Corso di Teoria degli Insiemi
Scuola di Logica AILA
Versione del 15 settembre 2006

Alessandro Andretta

alessandro.andretta@unito.it

Indice

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 M. Morse e J. Kelly e prende il nome di MK.

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 $A = B$.*

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 indiviuiamo 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.

[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.

- 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.

L'espressione

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

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

Esempi 1.3. (1) $x \notin x$, la formula usata nel paradosso di Russell, ha un un'unica variabile x, che è anche libera.

(2) 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: l'espressione $\int_0^1 f(x, y)\, dy$ e $\int_0^1 f(x, z)\, dz$ sono del tutto equivalenti e denotano una funzione nella variabile x, mentre $\int_0^1 f(x, x)\, dx$ denota un numero.

(3) 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 $(x \in y) \wedge \exists z(z \in x)$.

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

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

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

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

Osservazione 1.4. In matematica, ogni qual volta si dimostra che

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

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

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

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

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

dove φ è la formula che definisce 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 $\varphi(x, y_1, \dots, y_n)$ è una formula come sopra,

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

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

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

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

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 1.5. *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 $\emptyset$.

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 1.6. 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 1.7. *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 1.8. 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.

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:

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

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

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 1.5 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 1.9. *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

$$\{\emptyset\},\ \{\{\emptyset\}\},\ \{\{\{\emptyset\}\}\},\ \{\{\{\{\emptyset\}\}\}\},\quad \dots$$

oppure

(9) $$\{\emptyset\} = \boldsymbol{S}(\emptyset),\ \{\emptyset, \{\emptyset\}\} = \boldsymbol{S}(\{\emptyset\}),\ \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} = \boldsymbol{S}(\{\emptyset, \{\emptyset\}\}),\ \dots$$

dove

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

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

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

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

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

$$0 = \emptyset, \quad 1 = \boldsymbol{S}(0), \quad 2 = \boldsymbol{S}(1) = \boldsymbol{S}(\boldsymbol{S}(0)), \quad \dots$$

Proposizione 1.10. $\mathbb{N} \in \mathcal{S}$ *e se* $n \in \mathbb{N}$*, allora* $n = 0$ *oppure* $n = \boldsymbol{S}(m)$ *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 $\boldsymbol{S}(n) \in I$: essendo $I \in \mathcal{S}$ arbitrario, otteniamo che $\boldsymbol{S}(n) \in \bigcap \mathcal{S} = \mathbb{N}$. Quindi $\mathbb{N} \in \mathcal{S}$.

Sia $n \in \mathbb{N} \setminus \{0\}$ e supponiamo per assurdo che $n \neq \boldsymbol{S}(m)$ 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 1.11 (Principio di Induzione su $\mathbb{N}$ —prima formulazione)**.** *Sia* $I \subseteq \mathbb{N}$ *tale che* $0 \in I$ *e tale che* $\forall n\,(n \in I \Rightarrow \boldsymbol{S}(n) \in I)$. *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.

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 $x \mathrel{R} y$ 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 1.12. *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 8.

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

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

Osservazione 1.14. 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 1.13) 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 1.15. 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 1.16. *Non esiste nessuna funzione f tale che* $\mathrm{dom}(f) = \mathbb{N}$ *e*

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

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 $f(\boldsymbol{S}(n)) \in f(n) \cap \mathrm{ran}(f)$: contraddizione. □

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, $s = \langle a_0, a_1, \dots, a_{n-1}\rangle$ è la funzione di dominio $n = \{0, 1, \dots, n-1\}$ 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}. Per semplicità notazionale useremo spesso l'espressione $\bar{x}$ invece di $\langle x_0, \dots, x_{n-1}\rangle$ o di $(x_0, \dots, x_{n-1})$ 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 $f(x_0, \dots, x_{n-1})$ invece del più corretto, ma barocco, $f(\langle x_0, \dots, x_{n-1}\rangle)$.

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

$$\text{(11)}\quad \bigtimes_{i\in I} A_i = \{\, f \mid f \text{ è una funzione, } \mathrm{dom}(f) = I \text{ e } \forall i \in I\,(f(i) \in A_i)\,\}\,.$$

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 $A_0 \times A_1$.

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 $\mathrm{Cl}_{\mathcal{F}}(Y)$.

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

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 concreti, passibili di un'analisi di tipo algoritmico e, in linea di principio, analizzabili da un programma di computer. 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: $\exists I \, \exists J \, (I \in J \wedge \emptyset \in I \wedge \forall x \, (x \in I \Rightarrow \exists y \, (y = \boldsymbol{S}(x) \wedge y \in I)))$.

