}\,\boldsymbol{\psi})\,[g]\,.$$

Viceversa, se assumiamo quest'ultima formula, allora $\mathcal{A} \models \boldsymbol{\exists x}\,\boldsymbol{\varphi}[g]$ o $\mathcal{A} \models \boldsymbol{\exists x}\,\boldsymbol{\psi}[g]$. Supponiamo la prima: allora $\mathcal{A} \models \boldsymbol{\varphi}[g_{a/\boldsymbol{x}}]$ per qualche $a \in \|\mathcal{A}\|$, quindi $\mathcal{A} \models (\boldsymbol{\varphi} \boldsymbol{\vee} \boldsymbol{\psi})\,[g_{a/\boldsymbol{x}}]$, da cui $\mathcal{A} \models \boldsymbol{\exists x}\,(\boldsymbol{\varphi} \boldsymbol{\vee} \boldsymbol{\psi})\,[g]$. Questo dimostra la (95).

Supponiamo ora che $\mathcal{A} \models \boldsymbol{\exists x}\,(\boldsymbol{\varphi} \boldsymbol{\wedge} \boldsymbol{\psi})\,[g]$. Allora $\mathcal{A} \models (\boldsymbol{\varphi} \boldsymbol{\wedge} \boldsymbol{\psi})\,[g_{a/\boldsymbol{x}}]$ per qualche $a \in \|\mathcal{A}\|$, quindi $\mathcal{A} \models \boldsymbol{\varphi}[g_{a/\boldsymbol{x}}]$ e $\mathcal{A} \models \boldsymbol{\psi}[g_{a/\boldsymbol{x}}]$, da cui $\mathcal{A} \models \boldsymbol{\exists x}\,\boldsymbol{\varphi}[g]$ e $\mathcal{A} \models \boldsymbol{\exists x}\,\boldsymbol{\psi}[g]$. Quindi $\mathcal{A} \models (\boldsymbol{\exists x}\,\boldsymbol{\varphi} \boldsymbol{\wedge} \boldsymbol{\exists x}\,\boldsymbol{\psi})\,[g]$. Chiaramente (96) e (98) discendono da (95) e (97), rispettivamente.

Osservazione 21.11. Le implicazioni (97) e (98) non possono essere rovesciate. Consideriamo, per esempio, il linguaggio contenente due simboli di relazione 1-ari $\boldsymbol{R}$ e $\boldsymbol{S}$ e supponiamo che $\boldsymbol{\varphi}$ e $\boldsymbol{\psi}$ siano, rispettivamente, le formule atomiche $\boldsymbol{R}(\boldsymbol{x})$ e $\boldsymbol{S}(\boldsymbol{x})$. Sia $\mathcal{A}$ una struttura tale che $\boldsymbol{R}^{\mathcal{A}}$ e $\boldsymbol{S}^{\mathcal{A}}$

sono insiemi non vuoti e disgiunti. Allora $\mathcal{A} \models \exists \boldsymbol{x}\, \boldsymbol{\varphi}$ e $\mathcal{A} \models \exists \boldsymbol{x}\, \boldsymbol{\psi}$, ma $\mathcal{A} \not\models \exists \boldsymbol{x}\, (\boldsymbol{\varphi} \wedge \boldsymbol{\psi})$. Viceversa, se $\boldsymbol{R}^{\mathcal{A}}, \boldsymbol{S}^{\mathcal{A}} \neq \|\mathcal{A}\|$ e $\boldsymbol{R}^{\mathcal{A}} \cup \boldsymbol{S}^{\mathcal{A}} = \|\mathcal{A}\|$, allora $\mathcal{A} \models \forall \boldsymbol{x}\, (\boldsymbol{\varphi} \vee \boldsymbol{\psi})$, mentre $\mathcal{A} \not\models \forall \boldsymbol{x}\, \boldsymbol{\varphi}$ e $\mathcal{A} \not\models \forall \boldsymbol{x}\, \boldsymbol{\psi}$.

21.D.4. *Passaggio del quantificatore universale all'interno di un'implicazione.* Se $\boldsymbol{x}$ non occorre libera in $\boldsymbol{\varphi}$, allora la formula

$$\forall \boldsymbol{x}\, (\boldsymbol{\varphi} \Rightarrow \boldsymbol{\psi}) \Rightarrow (\boldsymbol{\varphi} \Rightarrow \forall \boldsymbol{x}\, \boldsymbol{\psi}) \tag{99}$$

è logicamente valida. Intuitivamente questo è ovvio: se per un qualsiasi $\boldsymbol{x}$ vale l'implicazione $\boldsymbol{\varphi} \Rightarrow \boldsymbol{\psi}$, allora, dato che $\boldsymbol{\varphi}$ non dice nulla su $\boldsymbol{x}$, segue che $\boldsymbol{\varphi} \Rightarrow \forall \boldsymbol{x}\, \boldsymbol{\psi}$. Diamone ora una dimostrazione rigorosa.

Sia $\mathcal{A}$ una $\boldsymbol{L}$-struttura e g un'assegnazione in $\mathcal{A}$ e supponiamo che

$$\mathcal{A} \models \forall \boldsymbol{x}\, (\boldsymbol{\varphi} \Rightarrow \boldsymbol{\psi})\, [g]\,. \tag{100}$$

Dobbiamo dimostrare che se $\mathcal{A} \models \boldsymbol{\varphi}[g]$ allora

$$\mathcal{A} \models \forall \boldsymbol{x}\, \boldsymbol{\psi}[g]\,. \tag{101}$$

Sia $a \in \|\mathcal{A}\|$ un elemento generico: per (100) si ha che $\mathcal{A} \models (\boldsymbol{\varphi} \Rightarrow \boldsymbol{\psi})\, [g_{a/\boldsymbol{x}}]$, cioè se $\mathcal{A} \models \boldsymbol{\varphi}[g_{a/\boldsymbol{x}}]$, allora $\mathcal{A} \models \boldsymbol{\psi}[g_a/\boldsymbol{x}]$. Dato che $\boldsymbol{x}$ non occorre libera in $\boldsymbol{\varphi}$, $\mathcal{A} \models \boldsymbol{\varphi}[g_{a/\boldsymbol{x}}]$ se e solo se $\mathcal{A} \models \boldsymbol{\varphi}[g]$. Quindi $\mathcal{A} \models \boldsymbol{\psi}[g_{a/\boldsymbol{x}}]$. Per l'arbitrarietà di a segue (101).

Se $\boldsymbol{x}$ occorre libera in $\boldsymbol{\varphi}$ la (99) non è logicamente valida: per esempio consideriamo la struttura $\mathbb{N}$ con un il predicato binario $\mid$ di divisibilità, cioè $n \mid m$ significa "n divide m". Siano $\boldsymbol{\varphi}(\boldsymbol{x}, \boldsymbol{y})$ e $\boldsymbol{\psi}(\boldsymbol{x}, \boldsymbol{z})$ le formule $\boldsymbol{y} \mid \boldsymbol{x}$ e $\boldsymbol{z} \mid \boldsymbol{x}$, rispettivamente. Sia poi g un'assegnazione tale che $g(\boldsymbol{x}) = 1$, $g(\boldsymbol{y}) = 2$ e $g(\boldsymbol{z}) = 4$. Dato che 2 non divide 1 e che 4 non divide qualsiasi numero, le formule $\boldsymbol{\varphi}$ e $\forall \boldsymbol{x}\, \boldsymbol{\psi}$ sono entrambe false in $\mathcal{N} = \langle \mathbb{N}, \mid \rangle$ per l'assegnazione g e quindi $\mathcal{N} \models (\boldsymbol{\varphi} \Rightarrow \forall \boldsymbol{x}\, \boldsymbol{\psi})\, [g]$. Viceversa, dato che l'essere pari non implica la divisibilità per 4, segue che $\mathcal{N} \not\models \forall \boldsymbol{x}\, (\boldsymbol{\varphi} \Rightarrow \boldsymbol{\psi})\, [g]$ e quindi

$$\mathcal{N} \not\models (\boldsymbol{\varphi} \Rightarrow \forall \boldsymbol{x}\, \boldsymbol{\psi}) \Rightarrow \forall \boldsymbol{x}\, (\boldsymbol{\varphi} \Rightarrow \boldsymbol{\psi})\, [g].$$

Esercizio 21.12. Dimostrare che il converso di (99), cioè la formula

$$(\boldsymbol{\varphi} \Rightarrow \forall \boldsymbol{x}\, \boldsymbol{\psi}) \Rightarrow \forall \boldsymbol{x}\, (\boldsymbol{\varphi} \Rightarrow \boldsymbol{\psi})$$

non è logicamente valida.

21.D.5. *Termini sostituibili.* La formula $\boldsymbol{\varphi}[\boldsymbol{t}/\boldsymbol{x}]$, ottenuta sostituendo il termine $\boldsymbol{t}$ a tutte le occorrenze libere di $\boldsymbol{x}$ in $\boldsymbol{\varphi}$ (vedi pag.169) non ha necessariamente lo stesso significato di $\boldsymbol{\varphi}$. Per esempio, la formula $\exists \boldsymbol{y}\, (\boldsymbol{y} \not\equiv \boldsymbol{x})$ asserisce che c'è un elemento diverso da $\boldsymbol{x}$, mentre se sostituiamo $\boldsymbol{y}$ al posto di $\boldsymbol{x}$, la formula risultante asserisce che c'è un oggetto diverso da sé stesso. La prima formula è vera in ogni struttura con almeno due elementi, la seconda è logicamente falsa. Vogliamo individuare quando è possibile sostituire

un termine $\boldsymbol{t}$ in una formula senza $\boldsymbol{\varphi}(\boldsymbol{x})$ in modo che $\boldsymbol{\varphi}[\boldsymbol{t}/\boldsymbol{x}]$ significhi che vale la proprietà $\boldsymbol{\varphi}$ del termine $\boldsymbol{t}$.

Definizione 21.13. Un termine $\boldsymbol{t}$ è **sostituibile** ad $\boldsymbol{x}$ in $\boldsymbol{\varphi}$ se in ogni occorrenza libera di $\boldsymbol{x}$ in $\boldsymbol{\varphi}$, nessuna delle variabili di $\boldsymbol{t}$ risulta vincolata. Formalmente la definizione è la seguente:

(i) se $\boldsymbol{\varphi}$ è atomica allora $\boldsymbol{t}$ è sempre sostituibile,

(ii) se $\boldsymbol{\varphi}$ è $\boldsymbol{\neg\psi}$ allora $\boldsymbol{t}$ è sostituibile ad $\boldsymbol{x}$ se è sostituibile ad $\boldsymbol{x}$ in $\boldsymbol{\psi}$,

(iii) se $\boldsymbol{\varphi}$ è $\boldsymbol{\psi} \,\square\, \boldsymbol{\chi}$ allora $\boldsymbol{t}$ è sostituibile ad $\boldsymbol{x}$ se è sostituibile in $\boldsymbol{\psi}$ e in $\boldsymbol{\chi}$,

(iv) se $\boldsymbol{\varphi}$ è $\boldsymbol{\exists x\,\psi}$ oppure $\boldsymbol{\forall x\,\psi}$, allora $\boldsymbol{t}$ è sostituibile ad $\boldsymbol{x}$,

(v) se $\boldsymbol{\varphi}$ è $\boldsymbol{\exists z\,\psi}$ oppure $\boldsymbol{\forall z\,\psi}$, dove $\boldsymbol{z}$ è distinta da $\boldsymbol{x}$, e le variabili di $\boldsymbol{t}$ sono $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_n$, allora $\boldsymbol{t}$ è sostituibile ad $\boldsymbol{x}$ in $\boldsymbol{\varphi}$ se e solo se $\boldsymbol{t}$ è sostituibile ad $\boldsymbol{x}$ in $\boldsymbol{\psi}$ e $\boldsymbol{z}$ non è tra le $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_n$.

In nessun altro caso $\boldsymbol{t}$ è sostituibile ad $\boldsymbol{x}$ in $\boldsymbol{\varphi}$.

La condizione (iv) può sembrare bizzarra, ma ricordiamoci che la sostituzione di un termine al posto di una variabile avviene solo quando l'occorrenza è libera.

Esercizio 21.14. (i) Dimostrare che se $\boldsymbol{t}$ è un termine chiuso oppure un termine le cui variabili non compaiono quantificate in $\boldsymbol{\varphi}$ oppure se $\boldsymbol{x}$ non occorre libera in $\boldsymbol{\varphi}$, allora $\boldsymbol{t}$ è sostituibile ad $\boldsymbol{x}$ in $\boldsymbol{\varphi}$.

(ii) Supponiamo $\boldsymbol{y}$ sia sostituibile ad $\boldsymbol{x}$ in $\boldsymbol{\varphi}$. Dimostrare che

$$(\boldsymbol{\varphi}[\boldsymbol{y}/\boldsymbol{x}])[\boldsymbol{x}/\boldsymbol{y}] = \boldsymbol{\varphi}\,.$$

La notazione $\mathcal{A} \models \boldsymbol{\varphi}[g]$ può risultare lievemente ambigua quando $\boldsymbol{\varphi}$ è della forma $\boldsymbol{\psi}[\boldsymbol{t}/\boldsymbol{x}]$, cioè quando $\boldsymbol{\varphi}$ è della forma $\boldsymbol{\psi}[\boldsymbol{t}/\boldsymbol{x}]$, cioè quando $\boldsymbol{\varphi}$ è ottenuta da $\boldsymbol{\psi}$ sostituendo il termine $\boldsymbol{t}$ alla variabile $\boldsymbol{x}$, per cui scriveremo $\mathcal{A} \models (\boldsymbol{\psi}[\boldsymbol{t}/\boldsymbol{x}])\,[g]$.

Proposizione 21.15. *Supponiamo che $\boldsymbol{t}$ sia sostituibile in $\boldsymbol{\varphi}$ per la variabile $\boldsymbol{x}$. Sia g un'assegnazione in una $\boldsymbol{L}$-struttura $\mathcal{A}$ e sia $a = \boldsymbol{t}^{\mathcal{A}}[g] \in A \stackrel{\text{def}}{=} \|\mathcal{A}\|$. Allora*

$$\mathcal{A} \models (\boldsymbol{\varphi}[\boldsymbol{t}/\boldsymbol{x}])\,[g] \quad \Leftrightarrow \quad \mathcal{A} \models \boldsymbol{\varphi}[g_{a/\boldsymbol{x}}]\,.$$

Dimostrazione. Se $\boldsymbol{\varphi}$ è atomica, o $\boldsymbol{\varphi}$ è $\boldsymbol{\neg\psi}$, oppure $\boldsymbol{\varphi}$ è $\boldsymbol{\psi \vee \chi}$, il risultato è banale. Supponiamo $\boldsymbol{\varphi}$ sia $\boldsymbol{\exists y\,\psi}$ e distinguiamo due casi.

Caso 1: $\boldsymbol{y = x}$. Allora $\boldsymbol{x}$ non occorre libera in $\boldsymbol{\varphi}$ e quindi $\boldsymbol{\varphi}[\boldsymbol{t}/\boldsymbol{x}]$ è $\boldsymbol{\varphi}$ e g e $g_{a/\boldsymbol{x}}$ coincidono sulle variabili libere di $\boldsymbol{\varphi}$. Segue che

$$\begin{aligned} \mathcal{A} \models (\boldsymbol{\varphi}[\boldsymbol{t}/\boldsymbol{x}])\,[g] &\Leftrightarrow \mathcal{A} \models \boldsymbol{\varphi}[g] \\ &\Leftrightarrow \mathcal{A} \models \boldsymbol{\varphi}[g_{a/\boldsymbol{x}}] \qquad \text{(per il Lemma 21.5)} \end{aligned}$$

Caso 2: $\boldsymbol{y \neq x}$. Allora $\boldsymbol{\varphi[t/x]}$ è $\boldsymbol{\exists y\, \psi[t/x]}$ e dato che $\boldsymbol{y}$ non occorre in $\boldsymbol{t}$, per ogni $b \in A$ si ha

$$a = \boldsymbol{t}^{\mathcal{A}}[g] = \boldsymbol{t}^{\mathcal{A}}[g_{b/\boldsymbol{y}}]\,. \tag{102}$$

Quindi

$$\begin{aligned}
\mathcal{A} \models (\boldsymbol{\varphi}[\boldsymbol{t}/\boldsymbol{x}])\,[g] &\Leftrightarrow \exists b \in A\ \mathcal{A} \models (\boldsymbol{\psi}[\boldsymbol{t}/\boldsymbol{x}])\,[g_{b/\boldsymbol{y}}] \\
&\Leftrightarrow \exists b \in A\ \mathcal{A} \models \boldsymbol{\psi}[(g_{b/\boldsymbol{y}})_{a/\boldsymbol{x}}] \qquad \text{(per ipo. ind. e (102))} \\
&\Leftrightarrow \exists b \in A\ \mathcal{A} \models \boldsymbol{\psi}[(g_{a/\boldsymbol{x}})_{b/\boldsymbol{y}}] \qquad \text{(per l'Esercizio 21.3)} \\
&\Leftrightarrow \mathcal{A} \models \boldsymbol{\exists y\, \psi}[g_{a/\boldsymbol{x}}] \\
&\Leftrightarrow \mathcal{A} \models \boldsymbol{\varphi}[g_{a/\boldsymbol{x}}]\,.
\end{aligned}$$

Il caso in cui $\boldsymbol{\varphi}$ è $\boldsymbol{\forall y\, \psi}$ è lasciato al lettore. □

Siamo ora in grado di dimostrare che la seguente formula è logicamente valida:

$$\boldsymbol{\forall x\, \varphi \Rightarrow \varphi[t/x]}$$

se $\boldsymbol{t}$ è sostituibile ad $\boldsymbol{x}$ in $\boldsymbol{\varphi}$. Per vedere ciò supponiamo che $\mathcal{A} \models \boldsymbol{\forall x\, \varphi}[g]$ e cerchiamo di verificare che $\mathcal{A} \models (\boldsymbol{\varphi}[\boldsymbol{t}/\boldsymbol{x}])\,[g]$. Per la Proposizione 21.15 questo è equivalente a dimostrare che $\mathcal{A} \models \boldsymbol{\varphi}[g_{a/\boldsymbol{x}}]$, il che è una conseguenza immediata della nostra ipotesi.

21.D.6. *Predicati* 1*-ari.* Sia $\boldsymbol{L}$ un linguaggio contenente un predicato 1-ario $\boldsymbol{P}$. L'enunciato

$$\boldsymbol{\exists x\, (P(x) \Rightarrow \forall x\, P(x))}$$

asserisce che se c'è un oggetto che gode della proprietà $\boldsymbol{P}$, allora tutti gli oggetti godono della proprietà $\boldsymbol{P}$. Data una qualsiasi struttura $\mathcal{A}$, se c'è un $a \notin \boldsymbol{P}^{\mathcal{A}}$ allora assegnando a a $\boldsymbol{x}$, si vede che

$$\mathcal{A} \models (\boldsymbol{P(x) \Rightarrow \forall x\, P(x)})\,[a] \tag{103}$$

in quanto l'assunzione nell'implicazione è falsa. Viceversa, se $\boldsymbol{P}^{\mathcal{A}} = A$, allora assegnando ad $\boldsymbol{x}$ un elemento arbitrario $a \in \|\mathcal{A}\|$, si ha che (103) vale.

21.D.7. *Una formula sorprendente.* L'enunciato del linguaggio $\boldsymbol{L}_{\mathrm{sgr}} = \{*\}$ (Esempio 20.C.2)

$$\boldsymbol{\forall x \forall y \forall z\, ((x * y) * z \equiv y) \Rightarrow \forall x \forall y\, (x \equiv y)}$$

è logicamente valido. Per vedere ciò consideriamo una $\boldsymbol{L}_{\mathrm{sgr}}$-struttura

$$\mathcal{A} = \langle A, \cdot \rangle$$

che soddisfa l'antecedente di questa implicazione, cioè tale che per ogni $x, y, z \in A$

$$(x \cdot y) \cdot z = y\,. \tag{104}$$

Dobbiamo verificare che $\mathcal{A} \models \boldsymbol{\forall x \forall y}\,(\boldsymbol{x \equiv y})$, cioè che A è un singoletto. Sostituendo y al posto di x nella (104) si ottiene $(x * x) * z = x$ e quindi

$$\forall x, y, z \in A\,[((x \cdot x) \cdot z) \cdot y = x \cdot y]\,. \tag{105}$$

Se invece sostituiamo nella (104) $x \cdot x$, z e y al posto di x, y e z, rispettivamente, si ottiene

$$\forall x, y, z \in A\,[((x \cdot x) \cdot z) \cdot y = z]$$

che assieme alla (105) implica $\forall x, y, z \in A\,[x \cdot y = z]$. Ma da questo si deduce subito che A deve essere un singoletto, come richiesto.

Quest'ultimo esempio ci fa vedere come non è sempre immediato stabilire se una formula sia logicamente valida o meno. Infatti si può dimostrare che non c'è nessun algoritmo in grado di stabilire la validità di una formula in un dato linguaggio. Tutto ciò è in netto contrasto con il calcolo proposizionale (§13), dove c'è un algoritmo (le tavole di verità) per stabilire se o meno una proposizione è una tautologia.

Esercizi

Esercizio 21.16. Dimostrare che se $\boldsymbol{s}$ e $\boldsymbol{t}$ sono sostituibili a $\boldsymbol{x}$ in $\boldsymbol{\varphi}$, allora

$$\boldsymbol{s \equiv t \Rightarrow \big(\varphi[s/x] \Leftrightarrow \varphi[t/x]\big)},$$

è logicamente valida.

Esercizio 21.17. Dimostrare che se $\boldsymbol{t}$ non è sostituibile ad $\boldsymbol{x}$ in $\boldsymbol{\varphi}$, allora $\boldsymbol{\forall x\, \varphi \Rightarrow \varphi[t/x]}$ non è logicamente valida.

22. Modelli

Definizione 22.1. Se $\mathcal{A} \in \mathfrak{Str}(\boldsymbol{L})$ e Σ è un insieme di enunciati, $\mathcal{A}$ è un **modello** di Σ se $\mathcal{A} \models \boldsymbol{\sigma}$, per ogni $\boldsymbol{\sigma} \in \Sigma$ e scriveremo

$$\mathcal{A} \models \Sigma\,.$$

$\mathfrak{Mod}_{\boldsymbol{L}}(\Sigma)$ è la classe delle $\boldsymbol{L}$-strutture che sono modelli di Σ. (Quando $\boldsymbol{L}$ è chiaro dal contesto scriveremo semplicemente $\mathfrak{Mod}(\Sigma)$.) Se Σ è un singoletto $\{\boldsymbol{\sigma}\}$, scriveremo $\mathfrak{Mod}(\boldsymbol{\sigma})$ invece di $\mathfrak{Mod}(\{\boldsymbol{\sigma}\})$.

Notazione. La scrittura

$$\bigvee_{1 \leq i \leq n} \boldsymbol{\varphi}_i$$

denota la disgiunzione $(\dots(\boldsymbol{\varphi}_1 \vee \boldsymbol{\varphi}_2) \vee \dots) \vee \boldsymbol{\varphi}_n$. Poichè $\boldsymbol{\varphi}_i \vee \boldsymbol{\varphi}_j$ è vera in $\mathcal{A}$ per l'assegnazione g se e solo se è vera $\boldsymbol{\varphi}_i$ oppure $\boldsymbol{\varphi}_j$, l'ordine con cui associamo le formule è irrilevante e quindi ha senso scrivere

$$\mathcal{A} \models \bigvee \Gamma[g]$$

per denotare $\mathcal{A} \models (\boldsymbol{\varphi}_1 \vee \dots \vee \boldsymbol{\varphi}_n)\,[g]$, dove $\Gamma = \{\boldsymbol{\varphi}_1, \dots, \boldsymbol{\varphi}_n\}$ è un insieme *finito* di formule. Analogamente possiamo definire

$$\bigwedge_{1 \le i \le n} \boldsymbol{\varphi}_i$$

e $\mathcal{A} \models \bigwedge \Gamma[g]$, con Γ finito. Infine, se $\mathcal{A}$ è una struttura, scriveremo "$\bar{a} \in A$" invece di "$a_1, \dots, a_n \in \|\mathcal{A}\|$".

Una classe di strutture $\mathfrak{K} \subseteq \mathfrak{Str}(\boldsymbol{L})$ è una

classe elementare in $\boldsymbol{L}$, in simboli: $\mathrm{EC}(\boldsymbol{L})$, sse

$$\mathfrak{K} = \mathfrak{Mod}(\boldsymbol{\sigma})$$

per qualche $\boldsymbol{L}$-enunciato $\boldsymbol{\sigma}$;

classe elementare generalizzata in $\boldsymbol{L}$, in simboli: $\mathrm{EC}_\Delta(\boldsymbol{L})$, sse

$$\mathfrak{K} = \mathfrak{Mod}(\Sigma)$$

per qualche insieme di $\boldsymbol{L}$-enunciati Σ.

classe pseudo-elementare in $\boldsymbol{L}$, in simboli: $\mathrm{PC}(\boldsymbol{L})$, sse

$$\mathfrak{K} = \left\{ \mathcal{A}' \upharpoonright \boldsymbol{L} \mid \mathcal{A}' \in \mathfrak{K}' \right\}$$

dove $\mathfrak{K}'$ è elementare in qualche linguaggio $\boldsymbol{L}' \supseteq \boldsymbol{L}$;

classe pseudo-elementare generalizzata in $\boldsymbol{L}$, in simboli: $\mathrm{PC}_\Delta(\boldsymbol{L})$, sse

$$\mathfrak{K} = \left\{ \mathcal{A}' \upharpoonright \boldsymbol{L} \mid \mathcal{A}' \in \mathfrak{K}' \right\}$$

dove $\mathfrak{K}'$ è elementare generalizzata in qualche linguaggio $\boldsymbol{L}' \supseteq \boldsymbol{L}$.[3]

Dalla definizione discende che

$$\begin{array}{ccc} \mathrm{EC} & \Longrightarrow & \mathrm{PC} \\ \Downarrow & & \Downarrow \\ \mathrm{EC}_\Delta & \Longrightarrow & \mathrm{PC}_\Delta \end{array}$$

Se $\mathfrak{K} = \mathfrak{Mod}(\Sigma)$ e Σ è finito allora $\mathfrak{K} = \mathfrak{Mod}(\bigwedge \Sigma)$ è EC. Per questo motivo, le classi elementari si dicono anche **finitamente assiomatizzabili**, mentre le classi elementari generalizzate si dicono **assiomatizzabili**. Osserviamo che $\emptyset$ e $\mathfrak{Str}(\boldsymbol{L})$ sono sempre finitamente assiomatizzabili, per ogni $\boldsymbol{L}$. Se $\mathfrak{K}$ è

[3] Gli acronimi EC e PC stanno per *Elementary Class* e *Pseudo-elementary Class*.

$\mathfrak{Mod}(\boldsymbol{\sigma})$ allora anche $\mathfrak{Str}(\boldsymbol{L})\setminus\mathfrak{K} = \mathfrak{Mod}(\boldsymbol{\neg\sigma})$. In altre parole: il complemento di una classe elementare è elementare.

Spesso in logica un insieme di enunciati si dice **teoria del prim'ordine** o, semplicemente, **teoria**. Un insieme di assiomi per una teoria T è un insieme Σ di enunciati tale che

$$\mathfrak{Mod}(\Sigma) = \mathfrak{Mod}(T)\,.$$

Una teoria T si dice **finitamente assiomatizzabile** se ammette un insieme finito di assiomi, ovvero se $\mathfrak{Mod}(T)$ è una classe elementare.

22.A. Esempi. Vedremo ora alcuni esempi di classi di strutture matematiche che sono assiomatizzabili.

22.A.1. *Insiemi infiniti.* Consideriamo il linguaggio minimale $\boldsymbol{L}_\emptyset$ dell'Esempio 20.C.1. Le formule atomiche sono della forma $\boldsymbol{x} \equiv \boldsymbol{y}$ e le $\boldsymbol{L}$-strutture sono gli insiemi non-vuoti. L'enunciato $\boldsymbol{\varepsilon}_{\geq n}$ (con $n \geq 2$) definito da

$$\boldsymbol{\exists x}_1 \ldots \boldsymbol{\exists x}_n \Big(\bigwedge_{1\leq i<j\leq n} \boldsymbol{x}_i \not\equiv \boldsymbol{x}_j \Big) \tag{106}$$

asserisce che ci sono almeno n oggetti distinti, quindi

$$A \models \boldsymbol{\varepsilon}_{\geq n} \quad \Leftrightarrow \quad |A| \geq n\,.$$

$A \models \{\, \boldsymbol{\varepsilon}_{\geq n} \mid n \geq 2 \,\}$ se e solo se $|A| \geq \omega$. Se $\boldsymbol{\varepsilon}_{\leq n}$ è l'enunciato $\boldsymbol{\neg}(\boldsymbol{\varepsilon}_{\geq n+1})$, si ha che $A \models \boldsymbol{\varepsilon}_{\leq n}$ se e solo se $|A| \leq n$. L'enunciato

$$\boldsymbol{\varepsilon}_n \stackrel{\text{def}}{=} \boldsymbol{\varepsilon}_{\leq n} \boldsymbol{\wedge} \boldsymbol{\varepsilon}_{\geq n} \tag{107}$$

asserisce che esistono esattamente n elementi, quindi $|A| = n$ se e solo se $A \models \boldsymbol{\varepsilon}_n$. Quindi $\{\, \boldsymbol{\varepsilon}_{\geq n} \mid n \geq 2 \,\}$ è la teoria degli insiemi infiniti.

22.A.2. *Gruppi privi di torsione.* La classe dei gruppi è assiomatizzabile nel linguaggio dei gruppi

$$\boldsymbol{L}_{\mathrm{grp}} = \{*, {}^{-1}, \boldsymbol{e}\}$$

mediante gli enunciati

$$\boldsymbol{\forall x}\,\boldsymbol{\forall y}\,\boldsymbol{\forall z}\,((\boldsymbol{x} * \boldsymbol{y}) * \boldsymbol{z} \equiv \boldsymbol{x} * (\boldsymbol{y} * \boldsymbol{z})) \tag{A}$$

$$\boldsymbol{\forall x}\,(\boldsymbol{x} * \boldsymbol{e} \equiv \boldsymbol{x} \;\boldsymbol{\wedge}\; \boldsymbol{e} * \boldsymbol{x} \equiv \boldsymbol{x}) \tag{N}$$

$$\boldsymbol{\forall x}\,\big(\boldsymbol{x} * \boldsymbol{x}^{-1} \equiv \boldsymbol{e} \;\boldsymbol{\wedge}\; \boldsymbol{x}^{-1} * \boldsymbol{x} \equiv \boldsymbol{e}\big) \tag{I}$$

vale a dire la proprietà associativa, l'esistenza dell'elemento neutro, l'esistenza di inversi. Le teoria dei gruppi (nel linguaggio $\boldsymbol{L}_{\mathrm{grp}}$) ha per assiomi (A), (N) e (I). Se scegliamo di lavorare in un linguaggio $\boldsymbol{L}$ più povero, contenente solo il simbolo di operazione $*$ e il simbolo per l'elemento neutro $\boldsymbol{e}$, dobbiamo rimpiazzare (I) con

$$\boldsymbol{\forall x}\,\boldsymbol{\exists y}\,(\boldsymbol{x} * \boldsymbol{y} \equiv \boldsymbol{e} \;\boldsymbol{\wedge}\; \boldsymbol{y} * \boldsymbol{x} \equiv \boldsymbol{e})\,. \tag{I$'$}$$

Sia $\boldsymbol{x}^n$ ($n \in \omega$) il termine definito nell'Esempio 20.C.2 e consideriamo l'enunciato

$$(\boldsymbol{\tau}_n) \qquad \forall \boldsymbol{x}\,(\boldsymbol{x} \not\equiv \boldsymbol{e} \Rightarrow \boldsymbol{x}^n \not\equiv \boldsymbol{e})\,.$$

Una $\boldsymbol{L}_{\mathrm{grp}}$-struttura $\mathcal{G}$ è un gruppo privo di elementi di torsione se e solo se

$$\mathcal{G} \models \{(\mathrm{A}), (\mathrm{N}), (\mathrm{I})\} \cup \{\, \boldsymbol{\tau}_n \mid n \geq 1 \,\}\,.$$

Quindi la classe dei gruppi privi di torsione è EC_Δ in $\boldsymbol{L}_{\mathrm{grp}}$ e $\{(\mathrm{A}), (\mathrm{N}), (\mathrm{I})\} \cup \{\, \boldsymbol{\tau}_n \mid n \geq 1 \,\}$ è la teoria dei gruppi privi di torsione.

22.A.3. *Polinomi.* Nel linguaggio $\boldsymbol{L}_{\mathrm{ring}} = \{+, \cdot, -, \mathbf{0}, \mathbf{1}\}$, introdotto in 20.C.3 a pagina 164, le classi degli anelli unitari, dei domini di integrità, dei campi, etc. sono elementari.

Se $\mathcal{A} \in \mathfrak{Str}(\boldsymbol{L}_{\mathrm{ring}})$ è un anello commutativo unitario, l'insieme

$$A^* = \left\{ \boldsymbol{t}^{\mathcal{A}} \mid \boldsymbol{t} \text{ termine chiuso di } \boldsymbol{L}_{\mathrm{ring}} \right\}$$

è il sotto-anello minimale di A, cioè quello generato dall'unità. Se le variabili di $\boldsymbol{t}$ sono $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n, \boldsymbol{y}_1, \ldots, \boldsymbol{y}_m$, allora il termine $\boldsymbol{t}$ determina un elemento di $A^*[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$ l'anello dei polinomi in $n+m$ variabili a coefficienti in A^*. Viceversa, ogni polinomio di $A[X_1, \ldots, X_n]$ è della forma $p(a_1, \ldots, a_m)$, dove $p \in A^*[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$ e $a_1, \ldots, a_m \in A$, cioè è ottenuto da un polinomio a coefficienti in A^* in $n+m$ variabili rimpiazzando m variabili con elementi di A, per qualche m. In particolare ogni polinomio di

$$a_n X^n + \cdots + a_1 X + a_0 \in A[X]$$

è determinato da un termine $\boldsymbol{y}_n \cdot \boldsymbol{x}^n + \cdots + \boldsymbol{y}_1 \cdot \boldsymbol{x} + \boldsymbol{y}_0$ e da un $n+1$-upla $(a_n, \ldots, a_0)$ di elementi di A. L'enunciato $\boldsymbol{\varphi}_n$

$$\forall \boldsymbol{y}_n \ldots \forall \boldsymbol{y}_0\,(\boldsymbol{y}_n \not\equiv \mathbf{0} \Rightarrow \exists \boldsymbol{x}\,(\boldsymbol{y}_n \cdot \boldsymbol{x}^n + \ldots + \boldsymbol{y}_1 \cdot \boldsymbol{x} + \boldsymbol{y}_0 \equiv \mathbf{0}))\,,$$

dove $\boldsymbol{x}^n$ è definito come nell'Esempio 20.C.2, significa che ogni polinomio di grado n ha almeno una radice. Quindi se $\mathcal{A}$ è un campo, $\mathcal{A} \models \{\, \boldsymbol{\varphi}_n \mid n \geq 1 \,\}$ se e solo se è algebricamente chiuso. In altre parole: la classe dei campi algebricamente chiusi è EC_Δ in $\boldsymbol{L}_{\mathrm{ring}}$.

A volte non è così immediato stabilire che una classe $\mathfrak{K}$ è elementare. Consideriamo il caso degli anelli **locali**, cioè anelli commutativi unitari con un unico ideale massimale. Questa definizione usa una quantificazione sui *sottoinsiemi* dell'anello (e non sugli elementi) e quindi non può essere tradotta in una formula di $\boldsymbol{L}_{\mathrm{ring}}$ o di una qualche sua estensione. Tuttavia la classe degli anelli locali è elementare in $\boldsymbol{L}_{\mathrm{ring}}$ (Esercizio 22.9.)

22.A.4. *Ordini.* Consideriamo il linguaggio $\boldsymbol{L}_{\mathrm{ord}} = \{\leq\}$. La classe dei preordini, degli ordini, degli ordini lineari, etc. sono elementari. La classe degli ordini mal-fondati è PC_Δ in $\boldsymbol{L}_{\mathrm{ord}}$: infatti basta considerare gli enunciati che caratterizzano gli ordini (proprietà riflessiva, antisimmetrica e transitiva) con in aggiunta gli enunciati

$$(\boldsymbol{c}_{n+1} \leq \boldsymbol{c}_n) \boldsymbol{\wedge} \boldsymbol{\neg} (\boldsymbol{c}_n \leq \boldsymbol{c}_{n+1})$$

dove le $\boldsymbol{c}_n$ sono delle costanti.

22.A.5. *Il calcolo proposizionale.* Fissato un insieme L di lettere, nella sezione 13 abbiamo definito l'insieme $\mathrm{Prop}(L)$ delle proposizioni su L. Il linguaggio $\boldsymbol{L}$ associato ad L ha un unico simbolo di relazione 1-ario $\boldsymbol{U}$ e un simbolo di costante $\mathring{A}$, per ogni $A \in L$. Ad ogni $\boldsymbol{p}$ possiamo associare un enunciato $\boldsymbol{\sigma_p} \in \mathrm{Sent}(\boldsymbol{L})$: alle lettere proposizionali $A \in L$ associamo l'enunciato $\boldsymbol{U}(\mathring{A})$, e poi estendiamo l'assegnazione in modo ovvio, ponendo $\boldsymbol{p} \boldsymbol{\vee} \boldsymbol{q} \mapsto \boldsymbol{\sigma_p} \boldsymbol{\vee} \boldsymbol{\sigma_q}$, $\boldsymbol{\neg p} \mapsto \boldsymbol{\neg \sigma_p}$, etc. Sempre nella sezione 13 abbiamo definito una valutazione per $\mathrm{Prop}(L)$ come una funzione $\mathcal{V}\colon L \to \{0,1\}$. Ogni valutazione $\mathcal{V}$ determina una $\boldsymbol{L}$-struttura

$$\mathcal{M}_{\mathcal{V}} = \langle L, \{\, A \in L \mid \mathcal{V}(A) = 1 \,\}, A \rangle_{A \in L}$$

dove $\{\, A \in L \mid \mathcal{V}(A) = 1 \,\}$ è l'interpretazione di $\boldsymbol{U}$ e A è l'interpretazione di $\mathring{A}$. Viceversa, ad ogni $\boldsymbol{L}$-struttura $\mathcal{M} = \langle M, \boldsymbol{U}^{\mathcal{M}}, \mathring{A}^{\mathcal{M}} \rangle_{A \in L}$ associamo la valutazione

$$\mathcal{V}_{\mathcal{M}}(A) = 1 \Leftrightarrow \mathring{A}^{\mathcal{M}} \in \boldsymbol{U}^{\mathcal{M}}.$$

Una facile induzione sull'altezza delle formule dimostra che

$$\begin{aligned} \mathcal{V}(\boldsymbol{p}) = 1 \quad &\Leftrightarrow \quad \mathcal{M}_{\mathcal{V}} \models \boldsymbol{\sigma_p} \qquad \text{e} \\ \mathcal{M} \models \boldsymbol{\sigma_p} \quad &\Leftrightarrow \quad \mathcal{V}_{\mathcal{M}}(\boldsymbol{p}) = 1\,. \end{aligned}$$

22.B. Due teorie molto particolari*. Le teorie degli esempi nella sezione 22.A cercano di descrivere le proprietà che valgono in tutte le strutture di una certa classe. Per esempio gli assiomi della teoria dei gruppi descrivono le proprietà che rendono una struttura di $\boldsymbol{L}_{\mathrm{grp}}$ un gruppo e un discorso analogo può essere fatto per la teoria delle algebre di Boole, degli anelli, degli ordini lineari densi, etc.[4] Ci sono però altre teorie (cioè sistemi di enunciati) che cercano di descrivere *una specifica struttura*, piuttosto che una classe di strutture di un certo tipo di similarità e l'esempio più antico è la geometria Euclidea, in cui gli assiomi descrivono le proprietà della geometria piana. Due altre teorie di questo genere sono l'**aritmetica di Peano** e la teoria degli insiemi.