Rimpiazzamento:

$$\forall F \, \big((\forall x \exists ! y (x, y) \in F \wedge \exists B \, (A \in B) \big) \Rightarrow \exists C \, (F[A] \in C) \big) \, . \tag{12}$$

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 $\subseteq$, $\{x, y\}$, $\cap$, $\emptyset$, $\bigcup$, $\boldsymbol{S}$ e $F[A]$. Lasciamo al lettore l'ulteriore sforzo di eliminare questi simboli definiti (Esercizio 1.23).

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 non ha diritto di cittadinanza in ZF. Gli assiomi di Estensionalità, Potenza, Coppia, Fondazione, Unione sono come in MK, eccetto che non è necessario asserire che si sta parlando di insiemi. Per esempio, l'Assioma della Coppia diventa

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

Lo Schema di Assiomi di Comprensione e l'Assioma del Rimpiazzamento e vengono sostituiti rispettivamente da

Schema di Assiomi di Separazione. *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 $x, B, y_1, \ldots, y_n$,

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

Schema di Assiomi del Rimpiazzamento. *Per ogni formula di* LST

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

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

$$\begin{aligned}(13) \quad & \forall A \, \forall z_1 \ldots \forall z_n \, (\forall x \, (x \in A \Rightarrow \exists! y \, \varphi(x, y, A, z_1, \ldots, z_n)) \Rightarrow \\ & \qquad \exists B \, \forall y \, (y \in B \Leftrightarrow \exists x \, (x \in A \wedge \varphi(x, y, A, z_1, \ldots, z_n)))) \, .\end{aligned}$$

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 (12) è un singolo assioma, mentre lo Schema di Assiomi del Rimpiazzamento[4] di ZF è una lista infinita di assiomi, uno per ogni φ.

[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.

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 intrdotta 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 .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 metamatematici, 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 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

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

insieme non vuoto e $\mathcal{O}$ è una topologia su Y. Nella teoria MK è possibile dimostrare teoremi della forma

$$\exists X\,(\neg\exists Y(X \in Y) \wedge \ldots X \ldots) \tag{14}$$

e

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

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 (14): 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 (14) 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 (15) 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 1.8 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 $y \in \boldsymbol{S}(x)$.

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. Sia X un insieme.

(i) Dimostrare che $\bigcup_{n \in \mathbb{N}} X^n$, la classe di tutte le successioni finite di elementi di X, è un insieme. Dimostrare che se C è una classe propria, anche $\bigcup_{n \in \mathbb{N}} C^n$ è una classe propria.

(ii) Dimostrare che la concatenazione è un'operazione binaria associativa su $\bigcup_{n \in \mathbb{N}} X^n$ e che $\emptyset$ è l'elemento neutro.

Esercizio 1.29. (i) Dimostrare che in presenza degli altri assiomi di MK, l'assioma di rimpiazzamento (12) è equivalente alla sua versione iniettiva:

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

Analogamente, dimostrare che in presenza degli altri assiomi di ZF, lo schema di assiomi di rimpiazzamento (13) è equivalente allo schema di assiomi:

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

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

allora

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

(ii) Dimostrare che in presenza degli altri assiomi di ZF, lo schema di assiomi di rimpiazzamento (13) implica lo schema di assiomi di separazione.

2. Insiemi ordinati

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

- **riflessiva su** X se $\forall x \in X(x \mathrel{R} x)$;
- **irriflessiva su** X se $\neg\exists x \in X(x \mathrel{R} x)$;
- **simmetrica su** X se $\forall x \in X\, \forall y \in X(x \mathrel{R} y \Rightarrow y \mathrel{R} x)$;
- **antisimmetrica su** X se $\forall x \in X\, \forall y \in X\bigl((x \mathrel{R} y \wedge y \mathrel{R} x) \Rightarrow x = y\bigr)$;
- **connessa su** X se $\forall x \in X\, \forall y \in X(x = y \vee x \mathrel{R} y \vee y \mathrel{R} x)$;
- **transitiva su** X se $\forall x \in X\, \forall y \in X\, \forall z \in X\bigl((x \mathrel{R} y \wedge y \mathrel{R} z) \Rightarrow x \mathrel{R} z\bigr)$;
- **regolare su** X se $\{\, y \in X \mid y \mathrel{R} x \,\}$ 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.

(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

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

[6] Una costruzione di X/E, per E non regolare, è data nell'Esercizio 4.26.

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

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, $x \nleq y$ 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

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

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.) Un ordine è **denso in sé stesso** se $(x; y) \neq \emptyset$ per ogni $x < y$. 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 $\{ x \in X \mid x$ è un maggiorante di $Y \}$.

estremo inferiore di Y se è un minorante di Y e se $\bar{x}$ è un maggiorante di $\{ x \in X \mid x$ 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 $\max \{ x \in X \mid x$ è un minorante di $Y \}$ e $\min \{ x \in X \mid x$ 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 $y = z$. $\square$

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.

B.1. 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 $\emptyset$.

B.2. $\mathbb{R}$ 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.

B.3. 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 (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: $\mathbb{R}$.

B.4. Se $f, g \in \mathbb{N}^{\mathbb{N}}$ poniamo

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

$\leq^*$ 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).

B.5. 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: $A_{n-1} \setminus A_n$, $A_{n-2} \setminus A_{n-1}, \dots$ $A_0 \setminus A_1$. 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 $i > m$, 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).

C. Un teorema di punto fisso. Se $R \subseteq X \times X$ e $S \subseteq Y \times Y$, un **morfismo** $f : \langle X, R \rangle \to \langle Y, S \rangle$ è una funzione $f : X \to Y$ 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 $f^{-1} : \langle Y, S \rangle \to \langle X, R \rangle$ è un morfismo, diremo che f è un **isomorfismo**. Nel caso di pre-ordini, un morfismo $f : \langle X, \leq \rangle \to \langle Y, \preccurlyeq \rangle$ si dice funzione **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 $f : X \to X$ 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 $F : A \to B$ e $G : B \to A$ sono iniettive allora $\exists H \, (H : A \to B$ bijettiva).*

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

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

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

$$\begin{gathered} G^{-1} \restriction (A \setminus C) : A \setminus C \to B \setminus F[C] \\ F \restriction C : C \to F[C] \end{gathered}$$

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 $\leq_{\mathrm{lex}}$:

$$\begin{aligned}
(x_1, y_1) \trianglelefteq (x_2, y_2) &\Leftrightarrow (x_1 \leq x_2 \wedge y_1 \preccurlyeq y_2) \\
(x_1, y_1) \leq_{\mathrm{lex}} (x_2, y_2) &\Leftrightarrow (x_1 < x_2 \vee (x_1 = x_2 \wedge y_1 \preccurlyeq y_2)) \, .
\end{aligned}$$

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 (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 (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 $\langle \mathbb{R}, < \rangle$. (Suggerimanto: $\mathbb{N}$ 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 $\boldsymbol{S}(x)$ è transitivo. Se α è un ordinale, anche $\boldsymbol{S}(\alpha)$ 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) $\alpha \in \beta \Leftrightarrow \boldsymbol{S}(\alpha) \in \boldsymbol{S}(\beta)$.

Proposizione 3.6. Ord *è una classe propria.*

Dimostrazione. Se $\alpha \in \mathrm{Ord}$ e $\beta \in \alpha$, allora $\beta \in \mathrm{Ord}$ per l'Esercizio 3.5(v). Quindi Ord è una classe transitiva. Se Ord fosse un insieme, allora sarebbe un ordinale e quindi $\mathrm{Ord} \in \mathrm{Ord}$, 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

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

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

$$\bar{\alpha} \cap A = \emptyset \, . \tag{16}$$

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 (16), $\gamma \notin A$, 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 1.16 otteniamo

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

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

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 $n \cap X = \emptyset$. Per l'Esercizio 3.5, $n > 0$ e quindi, per la Proposizione 1.10, $n = \boldsymbol{S}(m)$ per qualche $m \in \mathbb{N}$. Allora $m \in \mathrm{Ord}$ e quindi $\boldsymbol{S}(m) \in \mathrm{Ord} \cap \mathbb{N}$: 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 1.10 $\bar{n} = \boldsymbol{S}(\bar{m})$, 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. $\square$

Un ordinale α è **successore** se $\alpha = \boldsymbol{S}(\beta)$, per qualche β. Chiaramente $\alpha < \boldsymbol{S}(\alpha)$ e per il Esercizio 1.24, non esiste alcun β tale che $\alpha < \beta < \boldsymbol{S}(\alpha)$. In altre parole $\boldsymbol{S}(\alpha)$ 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 1.10 non esistono ordinali limite minori di $\mathbb{N}$. Basta quindi verificare che $\mathbb{N}$ non è successore. Se, per assurdo, $\mathbb{N} = \boldsymbol{S}(\alpha)$, allora $\alpha \in \mathbb{N}$, da cui $\boldsymbol{S}(\alpha) \in \mathbb{N}$, cioè $\mathbb{N} \in \mathbb{N}$: contraddizione. $\square$