[4] Da un certo punto di vista, sarebbe più giusto parlare di *definizioni di gruppo* piuttosto che di *assiomi di gruppo*.

22.B.1. *L'aritmetica d Peano.* Il linguaggio $\boldsymbol{L}_{\mathsf{PA}}$ contiene un simbolo di funzione 1-aria $\boldsymbol{s}$, due simboli di funzione 2ari $+$ e $\cdot$ e un simbolo di costante $\mathbf{0}$. Diamo ora una famiglia di enunciati che caratterizzano (o meglio: cercano di caratterizzare) la struttura $\langle \mathbb{N}, \mathbf{S}, +, \cdot, 0\rangle$:

(PA.1) $\forall \boldsymbol{x}\,(\boldsymbol{x} \not\equiv \mathbf{0} \Rightarrow \exists \boldsymbol{y}\,(\boldsymbol{s}(\boldsymbol{y}) \equiv \boldsymbol{x}))$, cioè ogni numero non nullo è il successore di qualche numero;

(PA.2) $\neg\exists \boldsymbol{x}\,(\boldsymbol{s}(\boldsymbol{x}) \equiv \mathbf{0})$, cioè 0 non è il successore di alcun numero;

(PA.3) $\forall \boldsymbol{x} \forall \boldsymbol{y}\,(\boldsymbol{s}(\boldsymbol{x}) \equiv \boldsymbol{s}(\boldsymbol{y}) \Rightarrow \boldsymbol{x} \equiv \boldsymbol{y})$, cioè, prendendo il contrappositivo, numeri distinti hanno successori distinti;

(PA.4) per ogni formula $\boldsymbol{\varphi}(\boldsymbol{x}, \boldsymbol{y}_1, \ldots, \boldsymbol{y}_n)$ in cui la $\boldsymbol{x}$ occorra libera,

$$\forall \boldsymbol{y}_1, \ldots, \boldsymbol{y}_n \Big[\boldsymbol{\varphi}(\mathbf{0}, \boldsymbol{y}_1, \ldots, \boldsymbol{y}_n) \wedge \forall \boldsymbol{x} \big(\boldsymbol{\varphi}(\boldsymbol{x}, \boldsymbol{y}_1, \ldots, \boldsymbol{y}_n) \Rightarrow \boldsymbol{\varphi}(\boldsymbol{s}(\boldsymbol{x}), \boldsymbol{y}_1, \ldots, \boldsymbol{y}_n) \big) \Rightarrow \forall \boldsymbol{x}\, \boldsymbol{\varphi}(\boldsymbol{x}, \boldsymbol{y}_1, \ldots, \boldsymbol{y}_n) \Big]$$

vale a dire: vale il principio di induzione per l'insieme dei numeri definiti dalla formula $\boldsymbol{\varphi}$;

(PA.5) $\forall \boldsymbol{x}\,(\boldsymbol{x} + \mathbf{0} \equiv \boldsymbol{x})$;

(PA.6) $\forall \boldsymbol{x} \forall \boldsymbol{y}\,(\boldsymbol{x} + \boldsymbol{s}(\boldsymbol{y}) \equiv \boldsymbol{s}(\boldsymbol{x} + \boldsymbol{y}))$;

(PA.7) $\forall \boldsymbol{x}\,(\boldsymbol{x} \cdot \mathbf{0} \equiv \mathbf{0})$;

(PA.8) $\forall \boldsymbol{x} \forall \boldsymbol{y}\,(\boldsymbol{x} \cdot \boldsymbol{s}(\boldsymbol{y}) \equiv \boldsymbol{x} \cdot \boldsymbol{y} + \boldsymbol{x})$.

Gli assiomi (PA.1)–(PA.8) sono noti come **assiomi dell'aritmetica di Peano**: i primi quattro sono gli analoghi degli assiomi di Dedekind-Peano (DPA.1)–(DPA.4) di pagina 73, mentre (PA.5)–(PA.8) servono per caratterizzare la somma e il prodotto. L'analogia con i postulati di Dedekind-Peano non deve indurre a pensare che le due trattazioni siano equivalenti. Infatti (PA.1)–(PA.8) sono formule (anzi: enunciati) del prim'ordine nel linguaggio $\boldsymbol{L}_{\mathsf{PA}}$, con l'intendimento che il principio d'induzione (PA.4) è in realtà una famiglia infinita di assiomi, un per ogni $\boldsymbol{\varphi}$. (Per questo motivo si dice che (PA.4) è uno *schema di assiomi*.) Invece l'assioma (DPA.4) non è una formula del prim'ordine, in quanto si quantifica su *sottoinsiemi arbitrari* P della struttura. Questa differenza, che a prima vista sembra modesta, è in realtà cruciale: per il Teorema 9.2 gli assiomi di Dedekind-Peano (DPA.1)–(DPA.4) caratterizzano i naturali a meno di isomorfismo, mentre per un risultato che vedremo nelle prossime sezioni (Teorema 23.10) ci sono modelli degli assiomi (PA.1)–(PA.8) di cardinalità arbitrariamente grande. Di più: ci sono modelli *numerabili* di questi assiomi che non sono isomorfi ad $\mathbb{N}$.

Osservazione 22.2. È possibile dedurre una serie di conseguenze logiche dagli assiomi dell'aritmetica di Peano (PA.1)–(PA.8). Per esempio potremmo

dimostrare che ogni numero è pari o dispari, in simboli

$$\forall \boldsymbol{x}\,(\boldsymbol{x} \not\equiv \mathbf{0} \Rightarrow \exists \boldsymbol{y}\,(\boldsymbol{x} \equiv \boldsymbol{s}(\boldsymbol{y}))\,. \tag{108}$$

La dimostrazione di questi fatti (cioè le usuali argomentazioni matematiche) può essere formalizzata in maniera soddisfacente: nella sezione 27.A vedremo che un'usuale dimostrazione matematica, come per esempio la deduzione di (108) a partire da (PA.1)–(PA.8), può essere visto come una stringa finita di formule. Osserviamo che questo modo di procedere è completamente diverso a quello adottato negli esempi della sezione 22.A dove consideravamo tutti i possibili modelli di una teoria T per "dimostrare" un enunciato a partire da T. Il fatto che i due approcci (considerare gli enunciati veri in tutti i modelli oppure dedurre a partire dagli assiomi) siano equivalenti è il contenuto del Teorema di Completezza forte 28.5.

22.B.2. *La teoria degli insiemi.* Come per l'aritmetica, così gli assiomi della teoria degli insiemi si prefiggono di caratterizzare le proprietà di una singola struttura: l'universo degli insiemi

$$\langle \mathrm{V}, \in \rangle$$

nel caso di ZF e l'aggregato di tutte le classi (proprie e non)

$$\langle \mathscr{C}, \in \rangle$$

nel caso di MK. E qui incontriamo il primo ostacolo: nella definizione (pag 155) abbiamo richiesto che l'universo di una struttura sia un *insieme* e non una classe propria o, ancora peggio, un aggregato di classi proprie, nozione che non è neppure formalizzabile in MK e men che meno in ZF. Il motivo di questa restrizione è presto detto: in ZF la nozione di soddisfazione in una struttura $\mathcal{A}$ è formalizzabile soltanto quando $\|\mathcal{A}\|$ è un insieme ma non per classi proprie quali V, mentre in MK la nozione di soddisfazione può essere data anche per strutture in cui $\|\mathcal{A}\|$ è una classe propria, ma non nel caso in cui $\|\mathcal{A}\|$ sia un aggregato di classi quale $\mathscr{C}$.

Un secondo problema, forse anche più delicato, è il seguente: gli assiomi della teoria degli insiemi introdotti nella sezione 1 sono enti matematici pre-insiemistici, grazie a quali sviluppiamo gli oggetti matematici usuali (i numeri naturali, i reali, gli spazi topologici, etc). In particolare, all'interno di una teoria degli insiemi (sia essa ZF o MK) possiamo introdurre i concetti di linguaggio, formula, modello, teoria etc. Abbiamo un apparente corto-circuito: gli assiomi di ZF o MK dovrebbero essere loro stessi oggetti della trattazione, un po' come se una persona fosse il genitore di un suo antenato. Ma questo circolo vizioso è solo apparente. Innanzitutto si definisce il linguaggio del prim'ordine $\boldsymbol{L}_{\mathrm{set}} = \{\mathring{\in}\}$, dove $\mathring{\in}$ è un simbolo di relazione 2-ario che, per esempio, possiamo identificare con la coppia $(2, 0)$. Quindi $\boldsymbol{L}_{\mathrm{set}}$ è un insieme ed è isomorfo al linguaggio $\boldsymbol{L}_{\mathrm{ord}} = \{<\}$ per gli ordini (vedi 22.A.4).

Possiamo poi definire le formule $\boldsymbol{\varphi}$ di $\boldsymbol{L}_{\text{set}}$ secondo lo schema della sezione 20.D. Osserviamo che la parola "formula" ha due significati distinti:

- Da un lato ci sono le formule di LST denotate mediante lettere greche φ, ψ, χ, ... e descritte in dettaglio nella sezione 1.B. Le "formule" in questa accezione sono enti pre-insiemistici e non sono insiemi.
- D'altro lato ci sono gli elementi di $\mathrm{Fml}(\boldsymbol{L}_{\text{set}})$ che sono denotati con lettere greche in neretto $\boldsymbol{\varphi}$, $\boldsymbol{\psi}$, $\boldsymbol{\chi}$, ... Le "formule" in questa accezione sono insiemi, infatti elementi di V_ω.

Ad ogni formula φ di LST possiamo associare l'analogo elemento di $\mathrm{Fml}(\boldsymbol{L}_{\text{set}})$ e questo elemento viene indicato con $\ulcorner\varphi\urcorner$. Per esempio l'assioma di estensionalità

$$(\mathsf{Ext}) \qquad \forall \mathsf{v}_0\, \forall \mathsf{v}_1\, (\forall \mathsf{v}_2(\mathsf{v}_2 \in \mathsf{v}_0 \Leftrightarrow \mathsf{v}_2 \in \mathsf{v}_1) \Rightarrow \mathsf{v}_0 = \mathsf{v}_1)$$

è una formula (anzi: un enunciato) di LST, mentre la sua codifica in $\boldsymbol{L}_{\text{set}}$ è la stringa

$$(\ulcorner\mathsf{Ext}\urcorner) \qquad \langle \boldsymbol{\forall}, \boldsymbol{v}_0, \boldsymbol{\forall}, \boldsymbol{v}_1, \boldsymbol{\Rightarrow}, \boldsymbol{\forall}, \boldsymbol{v}_2, \boldsymbol{\Leftrightarrow}, \mathring{\in}, \boldsymbol{v}_2, \boldsymbol{v}_0, \mathring{\in}, \boldsymbol{v}_2, \boldsymbol{v}_1, \boldsymbol{\equiv} \boldsymbol{v}_0, \boldsymbol{v}_1 \rangle\,.$$

le liste infinite di assiomi ZF e MK individuano dei sottoinsiemi di $\mathrm{Sent}(\boldsymbol{L}_{\text{set}})$ che indicheremo come $\ulcorner\mathsf{ZF}\urcorner$ e $\ulcorner\mathsf{MK}\urcorner$.

Una $\boldsymbol{L}_{\text{set}}$-struttura è una

$$\mathcal{M} = \langle M, E \rangle$$

tale che $E \subseteq M \times M$.

Esercizio 22.3. Sia $\mathcal{M} = \langle M, E \rangle$. Dimostrare che:

(i) $\mathcal{M}$ soddisfa l'assioma di estensionalità, cioè $\mathcal{M} \models \ulcorner\mathsf{Ext}\urcorner$ se e solo se E è estensionale su M (Definizione 4.16).

(ii) $\mathcal{M}$ soddisfa l'assioma della coppia se e solo se per ogni $x, y \in M$ c'è uno $z \in M$ tale che

$$x\ E\ z\ \wedge\ y\ E\ z\ \wedge\ \forall w \in M\, (w\ E\ z \Rightarrow (w = x\ \vee\ w = y))\,.$$

Con un piccolo abuso di linguaggio, diremo che $\mathcal{M}$ soddisfa ZF o MK se $\mathcal{M}$ soddisfa $\ulcorner\mathsf{ZF}\urcorner$ o $\ulcorner\mathsf{MK}\urcorner$. Osserviamo che

$$\mathcal{M} \models \ulcorner\text{Assioma di Fondazione}\urcorner$$

significa che per ogni $x \in M$ tale che

$$P_x \stackrel{\text{def}}{=} \{\, y \in M \mid y\ E\ x \,\} \neq \emptyset$$

c'è un $\bar{x} \in P_x$ tale che

$$P_x \cap P_{\bar{x}} = \emptyset\,.$$

Questa è un'ipotesi più debole che la ben-fondatezza di E su M, dato che non tutti i sottoinsiemi di M sono della forma P_x per qualche $x \in M$. Quindi è possibile che $\mathcal{M}$ soddisfi gli assiomi di ZF o di MK e pur tuttavia E non sia ben-fondata. Nel caso in cui E sia ben-fondata su M e $\mathcal{M}$ soddisfa l'estensionalità, allora per la Proposizione 4.18

$$\boldsymbol{\pi}_{M,E} \colon \langle M, E\rangle \to \langle \overline{M}, \in\rangle$$

è un isomorfismo e $\overline{M}$ è transitivo. I modelli transitivi, vale a dire della froma $\langle M, \in\rangle$ con M transitivo sono centrali in teoria degli insiemi.

Esercizi

Esercizio 22.4. Sia $\boldsymbol{L}_{\text{sgrp}} = \{*\}$ il linguaggio dei semigruppi (Esempio 20.C.2). Trovare un insieme Σ di $\boldsymbol{L}_{\text{sgrp}}$-enunciati tale che

$$\forall \mathcal{A} \in \mathfrak{Str}(\boldsymbol{L}_{\text{sgrp}})\,(\mathcal{A} \text{ è un gruppo} \Leftrightarrow \mathcal{A} \models \Sigma)\,.$$

Sia $\boldsymbol{L} = \{+, \cdot\}$ il linguaggio con due simboli di operazione binaria. Trovare un insieme Σ di $\boldsymbol{L}$-enunciati tale che

$$\forall \mathcal{A} \in \mathfrak{Str}(\boldsymbol{L})\,(\mathcal{A} \text{ è un campo} \Leftrightarrow \mathcal{A} \models \Sigma)\,.$$

Esercizio 22.5. Sia $\boldsymbol{L} = \{U\}$ il linguaggio con un unico simbolo di relazione 1-aria. Le $\boldsymbol{L}$-strutture $\langle A, B\rangle$ sono insiemi non-vuoti con un sottoinsieme privilegiato.

(i) Quante sono—a meno di isomorfismo—le $\boldsymbol{L}$-strutture di cardinalità n? Di cardinalità $\kappa \geq \omega$?

(ii) Trovare un insieme di enunciati Σ tale che $\langle A, B\rangle \models \Sigma$ se e solo se A, B, $A \setminus B$ sono infiniti.

Esercizio 22.6. Sia $\boldsymbol{L} = \{\boldsymbol{R}\}$ il linguaggio con un unico simbolo di relazione 2-aria. Trovare un sistema di enunciati Σ tale che $\mathcal{A} \models \Sigma$ se e solo se $\boldsymbol{R}^{\mathcal{A}}$ è una funzione $f \colon A \to A$. Aggiungere degli enunciati a Σ in modo che:

(i) f sia iniettiva,

(ii) f sia suriettiva,

(iii) nessuna delle iterate $f^{(n)}$ di f abbia punti fissi.

Esercizio 22.7. Dimostrare che la classe dei campi di caratteristica p (con p numero primo) è EC e che la classe dei campi di caratteristica 0 è EC_Δ.

Esercizio 22.8. Un gruppo abeliano $(G, +)$ è **divisibile** se per ogni $n > 0$ e ogni $x \in G$ c'è un $y \in G$ tale che

$$ny \stackrel{\text{def}}{=} \underbrace{y + \cdots + y}_{n} = x\,.$$

Dimostrare che:

(i) La classe dei gruppi abeliani è EC_Δ nel linguaggio $\{+\}$.

(ii) I gruppi divisibili sono tutti e soli gli spazi vettoriali su $\mathbb{Q}$.

Esercizio 22.9. Dimostrare che un anello commutativo unitario R è locale se e solo se $0 \neq 1$ e x o $1 - x$ è invertibile, per ogni $x \in R$ (si veda [**AM69**]). (Un elemento u di un anello R è invertibile se $uv = 1$, per qualche $v \in R$.)

Verificare che la classe degli anelli locali è elementare in $\boldsymbol{L}_{\mathrm{ring}}$.

Esercizio 22.10. Dimostrare che se $\lambda > \omega$ è limite $\langle \mathrm{V}_\lambda, \in\rangle$ è un modello di ZC Se $\mathcal{M}$ soddisfa un numero sufficiente di assiomi di MK, allora in $\mathcal{M}$ devono esistere classi proprie, cioè devono esistere $x \in \mathrm{V}_\alpha$ tali che $\forall y \in \mathrm{V}_\alpha\,(x \notin y)$. Quindi α deve essere un ordinale successore $\beta \dotplus 1$: gli elementi di V_β sono gli $\mathcal{M}$-insiemi, mentre le $\mathcal{M}$-classi sono gli elementi di $\mathrm{V}_{\beta\dotplus 1} \setminus \mathrm{V}_\beta$. è facile verificare che $\langle \mathrm{V}_{\beta\dotplus 1}, \in\rangle$ è un modello per gli Assiomi di Estensionalità, Costruzione di Classi, Fondazione e Unione.

23. Il teorema di compattezza

Definizione 23.1. Se Σ e Δ sono insiemi di $\boldsymbol{L}$-enunciati, diremo che Δ è una **conseguenza logica di Σ nel linguaggio $\boldsymbol{L}$**, in simboli

$$\Sigma \models_{\boldsymbol{L}} \Delta\,,$$

se $\mathfrak{Mod}(\Sigma) \subseteq \mathfrak{Mod}(\Delta)$, cioè se

$$\forall \mathcal{A} \in \mathfrak{Str}(\boldsymbol{L})\,(\mathcal{A} \models \Sigma \Rightarrow \mathcal{A} \models \Delta)\,.$$

Esercizio 23.2. Se $\boldsymbol{L}' \subseteq \boldsymbol{L}$ e $\Sigma, \Delta \subseteq \mathrm{Sent}(\boldsymbol{L}')$, allora

$$\Sigma \models_{\boldsymbol{L}} \Delta \quad \Leftrightarrow \quad \Sigma \models_{\boldsymbol{L}'} \Delta\,.$$

Quindi la nozione di conseguenza logica essenzialmente non dipende dal linguaggio $\boldsymbol{L}$, per cui diremo semplicemente che Δ è conseguenza logica di Σ. Se $\Sigma = \emptyset$ scriveremo $\models \Delta$ e se Σ e Δ sono i singoletti $\{\boldsymbol{\sigma}\}$ e $\{\boldsymbol{\tau}\}$, scriveremo $\boldsymbol{\sigma} \models \boldsymbol{\tau}$. Due enunciati $\boldsymbol{\sigma}$ e $\boldsymbol{\tau}$ si dicono **logicamente equivalenti** se

Un insieme Σ di $\boldsymbol{L}$-enunciati è **soddisfacibile** se $\mathfrak{Mod}(\Sigma) \neq \emptyset$. Un insieme di enunciati Σ si dice **finitamente soddisfacibile** se e solo se ogni sottoinsieme finito $\Sigma_0 \subseteq \Sigma$ è soddisfacibile. Chiaramente ogni insieme di enunciati soddisfacibile è finitamente soddisfacibile e se l'insieme è finito vale anche il converso. Il seguente **Teorema di Compattezza**, dimostrato da K. Gödel nel 1930, asserisce questo fatto è vero in generale:

Teorema 23.3. *Se Σ è un insieme di enunciati, Σ è finitamente soddisfacibile se e solo se Σ è soddisfacibile.*

La dimostrazione del Teorema è rimandata alla sezione 23.B. Osserviamo che per l'Esempio 22.A.5, questo risultato generalizza il Teorema 14.8 di Compattezza per il calcolo proposizionale.

23.A. Conseguenze del Teorema di Compattezza.

Corollario 23.4. *Se Σ è un insieme di enunciati e $\boldsymbol{\sigma}$ un enunciato, allora $\Sigma \models \boldsymbol{\sigma}$ se e solo se $\Sigma_0 \models \boldsymbol{\sigma}$ per qualche $\Sigma_0 \subseteq \Sigma$ finito.*

Dimostrazione. Se, per assurdo, $\Sigma_0 \not\models \boldsymbol{\sigma}$ per ogni $\Sigma_0 \subseteq \Sigma$ finito, allora $\Sigma \cup \{\boldsymbol{\neg\sigma}\}$ sarebbe finitamente soddisfacibile e quindi soddisfacibile. Ma ogni modello di $\Sigma \cup \{\boldsymbol{\neg\sigma}\}$ è un modello di Σ: contraddizione. □

Teorema 23.5. *Se $\mathfrak{K}$ e $\mathfrak{Str}(\boldsymbol{L}) \setminus \mathfrak{K}$ sono* EC_Δ*, allora $\mathfrak{K}$ e $\mathfrak{Str}(\boldsymbol{L}) \setminus \mathfrak{K}$ sono* EC*.*

Dimostrazione. Supponiamo Σ e Γ siano insiemi di enunciati che assiomatizzano $\mathfrak{K}$ e $\mathfrak{Str}(\boldsymbol{L}) \setminus \mathfrak{K}$, rispettivamente. Allora $\Sigma \cup \Gamma$ non è soddisfacibile e quindi, per compattezza, esistono $\{\boldsymbol{\sigma}_0, \dots, \boldsymbol{\sigma}_n\} \subseteq \Sigma$ e $\{\boldsymbol{\gamma}_0, \dots, \boldsymbol{\gamma}_m\} \subseteq \Gamma$ tali che

$$\{\boldsymbol{\sigma}_0, \dots, \boldsymbol{\sigma}_n, \boldsymbol{\gamma}_0, \dots, \boldsymbol{\gamma}_m\}$$

non è soddisfacibile. Chiaramente

$$\mathcal{A} \in \mathfrak{K} \quad \Rightarrow \quad \mathcal{A} \models \bigwedge_{i \le n} \boldsymbol{\sigma}_i$$

$$\mathcal{A} \notin \mathfrak{K} \quad \Rightarrow \quad \mathcal{A} \models \bigwedge_{i \le m} \boldsymbol{\gamma}_i \,.$$

Se, per assurdo, $\mathcal{A}_0 \models \bigwedge_{i \le n} \boldsymbol{\sigma}_i$ per qualche $\mathcal{A}_0 \notin \mathfrak{K}$, allora

$$\mathcal{A} \models \{\boldsymbol{\sigma}_1, \dots, \boldsymbol{\sigma}_n, \boldsymbol{\gamma}_1, \dots, \boldsymbol{\gamma}_m\} \,,$$

una contraddizione. Quindi $\mathfrak{K}$ è assiomatizzata da $\bigwedge_{i \le n} \boldsymbol{\sigma}_i$ e la classe complementare $\mathfrak{Str}(\boldsymbol{L}) \setminus \mathfrak{K}$ è assiomatizzata da $\bigwedge_{i \le m} \boldsymbol{\gamma}_i$. □

Il seguente risultato fornisce un metodo generale per provare che una classe assiomatizzabile non è finitamente assiomatizzabile, nemmeno ampliando il linguaggio.

Teorema 23.6. *Sia Δ un insieme di enunciati di $\boldsymbol{L}$ e siano $\boldsymbol{\sigma}_n$ degli enunciati di un linguaggio $\boldsymbol{L}' \supseteq \boldsymbol{L}$. Sia $\mathfrak{K} = \mathfrak{Mod}(\Sigma)$, dove $\Sigma = \Delta \cup \{\, \boldsymbol{\sigma}_n \mid n \in \omega \,\}$, così che $\mathfrak{K}$ è una classe* $\mathrm{EC}_\Delta(\boldsymbol{L}')$ *e quindi* $\mathrm{PC}_\Delta(\boldsymbol{L})$*. Supponiamo che*

$$\forall m \in \omega \, (\Delta \cup \{\, \boldsymbol{\sigma}_n \mid n < m \,\} \not\models_{\boldsymbol{L}'} \Sigma) \,.$$

Allora $\mathfrak{K}$ non è $\mathrm{PC}(\boldsymbol{L})$*.*

Dimostrazione. Per assurdo supponiamo esista un linguaggio $\boldsymbol{L}'' \supseteq \boldsymbol{L}$ ed un enunciato $\boldsymbol{\tau} \in \mathrm{Sent}(\boldsymbol{L})$ tali che $\mathfrak{K}$ è la classe delle contrazioni dei modelli di $\boldsymbol{\tau}$,

$$\mathfrak{K} = \left\{ \mathcal{A}'' \restriction \boldsymbol{L} \mid \mathcal{A}'' \in \mathfrak{Mod}_{\boldsymbol{L}''}(\boldsymbol{\tau}) \right\}.$$

Rimpiazzando, se necessario, $\boldsymbol{L}''$ con $\boldsymbol{L}' \cup \boldsymbol{L}''$ possiamo supporre $\boldsymbol{L}' \subseteq \boldsymbol{L}''$. Poiché $\Sigma \models_{\boldsymbol{L}''} \boldsymbol{\tau}$, per il Corollario 23.4 c'è un $\Sigma_0 \subseteq \Sigma$ finito tale che $\Sigma_0 \models_{\boldsymbol{L}''} \boldsymbol{\tau}$ e quindi c'è un $m \in \omega$ tale che

$$\Delta \cup \{ \boldsymbol{\sigma}_n \mid n < m \} \models_{\boldsymbol{L}''} \boldsymbol{\tau}$$

e poiché $\boldsymbol{\tau} \models_{\boldsymbol{L}''} \Sigma$, per transitività della nozione di conseguenza logica si ha che $\Delta \cup \{ \boldsymbol{\sigma}_n \mid n < m \} \models_{\boldsymbol{L}''} \Sigma$ e quindi, per l'Esercizio 23.2, $\Delta \cup \{ \boldsymbol{\sigma}_n \mid n < m \} \models_{\boldsymbol{L}'} \Sigma$, contro la nostra ipotesi. □

Corollario 23.7. *Le seguenti classi son* $\mathrm{EC}_\Delta(\boldsymbol{L})$ *ma non* $\mathrm{PC}(\boldsymbol{L})$*:*

(a) *La classe degli insiemi (gruppi, anelli, campi, ordini, algebre di Boole) infiniti, nel linguaggio minimale* $\boldsymbol{L}_\emptyset$ *(rispettivamente* $\boldsymbol{L}_{\mathrm{grp}}$*,* $\boldsymbol{L}_{\mathrm{ring}}$*, etc.)*

(b) *La classe dei gruppi privi di torsione.*

(c) *La classe dei campi di caratteristica* 0*.*

Quindi, utilizzando il Teorema 23.5 si ha

Corollario 23.8. *Le seguenti classi sono* EC_Δ *ma non* PC*:*

(a) *La classe degli insiemi (gruppi, anelli, campi, ordini, algebre di Boole) finiti.*

(b) *La classe dei gruppi che hanno elementi di torsione.*

(c) *La classe dei campi di caratteristica finita.*

Osservazione 23.9. Il Teorema 23.6 *non dice* che se una classe che ha soltanto strutture infinite allora non è elementare! Infatti ci sono molte classi elementari che hanno solo strutture infinite, per esempio la classe degli ordini lineari densi, la classe delle algebre di Boole prive di atomi, la classe dei corpi non commutativi (Teorema di Wedderburn, vedi pag.248), etc.

Il seguente risultato è noto come "Teorema di Löwenheim-Skolem all'insù".

Teorema 23.10. *Se* Σ *è un insieme di enunciati tale che per ogni* $n > 0$ *esiste un modello di* Σ *con almeno* n *elementi. (In particolare questo vale se* Σ *ha un modello infinito.) Allora* Σ *ha modelli di cardinalità arbitrariamente grande,*

$$\forall \kappa \, \exists \mathcal{B} \in \mathfrak{Mod}(\Sigma) \ \ \mathrm{card}(\mathcal{B}) \geq \kappa \,.$$

Dimostrazione. Sia $\tilde{\boldsymbol{L}} = \boldsymbol{L} \cup \{ \boldsymbol{d}_\alpha \mid \alpha < \kappa \}$ l'espansione di $\boldsymbol{L}$ mediante nuove costanti e sia $\tilde{\Sigma} = \Sigma \cup \{ \boldsymbol{d}_\alpha \not\equiv \boldsymbol{d}_\beta \mid \alpha < \beta < \kappa \} \subseteq \mathrm{Sent}(\tilde{\boldsymbol{L}})$. Sia $\Delta \subseteq \tilde{\Sigma}$ un sottoinsieme finito: allora esiste $n \in \omega$ ed esistono $\{ \alpha_i \mid i < n \} \subseteq \kappa$ tali che

$$\Delta \subseteq \Sigma \cup \left\{ \boldsymbol{d}_{\alpha_i} \not\equiv \boldsymbol{d}_{\alpha_j} \mid 0 \leq i < j < n \right\}.$$

Sia $\mathcal{A} \models \Sigma$ un modello con almeno n elementi $a_0, \ldots, a_{n-1}$ e sia $\tilde{\mathcal{A}}$ l'espansione di $\mathcal{A}$ al linguaggio $\tilde{\boldsymbol{L}}$ così definita:

$$\boldsymbol{d}_\alpha^{\tilde{\mathcal{A}}} = \begin{cases} a_i & \text{se } \alpha = \alpha_i \\ a_0 & \text{altrimenti.} \end{cases}$$

È immediato verificare che $\tilde{\mathcal{A}} \models \Delta$. Abbiamo quindi dimostrato che Σ è finitamente soddisfacibile. Per compattezza c'è un modello $\tilde{\mathcal{B}} \models \tilde{\Sigma}$ la cui cardinalità è $\geq \kappa$, poiché $\boldsymbol{d}_\alpha^{\tilde{\mathcal{A}}} \neq \boldsymbol{d}_\beta^{\tilde{\mathcal{A}}}$ quando $0 < \alpha < \beta < \kappa$. Sia $\mathcal{B}$ la contrazione di $\tilde{\mathcal{B}}$ ad $\boldsymbol{L}$. Allora $\mathcal{B}$ è il modello cercato. □

Corollario 23.11. *Sia Σ un insieme di enunciati i cui modelli sono tutti di cardinalità finita. Allora i modelli di Σ hanno cardinalità uniformemente limitata, cioè*

$$\exists n \in \omega \, \forall \mathcal{A} \in \mathfrak{Mod}(\Sigma) \;\; \mathrm{card}(\mathcal{A}) \leq n \,.$$

Il Teorema 23.10 implica, in particolare, che ci sono gruppi (o gruppi privi di torsione, campi di caratteristica fissata, campi algebricamente chiusi, algebre di Boole, etc.) di cardinalità arbitrariamente grande.

Nella sezione 17 abbiamo dimostrato il Teorema 17.1 di Ramsey nel caso infinito: per ogni insieme infinito A, se coloriamo gli elementi di $[A]^r$ con k colori, allora c'è sempre un $H \subseteq A$ infinito tale che $[H]^r$ è monocromatico. Mediante il Teorema di Compattezza possiamo dimostrare la sua versione finita.

Teorema 23.12 (Teorema di Ramsey nel caso finito)**.** *Per ogni $r, k, n > 0$ esiste un m tale che ogni colorazione $f \colon [m]^r \to k$ ammette un sottoinsieme $H \subseteq m$ monocromatico di cardinalità n.*

Dimostrazione. Per semplicità notazionale supponiamo $r = 2$. Fissiamo $k \geq 2$. Consideriamo il linguaggio $\boldsymbol{L}$ che ha k predicati 2-ari $\boldsymbol{C}_0, \ldots, \boldsymbol{C}_{k-1}$ che rappresentano i colori. Consideriamo l'insieme degli enunciati che asseriscono che ogni coppia non ordinata di oggetti è colorata con un unico colore e che ci sono infiniti elementi:

(i) $\boldsymbol{\forall x \forall y} \, (\boldsymbol{C}_h(\boldsymbol{x}, \boldsymbol{y}) \boldsymbol{\Rightarrow} \boldsymbol{C}_h(\boldsymbol{y}, \boldsymbol{x}))$, per tutti gli $h < k$,

(ii) $\boldsymbol{\forall x \forall y} \left(\boldsymbol{x \not\equiv y} \boldsymbol{\Rightarrow} \bigvee_{h \leq k} \boldsymbol{C}_h(\boldsymbol{x}, \boldsymbol{y}) \right)$,

(iii) $\boldsymbol{\neg \exists x \exists y} \, (\boldsymbol{C}_h(\boldsymbol{x}, \boldsymbol{y}) \boldsymbol{\wedge} \boldsymbol{C}_i(\boldsymbol{x}, \boldsymbol{y}))$, per tutti gli $h < i < k$,

(iv) $\boldsymbol{\varepsilon}_{\geq n}$, per $n > 1$, dove $\boldsymbol{\varepsilon}_{\geq n}$ è come in (106).

Per (iv) se una $\boldsymbol{L}$-struttura $\mathcal{A} = \langle A, \boldsymbol{C}_0^{\mathcal{A}}, \dots, \boldsymbol{C}_{k-1}^{\mathcal{A}} \rangle$ soddisfa Σ allora A è infinito e posto $\bar{C}_i = \{\, \{x, y\} \in [A]^2 \mid (x, y) \in \boldsymbol{C}_i^{\mathcal{A}} \,\}$, gli insiemi $\bar{C}_0, \dots, \bar{C}_{k-1}$ sono disgiunti e $\bar{C}_0 \cup \dots \cup \bar{C}_{k-1} = [A]^2$. Viceversa, se A è infinito e $[A]^2$ è colorato con k colori, cioè ci sono $\bar{C}_0, \dots, \bar{C}_{k-1}$ sottoinsiemi disgiunti di A tali che $\bar{C}_0 \cup \dots \cup \bar{C}_{k-1} = [A]^2$, allora posto $\boldsymbol{C}_i^{\mathcal{A}} = \{\, (x, y) \mid \{x, y\} \in \bar{C}_i \,\}$ si ha che $\mathcal{A} \models \Sigma$. Fissiamo un modello $\mathcal{A}$ di Σ. Per il Teorema 17.1 di Ramsey nel caso infinito c'è un sottoinsieme omogeneo infinito di A. Per ogni n fissato, $\mathcal{A}$ soddisfa l'enunciato $\boldsymbol{\varphi}_n$ che dice:

($\boldsymbol{\varphi}_n$) Ci sono elementi distinti $\boldsymbol{x}_0, \dots, \boldsymbol{x}_{n-1}$ tali che $[\{\boldsymbol{x}_0, \dots, \boldsymbol{x}_{n-1}\}]^2$ è monocromatico di colore $\boldsymbol{C}_h$, per qualche $h < k$

in simboli

$$\boldsymbol{\exists x}_0 \dots \boldsymbol{\exists x}_{n-1} \Big[\bigwedge_{i<j<n} \boldsymbol{x}_i \not\equiv \boldsymbol{x}_j \boldsymbol{\wedge} \big(\bigvee_{h<k} \bigwedge_{i<j<n} \boldsymbol{C}_h(\boldsymbol{x}_i, \boldsymbol{x}_j) \big) \Big] .$$

Essendo $\mathcal{A}$ arbitrario in $\mathfrak{Mod}(\Sigma)$ questo prova che

$$\Sigma \models \boldsymbol{\varphi}_n$$

per ogni n. Per il Teorema di Compattezza, fissato n possiamo trovare un $\Sigma' \subset \Sigma$ finito tale che $\Sigma' \models \boldsymbol{\varphi}_n$. Sia m massimo tale che $\boldsymbol{\varepsilon}_{\geq n} \in \Sigma'$. Una colorazione con k colori di $[m]^2$ induce un modello $\mathcal{A}'$ di Σ' di cardinalità m. Poiché $\mathcal{A}' \models \boldsymbol{\varphi}_n$, ne consegue che c'è un $H \subset m$ di cardinalità n che è monocromatico. □

23.B. Ultraprodotti e compattezza. Il Teorema di Compattezza è una conseguenza del seguente risultato sugli ultraprodotti.

Teorema 23.13 (Łos)**.** *Sia U un ultrafiltro su X e siano $\mathcal{A}_x$ delle $\boldsymbol{L}$-strutture, con $x \in X$. Per ogni formula $\boldsymbol{\varphi}(\boldsymbol{x}_1, \dots, \boldsymbol{x}_n)$ e per ogni $g_1, \dots, g_n \in \bigtimes_{x \in X} A_x$*

$$\prod_U \mathcal{A}_x \models \boldsymbol{\varphi}[[g_1], \dots, [g_n]] \quad \Leftrightarrow \quad X_{\boldsymbol{\varphi}, g_1, \dots, g_n} \in U ,$$

dove $X_{\boldsymbol{\varphi}, g_1, \dots, g_n} = \{\, x \in X \mid \mathcal{A}_x \models \boldsymbol{\varphi}[g_1(x), \dots, g_n(x)] \,\}$.

Dimostrazione. La dimostrazione procede per induzione su $\mathrm{ht}(\boldsymbol{\varphi})$. Se $\boldsymbol{\varphi}$ è atomica, il risultato discende dalla definizione di $\prod_U \mathcal{A}_x$. Negli altri casi, al fine di semplificare la notazione, assumiamo $n = 2$, ma—come risulterà evidente—la dimostrazione è del tutto generale. Se $\boldsymbol{\varphi} = \boldsymbol{\neg\psi}$, allora

$$\begin{aligned} \prod_U \mathcal{A}_x \models \boldsymbol{\varphi}[[g_1], [g_2]] &\Leftrightarrow \prod_U \mathcal{A} \not\models \boldsymbol{\psi}[[g_1], [g_2]] \\ &\Leftrightarrow X_{\boldsymbol{\psi}, g_1, g_2} \notin U \\ &\Leftrightarrow X_{\boldsymbol{\varphi}, g_1, g_2} \in U \end{aligned}$$

dove nell'ultimo passaggio abbiamo usato che $X_{\boldsymbol{\varphi},g_1,g_2} = X \setminus X_{\boldsymbol{\psi},g_1,g_2}$ e la parte (b) della Proposizione 12.7.

Se $\boldsymbol{\varphi} = \boldsymbol{\psi} \boldsymbol{\vee} \boldsymbol{\chi}$, allora

$$\begin{aligned}\prod_U \mathcal{A}_x \models \boldsymbol{\varphi}[[g_1],[g_2]] &\Leftrightarrow \Big(\prod_U \mathcal{A} \models \boldsymbol{\psi}[[g_1],[g_2]]\Big) \vee \Big(\prod_U \mathcal{A} \models \chi[[g_1],[g_2]]\Big)\\ &\Leftrightarrow X_{\boldsymbol{\psi},g_1,g_2} \in U \vee X_{\chi,g_1,g_2} \in U\\ &\Leftrightarrow X_{\boldsymbol{\psi},g_1,g_2} \cup X_{\chi,g_1,g_2} \in U\\ &\Leftrightarrow X_{\boldsymbol{\psi}\vee\chi,g_1,g_2} \in U\end{aligned}$$

dove abbiamo usato la parte (c) della Proposizione 12.7 e che $X_{\boldsymbol{\psi}\boldsymbol{\vee}\boldsymbol{\chi},g_1,g_2} = X_{\boldsymbol{\psi},g_1,g_2} \cup X_{\boldsymbol{\chi},g_1,g_2}$.

Supponiamo ora $\boldsymbol{\varphi} = \boldsymbol{\exists y}\, \boldsymbol{\psi}$. Se $\prod_U \mathcal{A}_x \models \boldsymbol{\varphi}[[g_1],[g_2]]$ allora c'è un $h \in \bigtimes_{x\in X} A_x$ tale che $\prod_U \mathcal{A}_x \models \boldsymbol{\psi}[[h],[g_1],[g_2]]$ e quindi, per ipotesi induttiva, $X_{\boldsymbol{\psi},h,\bar{g}} \in U$. Poiché $X_{\boldsymbol{\varphi},g_1,g_2} \supseteq X_{\boldsymbol{\psi},h,g_1,g_2}$, segue che $X_{\boldsymbol{\varphi},g_1,g_2} \in U$. Viceversa, supponiamo $X_{\boldsymbol{\varphi},g_1,g_2} \in U$. Sia $h \in \bigtimes_{x\in X} A_x$ la funzione definita da

$$h(x) = \begin{cases} \text{un } a \in A_x \text{ tale che } \mathcal{A}_x \models \boldsymbol{\psi}[a, g_1(x), g_2(x)] & \text{se } x \in X_{\boldsymbol{\varphi},g_1,g_2},\\ a_x^* & \text{altrimenti,}\end{cases}$$

dove $a_x^* \in A_x$ è un elemento fissato. Allora $X_{\boldsymbol{\varphi},\bar{g}} \subseteq X_{\boldsymbol{\psi},h,g_1,g_2}$ e quindi $X_{\boldsymbol{\psi},h,g_1,g_2} \in U$. Per ipotesi induttiva, questo implica che $\prod_U \mathcal{A}_x \models \boldsymbol{\psi}[[h],[g_1],[g_2]]$ e quindi $\prod_U \mathcal{A}_x \models \boldsymbol{\varphi}[[g_1],[g_2]]$. □

Osserviamo che l'Assioma di Scelta è stato usato per definire la funzione h.

Corollario 23.14. *Ogni classe* EC_Δ *è chiusa per ultraprodotti.*

Dimostrazione del Teorema di Compattezza. Sia

$$X = \{\, x \subseteq \Sigma \mid x \text{ è finito} \,\}$$

e per ogni $x \in X$ sia $\mathcal{A}_x$ un modello di x. Sia

$$S(x) \stackrel{\text{def}}{=} \{\, y \in X \mid x \subseteq y \,\}.$$

Poichè $S(x_1) \cap \cdots \cap S(x_n) = S(x_1 \cup \cdots \cup x_n)$, l'insieme

$$\{\, S(x) \mid x \in X \,\} \subseteq \mathscr{P}(X)$$

è una base per un filtro F su X. Sia $U \supseteq F$ un ultrafiltro che estende F. Vogliamo dimostrare che per ogni $\boldsymbol{\sigma} \in \Sigma$

$$\prod_U \mathcal{A}_x \models \boldsymbol{\sigma}.$$

Ciò segue immediatamente dal Teorema di Łos e da $\{\, x \in X \mid \mathcal{A}_x \models \boldsymbol{\sigma} \,\} \supseteq S(\{\boldsymbol{\sigma}\}) \in F \subseteq U$. □

Esercizi

Esercizio 23.15. Dimostrare che la relazione di conseguenza logica è un pre-ordine su $\mathscr{P}(\mathrm{Sent}(\boldsymbol{L}))$ i cui elementi minimali sono gli insiemi Σ non soddisfacibili.

Esercizio 23.16. Generalizzare il Teorema 23.5 dimostrando che se $\mathfrak{K}$ e $\mathfrak{Str}(\boldsymbol{L}) \setminus \mathfrak{K}$ sono PC_Δ, allora $\mathfrak{K}$ e $\mathfrak{Str}(\boldsymbol{L}) \setminus \mathfrak{K}$ sono PC.

Esercizio 23.17. Dimostrare in dettaglio i Corollari 23.7 e 23.8.

Esercizio 23.18. Ricordiamo (vedi pagina 77) che un ordine lineare è omogeneo se presi due intervalli aperti, questi sono isomorfi; è ultraomogeneo se ogni automorfismo parziale può essere esteso ad un automorfismo. Dimostrare che la classi degli ordini lineari omogenei e ultraomogenei sono, rispettivamente, PC e PC_Δ nel linguaggio $\boldsymbol{L} = \{\leq\}$.

Esercizio 23.19. Dimostrare che la classe degli ordini mal-fondati è pseudo-elementare generalizzata (PC_Δ) nel linguaggio $\{\leq\}$, ma non è pseudo-elementare (PC) cioè non è finitamente assiomatizzabile in nessun $\boldsymbol{L} \supseteq \{\leq\}$.

Esercizio 23.20. Dimostrare che le seguenti classi di strutture non sono assiomatizzabili, neppure ampliando il linguaggio (PC).

(i) Le strutture (insiemi, gruppi, anelli, ordini, etc.) finite.

(ii) I gruppi di torsione.

(iii) I campi di caratteristica positiva.

(iv) Gli ordini ben fondati.

Esercizio 23.21. Sia U un ultrafiltro su un insieme $I \neq \emptyset$ e siano $\mathcal{A}_i \in \mathfrak{Str}(\boldsymbol{L})$, con $i \in I$. Dimostrare che se $\boldsymbol{L}' \subseteq \boldsymbol{L}$ allora

$$\left(\prod_U \mathcal{A}_i\right) \restriction \boldsymbol{L}' = \prod_U \left(\mathcal{A}_i \restriction \boldsymbol{L}'\right).$$

Concludere che una classe PC_Δ è chiusa per ultraprodotti.

Esercizio 23.22. Dedurre il Teorema 17.1 di Ramsey nel caso infinito dalla sua versione nel caso finito (Teorema 23.12).

24. Teorie e mappe elementari

24.A. Teorie. Fissiamo un linguaggio $\boldsymbol{L}$ ed un insieme $\Delta \subseteq \mathrm{Sent}(\boldsymbol{L})$. La relazione

$$\Delta \cup \{\boldsymbol{\sigma}\} \models \boldsymbol{\tau}$$

definisce un pre-ordine su $\mathrm{Sent}(\boldsymbol{L})$ e quindi induce una relazione d'equivalenza

$$\boldsymbol{\sigma} \sim_\Delta \boldsymbol{\tau} \quad \Leftrightarrow \quad (\Delta \cup \{\boldsymbol{\sigma}\} \models \boldsymbol{\tau} \ \wedge \ \Delta \cup \{\boldsymbol{\tau}\} \models \boldsymbol{\sigma})$$

che si legge: $\boldsymbol{\sigma}$ e $\boldsymbol{\tau}$ sono equivalenti modulo Δ. Quando $\Delta = \emptyset$ diremo che $\boldsymbol{\sigma}$ e $\boldsymbol{\tau}$ sono logicamente equivalenti.

Esercizio 24.1. Dimostrare che:

(i)
$$\Delta \cup \{\boldsymbol{\sigma}\} \models \boldsymbol{\tau} \quad \Leftrightarrow \quad \Delta \models (\boldsymbol{\sigma} \Rightarrow \boldsymbol{\tau})$$
e
$$\boldsymbol{\sigma} \sim_\Delta \boldsymbol{\tau} \quad \Leftrightarrow \quad \Delta \models (\boldsymbol{\sigma} \Leftrightarrow \boldsymbol{\tau})\,.$$

(ii) $\Delta \models \boldsymbol{\sigma} \vee \boldsymbol{\neg\sigma}$.

(iii) Se Δ non è soddisfacibile, allora tutti gli enunciati sono $\sim_\Delta$ equivalenti.

(iv) Se Δ è soddisfacibile e $\boldsymbol{\sigma} \in \mathrm{Sent}(\boldsymbol{L})$, allora $\Delta \not\models \boldsymbol{\sigma} \wedge \boldsymbol{\neg\sigma}$; quindi $\boldsymbol{\sigma} \wedge \boldsymbol{\neg\sigma}$ e $\boldsymbol{\sigma} \vee \boldsymbol{\neg\sigma}$ non sono $\sim_\Delta$ equivalenti.

(v) $\Delta \subseteq \Gamma$ implica che la relazione d'equivalenza $\sim_\Delta$ raffina $\sim_\Gamma$, vale a dire
$$\boldsymbol{\sigma} \sim_\Delta \boldsymbol{\tau} \quad \Rightarrow \quad \boldsymbol{\sigma} \sim_\Gamma \boldsymbol{\tau}\,.$$

Proposizione 24.2. *Supponiamo Δ sia un insieme soddisfacibile di enunciati. L'insieme quoziente $\mathrm{Sent}(\boldsymbol{L})/\!\sim_\Delta$ è un'algebra di Boole con le operazioni*

$$[\boldsymbol{\sigma}]_\Delta \curlyvee [\boldsymbol{\tau}]_\Delta = [\boldsymbol{\sigma} \vee \boldsymbol{\tau}]_\Delta$$
$$[\boldsymbol{\sigma}]_\Delta \curlywedge [\boldsymbol{\tau}]_\Delta = [\boldsymbol{\sigma} \wedge \boldsymbol{\tau}]_\Delta$$
$$[\boldsymbol{\sigma}]^*_\Delta = [\boldsymbol{\neg\sigma}]_\Delta\,.$$

L' 1 *dell'algebra è la classe d'equivalenza $\top$ delle tautologie proposizionali; lo* 0 *è la classe d'equivalenza $\bot$ delle contraddizioni proposizionali.*

Dimostrazione. La parte (iv) dell'Esercizio 24.1 garantisce che $\top \neq \bot$. Se $\boldsymbol{\sigma} \sim_\Delta \boldsymbol{\sigma'}$ e $\boldsymbol{\tau} \sim_\Delta \boldsymbol{\tau'}$, cioè $\Delta \models (\boldsymbol{\sigma} \Leftrightarrow \boldsymbol{\sigma'})$ e $\Delta \models (\boldsymbol{\tau} \Leftrightarrow \boldsymbol{\tau'})$, allora

$$\boldsymbol{\sigma} \vee \boldsymbol{\tau} \Leftrightarrow \boldsymbol{\sigma'} \vee \boldsymbol{\tau'}$$
$$\boldsymbol{\sigma} \wedge \boldsymbol{\tau} \Leftrightarrow \boldsymbol{\sigma'} \wedge \boldsymbol{\tau'}$$
$$\boldsymbol{\neg\sigma} \Leftrightarrow \boldsymbol{\neg\sigma'}$$

sono conseguenze logiche di Δ e quindi

$$\boldsymbol{\sigma} \vee \boldsymbol{\tau} \sim_\Delta \boldsymbol{\sigma'} \vee \boldsymbol{\tau'}$$
$$\boldsymbol{\sigma} \wedge \boldsymbol{\tau} \sim_\Delta \boldsymbol{\sigma'} \wedge \boldsymbol{\tau'}$$
$$\boldsymbol{\neg\sigma} \sim_\Delta \boldsymbol{\neg\sigma'}$$

Quindi le definizioni delle operazioni $\curlyvee$, $\curlywedge$ e * non dipendono dai rappresentanti. La verifica che queste operazioni soddisfano (56)–(60) è lasciata al lettore. □

L'insieme quoziente

$$\mathrm{Sent}(\boldsymbol{L})/\Delta \stackrel{\mathrm{def}}{=} \mathrm{Sent}(\boldsymbol{L})/\sim_\Delta$$

si dice **algebra di Lindembaum** generata dalla teoria Δ. Quando $\Delta = \emptyset$ abbiamo l'**algebra degli enunciati logicamente equivalenti**.

Se $\boldsymbol{\sigma} \in \Delta$, allora $\Delta \models \boldsymbol{\sigma}$, il viceversa non vale in generale. Una **teoria chiusa** T è una teoria (cioè un insieme di enunciati) chiusa per conseguenza logica, ovvero

$$T \models \boldsymbol{\sigma} \quad \Rightarrow \quad \boldsymbol{\sigma} \in T\,,$$

per ogni enunciato $\boldsymbol{\sigma}$.

Supponiamo $\Sigma \subseteq \mathrm{Sent}(\boldsymbol{L})$ sia un insieme soddisfacibile e massimale, vale a dire $\Sigma \subset \Delta \subseteq \mathrm{Sent}(\boldsymbol{L}) \Rightarrow \mathfrak{Mod}(\Delta) = \emptyset$. Se $\boldsymbol{\sigma} \notin \Sigma$ allora $\Sigma \cup \{\boldsymbol{\sigma}\}$ non è soddisfacibile, quindi fissato un $\mathcal{A} \in \mathfrak{Mod}(\Sigma)$ si ha che $\mathcal{A} \not\models \boldsymbol{\sigma}$, da cui $\Sigma \not\models \boldsymbol{\sigma}$. In altre parole: se $\Sigma \models \boldsymbol{\sigma}$ allora $\boldsymbol{\sigma} \in \Sigma$, cioè Σ è una teoria chiusa. Un insieme di enunciati che sia soddisfacibile e massimale si dice **teoria completa**.

Esercizio 24.3. Dimostrare che:

(i) Ogni teoria completa è chiusa, ma non viceversa.

(ii) Se T è una teoria chiusa e se $\boldsymbol{\sigma}, \boldsymbol{\tau} \in \mathrm{Sent}(\boldsymbol{L})$, allora

$$\boldsymbol{\sigma} \boldsymbol{\wedge} \boldsymbol{\tau} \in T \quad \Leftrightarrow \quad \boldsymbol{\sigma} \in T \wedge \boldsymbol{\tau} \in T\,.$$

(iii) Se T è una teoria completa e se $\boldsymbol{\sigma} \in \mathrm{Sent}(\boldsymbol{L})$, allora

$$\boldsymbol{\sigma} \notin T \quad \Leftrightarrow \quad \boldsymbol{\neg\sigma} \in T\,.$$

(iv) Una teoria Σ è soddisfacibile se e solo se $\{\, [\boldsymbol{\sigma}] \mid \boldsymbol{\sigma} \in \Sigma \,\}$ è una sotto-base per un filtro.

(v) Una teoria chiusa T è soddisfacibile se e solo se $\{\, [\boldsymbol{\sigma}] \mid \boldsymbol{\sigma} \in T \,\}$ è un filtro proprio.

(vi) Una teoria T è completa se e solo se $\{\, [\boldsymbol{\sigma}] \mid \boldsymbol{\sigma} \in T \,\}$ è un ultrafiltro.

Definizione 24.4. Per $\mathcal{A} \in \mathfrak{Str}(\boldsymbol{L})$

$$\mathrm{Th}(\mathcal{A}) = \{\, \boldsymbol{\sigma} \in \mathrm{Sent}(\boldsymbol{L}) \mid \mathcal{A} \models \boldsymbol{\sigma} \,\}$$

si dice **teoria di** $\mathcal{A}$.

Esercizio 24.5. Dimostrare che $\mathrm{Th}(\mathcal{A})$ è una teoria completa, $\mathcal{A} \in \mathfrak{Mod}(\mathrm{Th}(\mathcal{A}))$ e ogni teoria completa è della forma $\mathrm{Th}(\mathcal{A})$ per qualche $\mathcal{A}$.

24.B. Preservazione di formule in strutture. Una formula $\boldsymbol{\varphi}$ costituita da un blocco di quantificatori esistenziali applicati ad una formula priva di quantificatori $\boldsymbol{\psi}$

$$\boldsymbol{\exists x}_1 \ldots \boldsymbol{\exists x}_n \, \boldsymbol{\psi}$$

si dice **formula esistenziale** o $\exists$**-formula**. Analogamente, una **formula universale** o $\forall$**-formula** è della forma

$$\boldsymbol{\forall x}_1 \ldots \boldsymbol{\forall x}_n \, \boldsymbol{\psi}$$

con $\boldsymbol{\psi}$ priva di quantificatori.

Proposizione 24.6. *Siano* $\boldsymbol{\varphi}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)$ *una formula,* $\bar{a} \in A$ *e* $\mathcal{A} \subseteq \mathcal{B}$.

(a) *Se* $\boldsymbol{\varphi}$ *è priva di quantificatori*

$$\mathcal{A} \models \boldsymbol{\varphi}[\bar{a}] \quad \Leftrightarrow \quad \mathcal{B} \models \boldsymbol{\varphi}[\bar{a}] \, .$$

(b) *Se* $\boldsymbol{\varphi}$ *è una* $\forall$*-formula*

$$\mathcal{B} \models \boldsymbol{\varphi}[\bar{a}] \quad \Rightarrow \quad \mathcal{A} \models \boldsymbol{\varphi}[\bar{a}] \, .$$

(c) *Se* $\boldsymbol{\varphi}$ *è una* $\exists$*-formula*

$$\mathcal{A} \models \boldsymbol{\varphi}[\bar{a}] \quad \Rightarrow \quad \mathcal{B} \models \boldsymbol{\varphi}[\bar{a}] \, .$$

Dimostrazione. (a) Per induzione su $\mathrm{ht}(\boldsymbol{\varphi})$. Se $\boldsymbol{\varphi}$ è atomica (vale a dire $\boldsymbol{t}_1 \equiv \boldsymbol{t}_2$ o $R(\boldsymbol{t}_1, \ldots, \boldsymbol{t}_n)$) allora il risultato segue da (84) e dalla definizione di sotto-struttura. Se $\boldsymbol{\varphi}$ è $\boldsymbol{\neg\psi}$, allora

$$\begin{aligned} \mathcal{A} \models \boldsymbol{\varphi}[\bar{a}] \quad &\Leftrightarrow \quad \neg(\mathcal{A} \models \boldsymbol{\psi}[\bar{a}]) \\ &\Leftrightarrow \quad \neg(\mathcal{B} \models \boldsymbol{\psi}[\bar{a}]) \qquad\qquad \text{(per ip. ind.)} \\ &\Leftrightarrow \quad \mathcal{B} \models \boldsymbol{\varphi}[\bar{a}] \, . \end{aligned}$$

Se $\boldsymbol{\varphi}$ è $\boldsymbol{\psi} \boldsymbol{\vee} \boldsymbol{\chi}$, allora

$$\begin{aligned} \mathcal{A} \models \boldsymbol{\varphi}[\bar{a}] \quad &\Leftrightarrow \quad (\mathcal{A} \models \boldsymbol{\psi}[\bar{a}] \vee \mathcal{A} \models \boldsymbol{\chi}[\bar{a}]) \\ &\Leftrightarrow \quad (\mathcal{B} \models \boldsymbol{\psi}[\bar{a}] \vee \mathcal{B} \models \boldsymbol{\chi}[\bar{a}]) \qquad \text{(per ip. ind.)} \\ &\Leftrightarrow \quad \mathcal{B} \models \boldsymbol{\varphi}[\bar{a}] \, . \end{aligned}$$

(b) Sia $\boldsymbol{\varphi}$ la formula $\boldsymbol{\forall y}_1 \ldots \boldsymbol{\forall y}_m \boldsymbol{\psi}$ e supponiamo $\mathcal{B} \models \boldsymbol{\varphi}[\bar{a}]$, vale a dire $\forall b_1 \ldots \forall b_m \in B \, \big(\mathcal{B} \models \boldsymbol{\psi}[\bar{b}, \bar{a}]\big)$. Quindi, per ogni $b_1, \ldots, b_m \in A \subseteq B$, vale $\mathcal{B} \models \boldsymbol{\psi}[\bar{b}, \bar{a}]$ e allora, per la parte (a), vale $\mathcal{A} \models \boldsymbol{\psi}[\bar{b}, \bar{a}]$. Abbiamo mostrato che $\forall b_1 \ldots \forall b_m \in A \big(\mathcal{A} \models \boldsymbol{\psi}[\bar{b}, \bar{a}]\big)$, cioè $\mathcal{A} \models \boldsymbol{\varphi}[\bar{a}]$.

(c) segue da (b). □

Una formula $\boldsymbol{\varphi}$ costituita da un blocco di quantificatori universali, seguito da un blocco di quantificatori esistenziali, applicati ad una formula $\boldsymbol{\psi}$ priva di quantificatori

$$\boldsymbol{\forall x}_1 \ldots \boldsymbol{\forall x}_n \, \boldsymbol{\exists y}_1 \ldots \boldsymbol{\exists} \, \boldsymbol{y}_m \boldsymbol{\psi}$$

si dice ∀∃-formula.

Proposizione 24.7. *Sia* $\boldsymbol{\varphi}$ *una* ∀∃*-formula soddisfatta in ogni* $\mathcal{A}_n$*, dove* $\mathcal{A}_0 \subseteq \mathcal{A}_1 \subseteq \dots$*. Allora* $\bigcup_n \mathcal{A}_n \models \boldsymbol{\varphi}$*.*

Dimostrazione. Poiché la chiusura universale di una ∀∃-formula è una ∀∃-formula, possiamo supporre che $\boldsymbol{\varphi}$ sia un enunciato. Fissiamo $\boldsymbol{\psi}$ priva di quantificatori tale che

$$\boldsymbol{\varphi} = \forall \boldsymbol{x}_1 \dots \forall \boldsymbol{x}_n \exists \boldsymbol{y}_1 \dots \exists \boldsymbol{y}_m \, \boldsymbol{\psi} \,.$$

Fissiamo $a_1, \dots, a_n \in \bigcup_i A_i$ e sia N sufficientemente grande per cui $a_1, \dots, a_n \in A_N$. Allora $\mathcal{A}_N \models \boldsymbol{\varphi}$ implica che

$$\mathcal{A}_N \models (\exists \boldsymbol{y}_1 \dots \exists \boldsymbol{y}_m \, \boldsymbol{\psi})\, [a_1, \dots, a_n] \,.$$

Per la parte (b) della Proposizione 24.6 segue che $\bigcup_n \mathcal{A}_n \models \boldsymbol{\varphi}$. □

24.C. Equivalenza elementare. Diremo che due $\boldsymbol{L}$-strutture $\mathcal{A}$ e $\mathcal{B}$ sono **elementarmente equivalenti**

$$\mathcal{A} \equiv \mathcal{B}$$

se e solo se $(\mathcal{A} \models \boldsymbol{\sigma}) \Leftrightarrow (\mathcal{B} \models \boldsymbol{\sigma})$, per ogni enunciato $\boldsymbol{\sigma}$; equivalentemente se e solo se $\mathrm{Th}(\mathcal{A}) = \mathrm{Th}(\mathcal{B})$. Un morfismo $\pi\colon \mathcal{A} \to \mathcal{B}$ è un'**immersione elementare** se per ogni formula $\boldsymbol{\varphi}(\boldsymbol{x}_1, \dots, \boldsymbol{x}_n)$ e ogni $\bar{a} \in A$

$$\mathcal{A} \models \boldsymbol{\varphi}[\bar{a}] \quad \Leftrightarrow \quad \mathcal{B} \models \boldsymbol{\varphi}[\pi(\bar{a})] \,.$$

Esercizio 24.8. Sia $\pi\colon \mathcal{A} \to \mathcal{B}$ un morfismo. Dimostrare che:

(i) Se π è un isomorfismo allora è un'immersione elementare.

(ii) Se π è elementare allora è iniettiva.

(iii) Se per ogni formula $\boldsymbol{\varphi}$ e ogni $\bar{a} \in A$

$$\mathcal{A} \models \boldsymbol{\varphi}[\bar{a}] \quad \Rightarrow \quad \mathcal{B} \models \boldsymbol{\varphi}[\pi(\bar{a})]$$

allora π è elementare.

Se c'è un'immersione elementare di $\mathcal{A}$ in $\mathcal{B}$ diremo che $\mathcal{A}$ **si immerge elementarmente** in $\mathcal{B}$

$$\mathcal{A} \preccurlyeq \mathcal{B} \,.$$

Se $\mathcal{A} \subseteq \mathcal{B}$ e la funzione di inclusione è un'immersione elementare diremo che $\mathcal{A}$ è una **sotto-struttura elementare** di $\mathcal{B}$,

$$\mathcal{A} \preccurlyeq \mathcal{B} \,,$$

e se $\mathcal{A} \neq \mathcal{B}$ diremo che $\mathcal{A}$ è una **sotto-struttura elementare propria** di $\mathcal{B}$, in simboli $\mathcal{A} \prec \mathcal{B}$. Le espressioni $\mathcal{A} \subseteq \mathcal{B}$ e $\mathcal{A} \subset \mathcal{B}$ significano che $\mathcal{A}$ è isomorfa ad una sotto-struttura di $\mathcal{B}$ e, rispettivamente, ad una sotto-struttura propria di $\mathcal{B}$.

Esercizio 24.9. Verificare che le Proposizioni 24.6 e 24.7 si generalizzano al caso delle immersioni. Per esempio: se $\boldsymbol{\varphi}(\boldsymbol{x}_1, \dots, \boldsymbol{x}_n)$ è priva di quantificatori e $\pi\colon \mathcal{A} \to \mathcal{B}$ è un'immersione,

$$\mathcal{A} \models \boldsymbol{\varphi}[\bar{a}] \quad \Leftrightarrow \quad \mathcal{B} \models \boldsymbol{\varphi}[\pi(\bar{a})]\,.$$

Esercizio 24.10. Consideriamo ora il caso di un ultrapotenza $\mathcal{A}^X/U$, cioè $\prod_U \mathcal{A}_x$ con $\mathcal{A}_x = \mathcal{A}$ per ogni $x \in X$. Per ogni $a \in A$ sia $c_a\colon X \to A$ la funzione costante $c_a(x) = a$ per ogni $x \in X$ e sia $\pi\colon \mathcal{A} \to \mathcal{A}^X/U$, $\pi(a) = [c_a]$. Dimostrare che π è elementare.

Sia $\mathcal{A} \in \mathfrak{Str}(\boldsymbol{L})$, sia

$$\boldsymbol{L}_A = \boldsymbol{L} \cup \{\, \mathring{a} \mid a \in A \,\}$$

il linguaggio espanso con un nuovo simbolo di costante per ogni elemento di A e sia $\langle \mathcal{A}, a\rangle_{a\in A}$ l'espansione canonica di $\mathcal{A}$ ad A. Il **diagramma** di $\mathcal{A}$ è l'insieme di tutte le formule atomiche e loro negazioni che valgono in $\langle \mathcal{A}, a\rangle_{a\in A}$

$$\begin{aligned}\mathrm{Diag}(\mathcal{A}) &= \{\, \boldsymbol{\varphi}[\bar{a}] \mid \mathcal{A} \models \boldsymbol{\varphi}[\bar{a}] \text{ e } \boldsymbol{\varphi} \text{ è atomica, o } \boldsymbol{\varphi} = \boldsymbol{\neg\psi} \text{ con } \boldsymbol{\psi} \text{ atomica} \,\}\\ &= \mathrm{Th}(\langle \mathcal{A}, a\rangle_{a\in A}) \cap \big(\mathrm{AtFml}(\boldsymbol{L}_A) \cup \{\, \boldsymbol{\neg\psi} \mid \boldsymbol{\psi} \in \mathrm{AtFml}(\boldsymbol{L}_A) \,\}\big),\end{aligned}$$

Il **diagramma elementare** di $\mathcal{A}$ è l'insieme di tutte le formule che valgono in $\langle \mathcal{A}, a\rangle_{a\in A}$

$$\begin{aligned}\mathrm{EDiag}(\mathcal{A}) &= \{\, \boldsymbol{\varphi}[\bar{a}] \mid \mathcal{A} \models \boldsymbol{\varphi}[\bar{a}] \,\}\\ &= \mathrm{Th}(\langle \mathcal{A}, a\rangle_{a\in A})\,.\end{aligned}$$

Teorema 24.11. *Le seguenti affermazioni sono equivalenti:*

(a) $\mathcal{A} \preccurlyeq \mathcal{B}$,

(b) *c'è un'espansione* $\tilde{\mathcal{B}}$ *di* $\mathcal{B}$ *nel linguaggio* $\boldsymbol{L}_A = \boldsymbol{L} \cup \{\, \mathring{a} \mid a \in A \,\}$ *tale che* $\tilde{\mathcal{B}} \models \mathrm{EDiag}(\mathcal{A})$.

Dimostrazione. (a) $\Rightarrow$ (b): Se $\pi\colon \mathcal{A} \to \mathcal{B}$ è elementare, allora ponendo

$$(\mathring{a})^{\tilde{\mathcal{B}}} = \pi(a) \qquad (a \in A)$$

otteniamo l'espansione $\tilde{\mathcal{B}} = \langle \mathcal{B}, \pi(a)\rangle_{a\in A}$. Verifichiamo che $\tilde{\mathcal{B}} \models \boldsymbol{\sigma}$ per ogni $\boldsymbol{\sigma} \in \mathrm{EDiag}(\mathcal{A})$: Se $\boldsymbol{\sigma} \in \mathrm{Sent}(\boldsymbol{L}_A)$ allora $\boldsymbol{\sigma}$ è della forma $\boldsymbol{\varphi}[\mathring{a}_1/\boldsymbol{x}_1, \dots, \mathring{a}_n/\boldsymbol{x}_n]$, dove $\boldsymbol{\varphi}(\boldsymbol{x}_1, \dots, \boldsymbol{x}_n)$ è una $\boldsymbol{L}$-formula e quindi

$$\begin{aligned}\langle \mathcal{A}, a\rangle_{a\in A} \models \boldsymbol{\sigma} &\Leftrightarrow \mathcal{A} \models \boldsymbol{\varphi}[a_1, \dots, a_n]\\ &\Leftrightarrow \mathcal{B} \models \boldsymbol{\varphi}[\pi(a_1), \dots, \pi(a_n)]\\ &\Leftrightarrow \tilde{\mathcal{B}} \models \boldsymbol{\sigma}\,.\end{aligned}$$

(b) $\Rightarrow$ (a): Supponiamo $\tilde{\mathcal{B}}$ sia una $\boldsymbol{L}_A$-struttura che soddisfa $\mathrm{EDiag}(\mathcal{A})$. Allora, per ogni coppia $a_1, a_2 \in A$

$$\begin{aligned} a_1 \neq a_2 &\Leftrightarrow (\mathring{a}_1 \neq \mathring{a}_2) \in \mathrm{EDiag}(\mathcal{A}) \\ &\Leftrightarrow \tilde{\mathcal{B}} \models \mathring{a}_1 \not\equiv \mathring{a}_2 \\ &\Leftrightarrow (\mathring{a}_1)^{\tilde{\mathcal{B}}} \neq (\mathring{a}_2)^{\tilde{\mathcal{B}}} . \end{aligned}$$

Quindi $\pi\colon A \to B$, $\pi(a) = (\mathring{a})^{\tilde{\mathcal{B}}}$, è una funzione iniettiva. Se $\boldsymbol{\varphi}(\boldsymbol{x}_1, \dots, \boldsymbol{x}_n)$ è una $\boldsymbol{L}$-formula e $a_1, \dots, a_n \in A$, allora

$$\begin{aligned} \mathcal{A} \models \boldsymbol{\varphi}[a_1, \dots, a_n] &\Leftrightarrow \boldsymbol{\varphi}[\mathring{a}_1/\boldsymbol{x}_1, \dots, \mathring{a}_n/\boldsymbol{x}_n] \in \mathrm{EDiag}(\mathcal{A}) \\ &\Leftrightarrow \tilde{\mathcal{B}} \models \boldsymbol{\varphi}[\mathring{a}_1/\boldsymbol{x}_1, \dots, \mathring{a}_n/\boldsymbol{x}_n] \\ &\Leftrightarrow \mathcal{B} \models \boldsymbol{\varphi}[\pi(a_1), \dots, \pi(a_n)] . \end{aligned}$$

Quindi π è elementare. □

Esercizio 24.12. Siano $\mathcal{A}, \mathcal{B} \in \mathfrak{Stt}(\boldsymbol{L})$. Dimostrare che le seguenti condizioni sono equivalenti:

(i) $\mathcal{A} \subseteq \mathcal{B}$,

(ii) c'è un'espansione $\tilde{\mathcal{B}}$ di $\mathcal{B}$ nel linguaggio $\boldsymbol{L} \cup \{\, \mathring{a} \mid a \in \|\mathcal{A}\| \,\}$ tale che $\tilde{\mathcal{B}} \models \mathrm{Diag}(\mathcal{A})$.

Teorema 24.13 (Tarski-Vaught)**.** *Se $\pi\colon \mathcal{A} \to \mathcal{B}$ è un'immersione le seguenti condizioni sono equivalenti:*

(a) *π è elementare,*

(b) *per ogni formula $\boldsymbol{\varphi}(\boldsymbol{y}, \boldsymbol{x}_1, \dots, \boldsymbol{x}_n)$ e ogni $\bar{a} \in A$*

$$\mathcal{B} \models (\boldsymbol{\exists y \varphi})[\pi(\bar{a})] \quad \Leftrightarrow \quad \exists b \in A\, (\mathcal{B} \models \boldsymbol{\varphi}[\pi(b), \pi(\bar{a})]) .$$

Dimostrazione. (a) $\Rightarrow$ (b): Se $\mathcal{B} \models (\boldsymbol{\exists y \varphi})[\pi(\bar{a})]$ allora, per l'elementarità di π, $\mathcal{A} \models (\boldsymbol{\exists y \varphi})[\bar{a}]$ e quindi $\mathcal{A} \models \boldsymbol{\varphi}[b, \bar{a}]$ per qualche $b \in A$, da cui $\mathcal{B} \models \boldsymbol{\varphi}[\pi(b), \pi(\bar{a})]$.

(b) $\Rightarrow$ (a): Per induzione su $\mathrm{ht}(\boldsymbol{\psi})$ dimostriamo che

$$\mathcal{A} \models \boldsymbol{\psi}[\bar{a}] \quad \Leftrightarrow \quad \mathcal{B} \models \boldsymbol{\psi}[\pi(\bar{a})] . \tag{109}$$

Se $\boldsymbol{\psi}$ è atomica allora (109) vale per l'Esercizio 24.9. Se $\boldsymbol{\psi}$ è $\boldsymbol{\neg \psi}_1$ o $\boldsymbol{\psi}_1 \boldsymbol{\vee} \boldsymbol{\psi}_2$, allora (109) vale per ipotesi induttiva e per la definizione di soddisfazione. Quindi possiamo supporre che $\boldsymbol{\psi}$ sia $\boldsymbol{\exists y \varphi}$:

$$\begin{aligned} \mathcal{A} \models (\boldsymbol{\exists y \varphi})[\bar{a}] &\Leftrightarrow \exists b \in A\, (\mathcal{A} \models \boldsymbol{\psi}[b, \bar{a}]) \\ &\Leftrightarrow \exists b \in A\, (\mathcal{B} \models \boldsymbol{\psi}[\pi(b), \pi(\bar{a})]) \quad \text{(per ipotesi induttiva)} \\ &\Leftrightarrow \mathcal{B} \models (\boldsymbol{\exists y \varphi})[\pi(\bar{a})] \quad \text{(per la nostra ipotesi.)} \end{aligned}$$

□

Corollario 24.14. *Le seguenti condizioni sono equivalenti:*

(a) $\mathcal{A} \preccurlyeq \mathcal{B}$

(b) $\mathcal{A} \subseteq \mathcal{B}$ *e per ogni formula* $\boldsymbol{\varphi}(\boldsymbol{y}, \boldsymbol{x}_1, \dots, \boldsymbol{x}_n)$ *e ogni* $\bar{a} \in A$

$$\mathcal{B} \models (\boldsymbol{\exists y \varphi})[\bar{a}] \quad \Leftrightarrow \quad \exists b \in A\, (\mathcal{B} \models \boldsymbol{\varphi}[b, \bar{a}])\,.$$

Proposizione 24.15. *Supponiamo che* $\mathcal{A}_0 \preccurlyeq \mathcal{A}_1 \preccurlyeq \mathcal{A}_2 \preccurlyeq \dots$ $(n \in \omega)$. *Allora* $\mathcal{A}_n \preccurlyeq \bigcup_{m\in\omega} \mathcal{A}_m$, *per ogni* $n \in \omega$.

Dimostrazione. Dimostriamo per induzione su $\mathrm{ht}(\boldsymbol{\varphi})$ che

$$\mathcal{A}_n \models \boldsymbol{\varphi}[\bar{a}] \quad \Leftrightarrow \quad \bigcup_m \mathcal{A}_m \models \boldsymbol{\varphi}[\bar{a}]$$

per ogni n e ogni $\bar{a} \in A$. Il caso non banale è quando $\boldsymbol{\varphi} = \boldsymbol{\exists y \psi}$ e $\bigcup_m \mathcal{A}_m \models (\boldsymbol{\exists y \psi})[\bar{a}]$. Allora $\bigcup_m \mathcal{A}_m \models \boldsymbol{\psi}[b', \bar{a}]$, per qualche $b' \in \bigcup_m A_m$. Sia $n' \geq n$ tale che $b' \in A_{n'}$. Allora per ipotesi induttiva $\mathcal{A}_{n'} \models (\boldsymbol{\exists y \psi})[\bar{a}]$ e quindi $\mathcal{A}_n \models (\boldsymbol{\exists y \psi})[\bar{a}]$, per $\mathcal{A}_n \preccurlyeq \mathcal{A}_{n'}$. □

24.D. Funzioni di Skolem. Fissiamo una $\boldsymbol{L}$-struttura $\mathcal{A}$. Ad ogni formula $\boldsymbol{\varphi}$ con variabili libere $\boldsymbol{y}, \boldsymbol{x}_1, \dots, \boldsymbol{x}_n$ associamo

$$h_{\boldsymbol{\varphi}} \colon A^n \to A$$

la **funzione di Skolem per** $\boldsymbol{\exists y \varphi}$ definita da

$$h_{\boldsymbol{\varphi}}(a_1, \dots, a_n) = \begin{cases} \text{un } b \text{ tale che } \mathcal{A} \models \boldsymbol{\varphi}[b, \bar{a}] & \text{se } \mathcal{A} \models (\boldsymbol{\exists y \varphi})[\bar{a}] \\ a^* & \text{altrimenti,} \end{cases}$$

dove a^* è un elemento fissato di A. Le funzioni $h_{\boldsymbol{\varphi}}$ sono definite usando l'Assioma di Scelta: fissata una $C \colon \mathscr{P}(A) \to A$ tale che $C(X) \in X$ se $X \neq \emptyset$ e $C(\emptyset) = a^*$, poniamo

$$h_{\boldsymbol{\varphi}}(\bar{a}) = C(\{\, b \in A \mid \mathcal{A} \models \boldsymbol{\varphi}[b, \bar{a}] \,\})$$

Osserviamo che se $\boldsymbol{y}$ è l'unica variabile libera di $\boldsymbol{\varphi}$, allora $h_{\boldsymbol{\varphi}} \colon A^0 \to A$ è—essenzialmente—un elemento di A: un testimone del fatto che $\mathcal{A} \models \boldsymbol{\exists y \varphi}$ oppure a^*. Sia $H(\mathcal{A})$ l'insieme delle funzioni di Skolem per $\mathcal{A}$.