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) *$\alpha < \beta \Leftrightarrow \boldsymbol{S}(\alpha) \leq \beta$;*

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

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

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

(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 $\beta \in \boldsymbol{S}(\alpha)$ è impossibile, segue che $\beta = \boldsymbol{S}(\alpha)$ o $\boldsymbol{S}(\alpha) \in \beta$. 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) $\beta \in \bigcup \boldsymbol{S}(\alpha)$ se e solo se $\beta \in \gamma \in \alpha$ per qualche γ oppure $\beta \in \alpha$. Quindi $\beta \in \bigcup \boldsymbol{S}(\alpha) \Leftrightarrow \beta \in \alpha$.

(f) Da (d) otteniamo $\bigcup \alpha \leq \alpha$. Se $\bigcup \alpha < \alpha$, allora per (c) $\boldsymbol{S}(\bigcup \alpha) \leq \alpha$, quindi è sufficiente dimostrare che non vale la disuguaglianza stretta: se $\boldsymbol{S}(\bigcup \alpha) \in \alpha$ allora $\bigcup \alpha \in \boldsymbol{S}(\bigcup \alpha)$ 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. Per l'Esercizio 3.5 $\bigcup A \in$ Ord e poiché $\bigcup A$ è il più piccolo insieme contenete ogni $\alpha \in A$, $\bigcup A = \sup A$, per la Proposizione 3.13. □

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
- $0 \in I$,
- $\forall \alpha \in A\big(\exists \beta(\alpha = \boldsymbol{S}(\beta) \ \wedge\ \beta \in I) \Rightarrow \alpha \in I\big)$,
- $\forall \alpha \in A\big((\alpha \text{ limite e } \forall \beta < \alpha\ \beta \in I) \Rightarrow \alpha \in I\big)$.

Allora $I = A$.

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

$$\forall \gamma \in \alpha\, (\gamma \leq f(\gamma)) \tag{17}$$

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 (17)

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 (17) con f e f^{-1} otteniamo $\gamma \leq f(\gamma)$ e $\gamma \leq f^{-1}(\gamma)$, cioè f è l'identità. $\square$

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.

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 $n = \boldsymbol{S}(n')$ e $f \colon n \rightarrowtail m$. Chiaramente $m > 0$, cioè $m = \boldsymbol{S}(m')$. 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, $n' \leq m'$. L'Esercizio 3.5(vii) implica che $n \leq m$.

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

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 $\boldsymbol{S}(\omega)$, $\boldsymbol{S}(\boldsymbol{S}(\omega))$, $\boldsymbol{S}(\boldsymbol{S}(\boldsymbol{S}(\omega)))$,... 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 $|\alpha| = |\boldsymbol{S}(\alpha)|$,*

(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) $f\colon \boldsymbol{S}(\alpha) \to \alpha$

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

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. □

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 isomorfismoe 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

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

Per l'Esercizio 3.22(i) l'insieme A è chiuso sotto l'operazione $\boldsymbol{S}$ 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 $\alpha^+ \in A$): contraddizione. 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 in bijezione con ω si dice **numerabile**; il cardinale ω^+ viene denotato con

$$\omega_1$$

ed è il primo cardinale non-numerabile o più che numerabile.

Teorema 3.24. *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 3.25. Card *è una classe propria.*

Esercizi

Esercizio 3.26. 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 3.27. 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 3.28. Dimostrare che se $\alpha \geq \omega$, allora $\alpha^+ = \{\, \beta \mid \exists f\, (f\colon \beta \rightarrowtail \alpha) \,\}$.

Esercizio 3.29. 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 $\left\langle f^{(n)} \mid n \in \mathbb{N} \right\rangle$ 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* $G = \left\langle f^{(n)} \mid n \in \mathbb{N} \right\rangle$ delle iterate? Non è per nulla ovvio che i vari assiomi di MK 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 4.27 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

$$F(n,p) = f \circ p(n-1)\,. \tag{18}$$

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

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

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

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

A.1. Prendendo $A = B$, $h\colon A \to A$ la funzione identica e F come in (18) otteniamo $G\colon A \times \omega \to A$ tale che $G(a,n) = f^{(n)}(a)$.

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

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

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

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

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

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

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

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

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

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

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 $(z,x) \in Z \times X$*

$$G(z,x) = F(z,x,G \restriction \{\, (z,y) \mid y \mathrel{R} x \,\}) \,. \tag{19}$$

Dimostrazione. Supponiamo che $G, G'\colon Z \times X \to \mathrm{V}$ soddisfino (19) 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

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

da cui $G(\bar{z},\bar{x}) = F(\bar{z},\bar{x},p) = G'(\bar{z},\bar{x})$: una contraddizione. Quindi l'unicità è stabilita.

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

- $\mathrm{dom}(p) \subseteq Z \times X$,
- $\forall (z,x) \in \mathrm{dom}(p) \, \forall y \in X \, (y \mathrel{R} x \Rightarrow (z,y) \in \mathrm{dom}(p))$,
- $\forall (z,x) \in \mathrm{dom}(p) \, (p(z,x) = F(z,x,p \restriction \{\, (z,y) \mid y \mathrel{R} x \,\}))$.

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

$$\{\, x \in X \mid \exists z \in Z \; p(z,x) \neq q(z,x) \,\} \neq \emptyset$$

e per la ben fondatezza sia $\bar{x}$ un elemento R-minimale di questo insieme e sia $\bar{z} \in Z$ tale che $p(\bar{z}, \bar{x}) \neq q(\bar{z}, \bar{x})$. Per la definizione di $\mathcal{G}$,

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

e per la R-minimalità di $\bar{x}$

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

da cui $p(\bar{z}, \bar{x}) = q(\bar{z}, \bar{x})$, 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 $Z \times X \setminus \operatorname{dom}(G) \neq \emptyset$, sia $\bar{x}$ un elemento R-minimale di $\{ x \in X \mid \exists z \in Z \ (z, x) \notin \operatorname{dom}(G) \}$ e sia $\bar{z} \in Z$ tale che $(\bar{z}, \bar{x}) \notin \operatorname{dom}(G)$. Allora

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

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 $(\bar{z}, \bar{x}) \in \operatorname{dom}(G)$, contrariamente alla nostra assunzione. Ne segue che G è la relazione funzionale cercata. □

Corollario 4.3. *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*

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

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

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

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 4.5. *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 $g\colon \omega \to \boldsymbol{S}(n)$

$$g(0) = 0\,,$$
$$g(\boldsymbol{S}(i)) = \min \{ j \leq n \mid x_{g(i)} \prec x_j \}\,.$$

(Per ipotesi l'insieme $\{ j \leq n \mid x_{g(i)} \prec x_j \}$ 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 $j = \boldsymbol{S}(n)$. Se $i < n$, allora $x_{g(i)} \prec x_{g(n)}$ per ipotesi induttiva e $x_{g(n)} \prec x_{g(\boldsymbol{S}(n))} = x_{g(j)}$ per costruzione e quindi $x_{g(i)} \prec x_{g(j)}$; se $i = n$, 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 4.6. *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 4.7. *Per ogni insieme fissato 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 4.6 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 $\preceq$. $\square$

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

C.1. 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

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

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

Esercizio 4.8. Verificare che l'esistenza di $\boldsymbol{\varrho}_{R,X}$ discende dal Teorema 4.2 e dimostrare che:

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

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

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 4.9. (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 4.10. (a) $\mathrm{rank}(\mathscr{P}(x)) = \boldsymbol{S}(\mathrm{rank}(x))$.

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

Dimostrazione. (a) Poiché $x \in \mathscr{P}(x)$ si ha che $\boldsymbol{S}(\mathrm{rank}(x)) \leq \mathrm{rank}(\mathscr{P}(x))$. Viceversa se $y \subseteq x$, allora $\boldsymbol{S}(\mathrm{rank}(y)) \leq \boldsymbol{S}(\mathrm{rank}(x))$ per l'Esercizio 4.9 e quindi $\mathrm{rank}(\mathscr{P}(x)) = \sup \{ \boldsymbol{S}(\mathrm{rank}(y)) \mid y \subseteq x \} \leq \boldsymbol{S}(\mathrm{rank}(x))$.