Teorema 24.16. *Per ogni* $X \subseteq A$, *la chiusura di* X *sotto le funzioni in* $H(\mathcal{A})$ *è una sotto-struttura elementare di* $\mathcal{A}$,

$$\mathrm{Cl}_{H(\mathcal{A})}(X) \preccurlyeq \mathcal{A}\,.$$

Dimostrazione. La funzione di Skolem della formula $\boldsymbol{y} \not\equiv \boldsymbol{y}$ garantisce che $a^* \in C = \mathrm{Cl}_{H(\mathcal{A})}(X)$, quindi $C \neq \emptyset$. Per ogni simbolo di costante $\boldsymbol{c}$ la chiusura di C sotto la funzione 0-aria di Skolem $h_{\boldsymbol{\varphi}}$, dove $\boldsymbol{\varphi}$ è $\boldsymbol{y} = \boldsymbol{c}$, garantisce che $\boldsymbol{c}^{\mathcal{A}} \in C$. Per ogni simbolo $\boldsymbol{f}$ di funzione n-aria, la chiusura di C sotto la funzione di Skolem $h_{\boldsymbol{\psi}}$, dove $\boldsymbol{\psi}$ è $\boldsymbol{y} = \boldsymbol{f}(\boldsymbol{x}_1, \dots, \boldsymbol{x}_n)$, garantisce che C è chiuso sotto $\boldsymbol{f}^{\mathcal{A}}$. Poiché l'interpretazione dei simboli di relazione non

costituisce un problema, segue che C è (l'universo di) una sottostruttura di $\mathcal{A}$. Per il Teorema di Tarski-Vaught è sufficiente verificare che se $\mathcal{A} \models (\exists \boldsymbol{y}\boldsymbol{\varphi})[\bar{c}]$ per qualche $\bar{c} \in C$, allora c'è un $b \in C$ tale che $\mathcal{A} \models \boldsymbol{\varphi}[b, \bar{c}]$. Ma ciò è immediato prendendo $b = h_{\boldsymbol{\varphi}}(\bar{c})$. □

Il seguente risultato, noto come il "Teorema di Löwenheim-Skolem all'ingiù" asserisce, in particolare, che ogni struttura più che numerabile in un linguaggio numerabile ha una sotto-struttura elementare numerabile.

Teorema 24.17. *Se $\mathcal{A} \in \mathfrak{Stt}(\boldsymbol{L})$ e κ è un cardinale infinito tale che*

$$\operatorname{card}(\boldsymbol{L}) \leq \kappa \leq \operatorname{card}(\mathcal{A}) \,,$$

allora per ogni $X \subseteq A$ con $|X| \leq \kappa$ c'è una $\mathcal{B} \preccurlyeq \mathcal{A}$ con $X \subseteq B$ e $\operatorname{card}(\mathcal{B}) \leq \kappa$.

Dimostrazione. Sia $Y \subseteq A$ tale che $X \subseteq Y$ e $|Y| = \kappa$. Poiché

$$|H(\mathcal{A})| \leq |\operatorname{Fml}(\boldsymbol{L})| = |\boldsymbol{L}| \,,$$

segue dal Teorema 18.6 che

$$\kappa \leq |Y| \leq \left|\operatorname{Cl}_{H(\mathcal{A})}(Y)\right| \leq \kappa \,.$$

Per il Teorema 24.16 possiamo prendere $B = \operatorname{Cl}_{H(\mathcal{A})}(Y)$. □

Corollario 24.18. *Se $\mathcal{A}$ è una struttura infinita, allora*

$$\forall \kappa \geq \max\left(\operatorname{card}(\boldsymbol{L}), \operatorname{card}(\mathcal{A})\right) \, \exists \mathcal{B} \, (\mathcal{A} \preccurlyeq \mathcal{B} \ \wedge \ \kappa = \operatorname{card}(\mathcal{B})) \,.$$

Dimostrazione. $\Sigma = \operatorname{EDiag}(\mathcal{A})$. □

24.D.1. *Gruppi con elementi di torsione.* Sia G un gruppo tale che

$$\forall n \, \exists g \in G \, (o(g) \geq n) \,,$$

dove $o(g)$ è l'ordine di g, cioè il minimo $k \geq 1$ tale che $g^k = 1_G$, se esiste un k siffatto, oppure $o(g) = \infty$, se $\forall k \geq 1 \, (o(g) \neq 1_G)$. Sia

$$\Sigma = \operatorname{EDiag}(G) \cup \{ \, \boldsymbol{c}^n \neq 1 \mid n \geq 1 \, \} \,,$$

dove $\boldsymbol{c}$ è un nuovo simbolo di costante. Ogni sottoinsieme finito di $\{ \, \boldsymbol{c}^n \neq 1 \mid n \geq 1 \, \}$ è soddisfatto in un'espansione di G e quindi Σ è finitamente soddisfacibile. Quindi un modello di Σ è un gruppo H con un elemento privo di torsione e tale che $G \preccurlyeq H$.

24.D.2. *Buoni ordini.* Fissiamo un ordinale $\alpha \geq \omega$. Sia

$$\Sigma = \mathrm{EDiag}(\langle \alpha, < \rangle) \cup \{\, \boldsymbol{c}_{n+1} < \boldsymbol{c}_n \mid n \in \omega \,\}$$

dove le $\boldsymbol{c}_n$ sono nuovi simboli di costante. Fissato $N \in \omega$, consideriamo la struttura $\mathcal{A}$ di universo α dove

$$\boldsymbol{c}_n^{\mathcal{A}} = \begin{cases} N - n & \text{se } n \leq N, \\ 0 & \text{altrimenti.} \end{cases}$$

Allora $\mathcal{A}$ è un modello per $\mathrm{EDiag}(\langle \alpha, < \rangle) \cup \{\, \boldsymbol{c}_{n+1} < \boldsymbol{c}_n \mid n < N \,\}$. Poiché N è arbitrario, ne segue che Σ è finitamente soddisfacibile. Quindi c'è un ordine lineare $\langle A, < \rangle$ mal-fondato tale che $\langle \alpha, < \rangle \not\preccurlyeq \langle A, < \rangle$.

24.D.3. *Analisi non-standard.* Consideriamo il linguaggio $\boldsymbol{L}$ contenente

- simboli di costante $\mathring{x}$, per ogni $x \in \mathbb{R}$,
- simboli di funzione $\mathring{f}$, per ogni $f \colon \mathbb{R}^n \to \mathbb{R}$ e ogni $n \geq 1$,
- simboli di relazione $\mathring{R}$, per ogni $R \subseteq \mathbb{R}^n$ e ogni $n \geq 1$.

Sia $\mathcal{R} = \langle \mathbb{R}, \dots \rangle$ l'espansione canonica di $\mathbb{R}$ per $\boldsymbol{L}$. Fissimamo $\boldsymbol{c}$ un nuovo simbolo di costante e sia

$$\Sigma = \mathrm{Th}(\mathcal{R}) \cup \left\{\, 0 < \boldsymbol{c} < 2^{-n} \mid n \in \mathbb{N} \,\right\}.$$

Fissato $N \in \mathbb{N}$, consideriamo l'espansione $\tilde{\mathcal{R}}$ di $\mathcal{R}$ ad $\boldsymbol{L} \cup \{\boldsymbol{c}\}$ ottenuta ponendo $(\boldsymbol{c})^{\tilde{\mathcal{R}}} = 2^{-N}$. Allora $\tilde{\mathcal{R}} \models \mathrm{Th}(\mathcal{R}) \cup \{\, 0 < \boldsymbol{c} < 2^{-n} \mid n < N \,\}$, quindi, per l'arbitrarietà di N, Σ è finitamente soddisfacibile. Sia ${}^*\mathcal{R} = \langle {}^*\mathbb{R}, \dots \rangle$ un modello di Σ. Poichè la mappa

$$\mathbb{R} \to {}^*\mathbb{R}, \qquad x \mapsto (\mathring{x})^{{}^*\mathcal{R}}$$

è un'immersione elementare, possiamo supporre che $\mathbb{R} \subseteq {}^*\mathbb{R}$. Ogni relazione $R \subseteq \mathbb{R}^n$ e ogni funzione $f \colon \mathbb{R}^n \to \mathbb{R}$ si estende ad una relazione ${}^*R \subseteq {}^*\mathbb{R}^n$ o funzione ${}^*f \colon {}^*\mathbb{R}^n \to \mathbb{R}$. In particolare ${}^*\mathbb{R}$ è un campo ordinato. Un elemento $x \in {}^*\mathbb{R}$ si dice

infinitesimo se $0 < |x| < 2^{-n}$, per ogni $n \in \mathbb{N}$;

infinito se $n < |x|$, per ogni $n \in \mathbb{N}$;

finito se $|x| \leq n$, per qualche $n \in \mathbb{N}$.

Dati $x, y \in {}^*\mathbb{R}$ diremo che x e y sono **infinitamente vicini**, $x \approx y$, se $|x - y|$ è 0 oppure è un infinitesimo; che x è infinitesimo rispetto a y o che y è infinito rispetto a x se $\forall n \in \mathbb{N}\, (n \cdot |x| < |y|)$.

Esercizio 24.19. Dimostrare che:

(i) l'elemento $(\boldsymbol{c})^{{}^*\mathcal{R}}$ è un infinitesimo;

(ii) l'inverso di un infinitesimo è un infinito e, viceversa, l'inverso di un infinito è un infinitesimo;

(iii) per ogni infinitesimo ε esistono infinitesimi δ e η tali che δ è infinitesimo rispetto a ε ed ε è infinitesimo rispetto a δ. Analogamente, per ogni infinito N esistono infiniti M e L tali che N è infinito rispetto a M e L è infinito rispetto a N.

Si dimostra che una funzione $f\colon \mathbb{R} \to \mathbb{R}$ è continua nel punto $x_0 \in \mathbb{R}$ se e solo se $f(x_0 + \varepsilon) \approx f(x_0)$ per ogni infinitesimo ε. Analogamente è possibile definire i vari concetti dell'Analisi (differenziabilità, integrazione, etc.) in termini di infinitesimi. Lo studio della struttura ${}^*\mathcal{R}$ si dice *Analisi non-standard*.

Esercizi

Esercizio 24.20. Generalizzare la Proposizione 24.15 dimostrando che se

$$\big(\langle \mathcal{A}_x \mid x \in D\rangle\,, \langle \pi_{x,y} \mid x, y \in D \wedge x \leq y\rangle\big)$$

è un sistema diretto superiormente di strutture e mappe elementari, allora

$$\pi_{y,\infty}\colon \mathcal{A}_x \to \varinjlim_{x\in D} \mathcal{A}_x$$

è elementare, per ogni $y \in D$.

Esercizio 24.21. Dimostrare che se Σ è un insieme di enunciati in un linguaggio arbitrario che ha modelli finiti di cardinalità arbitrariamente grande, allora ha un modello di cardinalità $\leq 2^{\aleph_0}$.

Dare un esempio di una teoria (in un linguaggio necessariamente più che numerabile) che ha modelli finiti di cardinalità arbitrariamente grande, che ha un modello di cardinalità $2^{\aleph_0}$, ma nessun modello infinito di di cardinalità $< 2^{\aleph_0}$.

Esercizio 24.22. In questo esercizio daremo una nuova dimostrazione del Teorema 14.12 di Stone.

Sia $\boldsymbol{L}$ il linguaggio $\{X, \mathcal{F}, \mathring{\in}, C, U, I\}$ dove

- $X, \mathcal{F}$ sono simboli di relazione 1-arie,
- $\mathring{\in}, C$ sono simboli di relazione 2-arie,
- U, I sono simboli di relazione 3-arie.

Dare un insieme finito di assiomi Σ nel linguaggio $\boldsymbol{L}$ tale che ogni suo modello è isomorfo ad una struttura con universo $X \cup \mathcal{F}$, dove $X \neq \emptyset$, $X \cap \mathcal{F} = \emptyset$, $\mathcal{F} \subseteq \mathscr{P}(X)$ è una sub-algebra, la relazione $\mathring{\in}$ è interpretata come l'appartenenza tra elementi di X ed elementi di $\mathcal{F}$ e gli insiemi C, I e U sono,

rispettivamente, i grafi delle funzioni complementi, intersezione e unione in $\mathcal{F}$.

Sia B un'algebra di Boole e sia $\tilde{\boldsymbol{L}} = \boldsymbol{L} \cup \left\{ \mathring{b} \mid b \in B \right\}$. Dimostrare che $\mathrm{Diag}(B) \cup \Sigma$ è un insieme finitamente soddisfacibile di $\tilde{\boldsymbol{L}}$-enunciati. Concludere che B è isomorfa ad una sub-algebra di $\mathscr{P}(X)$, per qualche insieme X.

Esercizio 24.23. Il Teorema dei Quattro Colori asserisce che ogni carta geografica piana con un numero finito di regioni può essere colorata con 4 colori in modo che due regioni contigue siano sempre di colore diverso. Dimostrare che il Teorema vale anche per le carte piane con un numero infinito di regioni.

Esercizio 24.24. Se $(P, \leq)$ è un insieme parzialmente ordinato, un $I \subseteq P$ si dice **indipendente** se

$$\forall x, y \in P \, [x \neq y \Rightarrow (x \not\leq y \wedge y \not\leq x)] \, .$$

Un insieme indipendente interseca una catena in al più un punto, quindi se P è unione di n catene, allora ogni insieme indipendente ha cardinalità $\leq n$. R.P. Dilworth nel 1950 dimostrò il converso per gli ordini parziali *finiti*.

Teorema 24.25 (Dilworth)**.** *Sia $(P, \leq)$ un ordine parziale finito tale che ogni insieme indipendente ha cardinalità $\leq n$. Allora ci sono delle catene $C_0, \ldots, C_{n-1} \subseteq P$ tali che $\bigcup_{i<n} C_i = P$.*

Generalizzare questo risultato a *tutti* gli insiemi parzialmente ordinati.

25. Categoricità

Diremo che Σ è **completo** se è soddisfacibile ed è massimale rispetto all'inclusione, vale a dire: se $\Sigma \subset \Sigma' \subseteq \mathrm{Sent}(\boldsymbol{L})$, allora $\mathfrak{Mod}(\Sigma') = \emptyset$.

Una teoria T si dice

- **categorica** se ammette un unico modello (a meno di isomorfismi);
- **κ-categorica** se ammette un unico modello (a meno di isomorfismi) di cardinalità κ, dove κ è un cardinale infinito.

Per il Teorema di Lowenheim-Skolem all'insù, se T è categorica, allora il suo unico modello è finito.

Teorema 25.1. *Sia T una teoria in un linguaggio di cardinalità $\leq \kappa$ che ammetta un modello infinito e che sia κ-categorica. Allora T è completa.*

Dimostrazione. Se $\boldsymbol{\sigma} \in \mathrm{Sent}(\boldsymbol{L})$ testimonia che T non è completa, siano $\mathcal{A}$ e $\mathcal{B}$ modelli di T che soddisfano $\boldsymbol{\sigma}$ e $\boldsymbol{\neg\sigma}$, rispettivamente. Per il Teorema 23.10 di Löwenheim-Skolem all'insù possiamo supporre che $\mathrm{card}(\mathcal{A}) =$

$\mathrm{card}(\mathcal{B}) \geq \kappa$ e per il Teorema 24.17 di Löwenheim-Skolem all'ingiù possiamo supporre che $\mathrm{card}(\mathcal{A}) = \mathrm{card}(\mathcal{B}) = \kappa$. Ma quindi $\mathcal{A} \cong \mathcal{B}$, contraddicendo l'assunzione che $\mathcal{A} \models \boldsymbol{\sigma}$ e $\mathcal{B} \models \boldsymbol{\neg\sigma}$. □

25.A. Esempi.

25.A.1. *Insiemi infiniti.* La teoria T che ha per assiomi gli enunciati $\boldsymbol{\varepsilon}_{\geq n}$ di 106 è κ-categorica per ogni κ, dato che un modello di T di cardinalità κ è semplicemente un insieme di cardinalità κ.

25.A.2. *Gruppi abeliani.* Per ogni cardinale infinito κ i gruppi $\bigoplus_{\alpha<\kappa} \mathbb{Z}$ e $\bigoplus_{\alpha<\kappa} \mathbb{Z}/2\mathbb{Z}$ sono di cardinalità κ e non sono mai isomorfi. Quindi la teoria dei gruppi abeliani non è mai κ-categorica.

25.A.3. *Ordini lineari densi senza né primo né ultimo elemento.* Ricordiamo che un ordine lineare (stretto) si dice denso se tra due punti c'è sempre un punto. La classe degli ordini lineari densi, senza né primo né ultimo elemento è elementare e $\mathbb{Q}$ ed $\mathbb{R}$ sono esempi di ordini siffatti. Per il Teorema 9.3, la teoria degli ordini lineari densi, senza né primo né ultimo elemento è ω-categorica e quindi è completa. Per l'Esercizio 9.22, questa teoria non è $2^{\aleph_0}$-categorica: infatti si dimostra che per ogni cardinale più che numerabile κ è possibile costruire esempi di ordini lineari densi senza né primo né ultimo elemento di cardinalità κ e non isomorfi.

25.A.4. *Campi algebricamente chiusi.* ACF_p è la teoria dei campi algebricamente chiusi di caratteristica p, dove p è un numero primo oppure $p = 0$. (Il linguaggio è quello per gli anelli $\{+, -, \cdot, 0, 1\}$.) Sia $\mathbb{F} \models \mathrm{ACF}_p$, sia $\mathbb{F}'$ il suo sotto-campo primo e sia $X \subseteq \mathbb{F}$ una base di trascendenza di $\mathbb{F}$ su $\mathbb{F}'$. Osserviamo che $\mathbb{F}'$ è $\mathbb{Z}/p\mathbb{Z}$, se p è primo, o $\mathbb{Q}$ se $p = 0$; quindi $\mathbb{F}'$ è numerabile. La base di trascendenza X esiste per il Lemma di Zorn ed ha la cardinalità di $\mathbb{F}$, se $\mathbb{F}$ è più che numerabile. Se X e Y sono due basi di trascendenza per i campi $\mathbb{F}$ e $\mathbb{G}$ di ugual caratteristica e se $\pi\colon X \to Y$ è una bijezione, allora π si estende ad un isomorfismo $\pi\colon \mathbb{F} \to \mathbb{G}$. Quindi, se $\mathbb{F}$, $\mathbb{G}$ sono campi algebricamente chiusi di ugual caratteristica e più che numerabili, allora hanno basi di trascendenza di ugual cardinalità e quindi sono isomorfi. Abbiamo quindi verificato che ACF_p è κ-categorica, se $\kappa > \omega$.

Esercizio 25.2. Verificare che ACF_p non è $\aleph_0$-categorica.

25.B. Applicazioni.

25.B.1. *Principio di Lefschetz.* Dall'esempio **??** e dal Corollario 23.4 otteniamo

> Se $\boldsymbol{\sigma}$ è un enunciato nel linguaggio degli anelli $\{+, -, \cdot, 0, 1\}$ che vale in ogni campo di caratteristica 0, allora vale in ogni campo di caratteristica p, con p sufficientemente elevato.

In altre parole

$$\boldsymbol{\sigma} \in \mathrm{ACF}_0 \quad \Leftrightarrow \quad \exists n \forall p > n \, (p \text{ primo } \Rightarrow \boldsymbol{\sigma} \in \mathrm{ACF}_p) \, .$$

Una generalizzazione di questo è il seguente *Principio di Lefschetz*:

Teorema 25.3. *Sia $\boldsymbol{\sigma}$ è un enunciato nel linguaggio degli anelli $\{+, -, \cdot, 0, 1\}$. Allora $\boldsymbol{\sigma}$ vale in un campo algebricamente chiuso di caratteristica 0 se e solo se vale in campi algebricamente chiusi di caratteristica p, con p primo arbitrariamente grande.*

Dimostrazione. Sia ACF_p la teoria dei campi algebricamente chiusi di caratteristica p, con p primo oppure $p = 0$. Se $\mathbb{F}$ un campo algebricamente chiuso di caratteristica 0 e $\mathbb{F} \models \boldsymbol{\sigma}$, allora $\mathrm{ACF}_0 \models \boldsymbol{\sigma}$ per la completezza di ACF_0. Quindi per quanto sopra $\mathrm{ACF}_p \models \boldsymbol{\sigma}$, per tutti i primi p sufficientemente grandi.

Vice versa, supponiamo che

$$\forall n \in \mathbb{N} \, \exists p > n \, \exists \mathbb{F} \text{ campo algebricamente chiuso di caratteristica } p \text{ e } \mathbb{F} \models \boldsymbol{\sigma} \, .$$

Osserviamo che se $\mathbb{F}$ è algebricamente chiuso di caratteristica p e $\mathbb{F} \models \boldsymbol{\sigma}$, allora, per la completezza della teoria dei campi algebricamente chiusi di caratteristica p, ogni altro campo $\mathbb{F}'$ algebricamente chiuso di caratteristica p soddisfa $\boldsymbol{\sigma}$. Fissiamo un'enumerazione $\langle p_n \mid n \in \omega \rangle$ di tutti i numeri primi e sia $\mathbb{F}_n$ un campo algebricamente chiuso di caratteristica p_n. Sia $X = \{ \, n \in \omega \mid \mathbb{F}_n \models \boldsymbol{\sigma} \, \}$ e sia U un ultrafiltro su ω tale che $X \in U$. Per il Teorema 23.13 di Łos $\prod_U \mathbb{F}_n$ è un campo algebricamente chiuso di caratteristica 0 che soddisfa $\boldsymbol{\sigma}$ e quindi $k \models \boldsymbol{\sigma}$. □

25.B.2. *Variabili complesse.* Se A è un anello, una funzione $f \colon A^n \to A^n$ si dice polinomiale se $f = (f_1, \ldots, f_n)$, con $f_i \in A[X_1, \ldots, X_n]$. Il grado di f è $\max(\deg(f_1), \ldots, \deg(f_n))$. Dimostreremo il seguente

Teorema 25.4 (Ax)**.** *Ogni funzione polinomiale iniettiva $f \colon \mathbb{C}^n \to \mathbb{C}^n$ è suriettiva.*

Osserviamo che per ogni $n, d > 0$ c'è un enunciato $\boldsymbol{\sigma}_{n,d}$ del linguaggio degli anelli tale che $A \models \boldsymbol{\sigma}_{n,d}$ se e solo se

> ogni funzione polinomiale iniettiva
>
> $$A^n \to A^n$$
>
> di grado $\leq d$ è suriettiva,

per ogni anello commutativo unitario A. Quindi vogliamo dimostrare che per ogni $n, d > 0$

$$\mathbb{C} \models \boldsymbol{\sigma}_{n,d}$$

o, equivalentemente, che $\boldsymbol{\sigma}_{n,d} \in \mathrm{ACF}_0$. Per il Principio di Lefschetz è sufficiente dimostrare che $\boldsymbol{\sigma}_{n,d} \in \mathrm{ACF}_p$ per primi p arbitrariamente grandi: dimostreremo che ciò vale per *ogni* p.

Sia $\mathbb{F}$ un campo algebricamente chiuso di caratteristica p: vogliamo verificare che $\mathbb{F} \models \boldsymbol{\sigma}_{n,d}$. Per completezza di ACF_p, possiamo supporre che $\mathbb{F}$ sia $\widehat{\mathbb{Z}/p\mathbb{Z}}$, la chiusura algebrica di $\mathbb{Z}/p\mathbb{Z}$. Allora $\mathbb{F} = \bigcup_k \mathbb{F}_k$ dove gli $\mathbb{F}_k$ sono campi finiti (non algebricamente chiusi) di caratteristica p. Sia $f\colon \mathbb{F}^n \to \mathbb{F}^n$ una funzione polinomiale iniettiva di grado $\leq d$ e sia $\bar{b} \in \mathbb{F}^n$: vogliamo mostrare che c'è un $\bar{a}$ tale che $f(\bar{a}) = \bar{b}$. Sia k sufficientemente elevato tale che tutti i coefficienti di f e $b_1, \dots, b_n$ sono in $\mathbb{F}_k$. Quindi $f \restriction \mathbb{F}_k^n\colon \mathbb{F}_k^n \to \mathbb{F}_k^n$ è una funzione polinomiale iniettiva: ma ogni funzione iniettiva da un insieme finito in sé stesso è suriettiva, quindi esistono $a_1, \dots, a_n \in \mathbb{F}_k \subseteq \mathbb{F}$ tali che $f(\bar{a}) = \bar{b}$.

Esercizi

Esercizio 25.5. Sia $<_{\mathrm{lex}}$ l'ordine lineare stretto su ${}^{\omega}\mathbb{Z}$ dato da $x <_{\mathrm{lex}} y$ se e solo se $\exists n\,(x \restriction n = y \restriction n \wedge x(n) < y(n))$. Dimostrare che $<_{\mathrm{lex}}$ è un ordine lineare denso senza primo e ultimo elemento.

Esercizio 25.6. Dimostrare che ogni ordine lineare numerabile $\langle X, \trianglelefteq \rangle$ si immerge in $\langle \mathbb{Q}, \leq \rangle$.

26. Insiemi definibili

Definizione 26.1. Sia $\mathcal{A}$ una $\boldsymbol{L}$-struttura e sia $P \subseteq \|\mathcal{A}\|$. Un insieme $X \subseteq \|\mathcal{A}\|^n$, con $n > 0$, si dice **definibile con parametri in** P se esiste una formula $\boldsymbol{\varphi}(\boldsymbol{x}_1, \dots, \boldsymbol{x}_n, \boldsymbol{y}_1, \dots, \boldsymbol{y}_m)$ ed esistono $p_1, \dots, p_m \in P$, tali che

$$X = \{\, (a_1, \dots, a_n) \in A^n \mid \mathcal{A} \models \boldsymbol{\varphi}[a_1, \dots, a_n, p_1, \dots, p_m] \,\}$$

Diremo che X è definibile se è definibile con parametri in P, per qualche insieme P o, equivalentemente, se è definibile con parametri in A. Se l'insieme P dei parametri è vuoto, allora diremo che X è **definibile senza parametri**.

Un elemento $a \in A$ si dice definibile in $\mathcal{A}$ con parametri in P se $\{a\}$ è definibile con parametri in P. Chiaramente ogni elemento $a \in A$ è definibile con parametri in $\{a\}$. Diremo quindi che un elemento è definibile se è definibile senza parametri. In altre parole: un elemento $a \in A$ è definibile se è l'unico elemento di A che soddisfa una qualche formula $\boldsymbol{\varphi}(\boldsymbol{x})$ con un'unica variabile libera.

Lemma 26.2. (a) *Se $q_1, \dots, q_m$ sono definibili in $\mathcal{A}$ con parametri in P e $X \subseteq A^n$ è definibile con parametri in $\{q_1, \dots, q_m\} \cup P'$ allora X è definibile con parametri in $P \cup P'$.*

(b) *Se R è una relazione definibile in $\mathcal{A}$ con parametri in P, $\langle \mathcal{A}, R\rangle$ è l'espansione di $\mathcal{A}$ ottenuta aggiungendo la relazione R e X è definibile in $\langle \mathcal{A}, R\rangle$ con parametri in Q, allora X è definibile in $\mathcal{A}$ con parametri in $P \cup Q$.*

Dimostrazione. (a) Per semplicità notazionale consideriamo il caso in cui $m = 1$. Sia $\boldsymbol{\varphi}(\boldsymbol{x}, p_1, \dots, p_k)$ una formula che definisce q_1 con parametri in P e sia $\boldsymbol{\psi}(\boldsymbol{y}_1, \dots, \boldsymbol{y}_n, q_1, p'_1, \dots, p'_h)$ una formula che definisce X con parametri q_1 e $p'_1, \dots, p'_h \in P'$. Allora la formula

$$\boldsymbol{\exists x}\left(\boldsymbol{\varphi}(\boldsymbol{x}, p_1, \dots, p_k) \boldsymbol{\wedge} \boldsymbol{\psi}(\boldsymbol{y}_1, \dots, \boldsymbol{y}_n, \boldsymbol{x}, p'_1, \dots, p'_h)\right)$$

definisce X in $\mathcal{A}$ con parametri in $\{p_1, \dots, p_k\} \cup \{p'_1, \dots, p'_h\} \subseteq P \cup P'$.

(b) Per semplicità notazionale supponiamo R 1-aria e X n-aria. Sia $\boldsymbol{\varphi}(\boldsymbol{x}, p_1, \dots, p_k)$ una $\boldsymbol{L}$-formula che definisce R e sia $\tilde{\boldsymbol{\psi}}(\boldsymbol{y}_1, \dots, \boldsymbol{y}_n, p'_1, \dots, p'_h)$ una $\boldsymbol{L} \cup \{\mathring{R}\}$-formula che definisce X in $\langle \mathcal{A}, R\rangle$. La $\boldsymbol{L}$-formula

$$\boldsymbol{\psi}(\boldsymbol{y}_1, \dots, \boldsymbol{y}_n, p_1, \dots, p_k, p'_1, \dots, p'_h)$$

ottenuta da $\tilde{\boldsymbol{\psi}}$ rimpiazzando tutte le occorrenze della forma "$\mathring{R}(\boldsymbol{x})$" con "$\boldsymbol{\varphi}(\boldsymbol{x}, p_1, \dots, p_k)$" (per ogni scelta di variabile $\boldsymbol{x}$) definisce X in $\mathcal{A}$ con parametri $p_1, \dots, p_k, p'_1, \dots, p'_h \in P$, come richiesto. □

26.A. Esempi di insiemi definibili.

26.A.1. Sia $\langle G, \cdot\rangle$ un gruppo. L'elemento neutro $1_G \in G$ è definibile mediante la formula $\boldsymbol{\varphi}(\boldsymbol{u})$

$$\boldsymbol{\forall z}\,(\boldsymbol{z} * \boldsymbol{u} \equiv \boldsymbol{u} * \boldsymbol{z} \equiv \boldsymbol{z})\,.$$

La funzione "inverso" $I = \{\, (g, h) \in G \times G \mid g \cdot h = 1 \,\}$ è definibile con parametri in $\{1_G\}$ mediante la formula $\boldsymbol{\psi}(\boldsymbol{x}, \boldsymbol{y}, 1)$

$$\boldsymbol{x} \cdot \boldsymbol{y} \equiv 1\,.$$

Quindi I è definibile in $\langle G, \cdot\rangle$ senza parametri per il Lemma 26.2.

26.A.2. La relazione $<$ è definibile senza parametri in $\langle \mathbb{N}, +\rangle$ mediante la formula $\boldsymbol{\varphi}(\boldsymbol{x}, \boldsymbol{y})$

$$\boldsymbol{\exists z}\,(\boldsymbol{z} \not\equiv 0 \boldsymbol{\wedge} \boldsymbol{x} + \boldsymbol{z} \equiv \boldsymbol{y})\,.$$

(Stiamo usando il Lemma 26.2 e il fatto che lo 0 è definibile in quanto è l'elemento neutro dell'operazione $+$.)

26.A.3. Ogni numero naturale è definibile in $\langle \mathbb{N}, < \rangle$. Costruiamo induttivamente la formula $\boldsymbol{\varphi}_n(\boldsymbol{x})$ che definisce n: poniamo $\boldsymbol{\varphi}_0(\boldsymbol{x})$

$$\boldsymbol{\forall y}\,(\boldsymbol{x} \equiv \boldsymbol{y} \boldsymbol{\vee} \boldsymbol{x} < \boldsymbol{y})$$

e $\boldsymbol{\varphi}_{n+1}(\boldsymbol{x})$

$$\boldsymbol{\forall y}\,(\boldsymbol{\varphi}_0(\boldsymbol{y}) \boldsymbol{\vee} \ldots \boldsymbol{\vee} \boldsymbol{\varphi}_n(\boldsymbol{y}) \boldsymbol{\vee} \boldsymbol{x} \equiv \boldsymbol{y} \boldsymbol{\vee} \boldsymbol{x} < \boldsymbol{y})$$

Quindi, per la parte (b) del Lemma 26.2 ogni elemento di $\langle \mathbb{N}, + \rangle$ è definibile.

26.A.4. La relazione $\leq$ è definibile in $\langle \mathbb{R}, +, \cdot \rangle$ mediante la formula

$$\boldsymbol{\exists z}\,(\boldsymbol{x} + \boldsymbol{z} \cdot \boldsymbol{z} \equiv \boldsymbol{y})\,.$$

26.A.5. L'insieme $\mathbb{N}$ è definibile in $\langle \mathbb{Z}, +, \cdot \rangle$: per un teorema di Lagrange, ogni numero naturale è somma di quattro quadrati, quindi $\mathbb{N}$ è definito da $\boldsymbol{\varphi}(\boldsymbol{x})$

$$\boldsymbol{\exists y}_1\, \boldsymbol{\exists y}_2\, \boldsymbol{\exists y}_3\, \boldsymbol{\exists y}_4\, (\boldsymbol{y}_1 \cdot \boldsymbol{y}_1 + \boldsymbol{y}_2 \cdot \boldsymbol{y}_2 + \boldsymbol{y}_3 \cdot \boldsymbol{y}_3 + \boldsymbol{y}_4 \cdot \boldsymbol{y}_4 \equiv \boldsymbol{x})\,.$$

26.B. Automorfismi e insiemi definibili. Per la Proposizione 24.8, se $X \subseteq A^n$ è definito da $\boldsymbol{\varphi}$ e parametri $p_1, \ldots, p_m$, allora l'immagine di X via $\pi \in \mathrm{Aut}(\mathcal{A})$

$$\pi[X] = \{\, \pi(\bar{a}) \mid \bar{a} \in X \,\}$$

è definito da $\boldsymbol{\varphi}$ e parametri $\pi(p_1), \ldots, \pi(p_m)$. In particolare, se $p_1, \ldots, p_m$ sono lasciati fissi da π, allora $\pi[X] = X$. In altre parole abbiamo dimostrato che

Lemma 26.3. *Se $\pi \in \mathrm{Aut}(\mathcal{A})$, $\pi(p_i) = p_i$ $(i = 1, \ldots, m)$ e $\pi[X] \neq X$, allora X non è definibile in $\mathcal{A}$ con parametri $p_1, \ldots, p_m$.*

Poiché $z \mapsto \bar{z}$ è un automorfismo del campo complesso, ne segue che il numero i non è definibile in $\langle \mathbb{C}, +, \cdot, 0, 1 \rangle$.

Esercizi

Esercizio 26.4. Sia $\mathrm{Def}^n_{\mathcal{A}}(P)$ l'insieme dei sottoinsiemi di A^n definibili in $\mathcal{A}$ con parametri in P, $n \geq 1$. Dimostrare che $\mathrm{Def}^n_{\mathcal{A}}(P)$ è una sub-algebra di $\mathscr{P}(A^n)$.

Esercizio 26.5. Dimostrare che $\mathbb{N}$ e $<$ non sono definibili senza parametri né in $\langle \mathbb{Z}, + \rangle$ né in $\langle \mathbb{R}, + \rangle$.

Esercizio 26.6. Dimostrare che $\mathrm{Def}^1_{\langle \mathbb{R}, \leq \rangle}(p_1, \dots, p_n)$ è formato da unioni finite di intervalli[5] (chiusi, aperti, semi-aperti) con estremi in $\{p_1, \dots, p_n\}$ e dall'insieme vuoto. Concludere che in un ordine $\langle X, \leq \rangle$ lineare denso, senza né primo né ultimo elemento, i sottoinsiemi di X definibili con parametri sono le unioni finite di intervalli e l'insieme vuoto.

27. Sintassi

27.A. Derivazioni. Un **assioma logico** di un linguaggio $\boldsymbol{L}$ è una formula $\boldsymbol{\varphi}$ di $\boldsymbol{L}$ che è una tautologia, oppure è della forma:

(LAx-1) $\boldsymbol{\forall x\, (\varphi \Rightarrow \psi) \Rightarrow (\varphi \Rightarrow \forall x\, \psi)}$, se $\boldsymbol{x \notin Fv(\varphi)}$.

(LAx-2) $\boldsymbol{\forall x\, \varphi \Rightarrow \varphi[t/x]}$ se $\boldsymbol{t}$ è sostituibile ad $\boldsymbol{x}$ in $\boldsymbol{\varphi}$. In particolare $\boldsymbol{\forall x\, \varphi \Rightarrow \varphi}$.

(LAx-3) $\boldsymbol{t \equiv t}$, per ogni termine $\boldsymbol{t}$.

(LAx-4) $\boldsymbol{x \equiv y \Rightarrow t[x/z] \equiv t[y/z]}$, per ogni termine $\boldsymbol{t}$.

(LAx-5) $\boldsymbol{t \equiv s \Rightarrow \big(\varphi[t/x] \Leftrightarrow \varphi[s/x]\big)}$, se $\boldsymbol{t}$ e $\boldsymbol{s}$ sono sostituibili a $\boldsymbol{x}$ in $\boldsymbol{\varphi}$.

(LAx-6) $\boldsymbol{\exists x\, \varphi \Leftrightarrow \neg \forall x \neg \varphi}$.

Se $\boldsymbol{\varphi}$ è ottenuta da $\boldsymbol{\psi}$ mediante una quantificazione universale su una qualche variabile $\boldsymbol{x}$, cioè $\boldsymbol{\varphi = \forall x\, \psi}$, diremo che $\boldsymbol{\varphi}$ è stata ottenuta da $\boldsymbol{\psi}$ mediante la **regola di generalizzazione**:

$$\text{(Gen)} \qquad \frac{\boldsymbol{\psi}}{\boldsymbol{\forall x\, \psi}}$$

Diremo invece che $\boldsymbol{\varphi}$ è ottenuta mediante la **regola del *modus ponens*** da $\boldsymbol{\psi}$ e $\boldsymbol{\psi \Rightarrow \varphi}$,

$$\text{(MP)} \qquad \frac{\boldsymbol{\psi} \qquad \boldsymbol{\psi \Rightarrow \varphi}}{\boldsymbol{\varphi}}$$

Sia Γ un insieme di formule. Una **derivazione da** Γ nel linguaggio $\boldsymbol{L}$ è una sequenza finita di formule $\langle \boldsymbol{\varphi}_0, \dots, \boldsymbol{\varphi}_n \rangle$ tali che per ogni $i \leq n$

[5] Tra gli intervalli consideriamo anche le semirette e i singoletti $\{p_i\}$.

- $\boldsymbol{\varphi}_i \in \Gamma$, oppure
- $\boldsymbol{\varphi}_i$ è un assioma logico di $\boldsymbol{L}$, oppure
- $\boldsymbol{\varphi}_i$ è ottenuta mediante la regola di generalizzazione da $\boldsymbol{\varphi}_j$, per qualche $j < i$,
- $\boldsymbol{\varphi}_i$ è ottenuta mediante la regola di *modus ponens* a partire da $\boldsymbol{\varphi}_j$ e $\boldsymbol{\varphi}_k$, con $j, k < i$.

Diremo che $\boldsymbol{\varphi}$ è **derivabile da** Γ (ovvero che $\boldsymbol{\varphi}$ è un **teorema** di Γ) nel linguaggio $\boldsymbol{L}$, in simboli

$$\Gamma \vdash_{\boldsymbol{L}} \boldsymbol{\varphi}\,,$$

se esiste $\langle \boldsymbol{\varphi}_0, \dots, \boldsymbol{\varphi}_n \rangle$, derivazione da Γ in $\boldsymbol{L}$, tale che $\boldsymbol{\varphi} = \boldsymbol{\varphi}_n$. Quando il linguaggio $\boldsymbol{L}$ è chiaro dal contesto scriveremo semplicemente $\Gamma \vdash \boldsymbol{\varphi}$; se $\Gamma = \{\boldsymbol{\psi}\}$ o $\Gamma = \emptyset$, scriveremo, rispettivamente, $\boldsymbol{\psi} \vdash \boldsymbol{\varphi}$ e $\vdash \boldsymbol{\varphi}$. Se $\boldsymbol{\varphi} \vdash \boldsymbol{\psi}$ e $\boldsymbol{\psi} \vdash \boldsymbol{\varphi}$ diremo che $\boldsymbol{\varphi}$ e $\boldsymbol{\psi}$ sono derivabili l'una dall'altra, ovvero che $\boldsymbol{\varphi}$ e $\boldsymbol{\psi}$ sono **equiderivabili**.