(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 $\boldsymbol{S}(\mathrm{rank}(z)) \leq \mathrm{rank}(y)$ e quindi $\boldsymbol{S}(\mathrm{rank}(z)) \leq \sup\{\,\mathrm{rank}(y) \mid y \in x\,\}$. Per l'arbitrarietà di z, $\mathrm{rank}(\bigcup x) \leq \sup\{\,\mathrm{rank}(y) \mid y \in x\,\}$. □

Definizione 4.11. $\mathrm{V}_\alpha = \{\, x \mid \mathrm{rank}(x) < \alpha \,\}$.

Teorema 4.12. V_α *è un insieme transitivo e*

$$\mathrm{V}_\alpha = \bigcup_{\beta<\alpha} \mathscr{P}(\mathrm{V}_\beta)\,. \tag{20}$$

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 (20). 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 (20). Per l'Esercizio 4.9 $x \in \mathrm{V}_{\mathrm{rank}(x)}$ 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 4.13. (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) $\mathrm{V}_{\boldsymbol{S}(\alpha)} = \mathscr{P}(\mathrm{V}_\alpha)$.

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

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

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 4.14. 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 4.15. 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 4.16. (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 4.17. (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*

$$\forall x, y \in X\, (x \mathrel{R} y \Leftrightarrow \boldsymbol{\pi}_{R,X}(x) \in \boldsymbol{\pi}_{R,X}(y))\,. \tag{21}$$

(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 $\boldsymbol{\pi}_{R,X}(\bar{x}) \neq \boldsymbol{\pi}_{R,X}(\bar{y})$, 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'inietività, $x \mathrel{R} y$. Quindi per l'Esercizio 4.14 (21) 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 $\boldsymbol{S}(\boldsymbol{\pi}_{R,X}(y)) = \boldsymbol{S}(\boldsymbol{\varrho}_{R,X}(y))$ con $y \mathrel{R} x$, vale a dire $\boldsymbol{\pi}_{R,X}(x) = \boldsymbol{\varrho}_{R,X}(x)$. □

Definizione 4.18. Se R è un buon ordine su X la classe

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

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

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

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, $f(\boldsymbol{S}(\alpha)$ è il successore immediato di $f(\alpha)$ e se λ è limite, $f(\lambda)$ è il più piccolo $x \in X$ tale che $f(\alpha) \mathrel{R} x$, per ogni $\alpha < \lambda$.

Teorema 4.19. *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 4.17. L'unicità discende dalla Proposizione 3.16. □

C.3. Una funzione crescente $f\colon \mathrm{Ord} \to \mathrm{Ord}$ si dice **continua** se

$$\forall\lambda\bigl(\lambda \text{ limite } \Rightarrow f(\lambda) = \sup_{\alpha<\lambda} f(\alpha)\bigr)\,.$$

Esercizio 4.20. 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 4.21. *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 $\alpha_0 = \boldsymbol{S}(\alpha)$ e $\alpha_{\boldsymbol{S}(n)} = f(\alpha_n)$ 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 $\alpha_n < \alpha_{\boldsymbol{S}(n)}$ e quindi $\bar\alpha$ è limite. Allora

$$\begin{aligned} f(\bar\alpha) &= \sup_{\nu<\bar\alpha} f(\nu) \\ &= \sup_n f(\alpha_n) && \text{(per l'Esercizio 4.20)} \\ &= \sup_n \alpha_{\boldsymbol{S}(n)} \\ &= \bar\alpha\,. \end{aligned}$$

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

Definizione 4.22. $\aleph\colon \mathrm{Ord} \to \mathrm{Card} \setminus \omega$ è la funzione che enumera la classe dei cardinali infiniti, cioè

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

La definizione di $\aleph_\lambda$, per λ limite, è ben posta per il Teorema 3.24. 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

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

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

$$\mathrm{trcl}(X) = \Bigl\{x \mid \exists n > 0\,\exists f \in {}^{\boldsymbol{S}(n)}\mathrm{V}\bigl[x = f(0) \land \\ f(n) \in X \land \forall i < n\ f(i) \in f(\boldsymbol{S}(i))\bigr]\Bigr\}$$

In altre parole $x \in \operatorname{trcl}(X)$ 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 4.23. Dimostrare che $\operatorname{trcl}(X)$ è la più piccola classe transitiva contenente X. Se X è un insieme anche $\operatorname{trcl}(X)$ lo è e $\operatorname{trcl}(X) = \bigcup_n X_n$, dove $X_0 = X$ e $X_{n+1} = \bigcup X_n$.

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

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

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 4.24. La relazione $\tilde{R}$ è transitiva su X.

Proposizione 4.25. *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 $\Big\{ y \in X \mid y \; \tilde{R} \; \bar{x} \Big\} = \bigcup_{n \geq 1} Z_n$ è un insieme. $\square$

Esercizi

Esercizio 4.26. 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

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

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

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

è una classe. Dimostrare che

(i) $x \mathrel{E} y \Leftrightarrow [\![x]\!]_E = [\![y]\!]_E$,

(ii) $\neg(x \mathrel{E} y) \Leftrightarrow [\![x]\!]_E \cap [\![y]\!]_E = \emptyset$.

Esercizio 4.27. Sia $R \subseteq X \times X$ una relazione regolare, vale a dire: per ogni $y \in X$

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

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 3.26 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 4.28. 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.

5. Aritmetica ordinale

Per il Corollario 4.3 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 prossima sezione.)

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

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

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) $\alpha \leq \beta \Leftrightarrow \exists! \gamma\, (\alpha \dotplus \gamma = \beta)$.

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

$$\alpha \dotplus \beta'' < \boldsymbol{S}(\alpha \dotplus \beta'') = \alpha \dotplus \beta' \,,$$

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

$$\alpha \dotplus \beta' = \sup_{\gamma < \beta'} \alpha \dotplus \gamma \geq \alpha \dotplus \boldsymbol{S}(\beta) > \alpha \dotplus \beta \,.$$

(b) La funzione $\nu \mapsto \alpha \dotplus \nu$ è crescente e continua, quindi $\alpha \dotplus \lambda$ è limite per l'Esercizio 4.20. Se $\lambda = \sup_{i \in I} \lambda_i$, allora $\alpha \dotplus \lambda_i \leq \alpha \dotplus \lambda$ e quindi $\sup_{i \in I} \alpha \dotplus \lambda_i \leq \alpha \dotplus \lambda$. Viceversa, se $\beta < \alpha \dotplus \lambda$, allora fissiamo $\gamma < \lambda$ tale che $\beta < \alpha \dotplus \gamma$ e fissiamo $j \in I$ tale che $\gamma < \lambda_j$. Allora $\beta < \alpha \dotplus \gamma < \alpha \dotplus \lambda_j$, da cui segue l'asserto.

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

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

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

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

(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

$$\{\, \xi \mid \alpha \dotplus \xi < \beta \,\}$$

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

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

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

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

$$|\alpha \dotplus \beta| = |\alpha \times \{0\} \cup \beta \times \{1\}| \tag{22}$$

Esercizio 5.2. Dimostrare che

(i) $\forall \alpha \, (\alpha \dotplus 1 = \boldsymbol{S}(\alpha))$ e

(ii) $\forall \alpha \, (\alpha \geq \omega \Rightarrow 1 \dotplus \alpha = \alpha)$.

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

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

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

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

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

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) *$\alpha \cdot (\beta \dotplus \gamma) = \alpha \cdot \beta \dotplus \alpha \cdot \gamma$.*

(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 $\forall \beta > 0 \, \exists! \gamma \leq \beta \, \exists! \delta < \alpha \, (\alpha \cdot \gamma \dotplus \delta = \beta)$.*

---

[9] Si veda il Esercizio 3.27.

Dimostrazione. (a) Si dimostra come l'analoga affermazione (a) della Proposizione 5.1. La seconda affermazione discende dalla Proposizione 3.16.

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

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

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 Proposizione 5.1(a)

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

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 $\boldsymbol{S}(\gamma)$. 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 $\alpha \cdot \gamma \dotplus \delta = \xi$ 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,

$$|\alpha \cdot \beta| = |\alpha \times \beta| \ . \tag{23}$$

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

Esercizi

Esercizio 5.6. Dimostrare che se $\omega \leq \alpha$, $0 \leq n < \omega$ e $0 < m < \omega$ allora $(\alpha \dotplus n) \cdot m = \alpha \cdot m \dotplus n$.

Esercizio 5.7. Dimostrare che se λ è un ordinale limite, $0 \leq n < \omega$ e $1 < m < \omega$, allora $(\lambda \dotplus n)^{\cdot m} < \lambda^{\cdot m} \cdot 2$. Dedurre che $(\lambda \dotplus n)^{\cdot \omega} = \lambda^{\cdot \omega}$.