Osservazioni 27.1. (a) Se $\Gamma \vdash_{\boldsymbol{L}} \boldsymbol{\varphi}$, $\Gamma \subseteq \Gamma'$, $\boldsymbol{L} \subseteq \boldsymbol{L}'$ e $\Gamma' \subseteq \mathrm{Fml}(\boldsymbol{L}')$, allora $\Gamma' \vdash_{\boldsymbol{L}'} \boldsymbol{\varphi}$.

(b) La relazione $\vdash$ è transitiva: se $\Gamma \vdash \boldsymbol{\varphi}$ e $\boldsymbol{\varphi} \vdash \boldsymbol{\psi}$, allora $\Gamma \vdash \boldsymbol{\psi}$.

Esercizio 27.2. Dimostrare che se $\Gamma \vdash \boldsymbol{\varphi}$, allora $\Gamma_0 \vdash \boldsymbol{\varphi}$ per qualche $\Gamma_0 \subseteq \Gamma$ finito.

27.B. Esempi di derivazione.

27.B.1. *Congiunzioni.* $\Gamma \vdash \boldsymbol{\varphi} \boldsymbol{\wedge} \boldsymbol{\psi}$ se e solo se $\Gamma \vdash \boldsymbol{\varphi}$ e $\Gamma \vdash \boldsymbol{\psi}$:

Supponiamo $\Gamma \vdash \boldsymbol{\varphi} \boldsymbol{\wedge} \boldsymbol{\psi}$. Allora

$$\begin{array}{ll} \left.\begin{array}{c}\vdots\\ \boldsymbol{\varphi} \boldsymbol{\wedge} \boldsymbol{\psi}\end{array}\right\} \Gamma \vdash \boldsymbol{\varphi} \boldsymbol{\wedge} \boldsymbol{\psi} & \\ \boldsymbol{\varphi} \boldsymbol{\wedge} \boldsymbol{\psi} \boldsymbol{\Rightarrow} \boldsymbol{\varphi} & \text{(Taut)} \\ \boldsymbol{\varphi} & \text{(MP)} \end{array}$$

è una derivazione di $\boldsymbol{\varphi}$ da Γ. Analogamente si dimostra che $\Gamma \vdash \boldsymbol{\psi}$. Viceversa

$$\begin{array}{ll} \left.\begin{array}{c}\vdots\\ \boldsymbol{\varphi}\end{array}\right\} \Gamma \vdash \boldsymbol{\varphi} & \\ \left.\begin{array}{c}\vdots\\ \boldsymbol{\psi}\end{array}\right\} \Gamma \vdash \boldsymbol{\psi} & \\ \boldsymbol{\varphi} \boldsymbol{\Rightarrow} (\boldsymbol{\psi} \boldsymbol{\Rightarrow} \boldsymbol{\varphi} \boldsymbol{\wedge} \boldsymbol{\psi}) & \text{(Taut)} \\ \boldsymbol{\psi} \boldsymbol{\Rightarrow} \boldsymbol{\varphi} \boldsymbol{\wedge} \boldsymbol{\psi} & \text{(MP)} \\ \boldsymbol{\varphi} \boldsymbol{\wedge} \boldsymbol{\psi} & \text{(MP)} \end{array}$$

è una derivazione di $\boldsymbol{\varphi} \boldsymbol{\wedge} \boldsymbol{\psi}$ in Γ.

27.B.2. *Termini equivalenti.*

$$\vdash \boldsymbol{t}_1 \equiv \boldsymbol{s}_1 \boldsymbol{\wedge} \ldots \wedge \boldsymbol{t}_n \equiv \boldsymbol{s}_n \boldsymbol{\Rightarrow} [\boldsymbol{R}(\boldsymbol{t}_1, \ldots, \boldsymbol{t}_n) \boldsymbol{\Leftrightarrow} \boldsymbol{R}(\boldsymbol{t}_1, \ldots, \boldsymbol{t}_n)] \,.$$

Infatti

$$\begin{gathered} \boldsymbol{t}_n \equiv \boldsymbol{s}_n \boldsymbol{\Rightarrow} [\boldsymbol{R}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{n-1}, \boldsymbol{t}_n) \boldsymbol{\Leftrightarrow} \boldsymbol{R}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{n-1}, \boldsymbol{t}_n)] \\ \boldsymbol{t}_{n-1} \equiv \boldsymbol{s}_{n-1} \boldsymbol{\Rightarrow} [\boldsymbol{t}_n \equiv \boldsymbol{s}_n \boldsymbol{\Rightarrow} [\boldsymbol{R}(\boldsymbol{t}_1, \ldots, \boldsymbol{t}_n) \boldsymbol{\Leftrightarrow} \boldsymbol{R}(\boldsymbol{t}_1, \ldots, \boldsymbol{t}_n)]] \\ \vdots \\ \boldsymbol{t}_1 \equiv \boldsymbol{s}_1 \boldsymbol{\Rightarrow} [\boldsymbol{t}_2 \equiv \boldsymbol{s}_2 \boldsymbol{\Rightarrow} \cdots \boldsymbol{\Rightarrow} [\boldsymbol{t}_n \equiv \boldsymbol{s}_n \boldsymbol{\Rightarrow} [\boldsymbol{R}(\boldsymbol{t}_1, \ldots, \boldsymbol{t}_n) \boldsymbol{\Leftrightarrow} \boldsymbol{R}(\boldsymbol{t}_1, \ldots, \boldsymbol{t}_n)]] \cdots] \end{gathered}$$

sono assiomi di tipo (LAx-5) e dato che

$$\boldsymbol{\alpha}_1 \boldsymbol{\wedge} \ldots \boldsymbol{\wedge} \boldsymbol{\alpha}_n \boldsymbol{\Rightarrow} [\boldsymbol{\alpha}_1 \boldsymbol{\Rightarrow} [\boldsymbol{\alpha}_2 \boldsymbol{\Rightarrow} \ldots \boldsymbol{\beta}] \cdots]$$

è una tautologia, il risultato segue per MP.

27.B.3. *Da una contraddizione si può derivare una qualsiasi formula.* Se

$$\Gamma \vdash \boldsymbol{\psi} \boldsymbol{\wedge} \boldsymbol{\neg} \boldsymbol{\psi}$$

per qualche formula $\boldsymbol{\psi}$, allora $\Gamma \vdash \boldsymbol{\varphi}$, per ogni formula $\boldsymbol{\varphi}$.

Infatti

$$\begin{array}{ll} \left.\begin{array}{c} \vdots \\ \boldsymbol{\psi} \boldsymbol{\wedge} \boldsymbol{\neg} \boldsymbol{\psi} \end{array}\right\} \Gamma \vdash \boldsymbol{\psi} \boldsymbol{\wedge} \boldsymbol{\neg} \boldsymbol{\psi} & \\ (\boldsymbol{\psi} \boldsymbol{\wedge} \boldsymbol{\neg} \boldsymbol{\psi}) \boldsymbol{\Rightarrow} \boldsymbol{\varphi} & \text{(Taut)} \\ \boldsymbol{\varphi} & \text{(MP)} \end{array}$$

27.B.4. *Implicazioni.* Se $\Gamma \vdash \boldsymbol{\varphi} \boldsymbol{\Rightarrow} \boldsymbol{\psi}$ e $\Gamma \vdash \boldsymbol{\varphi} \boldsymbol{\Rightarrow} (\boldsymbol{\psi} \boldsymbol{\Rightarrow} \boldsymbol{\chi})$, allora $\Gamma \vdash \boldsymbol{\varphi} \boldsymbol{\Rightarrow} \boldsymbol{\chi}$.

Infatti:

$$\begin{array}{ll} \left.\begin{array}{c} \vdots \\ \boldsymbol{\varphi} \boldsymbol{\Rightarrow} \boldsymbol{\psi} \end{array}\right\} \Gamma \vdash \boldsymbol{\varphi} \boldsymbol{\Rightarrow} \boldsymbol{\psi} & \\ \left.\begin{array}{c} \vdots \\ \boldsymbol{\varphi} \boldsymbol{\Rightarrow} (\boldsymbol{\psi} \boldsymbol{\Rightarrow} \boldsymbol{\chi}) \end{array}\right\} \Gamma \vdash \boldsymbol{\varphi} \boldsymbol{\Rightarrow} (\boldsymbol{\psi} \boldsymbol{\Rightarrow} \boldsymbol{\chi}) & \\ (\boldsymbol{\varphi} \boldsymbol{\Rightarrow} \boldsymbol{\psi}) \boldsymbol{\Rightarrow} [(\boldsymbol{\varphi} \boldsymbol{\Rightarrow} (\boldsymbol{\psi} \boldsymbol{\Rightarrow} \boldsymbol{\chi})) \boldsymbol{\Rightarrow} (\boldsymbol{\varphi} \boldsymbol{\Rightarrow} \boldsymbol{\chi})] & \text{(Taut)} \\ (\boldsymbol{\varphi} \boldsymbol{\Rightarrow} (\boldsymbol{\psi} \boldsymbol{\Rightarrow} \boldsymbol{\chi})) \boldsymbol{\Rightarrow} (\boldsymbol{\varphi} \boldsymbol{\Rightarrow} \boldsymbol{\chi}) & \text{(MP)} \\ \boldsymbol{\varphi} \boldsymbol{\Rightarrow} \boldsymbol{\chi} & \text{(MP)} \end{array}$$

27.B.5. *L'antecedente di un'implicazione diventa un'ipotesi.*

$$\Gamma \vdash \boldsymbol{\varphi} \boldsymbol{\Rightarrow} \boldsymbol{\psi} \quad \Rightarrow \quad \Gamma \cup \{\boldsymbol{\varphi}\} \vdash \boldsymbol{\psi} \,.$$

Infatti, se $\Gamma \vdash \boldsymbol{\varphi} \boldsymbol{\Rightarrow} \boldsymbol{\psi}$, allora anche $\Gamma \cup \{\boldsymbol{\varphi}\} \vdash \boldsymbol{\varphi} \boldsymbol{\Rightarrow} \boldsymbol{\psi}$ e quindi $\Gamma \cup \{\boldsymbol{\varphi}\} \vdash \boldsymbol{\psi}$.

Il converso (cioè: $\Gamma \cup \{\boldsymbol{\varphi}\} \vdash \boldsymbol{\psi}$ implica $\Gamma \vdash \boldsymbol{\varphi} \boldsymbol{\Rightarrow} \boldsymbol{\psi}$) non vale in generale—Lemma 27.5.

27.B.6. *Una formula è equiderivabile con la una sua chiusura universale.* In altre parole:

$$\boldsymbol{\varphi} \vdash \forall \boldsymbol{x}_1 \dots \forall \boldsymbol{x}_n \, \boldsymbol{\varphi} \quad \text{e} \quad \forall \boldsymbol{x}_1 \dots \forall \boldsymbol{x}_n \, \boldsymbol{\varphi} \vdash \boldsymbol{\varphi} \, .$$

La prima affermazione discende dalla regola di generalizzazione (applicata n-volte). Per la seconda affermazione, consideriamo gli assiomi logici di tipo (LAx-2)

$$\begin{gathered} \forall \boldsymbol{x}_n \, \boldsymbol{\varphi} \Rightarrow \boldsymbol{\varphi} \\ \forall \boldsymbol{x}_{n-1} \forall \boldsymbol{x}_n \, \boldsymbol{\varphi} \Rightarrow \forall \boldsymbol{x}_n \, \boldsymbol{\varphi} \\ \vdots \\ \forall \boldsymbol{x}_1 \dots \forall \boldsymbol{x}_n \, \boldsymbol{\varphi} \Rightarrow \forall \boldsymbol{x}_2 \dots \forall \boldsymbol{x}_n \, \boldsymbol{\varphi} \, . \end{gathered}$$

Per la transitività dell'implicazione (conseguenza di MP e Taut), si ha che

$$\vdash \forall \boldsymbol{x}_1 \dots \forall \boldsymbol{x}_n \, \boldsymbol{\varphi} \Rightarrow \boldsymbol{\varphi} \, .$$

quindi per 27.B.5 prendendo $\Gamma = \emptyset$, $\forall \boldsymbol{x}_1 \dots \forall \boldsymbol{x}_n \, \boldsymbol{\varphi} \vdash \boldsymbol{\varphi}$.

27.B.7. *Dal quantificatore universale all'esistenziale.* Vale la seguente affermazione:

$$\vdash \boldsymbol{\varphi} \Rightarrow \exists \boldsymbol{x} \, \boldsymbol{\varphi} \, .$$

In particolare $\vdash \forall \boldsymbol{x} \, \boldsymbol{\varphi} \Rightarrow \exists \boldsymbol{x} \, \boldsymbol{\varphi}$.

Infatti:

$$\begin{array}{rl} \forall \boldsymbol{x} \, (\neg \boldsymbol{\varphi}) \Rightarrow \neg \boldsymbol{\varphi} & \text{(LAx-2)} \\ (\forall \boldsymbol{x} \, (\neg \boldsymbol{\varphi}) \Rightarrow \neg \boldsymbol{\varphi}) \Rightarrow (\boldsymbol{\varphi} \Rightarrow \exists \boldsymbol{x} \, \boldsymbol{\varphi}) & \text{(Taut) e (LAx-6)} \\ \boldsymbol{\varphi} \Rightarrow \exists \boldsymbol{x} \, \boldsymbol{\varphi} & \text{(MP)} \end{array}$$

La seconda affermazione discende dalla prima e da (LAx-2).

27.B.8. *Derivazioni e chiusura universale.* Denotiamo con $\tilde{\boldsymbol{\psi}}$ la chiusura universale di $\boldsymbol{\psi}$. Allora

$$\Gamma \vdash \boldsymbol{\varphi} \quad \Leftrightarrow \quad \tilde{\Gamma} \vdash \tilde{\boldsymbol{\varphi}} \, ,$$

dove $\tilde{\Gamma} = \{ \, \tilde{\boldsymbol{\gamma}} \mid \boldsymbol{\gamma} \in \Gamma \, \}$.

Supponiamo che $\Gamma \vdash \boldsymbol{\varphi}$. Per 27.B.6 ogni formula in Γ è derivabile da $\tilde{\Gamma}$ e quindi data una derivazione $\langle \boldsymbol{\alpha}_0, \dots, \boldsymbol{\alpha}_n \rangle$ una derivazione di $\boldsymbol{\varphi}$ da Γ, sostituendo ogni $\boldsymbol{\alpha}_i \in \Gamma$ con la sua derivazione da $\tilde{\Gamma}$, otteniamo una derivazione di $\boldsymbol{\varphi}$ da $\tilde{\Gamma}$. Applicando la regola di generalizzazione si ottiene $\tilde{\Gamma} \vdash \tilde{\boldsymbol{\varphi}}$.

Viceversa, data una derivazione di $\tilde{\boldsymbol{\varphi}}$ da $\tilde{\Gamma}$, possiamo rimpiazzare in questa derivazione tutte le formule del tipo $\tilde{\boldsymbol{\gamma}} = \forall \boldsymbol{x}_n \dots \forall \boldsymbol{x}_1 \, \boldsymbol{\gamma}$ (con $\boldsymbol{\gamma} \in \Gamma$) con la stringa

$$\boldsymbol{\gamma}, \ \forall \boldsymbol{x}_1 \, \boldsymbol{\gamma}, \ \dots, \ \forall \boldsymbol{x}_n \dots \forall \boldsymbol{x}_1 \, \boldsymbol{\gamma} \, .$$

La sequenza così ottenuta è una derivazione di $\tilde{\boldsymbol{\varphi}}$ da Γ. Per 27.B.6 otteniamo $\Gamma \vdash \boldsymbol{\varphi}$.

27.B.9. *Quantificazioni con nuove variabili.* Se $\boldsymbol{y}$ non occorre libera in $\boldsymbol{\varphi}$, allora

$$\vdash \forall \boldsymbol{x}\, \boldsymbol{\varphi} \Leftrightarrow \forall \boldsymbol{y}\, (\boldsymbol{\varphi}[\boldsymbol{y}/\boldsymbol{x}]) \quad \text{e} \quad \vdash \exists \boldsymbol{x}\, \boldsymbol{\varphi} \Leftrightarrow \exists \boldsymbol{y}\, (\boldsymbol{\varphi}[\boldsymbol{y}/\boldsymbol{x}])\,.$$

Verifichiamo la prima delle due biimplicazioni—la seconda è lasciata al lettore. Poiché $\boldsymbol{y}$ è sostituibile ad $\boldsymbol{x}$ in $\boldsymbol{\varphi}$, allora $(\boldsymbol{\varphi}[\boldsymbol{y}/\boldsymbol{x}])[\boldsymbol{x}/\boldsymbol{y}]$ è $\boldsymbol{\varphi}$ per la parte (ii) dell'Esercizio 21.14, quindi per 27.B.1 è sufficiente dimostrare una delle due implicazioni, per esempio $\vdash \forall \boldsymbol{x}\, \boldsymbol{\varphi} \Rightarrow \forall \boldsymbol{y}\, (\boldsymbol{\varphi}[\boldsymbol{y}/\boldsymbol{x}])$:

$$\begin{aligned}
&\forall \boldsymbol{x}\, \boldsymbol{\varphi} \Rightarrow \boldsymbol{\varphi}[\boldsymbol{y}/\boldsymbol{x}] && \text{(LAx-2)}\\
&\forall \boldsymbol{y}\, (\forall \boldsymbol{x}\, \boldsymbol{\varphi} \Rightarrow \boldsymbol{\varphi}[\boldsymbol{y}/\boldsymbol{x}]) && \text{(Gen)}\\
&\forall \boldsymbol{y}\, (\forall \boldsymbol{x}\, \boldsymbol{\varphi} \Rightarrow \boldsymbol{\varphi}[\boldsymbol{y}/\boldsymbol{x}]) \Rightarrow (\forall \boldsymbol{x}\, \boldsymbol{\varphi} \Rightarrow \forall \boldsymbol{y}(\boldsymbol{\varphi}[\boldsymbol{y}/\boldsymbol{x}])) && \text{(LAx-1)}\\
&\forall \boldsymbol{x}\, \boldsymbol{\varphi} \Rightarrow \forall \boldsymbol{y}(\boldsymbol{\varphi}[\boldsymbol{y}/\boldsymbol{x}]) && \text{(Gen)}\,.
\end{aligned}$$

27.C. Alcuni risultati sulle derivazioni.

Lemma 27.3. *Se $\boldsymbol{x}$ non occorre libera in $\boldsymbol{\varphi}$, allora*

$$\Gamma \vdash \forall \boldsymbol{x}\, (\boldsymbol{\varphi} \Rightarrow \boldsymbol{\psi}) \quad \Leftrightarrow \quad \Gamma \vdash \boldsymbol{\varphi} \Rightarrow \forall \boldsymbol{x}\, \boldsymbol{\psi}\,.$$

Dimostrazione. Supponiamo che $\Gamma \vdash \forall \boldsymbol{x}\, (\boldsymbol{\varphi} \Rightarrow \boldsymbol{\psi})$: dato che

$$\forall \boldsymbol{x}\, (\boldsymbol{\varphi} \Rightarrow \boldsymbol{\psi}) \Rightarrow (\boldsymbol{\varphi} \Rightarrow \forall \boldsymbol{x} \boldsymbol{\psi})$$

è un assioma, per MP si ha $\Gamma \vdash \boldsymbol{\varphi} \Rightarrow \forall \boldsymbol{x}\, \boldsymbol{\psi}$.

Viceversa, supponiamo che $\Gamma \vdash \boldsymbol{\varphi} \Rightarrow \forall \boldsymbol{x}\, \boldsymbol{\psi}$: dato che $\forall \boldsymbol{x}\, \boldsymbol{\psi} \Rightarrow \boldsymbol{\psi}$ è un assioma (LAx-2), per la transitività dell'implicazione si ha $\Gamma \vdash \boldsymbol{\varphi} \Rightarrow \boldsymbol{\psi}$ e per la regola di generalizzazione $\Gamma \vdash \forall \boldsymbol{x}\, (\boldsymbol{\varphi} \Rightarrow \boldsymbol{\psi})$. □

Poiché $\forall \boldsymbol{x}(\boldsymbol{\varphi} \wedge \boldsymbol{\psi}) \Rightarrow \boldsymbol{\varphi} \wedge \boldsymbol{\psi}$ è un assioma logico e $\boldsymbol{\varphi} \wedge \boldsymbol{\psi} \Rightarrow \boldsymbol{\varphi}$ è una tautologia, ne segue che $\vdash \forall \boldsymbol{x}(\boldsymbol{\varphi} \wedge \boldsymbol{\psi}) \Rightarrow \boldsymbol{\varphi}$. Usando la regola di generalizzazione e l'assioma (LAx-1) otteniamo $\vdash \forall \boldsymbol{x}(\boldsymbol{\varphi} \wedge \boldsymbol{\psi}) \Rightarrow \forall \boldsymbol{x} \boldsymbol{\varphi}$. Analogamente $\vdash \forall \boldsymbol{x}(\boldsymbol{\varphi} \wedge \boldsymbol{\psi}) \Rightarrow \forall \boldsymbol{x}\, \boldsymbol{\psi}$. Abbiamo quindi dimostrato la

Proposizione 27.4. $\vdash \forall \boldsymbol{x}(\boldsymbol{\varphi} \wedge \boldsymbol{\psi}) \Rightarrow (\forall \boldsymbol{x} \boldsymbol{\varphi} \wedge \forall \boldsymbol{x} \boldsymbol{\psi})$.

Lemma 27.5. *Sia Γ un insieme di formule e sia $\boldsymbol{\sigma}$ un enunciato. Se $\Gamma \cup \{\boldsymbol{\sigma}\} \vdash \boldsymbol{\varphi}$ allora $\Gamma \vdash \boldsymbol{\sigma} \Rightarrow \boldsymbol{\varphi}$.*

Dimostrazione. Supponiamo $\langle \boldsymbol{\alpha}_0, \ldots, \boldsymbol{\alpha}_n \rangle$ sia una derivazione di $\boldsymbol{\varphi}$ a partire da $\Gamma \cup \{\boldsymbol{\sigma}\}$. Dimostreremo per induzione su $0 \leq i \leq n$ che

$$\Gamma \vdash \boldsymbol{\sigma} \Rightarrow \boldsymbol{\alpha}_i\,.$$

Consideriamo i vari casi:

- $\boldsymbol{\alpha}_i$ è un assioma logico oppure $\boldsymbol{\alpha}_i \in \Gamma$. Allora

$$\langle \boldsymbol{\alpha}_i \Rightarrow (\boldsymbol{\sigma} \Rightarrow \boldsymbol{\alpha}_i),\ \boldsymbol{\alpha}_i,\ \boldsymbol{\sigma} \Rightarrow \boldsymbol{\alpha}_i \rangle$$

è una derivazione in Γ dal momento che la prima formula è una tautologia, la seconda è un assioma logico oppure è in Γ, la terza è ottenuta dalle prime due mediante *Modus ponens*.

- $\boldsymbol{\alpha}_i$ è $\boldsymbol{\sigma}$. Allora $\Gamma \vdash \boldsymbol{\sigma} \Rightarrow \boldsymbol{\alpha}_i$ in quanto è una tautologia.
- $\boldsymbol{\alpha}_i$ è ottenuta per (MP) da $\boldsymbol{\alpha}_m$ e $\boldsymbol{\alpha}_k$, dove $m, k < i$ e $\boldsymbol{\alpha}_k$ è $\boldsymbol{\alpha}_m \Rightarrow \boldsymbol{\alpha}_i$. Per ipotesi induttiva $\Gamma \vdash \boldsymbol{\sigma} \Rightarrow \boldsymbol{\alpha}_m$ e $\Gamma \vdash \boldsymbol{\sigma} \Rightarrow (\boldsymbol{\alpha}_m \Rightarrow \boldsymbol{\alpha}_i)$ e quindi $\Gamma \vdash \boldsymbol{\sigma} \Rightarrow \boldsymbol{\alpha}_i$ per 27.B.4.
- $\boldsymbol{\alpha}_i = \forall \boldsymbol{x}\, \boldsymbol{\alpha}_m$ con $m < i$. Per ipotesi induttiva $\Gamma \vdash \boldsymbol{\sigma} \Rightarrow \boldsymbol{\alpha}_m$, da cui $\Gamma \vdash \forall \boldsymbol{x}\, (\boldsymbol{\sigma} \Rightarrow \boldsymbol{\alpha}_m)$ per la regola di generalizzazione e quindi il risultato segue dal Lemma 27.3.

Quindi $\Gamma \vdash \boldsymbol{\sigma} \Rightarrow \boldsymbol{\alpha}_i$ per ogni $i \leq n$, come richiesto. □

Spesso in matematica per dimostrare che $\forall \boldsymbol{x}\, \boldsymbol{\varphi}(\boldsymbol{x})$ si ragiona così: si prende un elemento generico $\boldsymbol{c}$ e si dimostra che vale $\boldsymbol{\varphi}$ per l'elemento $\boldsymbol{c}$; data l'arbitrarietà di $\boldsymbol{c}$ si conclude che $\forall \boldsymbol{x}\, \boldsymbol{\varphi}(\boldsymbol{x})$. Il seguente risultato formalizza tutto questo.

Teorema 27.6. *Sia* $\Gamma \subseteq \mathrm{Fml}(\boldsymbol{L})$*, sia* $\boldsymbol{\varphi}$ *una* $\boldsymbol{L}$*-formula e sia* $\boldsymbol{c}$ *una nuova costante. Allora*

$$\Gamma \vdash_{\boldsymbol{L}} \forall \boldsymbol{x}\, \boldsymbol{\varphi} \quad \Leftrightarrow \quad \Gamma \vdash_{\boldsymbol{L} \cup \{\boldsymbol{c}\}} \boldsymbol{\varphi}[\boldsymbol{c}/\boldsymbol{x}]\,.$$

Dimostrazione. Se $\Gamma \vdash_{\boldsymbol{L}} \forall \boldsymbol{x}\, \boldsymbol{\varphi}$ allora $\Gamma \vdash_{\boldsymbol{L} \cup \{\boldsymbol{c}\}} \forall \boldsymbol{x}\, \boldsymbol{\varphi}$ e quindi dato che $\boldsymbol{c}$ è sostituibile ad $\boldsymbol{x}$, $\forall \boldsymbol{x}\, \boldsymbol{\varphi} \Rightarrow \varphi[\boldsymbol{c}/\boldsymbol{x}]$ è un assioma logico di tipo (LAx-2), quindi $\Gamma \vdash_{\boldsymbol{L} \cup \{\boldsymbol{c}\}} \boldsymbol{\varphi}[\boldsymbol{c}/\boldsymbol{x}]$.

Viceversa supponiamo $\langle \boldsymbol{\varphi}_0, \ldots, \boldsymbol{\varphi}_n \rangle$ sia una derivazione di $\boldsymbol{\varphi}[\boldsymbol{c}/\boldsymbol{x}]$ da Γ in $\boldsymbol{L} \cup \{\boldsymbol{c}\}$. Sia $\boldsymbol{y}$ una variabile che non occorre in nessuna $\boldsymbol{\varphi}_i$.

Fatto 27.6.1. *Per* $0 \leq i \leq n$*,*

$$\Gamma \vdash_{\boldsymbol{L}} \boldsymbol{\varphi}_i[\boldsymbol{y}/\boldsymbol{c}]\,. \tag{110}$$

Dimostrazione. Per induzione su i. Se $\boldsymbol{\varphi}_i \in \Gamma$ allora $\boldsymbol{c}$ non occorre in $\boldsymbol{\varphi}_i$, quindi $\boldsymbol{\varphi}[\boldsymbol{y}/\boldsymbol{c}] = \boldsymbol{\varphi}_i$ e (110) vale. Se $\boldsymbol{\varphi}_i$ è un assioma logico (tautologia o di tipo (LAx-1)–(LAx-6)), allora anche $\boldsymbol{\varphi}_i[\boldsymbol{y}/\boldsymbol{c}]$ è un assioma logico (dello stesso tipo) e quindi $\Gamma \vdash_{\boldsymbol{L}} \boldsymbol{\varphi}_i[\boldsymbol{y}/\boldsymbol{c}]$. Se $\boldsymbol{\varphi}_i$ è ottenuto da $\boldsymbol{\varphi}_j$ mediante la regola di generalizzazione, $\boldsymbol{\varphi}_i = \forall \boldsymbol{z} \boldsymbol{\varphi}_j$ e $j < i$, allora $\Gamma \vdash_{\boldsymbol{L}} \boldsymbol{\varphi}_j[\boldsymbol{y}/\boldsymbol{c}]$ per ipotesi induttiva e quindi $\Gamma \vdash_{\boldsymbol{L}} \boldsymbol{\varphi}_i[\boldsymbol{y}/\boldsymbol{c}]$ per (Gen). Infine, supponiamo $\boldsymbol{\varphi}_i$ sia ottenuto da $\boldsymbol{\varphi}_j$ e $\boldsymbol{\varphi}_k$ con $j, k < i$ mediante la regola del *Modus Ponens*. Allora $\Gamma \vdash_{\boldsymbol{L}} \boldsymbol{\varphi}_j[\boldsymbol{y}/\boldsymbol{c}]$ e $\Gamma \vdash_{\boldsymbol{L}} \boldsymbol{\varphi}_k[\boldsymbol{y}/\boldsymbol{c}]$ per ipotesi induttiva, quindi $\Gamma \vdash_{\boldsymbol{L}} \boldsymbol{\varphi}_i[\boldsymbol{y}/\boldsymbol{c}]$ per (MP). □

Ne segue che $\Gamma \vdash_{\boldsymbol{L}} (\boldsymbol{\varphi}[\boldsymbol{c}/\boldsymbol{x}])\,[\boldsymbol{y}/\boldsymbol{c}]$, cioè $\Gamma \vdash_{\boldsymbol{L}} \boldsymbol{\varphi}[\boldsymbol{y}/\boldsymbol{x}]$, da cui $\Gamma \vdash_{\boldsymbol{L}} \forall \boldsymbol{y}\, \boldsymbol{\varphi}[\boldsymbol{y}/\boldsymbol{x}]$, quindi per 27.B.9 $\Gamma \vdash_{\boldsymbol{L}} \forall \boldsymbol{x}\, \boldsymbol{\varphi}$. □

27.D. Forma normale prenessa.

Lemma 27.7. *Sia* $\boldsymbol{y}$ *una variabile diversa da* $\boldsymbol{x}$ *e che non occorre né in* $\boldsymbol{\varphi}$ *né in* $\boldsymbol{\psi}$*. Allora*

(111) $\boldsymbol{\varphi \vee \forall x\, \psi}$ *è equiderivabile con* $\boldsymbol{\forall y\, (\varphi \vee \psi[y/x])}$

(112) $\boldsymbol{\varphi \vee \exists x\, \psi}$ *è equiderivabile con* $\boldsymbol{\exists y\, (\varphi \vee \psi[y/x])}$

Dimostrazione. La variabile $\boldsymbol{y}$ è sostituibile ad $\boldsymbol{x}$ in $\boldsymbol{\psi}$ e quindi $\boldsymbol{\vdash \forall x\, \psi \Rightarrow \psi[y/x]}$, da cui $\boldsymbol{\vdash (\varphi \vee \forall x\, \psi) \Rightarrow (\varphi \vee \psi[y/x])}$. Per (Gen), (LAx-1) e (MP)

$$\boldsymbol{\vdash (\varphi \vee \forall x\, \psi) \Rightarrow \forall y\, (\varphi \vee \psi[y/x])}\,.$$

Viceversa, $\boldsymbol{\forall y\, (\varphi \vee \psi[y/x]) \Rightarrow (\varphi \vee \forall y\, \psi[y/x])}$ è un assioma logico (LAx-1) e per 27.B.9 $\boldsymbol{\vdash \forall y\, \psi[y/x] \Leftrightarrow \forall x\, \psi}$, quindi $\boldsymbol{\vdash \forall y\, (\varphi \vee \psi[y/x]) \Rightarrow (\varphi \vee \forall x\, \psi)}$. Ciò dimostra (111).

Argomentando come sopra:

$$\begin{aligned}
&\boldsymbol{\vdash \forall x\, \neg\psi \Rightarrow \neg\psi[y/x]}\\
&\boldsymbol{\vdash (\neg\varphi \wedge \forall x\, \neg\psi) \Rightarrow \forall y\, (\neg\varphi \wedge \neg\psi[y/x])}\\
&\boldsymbol{\vdash \exists y\, (\varphi \vee \psi[y/x]) \Rightarrow (\varphi \vee \exists x\, \psi)}\,.
\end{aligned}$$

Viceversa, per la Proposizione 27.4,

$$\begin{aligned}
&\boldsymbol{\vdash \forall y\, (\neg\varphi \wedge \neg\psi[y/x]) \Rightarrow \forall y\, \neg\varphi}\\
&\boldsymbol{\vdash \forall y\, (\neg\varphi \wedge \neg\psi[y/x]) \Rightarrow \forall y\, \neg\psi[y/x]}
\end{aligned}$$

e poiché $\boldsymbol{y}$ non occorre in $\boldsymbol{\neg\varphi}$,

$$\boldsymbol{\vdash \forall y\, \neg\psi[y/x] \Leftrightarrow \forall x\, \psi} \qquad \text{e} \qquad \boldsymbol{\vdash \neg\varphi \Leftrightarrow \forall y\, \varphi}\,,$$

da cui

$$\boldsymbol{\vdash \forall y\, (\neg\varphi \wedge \neg\psi[y/x]) \Rightarrow \neg\varphi \wedge \forall x\, \neg\psi[y/x]}\,.$$

Prendendo il contrapositivo si ha

$$\boldsymbol{(\varphi \vee \exists x\, \psi) \Rightarrow \exists y\, (\varphi \vee \psi[y/x])}\,.$$

Questo prova (112). □

Una formula si dice **normale prenessa** se è della forma

$$\boldsymbol{Q_1 x_1 \dots Q_n x_n\, \varphi}$$

dove $\boldsymbol{Q_i \in \{\exists, \forall\}}$ e $\boldsymbol{\varphi}$ è priva di quantificatori.

Teorema 27.8. *Ogni formula* $\boldsymbol{\varphi}$ *è equivalente ad una formula normale prenessa.*

Dimostrazione. Per induzione sulla complessità di $\boldsymbol{\varphi}$. Se $\boldsymbol{\varphi}$ è atomica (o più in generale: priva di quantificatori) allora è prenessa. Se $\boldsymbol{\varphi} = \neg\boldsymbol{\psi}$, per ipotesi induttiva c'è una formula prenessa $\boldsymbol{Q}_1\boldsymbol{x}_1 \dots \boldsymbol{Q}_n\boldsymbol{x}_n\, \boldsymbol{\alpha}$ equivalente a $\boldsymbol{\psi}$ e quindi $\boldsymbol{\varphi}$ è equivalente a $\breve{\boldsymbol{Q}}_1\boldsymbol{x}_1 \dots \breve{\boldsymbol{Q}}_n\boldsymbol{x}_n\, \neg\boldsymbol{\alpha}$, dove

$$\breve{\boldsymbol{Q}}_i = \begin{cases} \exists & \text{se } \boldsymbol{Q}_i = \forall\,, \\ \forall & \text{se } \boldsymbol{Q}_i = \exists\,. \end{cases}$$

Se $\boldsymbol{\varphi}$ è $\exists\boldsymbol{x}\,\boldsymbol{\psi}$ oppure $\forall\boldsymbol{x}\,\boldsymbol{\psi}$, il risultato segue immediatamente dall'ipotesi induttiva. Supponiamo infine che $\boldsymbol{\varphi}$ sia $\boldsymbol{\psi} \vee \boldsymbol{\chi}$ e che $\boldsymbol{\psi}$ e $\boldsymbol{\chi}$ siano equivalenti a formule prenesse $\boldsymbol{Q}_1\boldsymbol{x}_1 \dots \boldsymbol{Q}_n\boldsymbol{x}_n\, \boldsymbol{\alpha}$ e $\boldsymbol{Q}^*_1\boldsymbol{y}_1 \dots \boldsymbol{Q}^*_m\boldsymbol{y}_m\, \boldsymbol{\beta}$, rispettivamente. Applicando ripetutamente il Lemma precedente otteniamo che $\boldsymbol{\psi} \vee \boldsymbol{\chi}$ è equivalente a $\boldsymbol{Q}^*_1\boldsymbol{y}'_1 \dots \boldsymbol{Q}^*_m\boldsymbol{y}'_m\, (\boldsymbol{\psi} \vee \boldsymbol{\beta}[\boldsymbol{y}'_1/\boldsymbol{y}_1, \dots, \boldsymbol{y}'_m/\boldsymbol{y}_m])$ per opportune variabili $\boldsymbol{y}'_1, \dots, \boldsymbol{y}'_m$. Poiché lo scambio di due formule in una disgiunzione genera una formula equivalente, applicando nuovamente il Lemma otteniamo la formula

$$\boldsymbol{Q}_1\boldsymbol{x}'_1 \dots \boldsymbol{Q}_n\boldsymbol{x}'_n\, \boldsymbol{Q}^*_1\boldsymbol{y}'_1 \dots \boldsymbol{Q}^*_m\boldsymbol{y}'_m\, \big(\boldsymbol{\beta}[\boldsymbol{y}'_1/\boldsymbol{y}_1, \dots, \boldsymbol{y}'_m/\boldsymbol{y}_m] \vee \boldsymbol{\alpha}[\boldsymbol{x}'_1/\boldsymbol{x}_1, \dots, \boldsymbol{x}'_n/\boldsymbol{x}_n]\big)\,.$$

che è equivalente a $\boldsymbol{\varphi}$. □

27.E. Consistenza. Un insieme di formule Γ si dice **inconsistente** se

$$\Gamma \vdash \neg\forall\boldsymbol{x}(\boldsymbol{x} \equiv \boldsymbol{x})\,.$$

Dato che $\vdash \forall\boldsymbol{x}\,(x \equiv x)$ per (LAx-3) e la regola di generalizzazione e usando 27.B.3 si ha che Γ è inconsistente se e solo se da Γ si può derivare una qualsiasi formula.

Un insieme di formule Γ che non sia inconsistente si dice **consistente**; quindi Γ è consistente se $\Gamma \nvdash \boldsymbol{\varphi}$ per qualche $\boldsymbol{\varphi}$.

Esercizio 27.9. Dimostrare che:

(i) Γ è consistente se e solo se ogni sottoinsieme finito di Γ è consistente;

(ii) se $\mathcal{C} \subseteq \mathscr{P}(\mathrm{Fml}(\boldsymbol{L}))$ è linearmente ordinato da $\subseteq$ e se Γ è consistente per ogni $\Gamma \in \mathcal{C}$, allora $\bigcup \mathcal{C}$ è consistente;

(iii) ogni insieme consistente di formule può essere esteso ad un insieme consistente massimale di formule.

La parte (iii) dell'Esercizio qui sopra è nota come **Lemma di Lindembaum**.

Proposizione 27.10. *Sia Γ un insieme di $\boldsymbol{L}$-formule e sia $\boldsymbol{\sigma}$ un $\boldsymbol{L}$-enunciato. Allora $\Gamma \cup \{\boldsymbol{\sigma}\}$ è inconsistente se e solo se $\Gamma \vdash \neg\boldsymbol{\sigma}$. Equivalentemente: $\Gamma \cup \{\boldsymbol{\sigma}\}$ è consistente se e solo se $\Gamma \nvdash \neg\boldsymbol{\sigma}$.*

Dimostrazione. Se $\Gamma \vdash \boldsymbol{\neg\sigma}$, allora $\Gamma \cup \{\boldsymbol{\sigma}\} \vdash \boldsymbol{\sigma \wedge \neg\sigma}$ e quindi $\Gamma \cup \{\boldsymbol{\sigma}\}$ è inconsistente. Viceversa supponiamo $\Gamma \cup \{\boldsymbol{\sigma}\}$ sia inconsistente: allora da $\Gamma \cup \{\boldsymbol{\sigma}\}$ è possibile derivare ogni formula e quindi, in particolare, $\Gamma \cup \{\boldsymbol{\sigma}\} \vdash \boldsymbol{\sigma \wedge \neg\sigma}$. Per il Lemma 27.5, $\Gamma \vdash \boldsymbol{\sigma \Rightarrow (\sigma \wedge \neg\sigma)}$ e quindi $\Gamma \vdash \boldsymbol{(\sigma \vee \neg\sigma) \Rightarrow \neg\sigma}$. Ma $\boldsymbol{\sigma \vee \neg\sigma}$ è una tautologia, quindi per *Modus ponens* $\Gamma \vdash \boldsymbol{\neg\sigma}$. □

Esercizi

Esercizio 27.11. Sia $\Gamma \subseteq \mathrm{Fml}(\boldsymbol{L})$. Poniamo $\boldsymbol{\varphi} \sim \boldsymbol{\psi}$ se $\Gamma \vdash \boldsymbol{\varphi \Leftrightarrow \psi}$, cioè se $\boldsymbol{\varphi}$ e $\boldsymbol{\psi}$ sono equivalenti. Dimostrare che $\sim$ è una relazione di equivalenza su $\mathrm{Fml}(\boldsymbol{L})$ e che se Γ è consistente allora $\mathrm{Fml}(\boldsymbol{L})/\!\sim$ è un'algebra di Boole.

Esercizio 27.12. Supponiamo Γ sia consistente e massimale rispetto all'inclusione. Allora

$$\begin{aligned} \Gamma \vdash \boldsymbol{\varphi} \quad &\Leftrightarrow \quad \boldsymbol{\varphi} \in \Gamma \\ \boldsymbol{\varphi} \notin \Gamma \quad &\Leftrightarrow \quad \boldsymbol{\neg\varphi} \in \Gamma \\ \boldsymbol{\varphi \wedge \psi} \in \Gamma \quad &\Leftrightarrow \quad \boldsymbol{\varphi} \in \Gamma \wedge \boldsymbol{\psi} \in \Gamma\,. \end{aligned}$$

28. Il Teorema di Completezza

La Definizione 23.1 di conseguenza logica è stata data per insiemi di *enunciati*, ma può essere generalizzata ad insiemi di *formule* come segue: diremo che Γ_2 è **conseguenza logica** di Γ_1, in simboli $\Gamma_1 \models \Gamma_2$, se e solo se $\mathfrak{Mod}(\Gamma_1) \subseteq \mathfrak{Mod}(\Gamma_2)$, vale a dire per ogni $\mathcal{A} \in \mathfrak{Str}(\boldsymbol{L})$

$$\forall g\,(\mathcal{A} \models \Gamma_1[g]) \quad \Rightarrow \quad \forall g\,(\mathcal{A} \models \Gamma_2[g])\,.$$

Ogni assioma logico è logicamente valido:

Esercizio 28.1. Dimostrare che se $\boldsymbol{\varphi}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)$ è un assioma logico, allora $\mathcal{A} \models \boldsymbol{\varphi}[\bar{a}]$, per ogni $\bar{a} \in \|\mathcal{A}\|$.

Il seguente risultato mostra che le derivazioni generano conseguenze logiche.

Teorema 28.2. *Se* $\Gamma \subseteq \mathrm{Fml}$ *e* $\boldsymbol{\varphi} \in \mathrm{Fml}$*, allora*

$$\Gamma \vdash \boldsymbol{\varphi} \qquad \Rightarrow \qquad \Gamma \models \boldsymbol{\varphi}\,.$$

Dimostrazione. Sia $\mathcal{A}$ un modello di Γ e sia $\langle \boldsymbol{\varphi}_0, \ldots, \boldsymbol{\varphi}_n \rangle$ una derivazione di $\boldsymbol{\varphi}$ da Γ. Verifichiamo, per induzione su $i \leq n$, che

$$\mathcal{A} \models \boldsymbol{\varphi}_i\,.$$

Se $\boldsymbol{\varphi}_i$ è un assioma logico oppure $\boldsymbol{\varphi}_i \in \Gamma$ il risultato è immediato per l'Esercizio 28.1 o per la nostra ipotesi. Se $\boldsymbol{\varphi}_i(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)$ è $\boldsymbol{\forall y}\, \boldsymbol{\varphi}_j$ con $j < i$, allora $\mathcal{A} \models \boldsymbol{\varphi}_j(\boldsymbol{y}, \boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)$ per ipotesi induttiva, vale a dire

$$\forall \bar{a}, b \in A\, (\mathcal{A} \models \boldsymbol{\varphi}_j[b, \bar{a}])\,,$$

quindi $\forall \bar{a} \in A\, (\mathcal{A} \models \boldsymbol{\forall y}\, \boldsymbol{\varphi}_j)$, cioè $\mathcal{A} \models \boldsymbol{\varphi}_i$. Supponiamo infine che esistano $j, k < i$ per cui $\boldsymbol{\varphi}_k$ è $\boldsymbol{\varphi}_j \boldsymbol{\Rightarrow} \boldsymbol{\varphi}_i$. Per ipotesi $\mathcal{A} \models \boldsymbol{\varphi}_j$ e $\mathcal{A} \models \boldsymbol{\varphi}_j \boldsymbol{\Rightarrow} \boldsymbol{\varphi}_i$. Siano $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ le variabili libere di $\boldsymbol{\varphi}_i$ e siano $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_m$ variabili distinte dalle $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ tali che $\boldsymbol{Fv}(\boldsymbol{\varphi}_j \boldsymbol{\Rightarrow} \boldsymbol{\varphi}_i) \subseteq \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n, \boldsymbol{y}_1, \ldots, \boldsymbol{y}_m\}$. Dobbiamo verificare che per ogni $a_1, \ldots, a_n \in A$,

$$\mathcal{A} \models \boldsymbol{\varphi}_i[a_1, \ldots, a_n]\,.$$

Ma questo discende dal fatto che $\mathcal{A} \models (\boldsymbol{\varphi}_j \boldsymbol{\Rightarrow} \boldsymbol{\varphi}_i)[\bar{a}, \bar{b}]$ e $\mathcal{A} \models \boldsymbol{\varphi}_j[\bar{a}, \bar{b}]$, per ogni $a_1, \ldots, a_n, b_1, \ldots, b_m \in A$. □

Corollario 28.3. *Un insieme soddisfacibile di enunciati Σ è consistente.*

Dimostrazione. Supponiamo Σ sia inconsistente, cioè $\Sigma \vdash \boldsymbol{\sigma} \boldsymbol{\wedge} \boldsymbol{\neg} \boldsymbol{\sigma}$. Allora $\Sigma \models \boldsymbol{\sigma} \boldsymbol{\wedge} \boldsymbol{\neg} \boldsymbol{\sigma}$, quindi se $\mathcal{A}$ è un modello di Σ, allora $\mathcal{A} \models \boldsymbol{\sigma} \boldsymbol{\wedge} \boldsymbol{\neg} \boldsymbol{\sigma}$: assurdo. □

I Teoremi di Completezza (Gödel, 1930), asseriscono che vale il converso del Teorema e del Corollario.

Teorema 28.4 (Completezza Debole)**.** $\Gamma \models \boldsymbol{\varphi}$ *implica* $\Gamma \vdash \boldsymbol{\varphi}$.

Teorema 28.5 (Completezza Forte)**.** *Un insieme consistente di enunciati Σ è soddisfacibile. Allora $\mathcal{A} \models \Sigma$, per qualche $\mathcal{A}$. Infatti Σ ha un modello di cardinalità $\leq \mathrm{card}(\boldsymbol{L})$.*

Vediamo come il Teorema di Completezza Forte implica il Teorema di Completezza Debole:

Dimostrazione. Consideriamo prima il caso in cui $\Gamma, \{\boldsymbol{\varphi}\} \subseteq \mathrm{Sent}(\boldsymbol{L})$. Possiamo supporre che Γ sia consistente, altrimenti il risultato è banalmente vero. Se $\Gamma \nvdash \boldsymbol{\varphi}$ allora $\Gamma \cup \{\boldsymbol{\neg\varphi}\}$ è consistente per la Proposizione 27.10, quindi ammette un modello $\mathcal{A}$. Ma allora $\mathcal{A}$ testimonia che $\Gamma \not\models \boldsymbol{\varphi}$.

Supponiamo ora il caso in cui gli elementi di Γ e $\{\boldsymbol{\varphi}\}$ siano delle formule con eventualmente variabili libere. Utilizzando 27.B.8 e la sua notazione, si ha che

- $\Gamma \vdash \boldsymbol{\varphi}$ se e solo se $\tilde{\Gamma} \vdash \tilde{\boldsymbol{\varphi}}$ e
- $\Gamma \models \boldsymbol{\varphi}$ se e solo se $\tilde{\Gamma} \models \tilde{\boldsymbol{\varphi}}$, per definizione di soddisfazione.

Quindi ci siamo ricondotti al caso degli enunciati. □

Lemma 28.6. *Sia Σ una $\boldsymbol{L}$-teoria consistente, sia $\boldsymbol{c}$ una nuova costante e sia $\boldsymbol{\varphi}(\boldsymbol{x})$ una $\boldsymbol{L}$-formula con un'unica variabile libera. Allora la $\boldsymbol{L}\cup\{\boldsymbol{c}\}$-teoria $\Sigma \cup \{\boldsymbol{\exists x}\, \boldsymbol{\varphi} \boldsymbol{\Rightarrow} \boldsymbol{\varphi}[\boldsymbol{c}/\boldsymbol{x}]\}$ è consistente.*

Dimostrazione. Supponiamo, per assurdo, che

$$\Sigma \cup \{\boldsymbol{\exists x}\, \boldsymbol{\varphi} \boldsymbol{\Rightarrow} \boldsymbol{\varphi}[\boldsymbol{c}/\boldsymbol{x}]\} \vdash_{\boldsymbol{L}\cup\{\boldsymbol{c}\}} \boldsymbol{\sigma} \boldsymbol{\wedge} \boldsymbol{\neg}\boldsymbol{\sigma}\,.$$

Per il Lemma 27.5 si ha $\Sigma \vdash_{\boldsymbol{L}\cup\{\boldsymbol{c}\}} (\boldsymbol{\exists x}\, \boldsymbol{\varphi} \boldsymbol{\Rightarrow} \boldsymbol{\varphi}[\boldsymbol{c}/\boldsymbol{x}]) \boldsymbol{\Rightarrow} \boldsymbol{\sigma} \boldsymbol{\wedge} \boldsymbol{\neg}\boldsymbol{\sigma}$ e quindi

$$\Sigma \vdash_{\boldsymbol{L}\cup\{\boldsymbol{c}\}} \boldsymbol{\neg}(\sigma \boldsymbol{\wedge} \boldsymbol{\neg}\sigma) \boldsymbol{\Rightarrow} \boldsymbol{\neg}(\boldsymbol{\exists x}\, \boldsymbol{\varphi} \boldsymbol{\Rightarrow} \boldsymbol{\varphi}[\boldsymbol{c}/\boldsymbol{x}])\,.$$

Poiché $\boldsymbol{\neg}\,(\boldsymbol{\sigma} \boldsymbol{\wedge} \boldsymbol{\neg}\boldsymbol{\sigma})$ è una tautologia ne segue che $\Sigma \vdash_{\boldsymbol{L}\cup\{\boldsymbol{c}\}} (\boldsymbol{\exists x}\, \boldsymbol{\varphi}) \boldsymbol{\wedge} \boldsymbol{\neg}\boldsymbol{\varphi}[\boldsymbol{c}/\boldsymbol{x}]$. Il Teorema 27.6 implica che

$$\Sigma \vdash_{\boldsymbol{L}} \boldsymbol{\forall x}\big((\boldsymbol{\exists x}\, \boldsymbol{\varphi}) \boldsymbol{\wedge} \boldsymbol{\neg}\boldsymbol{\varphi}\big)$$

e quindi per il Lemma 27.7 $\Sigma \vdash_{\boldsymbol{L}} (\boldsymbol{\exists x}\, \boldsymbol{\varphi}) \boldsymbol{\wedge} (\boldsymbol{\forall x}\, \boldsymbol{\neg}\boldsymbol{\varphi})$. Per (LAx-6) $\Sigma \vdash_{\boldsymbol{L}} (\boldsymbol{\exists x}\, \boldsymbol{\varphi}) \boldsymbol{\wedge} \boldsymbol{\neg}(\boldsymbol{\exists x}\, \boldsymbol{\varphi})$, quindi Σ è inconsistente. □

Lemma 28.7. *Sia Σ un insieme consistente di $\boldsymbol{L}$-enunciati e sia C un insieme di nuove costanti di cardinalità* $\mathrm{card}(\boldsymbol{L})$*. Allora Σ può essere esteso ad un $\tilde{\Sigma}$ insieme consistente di enunciati di $\tilde{\boldsymbol{L}} = \boldsymbol{L} \cup C$ in modo che se $\boldsymbol{\varphi}(\boldsymbol{x})$ è una $\boldsymbol{L}$-formula con un'unica variabile libera, allora $\exists \boldsymbol{c} \in C$ tale che $\tilde{\Sigma} \vdash \boldsymbol{\exists x}\, \boldsymbol{\varphi} \boldsymbol{\Rightarrow} \boldsymbol{\varphi}[\boldsymbol{c}/\boldsymbol{x}]$.*

Dimostrazione. Sia $\kappa = \mathrm{card}(\boldsymbol{L})$ e siano $\langle \boldsymbol{c}_\gamma \mid \gamma < \kappa\rangle$ e $\langle \boldsymbol{\varphi}_\gamma \mid \gamma < \kappa\rangle$ enumerazioni di C e dell'insieme delle $\boldsymbol{L}$-formule con un'unica variabile libera. Sia

$$\Sigma_\alpha = \Sigma \cup \{\, \boldsymbol{\exists x}_\gamma\, \boldsymbol{\varphi}_\gamma \boldsymbol{\Rightarrow} \boldsymbol{\varphi}_\gamma[\boldsymbol{c}_\gamma/\boldsymbol{x}_\gamma] \mid \gamma \leq \alpha \,\} \qquad (\alpha < \kappa)$$

dove $\boldsymbol{x}_\gamma$ è l'unica variabile libera di $\boldsymbol{\varphi}_\gamma$. Utilizzando il Lemma 28.6 per α successore e l'Esercizio 27.9 per α limite si ha che ogni Σ_α è consistente. Per costruzione $\tilde{\Sigma} = \Sigma_\kappa$ soddisfa l'enunciato del Lemma. □

Un insieme Γ di $\boldsymbol{L}$-formule **ammette testimoni** se per ogni $\boldsymbol{L}$-formula $\boldsymbol{\varphi}$ con al più una variabile libera $\boldsymbol{x}$ c'è una costante $\boldsymbol{c}$ tale che

$$\Gamma \vdash \boldsymbol{\exists x}\, \boldsymbol{\varphi} \boldsymbol{\Rightarrow} \boldsymbol{\varphi}[\boldsymbol{c}/\boldsymbol{x}]\,.$$

La costante $\boldsymbol{c}$ si dice **testimone** per $\boldsymbol{\exists x}\, \boldsymbol{\varphi}$.

Osservazione 28.8. Se $\Gamma \subseteq \Gamma' \subseteq \mathrm{Fml}(\boldsymbol{L})$ e Γ ha testimoni, allora anche Γ' ha testimoni.

Teorema 28.9. *Se Σ è un insieme consistente di $\boldsymbol{L}$-enunciati esiste un insieme C di cardinalità κ di nuove costanti ed esiste un insieme Σ_∞ consistente di enunciati di $\boldsymbol{L}_\infty = \boldsymbol{L} \cup C$ tali che $\Sigma_\infty \supseteq \Sigma$ e Σ_∞ ha testimoni.*

Dimostrazione. Costruiremo induttivamente

- linguaggi $\boldsymbol{L} = \boldsymbol{L}_0 \subset \boldsymbol{L}_1 \subset \cdots \subset \boldsymbol{L}_n \subset \ldots$ tali che $\boldsymbol{L}_{n+1} = \boldsymbol{L}_n \cup C_n$ dove C_n è un insieme di costanti che non appartengono a $\boldsymbol{L}_n$ e $|C_n| = \mathrm{card}(\boldsymbol{L}_n) = \mathrm{card}(\boldsymbol{L})$,
- insiemi consistenti $\Sigma_n \subseteq \mathrm{Sent}(\boldsymbol{L}_n)$ tali che
  (i) $\Sigma = \Sigma_0 \subset \Sigma_1 \subset \cdots \subset \Sigma_n \subset \cdots$ e
  (ii) per ogni $\boldsymbol{L}_n$-formula $\boldsymbol{\varphi}(\boldsymbol{x})$ con un'unica variabile libera c'è un $\boldsymbol{c} \in C_n$ tale che $\Sigma_{n+1} \vdash \boldsymbol{\exists x\, \varphi \Rightarrow \varphi}[\boldsymbol{c}/\boldsymbol{x}]$.

Se $\boldsymbol{L}_0, \ldots, \boldsymbol{L}_n$, $C_0, \ldots, C_{n-1}$ e $\Sigma_0, \ldots, \Sigma_n$ sono stati costruiti e soddisfano i requisiti, allora il Lemma 28.7 garantisce l'esistenza di C_n (e quindi di $\boldsymbol{L}_{n+1}$) e di Σ_{n+1} come richiesto. Posto $C = \bigcup_n C_n$, $\boldsymbol{L}_\infty = \bigcup_n \boldsymbol{L}_n$ e $\Sigma_\infty = \bigcup_n \Sigma_n$ abbiamo che

- $|C| = \kappa$,
- $\Sigma_\infty \subseteq \mathrm{Sent}(\boldsymbol{L}_\infty)$ è consistente (Esercizio 27.9 parte (ii))
- Σ_∞ ammette testimoni: fissata una $\boldsymbol{L}_\infty$ formula $\boldsymbol{\varphi}(\boldsymbol{x})$ con un'unica variabile libera, sia n minimo tale che $\boldsymbol{\varphi}(\boldsymbol{x}) \in \mathrm{Fml}(\boldsymbol{L}_n)$. Per costruzione c'è un $\boldsymbol{c} \in C_n$ tale che $\Sigma_{n+1} \vdash_{\boldsymbol{L}_{n+1}} \boldsymbol{\exists x\, \varphi \Rightarrow \varphi}[\boldsymbol{c}/\boldsymbol{x}]$ e quindi $\Sigma_\infty \vdash_{\boldsymbol{L}_\infty} \boldsymbol{\exists x\, \varphi \Rightarrow \varphi}[\boldsymbol{c}/\boldsymbol{x}]$.

Questo conclude la dimostrazione. □

28.A. Dimostrazione del Teorema 28.5**.** Sia Σ un insieme consistente di $\boldsymbol{L}$-enunciati. Per il Lemma 28.7 possiamo aggiungere ad $\overline{\boldsymbol{L}}$ un insieme C di nuove costanti con $|C| = \mathrm{card}(\boldsymbol{L})$ e possiamo estender Σ ad un insieme consistente di $\overline{\boldsymbol{L}}$-enunciati Σ' in modo che Σ' abbia testimoni. Per la parte (iii) dell'Esercizio 27.9 (Lemma di Lindembaum) sia $\overline{\Sigma} \supseteq \Sigma'$ un insieme consistente e massimale di $\overline{\boldsymbol{L}}$-enunciati. Per la Proposizione 27.10 per ogni $\overline{\boldsymbol{L}}$-enunciato $\boldsymbol{\sigma}$

$$\overline{\Sigma} \vdash \boldsymbol{\sigma} \quad \Leftrightarrow \quad \boldsymbol{\sigma} \in \overline{\Sigma}\,.$$

Costruiremo un $\overline{\boldsymbol{L}}$-modello $\overline{\mathcal{A}}$ di $\overline{\Sigma}$: poiché $\Sigma \subseteq \Sigma' \subseteq \overline{\Sigma}$ si avrà che $\overline{\mathcal{A}} \models \Sigma'$ e quindi, passando alla contrazione $\mathcal{A}$ di $\overline{\mathcal{A}}$ a $\boldsymbol{L}$, otterremo il modello cercato. Sia $\sim$ la relazione di equivalenza su $\mathrm{ClTerm}(\overline{\boldsymbol{L}})$, l'insieme degli $\overline{\boldsymbol{L}}$-termini chiusi, definita da

$$\boldsymbol{t} \sim \boldsymbol{u} \quad \Leftrightarrow \quad (\boldsymbol{t} \equiv \boldsymbol{u}) \in \overline{\Sigma}\,.$$

(Nota bene: non stiamo chiedendo che i due termini $\boldsymbol{t}$ e $\boldsymbol{u}$ siano identici—chiediamo invece che $\overline{\Sigma}$ dimostri l'enunciato "$\boldsymbol{t} \equiv \boldsymbol{u}$".) L'universo di $\overline{\mathcal{A}}$ (e quindi anche di $\mathcal{A}$) è l'insieme

$$A = \mathrm{ClTerm}(\overline{\boldsymbol{L}})/{\sim}\,.$$

Dobbiamo ora definire l'interpretazione in $\overline{\mathcal{A}}$ delle relazioni, delle funzioni e delle costanti.

Se $\boldsymbol{R}$ è un $\overline{\boldsymbol{L}}$-simbolo (e quindi anche un $\boldsymbol{L}$-simbolo) di relazione n-ario, poniamo

$$\boldsymbol{R}^{\overline{\mathcal{A}}} = \left\{ \langle [\boldsymbol{t}_1]_\sim, \ldots, [\boldsymbol{t}_n]_\sim \rangle \in A^n \mid \boldsymbol{R}(\boldsymbol{t}_1, \ldots, \boldsymbol{t}_n) \in \overline{\Sigma} \right\}.$$

Prima di procedere dobbiamo verificare che la relazione $\boldsymbol{R}^{\overline{\mathcal{A}}}$ è ben definita: se $\boldsymbol{R}(\boldsymbol{t}_1, \ldots, \boldsymbol{t}_n) \in \overline{\Sigma}$ e se $\boldsymbol{t}_i \sim \boldsymbol{u}_i$ allora $\boldsymbol{t}_1 \equiv \boldsymbol{u}_1 \boldsymbol{\wedge} \ldots \boldsymbol{\wedge} \boldsymbol{t}_n \equiv \boldsymbol{u}_n \in \overline{\Sigma}$

$$\vdash \boldsymbol{t}_1 \equiv \boldsymbol{u}_1 \boldsymbol{\wedge} \ldots \boldsymbol{\wedge} \boldsymbol{t}_n \equiv \boldsymbol{u}_n \boldsymbol{\Rightarrow} (\boldsymbol{R}(\boldsymbol{t}_1, \ldots, \boldsymbol{t}_n) \boldsymbol{\Leftrightarrow} \boldsymbol{R}(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n))$$

per 27.B.2, ne deduciamo che $\boldsymbol{R}(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n) \in \overline{\Sigma}$ e quindi la definizione di $R^{\overline{\mathcal{A}}}$ non dipende dai rappresentanti scelti.

Se $\boldsymbol{f}$ è un $\overline{\boldsymbol{L}}$-simbolo (e quindi anche un $\boldsymbol{L}$-simbolo) di funzione n-ario, poniamo

$$\boldsymbol{f}^{\overline{\mathcal{A}}}([\boldsymbol{t}_1]_\sim, \ldots, [\boldsymbol{t}_n]_\sim) = [\boldsymbol{f}(\boldsymbol{t}_1, \ldots, \boldsymbol{t}_n)]_\sim .$$

In modo del tutto analogo a quanto fatto sopra si verifica che la definizione di $\boldsymbol{f}^{\overline{\mathcal{A}}}$ non dipende dai rappresentanti scelti.

Infine, se $\boldsymbol{c}$ è un $\overline{\boldsymbol{L}}$-simbolo di costante, poniamo

$$\boldsymbol{c}^{\overline{\mathcal{A}}} = [\boldsymbol{c}]_\sim .$$

Quindi abbiamo definito $\overline{\mathcal{A}}$. Se $\boldsymbol{t} \in \mathrm{ClTerm}$ possiamo definire per induzione sulla complessità di $\boldsymbol{t}$ l'elemento $\boldsymbol{t}^{\overline{\mathcal{A}}} \in A$ così:

$$\boldsymbol{t}^{\overline{\mathcal{A}}} = \begin{cases} \boldsymbol{c}^{\overline{\mathcal{A}}} & \text{se } \boldsymbol{t} \text{ è } \boldsymbol{c}, \\ \boldsymbol{f}^{\overline{\mathcal{A}}}(\boldsymbol{t}_1^{\overline{\mathcal{A}}}, \ldots, \boldsymbol{t}_n^{\overline{\mathcal{A}}}) & \text{se } \boldsymbol{t} \text{ è } \boldsymbol{f}(\boldsymbol{t}_1, \ldots, \boldsymbol{t}_n). \end{cases}$$

Esercizio 28.10. Dimostrare che per ogni $\boldsymbol{t} \in \mathrm{ClTerm}$ c'è almeno una costante $\boldsymbol{c} \in C$ tale che $\boldsymbol{t} \sim \boldsymbol{c}$ e che $\boldsymbol{t}^{\overline{\mathcal{A}}} = [\boldsymbol{t}]_\sim$.

Dobbiamo ora verificare che $\overline{\mathcal{A}} \models \overline{\Sigma}$. Infatti verificheremo che, per ogni enunciato $\boldsymbol{\sigma} \in \mathrm{Sent}(\overline{\boldsymbol{L}})$:

$$\boldsymbol{\sigma} \in \overline{\Sigma} \quad \Leftrightarrow \quad \overline{\mathcal{A}} \models \boldsymbol{\sigma}$$

La costruzione di $\mathcal{A}$ garantisce ciò vale quando $\boldsymbol{\sigma}$ è atomica.

Se $\boldsymbol{\sigma} = \boldsymbol{\neg\tau}$,

$$\begin{aligned} \boldsymbol{\sigma} \in \overline{\Sigma} &\Leftrightarrow \boldsymbol{\tau} \notin \overline{\Sigma} && \text{(per la massimalità di } \overline{\Sigma}) \\ &\Leftrightarrow \mathcal{A} \not\models \boldsymbol{\tau} && \text{(ip. ind.)} \\ &\Leftrightarrow \mathcal{A} \models \boldsymbol{\sigma} \end{aligned}$$

Se $\boldsymbol{\sigma} = \boldsymbol{\tau} \boldsymbol{\wedge} \boldsymbol{\chi}$ allora

$$\begin{aligned} \boldsymbol{\sigma} \in \overline{\Sigma} &\Leftrightarrow (\boldsymbol{\tau} \in \overline{\Sigma}) \wedge (\boldsymbol{\chi} \in \overline{\Sigma}) \\ &\Leftrightarrow (\overline{\mathcal{A}} \models \boldsymbol{\tau}) \wedge (\overline{\mathcal{A}} \models \boldsymbol{\chi}) && \text{(ip. ind.)} \\ &\Leftrightarrow \overline{\mathcal{A}} \models \boldsymbol{\tau} \boldsymbol{\wedge} \boldsymbol{\chi}. \end{aligned}$$

Se $\boldsymbol{\sigma} = \boldsymbol{\exists x\, \varphi}$, allora

$$\exists \boldsymbol{c} \in C \left(\boldsymbol{\exists x\, \varphi \Rightarrow \varphi}[\boldsymbol{c}/\boldsymbol{x}] \in \overline{\Sigma} \right).$$

Quindi $\boldsymbol{\sigma} \in \overline{\Sigma}$ implica $\boldsymbol{\varphi}[\boldsymbol{c}/\boldsymbol{x}] \in \overline{\Sigma}$ e allora, per ipotesi induttiva, $\overline{\mathcal{A}} \models \boldsymbol{\varphi}[\boldsymbol{c}^{\overline{\mathcal{A}}}]$, da cui $\overline{\mathcal{A}} \models \boldsymbol{\sigma}$. Viceversa se $\overline{\mathcal{A}} \models \boldsymbol{\sigma}$, allora c'è un $a \in \|\mathcal{A}\|$ tale che $\overline{\mathcal{A}} \models \boldsymbol{\varphi}[a]$. Sia $\boldsymbol{t} \in \mathrm{ClTerm}(\overline{L})$ tale che $[\boldsymbol{t}]_{\sim} = a$. Allora $\boldsymbol{t}^{\overline{\mathcal{A}}} = a$ e dato che $\boldsymbol{t}$ è sostituibile ad $\boldsymbol{x}$ in $\boldsymbol{\varphi}$ abbiamo $\overline{\mathcal{A}} \models \boldsymbol{\varphi}[\boldsymbol{t}/\boldsymbol{x}]$, per la Proposizione 21.15. Per ipotesi induttiva $\boldsymbol{\varphi}[\boldsymbol{t}/\boldsymbol{x}] \in \overline{\Sigma}$ e dato che l'enunciato $\boldsymbol{\varphi}[\boldsymbol{t}/\boldsymbol{x}] \boldsymbol{\Rightarrow \exists x \varphi}$ è il contrapositivo di un assioma logico di tipo (LAx-2) e quindi è in $\overline{\Sigma}$, ne segue che $\boldsymbol{\exists x \varphi} \in \overline{\Sigma}$ come richiesto.

Questo conclude la dimostrazione del Teorema di Completezza Forte.

Esercizi

Esercizio 28.11. Dimostrare che il Teorema di Completezza Forte implica il Teorema di Compattezza. Dimostrare che il Teorema di Completezza Debole e il Teorema di Compattezza implicano il Teorema di Completezza Forte.

Capitolo IV

Funzioni calcolabili

29. Ricorsione primitiva

Una funzione $f\colon \mathbb{N}^n \to \mathbb{N}$ si dice *effettiva* o *calcolabile* se esiste una procedura meccanica, un algoritmo, che calcola il valore di $f(x_1, \ldots, x_n)$ a partire da x_1, x_2, …, x_n. Naturalmente, per rendere questa definizione matematicamente ineccepibile, dobbiamo spiegare cosa intendiamo con *procedura meccanica* e *algoritmo*. Una possibile definizione è quella di funzioni calcolabili mediante un programma scritto in FORTRAN, in Basic, o in Pascal. Una definizione alternativa e completamente equivalente, è stata individuata negli anni venti del secolo scorso, ed è la classe delle funzioni ricorsive. In questa sezione ci limitiamo alla sottoclasse delle funzioni primitive ricorsive che comprende molte delle (ma non tutte le) funzioni effettivamente calcolabili.

29.A. Funzioni primitive ricorsive. Cominciamo con qualche definizione. Supponiamo f sia k-aria su $\mathbb{N}$. Se $g_1, \ldots, g_k$ sono n arie su $\mathbb{N}$, la **composizione** di f con $g_1, \ldots, g_k$ è la funzione n-aria

$$h(x_1, \ldots, x_n) = f(g_1(x_1, \ldots, x_n), \ldots, g_k(x_1, \ldots, x_n)) \tag{113}$$

La definizione data può apparire troppo restrittiva in quanto spesso capita che le g_i siano di arietà differente o che l'ordine delle variabili nelle g_i non sia lo stesso. Per esempio consideriamo la funzione 3-aria

$$h(x_1, x_2, x_3) = f(g_1(x_2, x_3), g_2(x_1), g_3(x_2, x_1, x_1)) \tag{114}$$

Per ricondurci a (113) dobbiamo utilizzare le **funzioni di proiezione**

$$\mathrm{proj}^n_k : \mathbb{N}^n \to \mathbb{N} \quad (x_1, \ldots, x_n) \mapsto x_k \qquad (1 \leq k \leq n).$$

Allora la funzione h di (114) è la composizione (nel senso di (113)) della funzione f con $\tilde{g}_1$, $\tilde{g}_2$ e $\tilde{g}_3$, dove $\tilde{g}_i$ è ottenuta da g_i $(i = 1, 2, 3)$ mediante

proiezioni:

$$\tilde{g}_1(\bar{x}) = g_1(\mathrm{proj}^3_2(\bar{x}), \mathrm{proj}^3_3(\bar{x}))$$
$$\tilde{g}_2(\bar{x}) = g_2(\mathrm{proj}^3_1(\bar{x}))$$
$$\tilde{g}_3(\bar{x}) = g_3(\mathrm{proj}^3_2(\bar{x}), \mathrm{proj}^3_1(\bar{x}), \mathrm{proj}^3_1(\bar{x}))$$

e $\bar{x}$ denota (x_1, x_2, x_3).

Se f è k-aria (con $k \geq 0$) e g è $k+2$ aria su $\mathbb{N}$, diremo che la funzione $k+1$-aria

(115)
$$h(x_1, \ldots, x_k, n) = \begin{cases} f(x_1, \ldots, x_k) & \text{se } n = 0, \\ g(x_1, \ldots, x_k, n-1, h(x_1, \ldots, x_k, n-1)) & \text{se } n > 0, \end{cases}$$

è ottenuta per **ricorsione primitiva a partire da f e g**. Naturalmente, se $k = 0$, la f è una costante.

Esercizio 29.1. Dimostrare che la funzione h in (115) è ben definita.

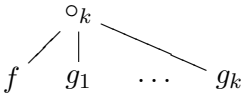
Definizione 29.2. L'insieme **PRec** delle **funzioni primitive ricorsive** è il più piccolo insieme di funzioni finitarie su $\mathbb{N}$ contenente

- le funzioni costanti $\mathrm{c}^n_k \colon \mathbb{N}^n \to \mathbb{N}$, $(x_1, \ldots, x_n) \mapsto k$, con $n, k \in \mathbb{N}$;
- le funzioni di proiezione $\mathrm{proj}^n_k \colon \mathbb{N}^n \to \mathbb{N}$;
- la funzione successore $\mathbf{S} = \mathbf{S} \restriction \mathbb{N} \colon \mathbb{N} \to \mathbb{N}$, $n \mapsto n+1$.

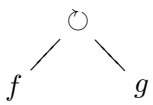
Useremo spesso $\bar{x}$ per denotare una generica n-upla $(x_1, \ldots, x_n)$.

Una funzione primitiva ricorsiva può essere efficacemente visualizzata come la radice di un albero etichettato (§77.B) in cui

- i nodi terminali sono etichettati mediante $\mathbf{S}$, proj^n_k e c^n_k.
- i nodi non terminali sono etichettati come $\circ_k$ e $\circlearrowright$, dove
  - i nodi successori di un nodo etichettato $\circ_k$, sono $k+1$, dove k è l'arietà della funzione rappresentata del nodo più a sinistra e tutte le rimanenti k funzioni hanno la medesima arietà,



  - i nodi successori di un nodo etichettato $\circlearrowright$, sono 2, dove se k è l'arietà della funzione rappresentata dal nodo a sinistra, allora la funzione rappresentata dal nodo a destra è $k+2$,



Applicando ripetutamente questa procedura alle f e g otteniamo un albero che descrive la funzione in questione. Un albero siffatto si dice **albero di programma** o semplicemente **programma**. della funzione primitiva ricorsiva in questione—nella prossima sezione vedremo numerosi esempi di alberi di programma per funzioni primitive ricorsive. L'insieme $\mathcal{T}_{\mathbf{PRec}}$ dei programmi (o meglio: degli alberi di programma) di funzioni primitive ricorsive è un sotto-insieme proprio della famiglia degli alberi etichettati mediante elementi di

$$\mathcal{S} = \{\mathbf{S}\,,\, \circlearrowleft\} \cup \{\, \circ_n \mid n > 0\,\} \cup \{\, \mathrm{c}_k^n \mid n, k \geq 0\,\} \cup \{\, \mathrm{proj}_k^n \mid n > k \geq 0\,\}\,.$$

La mappa $\mathcal{T}_{\mathbf{PRec}} \to \mathbf{PRec}$ che associa ad ogni $T \in \mathcal{T}_{\mathbf{PRec}}$ la funzione $f_T \in \mathbf{PRec}$ descritta da T, è suriettiva, ma non iniettiva—Osservazione 29.4. Possiamo anche vedere i programmi come parole su $(\mathcal{S}, a)$, dove $a(\circlearrowleft) = 2$, $a(\circ_k) = k + 1$ e $a(s)$ per tutti gli altri $s \in \mathcal{S}$. Naturalmente, non tutti gli elementi di $\mathrm{Words}(\mathcal{S}, a)$ sono programmi, dato che—per esempio—si richiede che se $\langle \circ_k, f, g_1, \dots g_k \rangle$, allora la funzione (descritta dal programma) f deve avere arietà k e le funzioni (descritte dai programmi) $g_1, \dots, g_k$ devono avere tutte la medesima arietà. Definiamo induttivamente la funzione $\mathrm{ar}\colon \mathrm{Words}(\mathcal{S}, a) \to \omega \cup \{-1\}$:

- Se $\mathrm{ht}(w) = 0$, allora

$$\mathrm{ar}(w) = \begin{cases} n & \text{se } w = \langle \mathrm{proj}_k^n \rangle, \\ n & \text{se } w = \langle \mathrm{c}_k^n \rangle, \\ 1 & \text{se } w = \langle \mathbf{S} \rangle. \end{cases}$$

- Se $\mathrm{ht}(w) > 0$, allora

$$\mathrm{ar}(w) = \begin{cases} n & \text{se } w = \langle \circ_k \rangle^\frown f^\frown g_1{}^\frown \cdots {}^\frown g_k \text{ e} \\ & \quad \mathrm{ar}(f) = k \text{ e } \mathrm{ar}(g_1) = \cdots = \mathrm{ar}(g_k) = n \geq 0, \\ n+1 & \text{se } w = \langle \circlearrowleft \rangle^\frown f^\frown g,\ \mathrm{ar}(f) = n+2 \text{ e } \mathrm{ar}(g) = n \geq 0, \\ -1 & \text{altrimenti.} \end{cases}$$

È immediato verificare che per ogni $w \in \mathrm{Words}(\mathcal{S}, a)$

$$w \text{ è un programma} \quad \Leftrightarrow \quad \mathrm{ar}(w) \geq 0\,.$$

Osservazione 29.3. Tutte le funzioni in **PRec** sono calcolabili secondo una qualsiasi ragionevole definizione di calcolabilità: infatti

- le funzioni $\mathbf{S}$, c_k^n, proj_k^n sono calcolabili,
- se h, f, g_1, …, g_k sono come in (113), allora per calcolare $h(x_1, \dots, x_n)$ basta calcolare i valori $g_1(x_1, \dots, x_n), \dots, g_k(x_1, \dots, x_n)$ e poi inserirli nella f e calcolarne il risultato,

- se h, g e f sono come in (115), allora per calcolare $h(x_1, \dots, x_n, i)$ è sufficiente calcolare i valori

$$\begin{aligned} a_0 &= h(x_1, \dots, x_n, 0) = f(x_1, \dots, x_n) \\ a_1 &= h(x_1, \dots, x_n, 1) = g(x_1, \dots, x_n, 0, a_0) \\ a_2 &= h(x_1, \dots, x_n, 2) = g(x_1, \dots, x_n, 1, a_1) \\ &\vdots \\ a_i &= h(x_1, \dots, x_n, i) = g(x_1, \dots, x_n, i-1, a_{i-1}) \end{aligned}$$

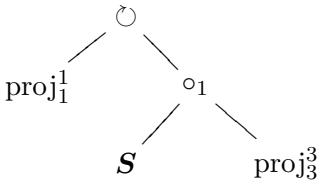
29.B. Esempi di funzioni primitive ricorsive.

29.B.1. La funzione identica $\mathrm{id} = \mathrm{id} \restriction \mathbb{N} \colon \mathbb{N} \to \mathbb{N}$ è proj^1_1 e quindi è in **PRec**. Il suo albero di programma è l'albero con un solo nodo: proj^1_1.

29.B.2. La funzione somma $f \colon \mathbb{N}^2 \to \mathbb{N}$, $f(x_1, x_2) = x_1 + x_2$, è primitiva ricorsiva. Infatti $\mathrm{id} = \mathrm{proj}^1_1$ e $h \stackrel{\text{def}}{=} \mathbf{S} \circ \mathrm{proj}^3_3$ sono primitive ricorsive e poiché

$$\begin{aligned} f(x_1, 0) &= x_1 = \mathrm{proj}^1_1(x_1) \\ f(x_1, x_2 + 1) &= \mathbf{S}(x_1 + x_2) = h(x_1, x_2, f(x_1, x_2)) \end{aligned}$$

ne segue che $f \in \mathbf{PRec}$. Il suo albero di programma è



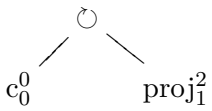
29.B.3. La funzione

$$x \dot{-} y = \begin{cases} x - y & \text{se } x \geq y, \\ 0 & \text{altrimenti,} \end{cases}$$

è primitiva ricorsiva. Infatti la funzione $g \colon \mathbb{N} \to \mathbb{N}$, $x \mapsto x \dot{-} 1$ è ottenuta per ricorsione primitiva

$$\begin{aligned} g(0) &= 0 = \mathrm{c}^0_0 \\ g(x+1) &= x = \mathrm{proj}^2_1(x, g(x)) \end{aligned}$$

e ha per albero di programma

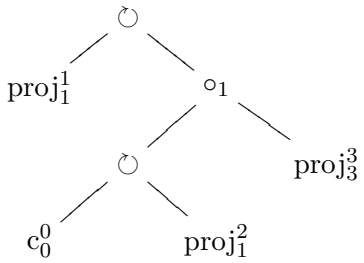


La funzione $(x_1, x_2) \mapsto x_1 \dot{-} x_2$ è definita per ricorsione primitiva

$$x_1 \dot{-} 0 = x_1 = \mathrm{proj}^1_1(x_1)$$
$$x_1 \dot{-} (x_2 + 1) = g(x_1 \dot{-} x_2) = g \circ \mathrm{proj}^3_3(x_1, x_2, x_1 \dot{-} x_2)$$

e ha per albero di programma

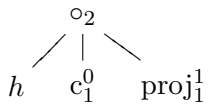
(116)



29.B.4. La funzione $\mathrm{sg}\colon \mathbb{N} \to \mathbb{N}$ definita da $\mathrm{sg}(0) = 0$ e $\mathrm{sg}(n+1) = 1$ è primitiva ricorsiva, dato che

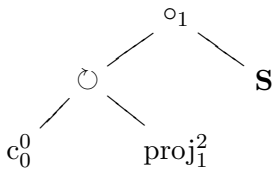
$$\mathrm{sg}(x_1) = 1 \dot{-} (1 \dot{-} x_1) = h\Big(\mathrm{c}^0_1(x_1), h\big(\mathrm{c}^0_1(x_1), \mathrm{proj}^1_1(x_1)\big)\Big).$$

dove $h(x, y) = x \dot{-} y$. L'albero di programma di $x_1 \mapsto 1 \dot{-} x_1$ è ottenuto da



sostituendo al nodo con etichetta h l'albero di programma (116). Lasciamo al lettore il compito di scrivere l'albero di programma per sg.

Osservazione 29.4. Per ciascuna funzione primitiva ricorsiva abbiamo individuato un albero di programma che la calcola, ma quest'albero non è unico: data una procedura per calcolare una $\bar{x} \mapsto f(\bar{x})$, posso calcolare $\bar{x} \mapsto \mathbf{S}(f(\bar{x})) \dot{-} 1$ e questo algoritmo genera un albero più complesso. Per esempio, alla funzione identità $x_1 \mapsto x_1$ oltre all'albero con un unico nodo etichettato proj^1_1, possiamo associare l'albero



Iterando questo ragionamento vediamo che *ogni* funzione primitiva ricorsiva ammette *infiniti* alberi di programma.

Esercizio 29.5. Dimostrare che le seguenti funzioni sono primitive ricorsive e per ciascuna di esse individuare un albero di programma.

(i) il prodotto $(x, y) \mapsto x \cdot y$;

(ii) l'esponenziazione $(x, y) \mapsto x^y$;

(iii) la funzione $(x_1, \dots, x_m) \mapsto f(x_{\sigma(1)}, \dots, x_{\sigma(n)})$, dove $f \in \mathbf{PRec}$ è n-aria e $\sigma\colon \{1, \dots, n\} \to \{1, \dots, m\}$;

(iv) le funzioni

$$(x_1, \dots, x_n, y) \mapsto \sum_{k=0}^{y} f(x_1, \dots, x_n, k)$$

$$(x_1, \dots, x_n, y) \mapsto \prod_{k=0}^{y} f(x_1, \dots, x_n, k)\,,$$

dove $f \in \mathbf{PRec}$ è $n+1$-aria. In particolare la funzione fattoriale $n \mapsto n!$ è primitiva ricorsiva;

(v) la funzione $(x, n) \mapsto f^{(n)}(x)$ che codifica la successione delle iterate $f^{(n)}$ di una $f\colon \mathbb{N} \to \mathbb{N}$ primitiva ricorsiva.

Un **insieme** $A \subseteq \mathbb{N}^n$ è **primitivo ricorsivo** se la sua funzione caratteristica $\boldsymbol{\chi}_A\colon \mathbb{N}^n \to \{0, 1\}$,

$$\boldsymbol{\chi}_A(\bar{x}) = 1 \Leftrightarrow \bar{x} \in A$$

è in **PRec**. Spesso scriveremo, secondo una pratica comune in logica matematica, $A(\bar{x})$ al posto di $\bar{x} \in A$ e diremo che A è un predicato primitivo ricorsivo n-ario.

29.C. Esempi di insiemi primitivi ricorsivi.

29.C.1. Se $A, B \subseteq \mathbb{N}^n$ sono insiemi primitivi ricorsivi, allora

$$\neg A \stackrel{\text{def}}{=} \mathbb{N}^n \setminus A$$

e $A \cap B$ sono insiemi primitivi ricorsivi, dato che $\boldsymbol{\chi}_{\neg A} = 1 \dot{-} \boldsymbol{\chi}_A$ e $\boldsymbol{\chi}_{A\cap B} = \boldsymbol{\chi}_A \cdot \boldsymbol{\chi}_B$. Quindi anche gli insiemi

$$A \cup B = \neg(\neg A \cap \neg B), \quad A \setminus B = A \cap \neg B \quad \text{e} \quad A \triangle B = (A \setminus B) \cup (B \setminus A)$$

sono primitivi ricorsivi.

29.C.2. Se $\{A_1, \dots, A_k\}$ è una partizione di $\mathbb{N}^n$ in insiemi primitivi ricorsivi, e se $g_1, \dots, g_k \in \mathbf{PRec}$ sono n-arie, allora la funzione $f\colon \mathbb{N}^n \to \mathbb{N}$ definita da

$$f(\bar{x}) = \begin{cases} g_1(\bar{x}) & \text{se } \bar{x} \in A_1, \\ g_2(\bar{x}) & \text{se } \bar{x} \in A_2, \\ \quad\vdots & \\ g_k(\bar{x}) & \text{se } \bar{x} \in A_k, \end{cases}$$

è primitiva ricorsiva, dato che

$$f(\bar{x}) = g_1(\bar{x}) \cdot \boldsymbol{\chi}_{A_1}(\bar{x}) + \dots + g_k(\bar{x}) \cdot \boldsymbol{\chi}_{A_k}(\bar{x})\,.$$

29.C.3. Il predicato $x \leq y$ (vale a dire: l'insieme $A = \{\, (x, y) \mid x \leq y \,\}$) è primitivo ricorsivo, visto che $\boldsymbol{\chi}_A(x, y) = 1 \dot{-} \operatorname{sg}(x \dot{-} y)$.

29.C.4. Se $A \subseteq \mathbb{N}^{n+1}$ è primitivo ricorsivo allora l'insieme

$$B = \left\{\, (\bar{x}, y) \in \mathbb{N}^{n+1} \mid \forall z \leq y \; A(\bar{x}, z) \,\right\}$$

è primitivo ricorsivo, perché la sua funzione caratteristica è $\prod_{k=0}^{y} \boldsymbol{\chi}_A(\bar{x}, k)$. Quindi anche

$$\begin{aligned} C &= \left\{\, (\bar{x}, y) \in \mathbb{N}^{n+1} \mid \exists z \leq y \; A(\bar{x}, z) \,\right\} \\ &= \neg \left\{\, (\bar{x}, y) \in \mathbb{N}^{n+1} \mid \forall z \leq y \; \neg A(\bar{x}, z) \,\right\} \end{aligned}$$

è primitivo ricorsivio. È usuale scrivere i predicati $B(\bar{x}, y)$ e $C(\bar{x}, y)$, rispettivamente,

$$\forall z \leq y \, A(\bar{x}, z) \quad \text{e} \quad \exists z \leq y \, A(\bar{x}, z)\,. \tag{117}$$

29.C.5. Se $A \subseteq \mathbb{N}^{n+1}$ è primitivo ricorsivo, la funzione $n+1$-aria

$$f(\bar{x}, y) = \begin{cases} \min \{\, z \leq y \mid A(\bar{x}, z) \,\} & \text{se questo insieme è non vuoto,} \\ 0 & \text{altrimenti,} \end{cases}$$

è primitiva ricorsiva. Infatti i predicati

$$\begin{aligned} A_0(\bar{x}, y) &: \quad \exists z \leq y \, A(\bar{x}, z) \\ A_1(\bar{x}, y) &: \quad (\forall z \leq y \, \neg A(\bar{x}, z)) \wedge A(\bar{x}, y+1) \end{aligned}$$

sono primitivi ricorsivi e la funzione f si può scrivere come

$$f(\bar{x}, y+1) = \begin{cases} f(\bar{x}, y) & \text{se } A_0(\bar{x}, y), \\ y+1 & \text{se } A_1(\bar{x}, y), \\ 0 & \text{altrimenti.} \end{cases}$$

Poiché la funzione $n+2$-aria

$$g(\bar{x}, y, w) = w \cdot \boldsymbol{\chi}_{A_0}(\bar{x}, y) + \mathbf{S}(y) \cdot \boldsymbol{\chi}_{A_1}(\bar{x}, y)$$

è primitiva ricorsiva, allora anche la f è primitiva ricorsiva dato che

$$f(\bar{x}, y) = \begin{cases} 0 & \text{se } y = 0, \\ g(\bar{x}, y-1, f(\bar{x}, y-1)) & \text{se } y > 0 \end{cases}$$

è ottenuta per ricorsione primitiva. Diremo che la funzione f di cui sopra è ottenuta per **minimalizzazione limitata** e scriveremo

$$f(\bar{x}, y) = \boldsymbol{\mu} z \leq y \, A(\bar{x}, z)\,. \tag{118}$$

Naturalmente, se $g(\bar{y})$ è primitiva ricorsiva, anche la funzione

$$h(\bar{x}, \bar{y}) = f(\bar{x}, g(\bar{y})) = \boldsymbol{\mu} z \leq g(\bar{y}) \, A(\bar{x}, z)\,. \tag{119}$$

è primitiva ricorsiva.

Esercizi

Esercizio 29.6. Dimostrare che i seguenti insiemi e funzioni sono primitivi ricorsivi:

(i) se $A \subseteq \mathbb{N}^n$ è primitivo ricorsivo e $f_1, \ldots, f_n \in \mathbf{PRec}$ sono k-arie, allora

$$B = \Big\{ \bar{x} \in \mathbb{N}^k \mid (f_1(\bar{x}), \ldots, f_n(\bar{x})) \in A \Big\}$$

è primitivo ricorsivo. Scriveremo $A\big(f_1(\bar{x}), \ldots, f_n(\bar{x})\big)$ invece di $B(\bar{x})$.

(ii) i predicati $x = y$, $x \neq y$ e $x < y$;

(iii) ogni sottoinsieme finito di $\mathbb{N}$ e quindi ogni $X \subseteq \mathbb{N}$ tale che $\mathbb{N} \setminus X$ è finito;

(iv) le funzioni q (quoziente) e r (resto) definite da
- $q(x, y) = r(x, y) = 0$ se $y = 0$,
- $x = q(x, y) \cdot y + r(x, y)$ e $r(x, y) < y$, se $y \neq 0$;

(v) i predicati $x \mid y$ ("x divide y"), "x è primo"e "x e y sono relativamente primi."

Esercizio 29.7. Dimostrare che **PRec** è numerabile.

Esercizio 29.8. Dimostrare che, per ogni $n > 0$, la famiglia dei sottoinsiemi primitivi ricorsivi di $\mathbb{N}^n$ è un'algebra di Boole numerabile.

Esercizio 29.9. Sia $\boldsymbol{p}\colon \mathbb{N} \to \mathbb{N}$ la funzione che enumera tutti i numeri primi, cioè $\boldsymbol{p}(0) = 2$, $\boldsymbol{p}(1) = 3$, ... e sia $f(0) = 2$ e $f(n+1) = f(n)!$. Dimostrare che $\boldsymbol{p}(n) \leq f(n)$ e che $\boldsymbol{p}$ è primitiva ricorsiva.

Note e osservazioni

Nell'Esercizio 29.9 la funzione f può essere sostituita da 2^{n+1}, ma questo dipende da un risultato non banale di teoria dei numeri noto come *Postulato di Bertrand* che asserisce che tra n e $2n$ c'è sempre un numero primo. Questo risultato è stato congetturato nel 1845 da J.L. Bertrand (1822–1900) e dimostrato da P.L. Chebyshev (1821–1894) nel 1850—per una dimostrazione si veda [**HW79**, Theorem 418, pag.343].

30. Sequenze finite

Consideriamo la funzione

$$\boldsymbol{J}\colon \mathbb{N}\times\mathbb{N}\to\mathbb{N} \qquad \boldsymbol{J}(x,y)=\frac{1}{2}(x+y)(x+y+1)+x\,. \tag{120}$$

Con facili calcoli otteniamo:

(i) se $x+y=x'+y'$ allora $\boldsymbol{J}(x,y)<\boldsymbol{J}(x'+y')$ se e solo se $x<x'$.

(ii) $(x+y)(x+y+1)+2x<(x+y+1)(x+y+2)$ e quindi $\boldsymbol{J}(x,y)<\boldsymbol{J}(0,x+y+1)$.

(iii) $y<y'\Rightarrow \boldsymbol{J}(0,y)<\boldsymbol{J}(0,y')$

Quindi se $x+y<x'+y'$ allora

$$\boldsymbol{J}(x,y)<\boldsymbol{J}(0,x+y+1)\le\boldsymbol{J}(0,x'+y')\le\boldsymbol{J}(x',y')\,.$$

Questo e ((i)) implicano che $\boldsymbol{J}$ è iniettiva. Viceversa, dato un $n\in\mathbb{N}$ sia $f(n)$ l'unico k tale che $\frac{1}{2}k(k+1)\le n<\frac{1}{2}(k+1)(k+2)$, cioè

$$f(n)=\boldsymbol{\mu}k\le n\,(2n<(k+1)(k+2)) \tag{121}$$

e siano $x=n\dot{-}f(n)$ e $y=f(n)\dot{-}x$. Allora $\boldsymbol{J}(x,y)=n$. Quindi $\boldsymbol{J}\colon\mathbb{N}^2\to\mathbb{N}$ è una bijezione primitiva ricorsiva. Le sue inverse sono le funzioni

$$(\cdot)_0,(\cdot)_1:\mathbb{N}\to\mathbb{N} \tag{122}$$

definite da $\boldsymbol{J}((n)_0,(n)_1)=n$, sono anch'esse primitive ricorsive. Infatti la funzione f in (121) è primitiva ricorsiva e

$$(n)_0=n\dot{-}f(n)\quad\text{e}\quad(n)_1=n\dot{-}(n)_0\,.$$

Esercizio 30.1. Dimostrare che: $\forall x,y\,(x,y\le\boldsymbol{J}(x,y))$ e $x\le x'\wedge y\le y'\Rightarrow\boldsymbol{J}(x,y)\le\boldsymbol{J}(x',y')$.

Lemma 30.2 (Gödel)**.** *C'è una funzione primitiva ricorsiva*

$$\boldsymbol{\beta}\colon\mathbb{N}^2\to\mathbb{N}$$

tale che

- *per ogni x e i, $\boldsymbol{\beta}(x,i)\le x\dot{-}1$ e*
- *per ogni $n\in\mathbb{N}$ e ogni stringa $\langle x_0,\dots,x_{n-1}\rangle\in\mathbb{N}^n$ c'è un x tale che $\boldsymbol{\beta}(x,i)=x_i$, per $i<n$.*

Inoltre c'è una funzione primitiva ricorsiva $\boldsymbol{\nu}\colon\mathbb{N}\to\mathbb{N}$ crescente tale che per ogni $x_0,\dots,x_{n-1}$ il minimo x tale che $\forall i<n\ \boldsymbol{\beta}(x,i)=x_i$ è minore o uguale a $\boldsymbol{\nu}(\max(n-1,x_0,\dots,x_{n-1}))$.

In altre parole: ogni sequenza finita può essere codificata da un numero naturale tramite la funzione $\boldsymbol{\beta}$ e la dimensione di tale codice è limitata superiormente da $\boldsymbol{\nu}$.

La dimostrazione del Lemma è rimandata alla sezione 30.A.

Definizione 30.3. La **codifica** di una stringa finita di numeri naturali $\bar{x} = (x_0, \ldots, x_{n-1}) \in \mathbb{N}^{<\omega}$ è il più piccolo numero naturale m tale che $\boldsymbol{\beta}(m, 0) = n$ e per ogni $i < n$

$$\boldsymbol{\beta}(m, i+1) = x_i \,.$$

Tale numero m lo si indica con $\langle\langle \bar{x} \rangle\rangle = \langle\langle x_0, \ldots, x_{n-1} \rangle\rangle$.

Osserviamo che $\langle\langle \emptyset \rangle\rangle = 0$, cioè la codifica della sequenza vuota è 0. Fissato $n > 0$, la funzione codifica ristretta a $\mathbb{N}^n$ è primitiva ricorsiva, dato che

$$\langle\langle x_0, \ldots, x_{n-1} \rangle\rangle = \boldsymbol{\mu} m \leq \boldsymbol{\nu}(\max(n-1, x_1, \ldots, x_n)) \big(\boldsymbol{\beta}(m, 0) = n \\ \wedge\ \boldsymbol{\beta}(m, 1) = x_0 \wedge \cdots \wedge \boldsymbol{\beta}(m, n) = x_{n-1}\big)$$

e $\boldsymbol{\beta} \in \mathbf{PRec}$. L'immagine della funzione codifica è l'**insieme dei numeri-sequenza**

$$\mathrm{Seq} = \{\, k \in \mathbb{N} \mid \exists \bar{x} \in \mathbb{N}^{<\omega}\ k = \langle\langle \bar{x} \rangle\rangle \,\} \,.$$

La **funzione lunghezza** $\boldsymbol{\ell}\colon \mathbb{N} \to \mathbb{N}$ è definita da

$$\boldsymbol{\ell}(x) = \boldsymbol{\beta}(x, 0)$$

La **funzione decodifica** $\boldsymbol{d}\colon \mathbb{N}^2 \to \mathbb{N}$ è definita da

$$\boldsymbol{d}(k, i) = \boldsymbol{\beta}(x, i+1) \,.$$

Quindi se $k = \langle\langle x_0, \ldots, x_{n-1} \rangle\rangle$ allora $n = \boldsymbol{\ell}(k)$ e $\boldsymbol{d}(k, i) = x_i$, per $i < n$. Per semplicità notazionale scriveremo $(\!(k)\!)_i$ al posto di $\boldsymbol{d}(k, i)$.

Dalla formula

$$(123) \quad m \in \mathrm{Seq} \quad \Leftrightarrow \quad m = 0 \vee \Big[\boldsymbol{\beta}(m, 0) > 0 \wedge \\ \forall m' < m \,\big(\boldsymbol{\beta}(m, 0) = \boldsymbol{\beta}(m', 0) \Rightarrow \exists i < \boldsymbol{\beta}(m, 0)\, \big(\boldsymbol{\beta}(m, i) \neq \boldsymbol{\beta}(m', i)\big)\big)\Big]$$

vediamo che Seq è primitivo ricorsivo.

La funzione "segmento iniziale" è definita da

$$\mathrm{IS}(\langle\langle x_0, \ldots, x_n \rangle\rangle, i) = \langle\langle x_0, \ldots, x_{i-1} \rangle\rangle$$

per $i < n$. La sua formula esplicita è

$$\mathrm{IS}(x, i) = \boldsymbol{\mu} y \leq x\, (\boldsymbol{\ell}(y) = i \ \wedge\ \forall j < i\, (\boldsymbol{\beta}(y, j) = \boldsymbol{\beta}(x, j))) \,.$$

La funzione "concatenazione" è definita da

$$\mathrm{Conc}(\langle\langle x_0, \ldots, x_n \rangle\rangle, \langle\langle y_0, \ldots, y_m \rangle\rangle) = \langle\langle x_0, \ldots, x_n, y_0, \ldots, y_m \rangle\rangle \,.$$

La sua formula esplicita è

$$\begin{aligned}\mathrm{Conc}(x,y) = \boldsymbol{\mu} z \leq \boldsymbol{\nu}(\max(x,y))\Big[&\boldsymbol{\ell}(z) = \boldsymbol{\ell}(x) + \boldsymbol{\ell}(y) \wedge \\ &\forall 1 \leq i \leq \boldsymbol{\ell}(x)\,(\boldsymbol{\beta}(z,i) = \boldsymbol{\beta}(x,i)) \wedge \\ &\forall 1 \leq i \leq \boldsymbol{\ell}(y)\,(\beta(y,i) = \boldsymbol{\beta}(z, \boldsymbol{\ell}(x) + i))\Big].\end{aligned}$$

Tanto IS quanto Conc sono primitive ricorsive. Per comodità tipografica scriveremo $n * m$ invece di $\mathrm{Conc}(n,m)$. Chiaramente la funzione $*$ è associativa su Seq, cioè se $n, m, k \in \mathrm{Seq}$

$$(n * m) * k = n * (m * k)$$

è il numero della sequenza ottenuta concatenando le sequenze codificate da n, m e k.

Teorema 30.4. *Siano g e h funzioni primitive ricorsive k-aria e $k+1$-aria rispettivamente. Allora c'è un'unica $f\colon \mathbb{N}^{k+1} \to \mathbb{N}$ tale che*

$$\begin{aligned}f(\bar{x}, 0) &= g(\bar{x}) \\ f(\bar{x}, n+1) &= h(\bar{x}, \langle\!\langle f(\bar{x},0), \dots, f(\bar{x},n)\rangle\!\rangle)\,.\end{aligned}$$

Inoltre tale f è primitiva ricorsiva.

Dimostrazione. Sia $\mathcal{G}$ l'insieme delle funzioni parziali finite da $\mathbb{N}^{k+1}$ a valori in $\mathbb{N}$ e sia $H\colon \mathbb{N}^k \times \mathcal{G} \to \mathbb{N}$ la funzione

$$H(\bar{x}, p) = \begin{cases} \langle\!\langle p(\bar{x},0), \dots, p(\bar{x},n)\rangle\!\rangle & \text{se } n+1 = \{\, i \in \mathbb{N} \mid (\bar{x}, i) \in \mathrm{dom}(p)\,\}, \\ g(\bar{x}) & \text{altrimenti.}\end{cases}$$

L'esistenza e unicità di f discendono dal teorema di ricorsione, dato che $f(\bar{x}, n) = H(\bar{x}, f \restriction \{\, (\bar{x}, i) \mid i < n\,\})$.

Resta quindi da provare che f è primitiva ricorsiva. La funzione $\tilde{h}\colon \mathbb{N}^{k+2} \to \mathbb{N}$

$$\tilde{h}(\bar{x}, n, m) = m * \langle\!\langle h(\bar{x}, m)\rangle\!\rangle$$

è primitiva ricorsiva e quindi lo è pure la funzione $F\colon \mathbb{N}^{k+1} \to \mathbb{N}$ definita da

$$\begin{aligned}F(\bar{x}, 0) &= \langle\!\langle g(\bar{x})\rangle\!\rangle \\ F(\bar{x}, n+1) &= \tilde{h}(\bar{x}, n, F(\bar{x}, n))\,.\end{aligned}$$

Ma $F(\bar{x}, n) = \langle\!\langle f(\bar{x},0), \dots, f(\bar{x},n)\rangle\!\rangle$ e quindi

$$f(\bar{x}, n) = \boldsymbol{d}\big(F(\bar{x}, n), \boldsymbol{\ell}(F(\bar{x}, n)) \dot{-} 1\big)\,.$$

Segue che f è primitiva ricorsiva. □

30.A. Costruzione della funzione $\boldsymbol{\beta}$. Osserviamo che due numeri $a, b > 1$ sono relativamente primi se e solo se

$$\forall c\,(b \mid ac \Rightarrow b \mid c)\,.$$

Infatti, se $ac = bd$ per qualche $d \geq 1$ e a e b sono relativamente primi, allora ogni potenza di primo p^k che divide b deve dividere c e quindi $b \mid c$. Viceversa se a e b non fossero relativamente primi, potrei trovare uno c tale che ac è il minimo comune multiplo di a e b, ma $b \nmid c$.

Fissiamo $k, z > 0$ e $j, x \geq 0$ e supponiamo che $k \mid z$ e che

$$1 + jz \mid x\,(1 + (j + k)z)\,.$$

Dato che $x\,(1 + (j + k)\,z) = x\,(1 + jz) + xkz$, si ha che $1 + jz \mid xkz$ e dato che z e $1 + jz$ sono relativamente primi, si ha che $1 + jz \mid xk$. Dato che $k \mid z$, si ha $1 + jz \mid xz$ e nuovamente per il fatto che z e $1 + jz$ sono relativamente primi, $1 + jz \mid x$. Abbiamo quindi dimostrato che

$$\forall x\,(1 + jz \mid x\,(1 + (j + k)\,z) \Rightarrow 1 + jz \mid x)$$

cioè che $1 + jz$ e $1 + (j + k)\,z$ sono relativamente primi, ovvero prendendo $i = j + k$

(124) $\qquad j < i \Rightarrow 1 + jz$ e $1 + (j + k)\,z$ sono relativamente primi.

Definiamo $\boldsymbol{\beta}\colon \mathbb{N}^2 \to \mathbb{N}$, come

$$\boldsymbol{\beta}(x, i) = \boldsymbol{\mu} n \leq x \dot{-} 1\,[(1 + (\boldsymbol{J}(n, i) + 1)(x)_1) \mid (x)_0]$$

Dobbiamo verificare che per ogni stringa $\langle x_0, x_1, \ldots, x_{n-1}\rangle$ di naturali c'è un x tale che $\forall i < n\ \boldsymbol{\beta}(x, i) = x_i$. Sia

$$c = \max\{\boldsymbol{J}(x_0, 0), \ldots, \boldsymbol{J}(x_{n-1}, n - 1)\} + 1$$

e sia z un numero divisibile per ogni $c' < c$, per esempio $z = c!$. Sia $y = \prod_{i<n} 1 + \boldsymbol{J}(x_i, i)z$. Dato che i numeri della forma $1 + jz$, con $j < c$, sono relativamente primi tra loro, si ha

(125) $\qquad 1 + jz \mid y \Leftrightarrow \exists i < n\,(j = \boldsymbol{J}(x_i, i))\,.$

Sia $x = \boldsymbol{J}(y, z)$. Per costruzione $x_i < 1 + \boldsymbol{J}(x_i, i)z \leq y \leq x$, da cui $x_i \leq x \dot{-} 1$. Sia $\boldsymbol{\nu}(m) = \boldsymbol{J}(g(m, f(m)), f(m))$, dove

$$f(m) = (\boldsymbol{J}(m, m) + 1)!$$
$$g(m, k) = (1 + \boldsymbol{J}(m, m)k)^m$$

Esercizio 30.5. Verificare che $\boldsymbol{\nu}$ è primitiva ricorsiva e che il numero x ottenuto a partire da $x_0, \ldots, x_{n-1}$ e $n - 1$ è limitato superiormente da $\boldsymbol{\nu}(\max(n - 1, x_0, \ldots, x_n))$.

Verifichiamo ora che $\boldsymbol{\beta}(x,i) = x_i$, per $i = 0, \dots, n-1$. Dato che $(x)_0 = y$ e $(x)_1 = z$ otteniamo

$$\boldsymbol{\beta}(x,i) = \boldsymbol{\mu} n \leq x \dot{-} 1\,[(1 + (\boldsymbol{J}(n,i) + 1)x) \mid y]\,.$$

Sappiamo che $(1 + (\boldsymbol{J}(x_i,i) + 1)x) \mid y$, quindi è sufficiente verificare che se $n < x_i$ allora $(1 + (\boldsymbol{J}(n,i) + 1)x) \nmid y$. Ma questo è una conseguenza immediata di (125).

30.B. Ricorsione primitiva su altri domini. Se $X \subseteq \mathbb{N}^k$ è primitivo ricorsivo, una funzione $f\colon X \to \mathbb{N}$ si dirà primitiva ricorsiva se la funzione $\hat{f}\colon \mathbb{N}^k \to \mathbb{N}$

$$\hat{f}(\bar{x}) = \begin{cases} f(\bar{x}) & \text{se } \bar{x} \in X, \\ 0 & \text{altrimenti,} \end{cases}$$

è primitiva ricorsiva.

Se $\varphi\colon \mathbb{N} \to D$ è una bijezione, diremo che $f\colon D^k \to D$ è primitiva ricorsiva relativamente a φ se la funzione $g = \varphi^{-1} \circ f \circ \bar{\varphi}\colon \mathbb{N}^k \to \mathbb{N}$

$$\begin{array}{ccc} \mathbb{N}^k & \xrightarrow{\;g\;} & \mathbb{N} \\ {\scriptstyle\bar{\varphi}}\downarrow & & \downarrow{\scriptstyle\varphi} \\ D^k & \xrightarrow{\;f\;} & D \end{array}$$

è primitiva ricorsiva, dove $\bar{\varphi}(x_1, \dots, x_n) = (\varphi(x_1), \dots, \varphi(x_n))$. Similmente

- una $f\colon \mathbb{N}^k \to D$ si dirà primitiva ricorsiva relativamente a φ se $\varphi \circ f\colon \mathbb{N}^k \to \mathbb{N}$ è primitiva ricorsiva e
- un insieme $X \subseteq D^k$ si dirà primitivo ricorsivo relativamente a φ se la sua funzione caratteristica $\boldsymbol{\chi}_X^{D^k}\colon D^k \to \mathbb{N}$ è primitiva ricorsiva.

Vediamo qualche esempio.

30.B.1. Consideriamo il caso in cui $D = \mathbb{N}^2$ e $\varphi = \boldsymbol{J}^{-1}$ dove $\boldsymbol{J}$ è come in (120). Poiché $\boldsymbol{J}$ e le sue inverse $(\cdot)_0$ e $(\cdot)_1$ sono primitive ricorsive, una $f\colon D \to \mathbb{N}$ è primitiva ricorsiva relativamente a φ se e solo se $f \in \mathbf{PRec}$.

Componendo più volte la funzione $\boldsymbol{J}$ possiamo definire una bijezione primitiva ricorsiva $\varphi\colon \mathbb{N} \to \mathbb{N}^k = D$ la cui inversa è anch'essa primitiva ricorsiva e dimostrare che una $f\colon D \to \mathbb{N}$ è primitiva ricorsiva relativamente a φ se e solo se $f \in \mathbf{PRec}$.

30.B.2. Generalizzando un poco l'esempio precedente e considerando la bijezione $\langle\!\langle\cdot\rangle\!\rangle\colon \mathbb{N}^{<\omega} \to \mathrm{Seq}$, diremo che una funzione $(\mathbb{N}^{<\omega})^k \to \mathbb{N}^{<\omega}$ è primitiva ricorsiva se e solo se la sua copia su Seq è primitiva ricorsiva. In particolare le operazioni di

concatenazione: $\mathbb{N}^{<\omega} \times \mathbb{N}^{<\omega} \to \mathbb{N}^{<\omega}$, $(s,t) \mapsto s^\frown t$,

segmento iniziale: $\mathbb{N}^{<\omega} \times \mathbb{N} \to \mathbb{N}^{<\omega}$, $(s, i) \mapsto s \restriction i$,
lunghezza: $\mathbb{N}^{<\omega} \to \mathbb{N}$, $s \mapsto \mathrm{lh}(s)$,

sono primitive ricorsive, dato che le corrispettive funzioni su Seq ($*$, IS e $\boldsymbol{\ell}$) sono primitive ricorsive.

30.B.3. Sia $\varphi\colon \mathbb{N} \to \mathbb{Z}$ data da

$$\begin{aligned} \varphi(2n) &= n \\ \varphi(2n+1) &= -n\,. \end{aligned} \tag{126}$$

Allora le seguenti funzioni e insiemi sono primitivi ricorsivi su $\mathbb{Z}$ relativamente a φ:

- le funzioni costanti e le funzioni di proiezione,
- le operazioni di somma, differenza, prodotto,
- tutti i sotto-insiemi $\mathbb{N}^k$ che sono primitivi ricorsivi nel senso solito.

Lemma 30.6. *Sia $S \subseteq \mathbb{N}$ primitivo ricorsivo e sia $a\colon S \to \mathbb{N}$ primitiva ricorsiva. Allora l'insieme* $\mathrm{Words}(S, a) \subseteq \mathbb{N}^{<\omega}$ *è primitivo ricorsivo, cioè*

$$\{\, \langle\!\langle w \rangle\!\rangle \mid w \in \mathrm{Words}(S, a) \,\}$$

è un sotto-insieme primitivo ricorsivo di $\mathbb{N}$.

Dimostrazione. Poiché Seq è un insieme primitivo ricorsivo, è sufficiente verificare che la funzione caratteristica di $\{\, \langle\!\langle w \rangle\!\rangle \mid w \in \mathrm{Words}(S, a) \,\}$ ristretta a Seq è primitiva ricorsiva. Si verifica facilmente che la funzione $f\colon \mathrm{Seq} \to \mathbb{Z}$

$$f(n) = \sum_{i < \boldsymbol{\ell}(n)} a(n) - 1$$

è primitiva ricorsiva e, per la Proposizione 7.6,

$$n \in \mathrm{Words}(S, a) \Leftrightarrow f(n) = -1 \ \wedge\ \forall i < \boldsymbol{\ell}(n)\ f(\mathrm{IS}(n, i)) \geq 0\,.$$

Quindi $\mathrm{Words}(S, a)$ è primitivo ricorsivo. □

30.C. Codifica delle funzioni primitive ricorsive. Ogni funzione primitiva ricorsiva è costruita a partire dalla funzioni di base mediante composizione e ricorsione primitiva ed è descritta da un albero di programma. Vogliamo associare a ciascun albero di programma un numero-sequenza che codifica l'albero e quindi la funzione che tale albero descrive. Associamo alle funzioni c^n_k, proj^n_k e $\mathbf{S}$ i numeri naturali

$$\mathtt{c}^{\mathtt{n}}_{\mathtt{k}} = \boldsymbol{J}(0, \boldsymbol{J}(n, k)), \quad \mathtt{proj}^{\mathtt{n}}_{\mathtt{k}} = \boldsymbol{J}(1, \boldsymbol{J}(n, k)), \quad \mathtt{S} = \boldsymbol{J}(2, 0)$$

e associamo alle operazioni composizione (113) e di ricorsione primitiva (115) i numeri

$$\mathtt{C} = \boldsymbol{J}(2, 1), \quad \mathtt{PR} = \boldsymbol{J}(2, 2)\,.$$

Osserviamo che i numeri $\mathtt{c}^{\mathtt{n}}_{\mathtt{k}}$, $\mathtt{proj}^{\mathtt{n}}_{\mathtt{k}}$, $\mathtt{S}$, $\mathtt{C}$ e $\mathtt{PR}$ sono tutti distinti. Possiamo ora associare ad ogni albero di programma T un numero-sequenza $\ulcorner T \urcorner$:

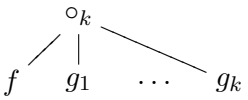
- se l'albero T ha altezza 0, cioè della forma

  $$\mathbf{S} \qquad \mathrm{c}^n_k \qquad \mathrm{proj}^n_k$$

  allora $\ulcorner T \urcorner$ è, rispettivamente,

  $$\langle\!\langle \mathtt{S} \rangle\!\rangle \qquad \langle\!\langle \mathtt{c}^{\mathtt{n}}_{\mathtt{k}} \rangle\!\rangle \qquad \langle\!\langle \mathtt{proj}^{\mathtt{n}}_{\mathtt{k}} \rangle\!\rangle$$

- se l'albero T è della forma

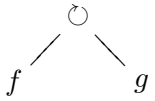
  

  associamo a T il numero sequenza

  $$\ulcorner T \urcorner = \langle\!\langle \mathtt{C} \rangle\!\rangle * \langle\!\langle f \rangle\!\rangle * \langle\!\langle g_1 \rangle\!\rangle * \cdots * \langle\!\langle g_n \rangle\!\rangle$$

  dove $\langle\!\langle f \rangle\!\rangle, \langle\!\langle g_1 \rangle\!\rangle, \ldots, \langle\!\langle g_n \rangle\!\rangle$ sono i numeri sequenza associati a (gli alberi di programma di) $f, g_1, \ldots, g_n$,

- se l'albero T è della forma

  associamo a T il numero sequenza

  $$\ulcorner T \urcorner = \langle\!\langle \mathtt{PR} \rangle\!\rangle * \langle\!\langle f \rangle\!\rangle * \langle\!\langle g \rangle\!\rangle$$

  dove $\langle\!\langle f \rangle\!\rangle, \langle\!\langle g \rangle\!\rangle$ sono i numeri sequenza associati a (gli alberi di programma di) f e g.

Osservazione 30.7. Data una $f \in \mathbf{PRec}$ scriveremo $\ulcorner f \urcorner$ per il numero-sequenza associato all'albero di programma di f. Questa notazione è ambigua, dato che ad ogni f primitiva ricorsiva possiamo associare infiniti alberi di programma (Osservazione 29.4), quindi verrà usata solo quando l'albero di programma in questione è chiaro dal contesto.

Vediamo qualche esempio:

- La funzione $x_1 + x_2$ (Esempio 29.B.2) ha come codice

  $$\langle\!\langle \mathtt{PR}, \mathtt{proj}^{\mathtt{1}}_{\mathtt{1}}, \mathtt{C}, \mathtt{S}, \mathtt{proj}^{\mathtt{3}}_{\mathtt{3}} \rangle\!\rangle.$$

- La funzione $x_1 \dot{-} 1$ (Esempio 29.B.3) ha come codice

  $$\langle\!\langle \mathtt{PR}, \mathtt{c}^{\mathtt{0}}_{\mathtt{0}}, \mathtt{proj}^{\mathtt{2}}_{\mathtt{1}} \rangle\!\rangle.$$

- La funzione $x_1 \dot{-} x_2$ (Esempio 29.B.3) ha come codice

  $$\langle\!\langle \mathtt{PR}, \mathtt{proj}^{\mathtt{1}}_{\mathtt{1}}, \mathtt{C}, \mathtt{PR}, \mathtt{c}^{\mathtt{0}}_{\mathtt{0}}, \mathtt{proj}^{\mathtt{2}}_{\mathtt{1}}, \mathtt{proj}^{\mathtt{3}}_{\mathtt{3}} \rangle\!\rangle.$$

$$\ulcorner\mathbf{PRec}\urcorner = \{\, \ulcorner T\urcorner \mid T \in \mathcal{T}_{\mathbf{PRec}} \,\}$$

è l'insieme dei codici per funzioni primitive ricorsive. La funzione

$$\ulcorner\mathbf{PRec}\urcorner \to \mathbf{PRec}, \qquad \ulcorner T\urcorner \mapsto f_T\,,$$

è una suriezione, dato che ogni funzione primitiva ricorsiva ammette un albero (infatti: infiniti alberi) di programma. Poiché $\ulcorner\mathbf{PRec}\urcorner \subseteq \omega$, segue che $|\mathbf{PRec}| = \aleph_0$.

Teorema 30.8. *L'insieme* $\ulcorner\mathbf{PRec}\urcorner \subseteq \mathrm{Seq}$ *è primitivo ricorsivo e la funzione* $\mathrm{ar}\colon \ulcorner\mathbf{PRec}\urcorner \to \mathbb{N}$ *è primitiva ricorsiva.*

30.D. Una funzione calcolabile ma non primitiva ricorsiva. Come abbiamo visto nell'Osservazione 29.3, ogni $f \in \mathbf{PRec}$ è calcolabile. Esibiremo ora una funzione $F\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ calcolabile, ma non primitiva ricorsiva.

Definizione 30.9. Sia $\mathcal{F}$ un insieme di funzioni finitarie su $\mathbb{N}$. Una funzione $F\colon \mathbb{N}^2 \to \mathbb{N}$ è universale per $\mathcal{F}$ se F parametrizza tutte le funzioni 1-arie di $\mathcal{F}$, vale a dire

$$\forall f \in \mathcal{F} \cap \mathbb{N}^{\mathbb{N}}\, \exists n \in \mathbb{N}\, \forall m \in \mathbb{N}\, (F(n,m) = f(m))\,.$$

Teorema 30.10. *Sia* $\mathcal{F}$ *un insieme di funzioni finitarie su* $\mathbb{N}$ *contenente la funzione identica* $\mathrm{id} \restriction \mathbb{N} = \mathrm{proj}^1_1$*, la funzione successore* $\mathbf{S}$ *e chiuso per composizione. Supponiamo che* $F\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *sia universale per* $\mathcal{F} \cap \mathbb{N}^{\mathbb{N}}$*. Allora* $F \notin \mathcal{F}$*.*

Dimostrazione. Supponiamo, per assurdo, che $F \in \mathcal{F}$ sia universale per $\mathcal{F} \cap \mathbb{N}^{\mathbb{N}}$ e sia $f(n) = F(n,n) + 1$, cioè

$$f(n) = \mathbf{S}\big(F(\mathrm{proj}^1_1(n), \mathrm{proj}^1_1(n))\big)\,.$$

Poiché $f \in \mathcal{F}$ c'è un $\bar n \in \mathbb{N}$ tale che $\forall x \in \mathbb{N}\, f(x) = F(\bar n, x)$. Quindi

$$F(\bar n, \bar n) = f(\bar n) = F(\bar n, \bar n) + 1\,,$$

una contraddizione. □

Corollario 30.11. *Non c'è nessuna funzione primitiva ricorsiva* 2*-aria universale per* $\mathbf{PRec}$*.*

Argomenteremo ora che c'è una $F\colon \mathbb{N}^2 \to \mathbb{N}$ universale per $\mathcal{F}$ che è calcolabile: per il teorema precedente questa funzione non può essere primitiva ricorsiva e quindi avremo esibito una funzione calcolabile ma non primitiva ricorsiva. Dati n ed m, verifichiamo innanzi tutto se $n \in \ulcorner\mathbf{PRec}\urcorner$: dato che $\ulcorner\mathbf{PRec}\urcorner$ è primitivo ricorsivo per (123), determinare se o meno $n \in \ulcorner\mathbf{PRec}\urcorner$ è effettivamente calcolabile. Se $n \notin \ulcorner\mathbf{PRec}\urcorner$, allora $F(n,m) = 0$, qualsiasi si m. Supponiamo invece che $n \in \ulcorner\mathbf{PRec}\urcorner$: a partire da n ci possiamo

ricostruire la funzione primitiva ricorsiva f di cui n è il codice e da questa calcoliamo $f(m)$. Questo è il valore di $F(n, m)$. Quindi F è calcolabile ed è universale per le funzioni primitive ricorsive 1-arie.

31. Funzioni ricorsive

Abbiamo visto nella sezione precedente un esempio di funzione calcolabile ma non primitiva ricorsiva.

31.A. Funzioni parziali ricorsive. Una funzione parziale finitaria su $\mathbb{N}$ è una f tale che $\mathrm{dom}(f) \subseteq \mathbb{N}^n$ e $\mathrm{ran}(f) \subseteq \mathbb{N}$. Se $f \neq \emptyset$, l'unico n tale che $\mathrm{dom}(f) \subseteq \mathbb{N}^n$ si dice arietà di f e si indica con $\mathrm{ar}(f)$; se $f = \emptyset$ poniamo $\mathrm{ar}(f) = 0$. Se $\bar{x} \in \mathbb{N}^n$ e $\mathrm{ar}(f) = n$, diremo che f **converge** in $\bar{x}$, in simboli $f(\bar{x})\downarrow$, se e solo $\bar{x} \in \mathrm{dom}(f)$; altrimenti diremo che f **diverge** in $\bar{x}$, in simboli $f(\bar{x})\uparrow$. Quando scriviamo "$f(\bar{x}) = y$" intendiamo dire che "$f(\bar{x})\downarrow$ e $f(\bar{x}) = y$".

Se f è parziale k-aria e $g_1, \dots g_k$ sono parziali n-arie su $\mathbb{N}$, la composizione di f con $g_1, \dots g_k$ è la funzione parziale n-aria

$$h(\bar{x}) = f(g_1(\bar{x}), \dots, g_k(\bar{x}))$$

dove si intende che

$$h(\bar{x})\downarrow \;\Leftrightarrow\; (g_1(\bar{x})\downarrow \wedge \dots \wedge g_k(\bar{x})\downarrow \wedge f(g_1(\bar{x}), \dots, g_k(\bar{x}))\downarrow)\,.$$

L'operatore $\boldsymbol{\mu}$ di **minimalizzazione** per funzioni parziali è così definito: se g è parziale $n+1$-aria su $\mathbb{N}$ allora $\boldsymbol{\mu} y\,[g(\bar{x}, y) = 0]$ è la funzione parziale n-aria f su $\mathbb{N}$ definita da

(127)
$$f(\bar{x}) = \begin{cases} \min\{\, y \mid g(\bar{x}, y) = 0 \wedge \forall z < y\,(g(\bar{x}, z)\downarrow)\,\} & \text{se questo insieme è } \neq \emptyset, \\ \uparrow & \text{altrimenti.} \end{cases}$$

L'operatore $\boldsymbol{\mu}$ può essere esteso agli insiemi: se $A \subseteq \mathbb{N}^{n+1}$ allora $\boldsymbol{\mu} y\, A(\bar{x}, y)$ è la funzione $\mathbb{N}^n \to \mathbb{N}$

$$\boldsymbol{\mu} y\,[\boldsymbol{\chi}_{\neg A}(\bar{x}, y) = 0] = \boldsymbol{\mu} y\,[\boldsymbol{\chi}_A(\bar{x}, y) = 1]$$

e poiché $\boldsymbol{\chi}_A$ è una funzione totale,

$$\boldsymbol{\mu} y\, A(\bar{x}, y) = \text{il più piccolo } y \text{ tale che } (\bar{x}, y) \in A\,.$$

L'insieme **Rec** delle **funzioni ricorsive** è il più piccolo insieme di funzioni parziali finitarie su $\mathbb{N}$ contenente le funzioni primitive ricorsive, chiuso per composizione e per minimalizzazione.

Il seguente risultato (di cui non diamo la dimostrazione) è uno dei pilastri della teoria della ricorsività. Ricordiamo che $\boldsymbol{J}\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ è una bijezione con funzioni inverse $n \mapsto (n)_0$ e $n \mapsto (n)_1$ definite in (122) e che tanto $\boldsymbol{J}$ quanto $(\cdot)_0$ e $(\cdot)_0$ sono primitive ricorsive.

Teorema 31.1 (Teorema di forma normale di Kleene)**.** *Per ogni $n > 0$ c'è un insieme primitivo ricorsivo $\mathrm{T}_n \subseteq \mathbb{N}^{n+2}$ tale che per ogni funzione f parziale n-aria su $\mathbb{N}$*

$$f \in \mathbf{Rec} \Leftrightarrow \exists e \in \mathbb{N}\, \forall \bar{x} \in \mathbb{N}^n\, (f(\bar{x}) = (\boldsymbol{\mu} y\, \mathrm{T}_n(e, \bar{x}, y))_0)\,.$$

In altre parole, la funzione

$$\Phi(e, \bar{x}) = (\boldsymbol{\mu} y\, \mathrm{T}_n(e, \bar{x}, y))_0 \tag{128}$$

è parziale ricorsiva $(n+1)$-aria e parametrizza tutte le funzioni parziali ricorsive n-arie, cioè

$$\bar{x} \mapsto \Phi(e, \bar{x})$$

è ricorsiva parziale n-aria e se $f \in \mathbf{Rec}$ è n-aria, allora esiste almeno un $e \in \mathbb{N}$ tale che

$$\forall \bar{x}\ f(\bar{x}) = \Phi(e, \bar{x})\,.$$

La funzione

$$\bar{x} \mapsto \Phi(e, \bar{x}) = (\boldsymbol{\mu} y\, \mathrm{T}_n(e, \bar{x}, y))_0$$

è denotata generalmente con $\boldsymbol{\varphi}_e^{(n)}$ o semplicemente $\boldsymbol{\varphi}_e$, quando n è chiaro dal contesto.

Per il Teorema 30.10, non tutte le funzioni parziali ricorsive possono essere estesa ad una funzione totale ricorsiva.

31.B. Insiemi ricorsivamente enumerabili. Un insieme $A \subseteq \mathbb{N}^n$ si dice **ricorsivo** se la sua funzione caratteristica è in **Rec**. Un insieme $A \subseteq \mathbb{N}^n$ si dice **ricorsivamente enumerabile** se $A = \mathrm{dom}(f)$, per qualche $f \in \mathbf{Rec}$.

Proposizione 31.2. (a) *Un insieme $A \subseteq \mathbb{N}^n$ è ricorsivo se e solo se $\neg A$ è ricorsivo.*

(b) *Ogni insieme ricorsivo è ricorsivamente enumerabile.*

(c) *Se $A, B \subseteq \mathbb{N}^n$ sono ricorsivamente enumerabili allora anche $A \cap B$ e $A \cup B$ lo sono.*

Dimostrazione. (a) $\boldsymbol{\chi}_{\neg A} = 1 - \boldsymbol{\chi}_A$.

(b) Sia $A \subseteq \mathbb{N}^n$ ricorsivo. La funzione $f(x) = \boldsymbol{\mu} y\, [y + 1 = x]$ è ricorsiva e $\mathrm{dom}(f) = \mathbb{N} \setminus \{0\}$. Allora $f \circ \boldsymbol{\chi}_A \in \mathbf{Rec}$ ha per dominio A.

(c) Supponiamo $A = \mathrm{dom}(f)$ e $B = \mathrm{dom}(g)$. Allora $A \cap B = \mathrm{dom}(f+g)$. Per il Teorema 31.1 esistono $a, b \in \mathbb{N}$ tali che

$$\begin{aligned} f(\bar{x}) &= (\boldsymbol{\mu} y\, \mathrm{T}_n(a, \bar{x}, y))_0 \\ g(\bar{x}) &= (\boldsymbol{\mu} y\, \mathrm{T}_n(b, \bar{x}, y))_0 \end{aligned} \tag{129}$$

e quindi $h(\bar{x}) = \boldsymbol{\mu} y\, [\mathrm{T}_n(a, \bar{x}, y) \vee \mathrm{T}_n(b, \bar{x}, y)]$ è ricorsiva e ha per dominio $A \cup B$. □

Teorema 31.3. *$A \subseteq \mathbb{N}^n$ è ricorsivo se e solo se A e $\neg A$ sono ricorsivamente enumerabili.*

Dimostrazione. Supponiamo $A = \mathrm{dom}(f)$ e $\neg A = \mathrm{dom}(g)$ con f e g come in (129) e sia

$$h(\bar{x}) = \boldsymbol{\mu} y \Big[\exists z < y\big((y = 2z \wedge \mathrm{T}_n(a, \bar{x}, z)) \vee (y = 2z + 1 \wedge \mathrm{T}_n(b, \bar{x}, z))\big)\Big].$$

Allora $\boldsymbol{\chi}_A = \boldsymbol{\chi}_P \circ h$ dove $P = \{\, 2n \mid n \in \mathbb{N} \,\}$.

L'implicazione inversa segue immediatamente da (a) e (b) della Proposizione 31.2 □

La proiezione di $A \subseteq \mathbb{N}^{n+1}$ è l'insieme $B = \{\, \bar{x} \in \mathbb{N}^n \mid \exists y\, (\bar{x}, y) \in A \,\}$.

Teorema 31.4. *La proiezione di un insieme ricorsivamente enumerabile è ricorsivamente enumerabile.*

Dimostrazione. Sia $A = \mathrm{dom}(f) \subseteq \mathbb{N}^{n+1}$ con $f \in \mathbf{Rec}$ e sia $B \subseteq \mathbb{N}^n$ la sua proiezione. Per il Teorema 31.1 possiamo supporre che

$$f(\bar{x}, y) = \big(\boldsymbol{\mu} z\, \mathrm{T}_{n+1}(a, y, \bar{x}, z)\big)_0$$

per qualche $a \in \mathbb{N}$. Allora

$$g(\bar{x}) = \boldsymbol{\mu} w\, \mathrm{T}_{n+1}(a, (w)_0, \bar{x}, (w)_1)$$

è ricorsiva n-aria e $\mathrm{dom}(g) = B$. □

Esercizio 31.5. Dimostrare che se $B \subseteq \mathbb{N}^{n+1}$ è ricorsivamente enumerabile allora ogni sua sezione

$$B^{(y)} = \{\, \bar{x} \in \mathbb{N}^n \mid (y, \bar{x}) \in B \,\}$$

è ricorsivamente enumerabile. Dimostrare che per ogni $n > 0$ c'è un insieme ricorsivamente enumerabile $U_n \subseteq \mathbb{N}^{n+1}$ universale per gli insiemi ricorsivamente enumerabili di $\mathbb{N}^n$, cioè tale che

$$\{\, A \subseteq \mathbb{N}^n \mid A \text{ ricorsivamente enumerabile} \,\} = \Big\{\, U_n^{(y)} \mid y \in \mathbb{N} \,\Big\}.$$

Teorema 31.6. *Se $A \subseteq \mathbb{N}^n$ è ricorsivamente enumerabile, allora esiste $B \subseteq \mathbb{N}^{n+1}$ primitivo ricorsivo la cui proiezione è A.*

Dimostrazione. Se $A = \mathrm{dom}(f)$ e f come in (129), allora

$$B = \big\{\, (\bar{x}, y) \in \mathbb{N}^{n+1} \mid \mathrm{T}_n(a, \bar{x}, y) \,\big\}$$

è l'insieme cercato. □

Corollario 31.7. *Se $f \in \mathbf{Rec}$ è n-aria, allora $f \subseteq \mathbb{N}^{n+1}$ è ricorsivamente enumerabile. Se inoltre la funzione è totale, allora f è ricorsivo.*

Dimostrazione. Osserviamo che

$$f = \left\{ (\bar{x}, y) \mid \exists z \left(\mathrm{T}_n(a, \bar{x}, z) \wedge \forall z' < z \neg \mathrm{T}_n(a, \bar{x}, z') \wedge (z)_0 = y \right) \right\},$$

quindi f è ricorsivamente enumerabile. Se f è totale, allora

$$(\bar{x}, y) \notin f \Leftrightarrow \exists z \, (f(\bar{x}) = z \wedge z \neq y),$$

vale a dire il complemento di f è ricorsivamente enumerabile e quindi f è ricorsivo. □

Teorema 31.8. *Sia f una funzione parziale n-aria su $\mathbb{N}$ tale che $f \subseteq \mathbb{N}^{n+1}$ è un insieme ricorsivamente enumerabile. Allora $f \in \mathbf{Rec}$.*

Dimostrazione. Per il Teorema 31.6 f è la proiezione di un $B \subseteq \mathbb{N}^{n+2}$ primitivo ricorsivo, vale a dire $f(\bar{x}) = y \Leftrightarrow \exists z \, ((y, \bar{x}, z) \in B)$. L'insieme $C = \{ (\bar{x}, w) \mid ((w)_0, \bar{x}, (w)_1) \in B \}$ è ricorsivo, quindi $f \in \mathbf{Rec}$ dato che

$$f(\bar{x}) = (\boldsymbol{\mu} w \, C(\bar{x}, w))_0 .$$

□

Corollario 31.9. *Se $f \in \mathbf{Rec}$ allora* $\mathrm{ran}(f)$ *è ricorsivamente enumerabile.*

Dimostrazione. $\mathrm{ran}(f)$ è proiezione del suo grafo. □

Corollario 31.10. *Se $\emptyset \neq A \subseteq \mathbb{N}$ è ricorsivamente enumerabile allora esiste $f \colon \mathbb{N} \to \mathbb{N}$ primitiva ricorsiva tale che $A = \mathrm{ran}(f)$.*

Dimostrazione. Sia $B \subseteq \mathbb{N} \times \mathbb{N}$ ricorsivo primitivo la cui proiezione è A e sia $(h_0, k_0) \in B$. La funzione $f \colon \mathbb{N} \to \mathbb{N}$

$$f(n) = \begin{cases} (n)_0 & \text{se } ((n)_0, (n)_1) \in B, \\ k_0 & \text{altrimenti,} \end{cases}$$

è primitiva ricorsiva e $\mathrm{ran}(f) = A$. □

Teorema 31.11. *Se $f \colon \mathbb{N} \to \mathbb{N}$ è strettamente crescente e ricorsiva, allora* $\mathrm{ran}(f)$ *è ricorsivo.*

Dimostrazione. Poiché f è strettamente crescente, $n \leq f(n)$ per ogni n e quindi

$$n \in \mathrm{ran}(f) \Leftrightarrow \exists k \leq n \, (n = f(k)) .$$

□

Appendice A

Algebra e topologia

In questa appendice richiamiamo alcuni concetti di algebra e di topologia che dovrebbero essere familiari a tutti. Questa è solo una breve lista di definizioni—per una trattazione esauriente di questi argomenti il lettore può consultare [**Hun80, Lan02**] per l'algebra e [**Kur92, CTV76**] per la topologia.

1. Algebra

Un **semigruppo** è un insieme $S \neq \emptyset$ dotato di un'operazione binaria $*$ che è associativa, cioè $(a*b)*c = a*(b*c)$. Se esiste un elemento $e \in S$ tale che $\forall a \in S\,(a*e = e*a = a)$ diremo che è un **monoide**. L'elemento e è unico e si dice elemento neutro. Un **gruppo** è un monoide in cui ogni elemento ha un inverso, cioè $\forall x \in S\,\exists y \in S\,(x*y = y*x = e)$. L'inverso di x è unico e lo si denota con x^{-1}. Un gruppo si dice **commutativo** o **abeliano** se l'operazione è commutativa, cioè $\forall x, y \in S\,(x*y = y*x)$. Spesso l'operazione nei gruppi abeliani la si indica con $+$ e l'elemento neutro con 0. Un **anello** è un insieme $A \neq \emptyset$ dotato di due operazioni $+$ e $\cdot$ e tale che

- $(A, +)$ è un gruppo abeliano in cui 0 denota l'elemento neutro,
- $(A, \cdot)$ è un semigruppo,
- vale la proprietà distributiva della somma rispetto al prodotto:

$$\forall x, y, z \in A\,((x+y)\cdot z = x\cdot z + y\cdot z)$$
$$\forall x, y, z \in A\,(z\cdot(x+y) = z\cdot x + z\cdot y)$$

Se c'è un $e \in A$ tale che $a \cdot e = e \cdot a = a$, per tutti gli $a \in A$, diremo che l'anello è **unitario** e l'elemento e viene denotato con 1. Un anello si dice **commutativo** se l'operazione $\cdot$ è commutativa. Un **dominio di integrità**

è un anello commutativo in cui non ci sono divisori dello 0, cioè $x \cdot y = 0 \Rightarrow x = 0 \vee y = 0$. Un **corpo**[1] è un anello unitario R in cui $0 \neq 1$ e ogni elemento non nullo ha un inverso, cioè

$$\forall x \in R \setminus \{0\}\, \exists y \in R \setminus \{0\}\, (x \cdot y = y \cdot x = 1)\,.$$

Un corpo commutativo si dice **campo**. Il tipico esempio di corpo non commutativo sono i quaternioni $\mathbb{H}$, mentre, per un teorema di Wedderburn, ogni corpo finito è un campo [**Wei95**]. Un campo $\Bbbk$ si dice **algebricamente chiuso** se ogni polinomio non nullo a coefficienti in $\Bbbk$ ha una soluzione in $\Bbbk$.

Uno **spazio vettoriale** su un campo $\Bbbk$ è un gruppo abeliano $\langle V, +, \mathbf{0}\rangle$con una funzione $\Bbbk \times V \to V$, $(r, \mathbf{v}) \mapsto r\mathbf{v}$ detta prodotto per scalare, che soddisfa le seguenti identità, per ogni $r, s \in \Bbbk$ e ogni $\mathbf{u}, \mathbf{v} \in V$:

$$\begin{aligned} r(\mathbf{u} + \mathbf{v}) &= r\mathbf{u} + r\mathbf{v} \\ (r + s)\mathbf{u} &= r\mathbf{u} + s\mathbf{u} \\ (r \cdot s)\mathbf{u} &= r(s\mathbf{u}) \\ 1_{\Bbbk}\mathbf{u} &= \mathbf{u}. \end{aligned}$$

Gli elementi di V si dicono vettori, gli elementi di $\Bbbk$ si dicono scalari.

Un insieme $X \subseteq V$ si dice linearmente dipendente se esistono $\mathbf{v}_1, \ldots, \mathbf{v}_n \in X$ ed esistono scalari $r_1, \ldots, r_n \in \Bbbk$ tali che

- $(r_1, \ldots, r_n) \neq (0_{\Bbbk}, \ldots, 0_{\Bbbk})$ e
- $\sum_{i=1}^{n} r_i \mathbf{v}_i = \mathbf{0}$.

Se X non è linearmente dipendente, diremo che è linearmente indipendente. Un $X \subseteq V$ è un insieme di generatori di V, se ogni $\mathbf{v} \in V$ può essere espresso come combinazione lineare $\mathbf{v} = \sum_{i=1}^{n} r_i \mathbf{v}_i$, per qualche $\mathbf{v}_1, \ldots, \mathbf{v}_n \in X$ e $r_1, \ldots, r_n \in \Bbbk$. Uno spazio vettoriale si dice **finitamente generato** se ha un insieme finito di generatori. Una **base** di uno spazio vettoriale V è un insieme linearmente indipendente di generatori di V. Spesso nel caso degli spazi non finitamente generati si parla di **basi di Hamel**.

2. Topologia

Uno **spazio topologico** è un insieme X dotato di una famiglia $\mathcal{T} \subseteq \mathscr{P}(X)$ tale che

(1) $\emptyset, X \in \mathcal{T}$,

(2) se $A, B \in \mathcal{T}$ allora $A \cap B \in \mathcal{T}$,

(3) se $\{ A_i \mid i \in I \} \subseteq \mathcal{T}$ allora $\bigcup_{i \in I} A_i \in \mathcal{T}$.

[1] In inglese *skew-field* o *division ring*

La famiglia $\mathcal{T}$ si dice **topologia** e i suoi elementi si dicono **aperti**. Quando la topologia $\mathcal{T}$ è chiara dal contesto diremo, con abuso di linguaggio, che X è uno spazio topologico.

Se $x \in V \subseteq X$ e se esiste U aperto tale che $x \in U \subseteq V$ diremo che V è un **intorno** del punto x. Se possiamo prendere $U = V$, cioè se V è aperto, parleremo di intorno aperto. Uno spazio si dice **primo-numerabile** ovvero che soddisfa al **primo assioma di numerabilità** se per ogni $x \in X$ esiste un insieme $\{ V_n \mid n \in \omega \}$ di intorni di x tale che ogni intorno di x contiene uno dei V_n. Un $x \in X$ si dice **punto isolato** Un insieme che sia simultaneamente chiuso ed aperto si dice **chiuso-aperto**. Gli spazi X in cui gli unici insiemi chiusi-aperti sono $\emptyset$ e X si dicono **connessi**. In caso contrario si dicono sconnessi.

Il complementare di un insieme aperto di dice **chiuso**. Se $Y \subseteq X$ l'**interno** di Y e la **chiusura** di Y sono, rispettivamente, il più grande aperto contenuto in Y e il più piccolo chiuso contenente Y, cioè

$$\begin{aligned} \operatorname{Int}(Y) &= \bigcup \{ U \subseteq Y \mid U \in \mathcal{T} \} \\ \operatorname{Cl}(Y) &= \bigcap \{ C \supseteq Y \mid X \setminus C \in \mathcal{T} \} . \end{aligned}$$

Se $Y \subseteq X$, la **topologia indotta** da X su Y è

$$\{ Y \cap U \mid U \in \mathcal{T} \}$$

e diremo che Y, con questa topologia, è un sottospazio di X. Una funzione tra due spazi topologici si dice **continua** se la controimmagine di un aperto è un aperto—la funzione di inclusione tra un sottospazio e lo spazio ambiente è continua.

Un sottoinsieme Y si dice **denso** in X se $\operatorname{Cl}(Y) = X$. Uno spazio che abbia un sotto-insieme denso e numerabile si dice **separabile**.

2.A. Basi. Una **base** per una topologia su X è una $\mathcal{B} \subseteq \mathscr{P}(X)$ chiusa per intersezioni finite e tale che $\forall x \in X \, \exists B \in \mathcal{B} \, (x \in B)$. La **topologia generata da** $\mathcal{B}$ è

$$\hat{\mathcal{B}} = \left\{ \bigcup_{i \in I} B_i \mid \{ B_i \mid i \in I \} \subseteq \mathcal{B} \right\} .$$

Diremo che $\mathcal{B}$ è una base per la topologia $\mathcal{T}$ se $\hat{\mathcal{B}} = \mathcal{T}$. Se uno spazio topologico ha una base numerabile diremo che è **secondo-numerabile** ovvero che soddisfa al **secondo assioma di numerabilità**. Per l'assioma delle scelte numerabili, uno spazio secondo-numerabile è anche separabile (Esercizio 16.31). Per ogni $\mathcal{S} \subseteq \mathscr{P}(X)$ la famiglia

$$\{ A_1 \cap \cdots \cap A_n \mid A_1, \ldots, A_n \in \mathcal{S} \} \cup \{ \emptyset, X \}$$

è una base per una topologia $\mathcal{T}$ su X e diremo che $\mathcal{S}$ è una **sotto-base** per questa topologia.

Data una famiglia di spazi topologici $(Y_i, \mathcal{T}_i)$ $(i \in I)$, un insieme X e delle funzioni $F_i \colon X \to Y_i$, la topologia indotta su X dalle F_i è quella generata dagli insiemi $F_i^{-1}[U_i]$, con $U \in \mathcal{T}_i$ e $i \in I$. Una base per questa topologia $\mathcal{T}$ su X è

$$\left\{ F_i^{-1}[U_i] \mid U_i \in \mathcal{T}_i, i \in J, J \subseteq I \text{ finito} \right\}.$$

Questa topologia rende ogni F_i continua ed è la minima topologia siffatta, nel senso che ogni topologia su X che rende tutte le F_i continue deve contenere $\mathcal{T}$. Se prendiamo come $X = \bigtimes_{i\in I} Y_i$ il prodotto cartesiano degli Y_i e $F_i \colon X \to Y_i$ è la funzione valutazione $f \mapsto f(i)$, si ottiene la **topologia prodotto** o **topologia di Tychonoff** i cui aperti di base sono della forma

$$\begin{aligned} \boldsymbol{N}(U_{i_0}, \dots, U_{i_n}) &= \{\, f \in \textstyle\bigtimes_{i\in I} Y_i \mid f(i_k) \in U_{i_k},\ k = 0, \dots, n \,\} \\ &= \textstyle\bigtimes_{j\in\{i_0,\dots,i_n\}} U_j \times \bigtimes_{i\in I\setminus\{i_0,\dots,i_n\}} Y_i \end{aligned}$$

dove $\{i_0, \dots, i_n\} \subseteq I$ e U_{i_k} è aperto in Y_{i_k}.

2.B. Assiomi di separazione. Gli spazi topologici possono essere classificati in base alla loro abilità di distinguere punti mediante aperti. Uno spazio topologico $(X, \mathcal{T})$ si dice

T_0 se punti distinti hanno famiglie degli intorni distinte,

$$x \neq y \quad \Rightarrow \quad \exists U \in \mathcal{T}\,((x \in U \wedge y \notin U) \vee (y \in U \wedge x \notin U))$$

T_1 se punti distinti sono distinguibili mediante aperti,

$$x \neq y \quad \Rightarrow \quad \exists U, V \in \mathcal{T}\,(x \in U \wedge y \notin U \wedge y \in V \wedge x \notin V)\,.$$

Equivalentemente: X è T_1 se $\{x\}$ è un chiuso, per ogni $x \in X$.

T_2 o di **Hausdorff** se punti distinti sono separabili mediante aperti,

$$x \neq y \quad \Rightarrow \quad \exists U, V \in \mathcal{T}\,(x \in U \wedge y \in V \wedge U \cap V = \emptyset)$$

T_3 o **regolare** se è possibile separare un punto x da un chiuso C mediante aperti, cioè

$$x \notin C \Rightarrow \exists U, V \in \mathcal{T}\,(x \in U \wedge C \subseteq V \wedge U \cap V = \emptyset)\,.$$

Equivalentemente: X è T_3 se per ogni aperto U e ogni $x \in U$, è possibile trovare un aperto V tale che $x \in V \subseteq \mathrm{Cl}(V) \subseteq U$. Se X è T_0, allora T_3 implica T_2.

2.C. Compattezza. Sia X uno spazio topologico e sia K un suo sottospazio. Un **ricoprimento aperto** di K è una famiglia $\{ A_i \mid i \in I \}$ di aperti che ricoprono K, cioè $K \subseteq \bigcup_{i\in I} A_i$. Diremo che K è **compatto** se da ogni ricoprimento aperto $\{ A_i \mid i \in I \}$ possiamo estrarre un sotto-ricoprimento finito, cioè se esiste $I_0 \subseteq I$ finito tale che $K \subseteq \bigcup_{i\in I_0} A_i$. In generale diremo che uno spazio topologico è compatto se lo è come sottospazio di sé stesso. Uno spazio è compatto se ogni famiglia $\mathcal{C}$ di chiusi ha la **proprietà dell'intersezione finita**: se $\forall C_1, \dots, C_n \in \mathcal{C}\,(C_1 \cap \dots \cap C_n \neq \emptyset)$, allora $\bigcap_{C\in\mathcal{C}} C \neq \emptyset$. Un chiuso di un compatto è compatto. Uno spazio compatto è T_3: se $x \notin C$ e C è chiuso (e quindi compatto), scegliamo aperti U_y e V_y disgiunti con $x \in U_y$ e $y \in V_y$. Poiché $\{ V_y \mid y \in C \}$ ricopre C possiamo estrarre un sotto-ricoprimento finito $\{V_{y_1}, \dots, V_{y_n}\}$. Allora $x \in U_{y_1} \cap \dots \cap U_{y_n} = U$, $C \subseteq V_{y_1} \cup \dots \cup V_{y_n} = V$ e $U \cap V = \emptyset$.

Uno spazio topologico si dice **localmente compatto** se è T_2 e ogni punto ha un intorno la cui chiusura è compatta. Equivalentemente: se U è aperto e $x \in U$ allora $\exists V$ aperto tale che $x \in V \subseteq \mathrm{Cl}(V) \subseteq U$ e $\mathrm{Cl}(V)$ è compatto.

2.D. Spazi metrici. Uno **spazio metrico** è un insieme X dotato di una **metrica** $d\colon X \times X \to [0; +\infty)$ che soddisfa alle tre proprietà:

- $d(x, y) = 0$ se e solo se $x = y$,
- $d(x, y) = d(y, x)$, per ogni $x, y \in X$,
- $d(x, y) \leq d(x, z) + d(z, y)$, per ogni $x, y, z \in X$.

La **palla aperta** di centro $x \in X$ e raggio $r > 0$ è l'insieme

$$B(x; r) = B_{(X,d)}(x; r) \stackrel{\text{def}}{=} \{ y \in X \mid d(x, y) < r \}$$

mentre la palla chiusa $B(x; r)^{\mathrm{Cl}}$ ha la medesima definizione, con $\leq$ al posto di $<$. Il **diamtero** di un insieme $A \subseteq X$ è

$$\operatorname{diam}(A) = \sup \{ d(x, y) \mid x, y \in A \}.$$

Un insieme si dice limitato se il suo diametro è $< \infty$.

Uno spazio metrico è anche uno spazio topologico, prendendo come sottobase la famiglia delle palle aperte. Inoltre la topologia così ottenuta è T_0 e T_3 e soddisfa al primo assioma di numerabilità. Uno spazio metrico separabile è anche secondo-numerabile: se D è un sottoinsieme denso e numerabile basta prendere come base $\{ B(x; q) \mid x \in D \ \wedge \ q \in \mathbb{Q}^+ \}$.

Una successione $(x_n)_n$ in uno spazio metrico (X, d) converge ad un $x \in X$ se $\forall \varepsilon > 0\, \exists N\, \forall n > N\, (d(x_n, x) < \varepsilon)$. Una successione si dice di **Cauchy** se

$$\forall \varepsilon > 0\, \exists N\, \forall n, m > N\ d(x_n, x_m) < \varepsilon.$$

Uno spazio metrico si dice **completo** se ogni successione di Cauchy converge in X. In questo caso la metrica si dirà **completa**

Indice analitico

Bibliografia

[AM69] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[CTV76] Checcucci, Tognoli, and Vesentini. *Lezioni di topologia generale*. Feltrinelli, Milano, 1976.

[Fol99] Gerald B. Folland. *Real analysis*. Pure and Applied Mathematics (New York). John Wiley & Sons Inc., New York, second edition, 1999. Modern techniques and their applications, A Wiley-Interscience Publication.

[Fre01] David H. Fremlin. *Measure Theory*, volume 1. Torres Fremlin, 2001.

[Fre02] David H. Fremlin. *Measure Theory*, volume 2. Torres Fremlin, 2002.

[Fre03] David H. Fremlin. *Measure Theory*, volume 4. Torres Fremlin, 2003.

[Fre04] David H. Fremlin. *Measure Theory*, volume 3. Torres Fremlin, 2004.

[Gol84] Robert Goldblatt. *Topoi*, volume 98 of *Studies in Logic and the Foundations of Mathematics*. North-Holland Publishing Co., Amsterdam, second edition, 1984. The categorial analysis of logic.

[Her06] Horst Herrlich. *Axiom of choice*, volume 1876 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 2006.

[HR98] Paul Howard and Jean E. Rubin. *Consequences of the axiom of choice*, volume 59 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 1998. With 1 IBM-PC floppy disk (3.5 inch; WD).

[Hun80] Thomas W. Hungerford. *Algebra*, volume 73 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1980. Reprint of the 1974 original.

[HW79] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. The Clarendon Press Oxford University Press, New York, fifth edition, 1979.

[Jec73] Thomas J. Jech. *The axiom of choice*. North-Holland Publishing Co., Amsterdam, 1973. Studies in Logic and the Foundations of Mathematics, Vol. 75.

[Jec03] Thomas Jech. *Set theory*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2003. The third millennium edition, revised and expanded.

[Kel55] John L. Kelley. *General topology*. D. Van Nostrand Company, Inc., Toronto-New York-London, 1955.

[Kop89] Sabine Koppelberg. *Handbook of Boolean algebras. Vol. 1.* North-Holland Publishing Co., Amsterdam, 1989. Edited by J. Donald Monk and Robert Bonnet.

[Kun80] Kenneth Kunen. *Set theory*, volume 102 of *Studies in Logic and the Foundations of Mathematics*. North-Holland Publishing Co., Amsterdam, 1980. An introduction to independence proofs.

[Kur92] Casimir Kuratowski. *Topologie. I et II.* Éditions Jacques Gabay, Sceaux, 1992. Part I with an appendix by A. Mostowski and R. Sikorski, Reprint of the fourth (Part I) and third (Part II) editions.

[Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[Lev02] Azriel Levy. *Basic set theory*. Dover Publications Inc., Mineola, NY, 2002. Reprint of the 1979 Springer edition.

[Lol94] Gabriele Lolli. *Dagli insiemi ai numeri*. Didattica. Bollati Boringhieri, 1994.

[MB89a] J. Donald Monk and Robert Bonnet, editors. *Handbook of Boolean algebras. Vol. 2*. North-Holland Publishing Co., Amsterdam, 1989.

[MB89b] J. Donald Monk and Robert Bonnet, editors. *Handbook of Boolean algebras. Vol. 3*. North-Holland Publishing Co., Amsterdam, 1989.

[ML98] Saunders Mac Lane. *Categories for the working mathematician*, volume 5 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1998.

[Mon69] J. Donald Monk. *Introduction to set theory*. McGraw-Hill Book Co., New York, 1969.

[Mor65] Anthony P. Morse. *A theory of sets*. Pure and Applied Mathematics, Vol. XVIII. Academic Press, New York, 1965.

[Oxt80] John C. Oxtoby. *Measure and category*, volume 2 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1980. A survey of the analogies between topological and measure spaces.

[RR85] Herman Rubin and Jean E. Rubin. *Equivalents of the axiom of choice. II*, volume 116 of *Studies in Logic and the Foundations of Mathematics*. North-Holland Publishing Co., Amsterdam, 1985.

[Rud91] Walter Rudin. *Functional analysis*. International Series in Pure and Applied Mathematics. McGraw-Hill Inc., New York, second edition, 1991.

[Sch97] Eric Schechter. *Handbook of analysis and its foundations*. Academic Press Inc., San Diego, CA, 1997.

[Wag93] Stan Wagon. *The Banach-Tarski paradox*. Cambridge University Press, Cambridge, 1993. With a foreword by Jan Mycielski, Corrected reprint of the 1985 original.

[Wei95] André Weil. *Basic number theory*. Classics in Mathematics. Springer-Verlag, Berlin, 1995. Reprint of the second (1973) edition.