Esercizio 5.8. Dimostrare che:

(i) se $\alpha < \beta$ allora $\omega^{\cdot \alpha} \dotplus \omega^{\cdot \beta} = \omega^{\cdot \beta}$. (Suggerimento: usare le Proposizioni 5.1 e 5.3;)

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

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

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

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

Esercizio 5.9. Dimostrare per ogni ordinale α sono equivalenti le seguenti affermazioni:

(i) α è additivamente indecomponibile;

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

(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 5.10. 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 5.11. Dimostrare per ogni ordinale α sono equivalenti le seguenti affermazioni:

(i) α è esponenzialmente indecomponibile;

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

Esercizio 5.12. (i) Dimostrare che $\forall \alpha > 2 \, (\alpha \dotplus \alpha < \alpha \cdot \alpha < \alpha^{\cdot \alpha})$.

(ii) Definiamo

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

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 **$\boldsymbol{\varepsilon}$-numeri**: il primo di questi è

$$\boldsymbol{\varepsilon}_0 = \sup\{\omega, \omega^{\cdot \omega}, \omega^{\cdot \omega^{\cdot \omega}}, \omega^{\cdot \omega^{\cdot \omega^{\cdot \omega}}}, \dots\} \, ,$$

Esercizio 5.13. 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

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

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

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

(i) Dimostrare che $\prec$ è un buon ordine di tipo $\omega^{\cdot \omega}$ su $\mathbb{N}[X]$, l'insieme dei polinomi a coefficienti in $\mathbb{N}$.

(ii) 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 $\prec$ su $\mathcal{F}$ è un buon ordine di tipo $\boldsymbol{\varepsilon}_0$, il primo punto fisso della funzione $\alpha \mapsto \omega^{\cdot \alpha}$.

Esercizio 5.15. 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

$$2^{2^{2+1}+2} + 2^{2^{2+1}+1} + 2^{2^{2+1}} + 2^{2^2+2+1} + 2^{2^2+2} + 2^{2^2} + 2^2$$
$$3^{3^{3+1}+3} + 3^{3^{3+1}+1} + 3^{3^{3+1}} + 3^{3^3+3+1} + 3^{3^3+3} + 3^{3^3} + 3^2 \cdot 2 + 3 \cdot 2 + 2$$
$$4^{4^{4+1}+4} + 4^{4^{4+1}+1} + 4^{4^{4+1}} + 4^{4^4+4+1} + 4^{4^4+4} + 4^{4^4} + 4^2 \cdot 2 + 4 \cdot 2 + 1$$
$$5^{5^{5+1}+5} + 5^{5^{5+1}+1} + 5^{5^{5+1}} + 5^{5^5+5+1} + 5^{5^5+5} + 5^{5^5} + 5^2 \cdot 2 + 5 \cdot 2$$
$$\vdots$$

Dimostrare che ogni sequenza di Goodstein termina a 0, cioè

$$\forall n \in \mathbb{N}\, \exists k\ G_n(k) = 0\,.$$

6. Successioni finite

Le operazioni aritmetiche su ω ci permettono di dimostrare rigorosamente fatti sulle successioni finite.

Definizione 6.1. Se s e t sono funzioni che hanno per dominio un ordinale e tali che $\operatorname{dom}(s) < \omega$ e $\operatorname{dom}(t) \leq \omega$, la **concatenazione** di s e t è la funzione $s^\frown t$ di domino $\operatorname{dom}(s) \dotplus \operatorname{dom}(t) \leq \omega$ definita da

$$s^\frown t(n) = \begin{cases} s(n) & \text{se } n \in \operatorname{dom}(s), \\ t(m) & \text{se } n = \operatorname{dom}(s) \dotplus m. \end{cases}$$

Quindi se $s = \langle a_0, a_1, \ldots, a_{n-1} \rangle$ e $t = \langle b_0, b_1, \ldots, \rangle$, allora

$$s^\frown t = \langle a_0, a_1, \ldots, a_{n-1}, b_0, b_1, \ldots, \rangle\,.$$

Esercizio 6.2. (i) Verificare che la definizione è ben data e che $\operatorname{dom}(s^\frown t) = \omega$ se e solo se $\operatorname{dom}(t) = \omega$.

(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 X, e dato un $Y \subseteq X$, la sotto-struttura generata da Y è il più piccolo $Z \neq \emptyset$ chiuso sotto le operazioni e tale che $Y \subseteq Z \subseteq X$. Nel caso degli anelli unitari, per esempio, si considera l'anello primo R di X (vale a dire il sotto-anello generato dall'unità) e l'insieme di tutti i polinomi in più variabili a coefficienti in R,

$$\bigcup_n R[\mathsf{x}_1, \ldots, \mathsf{x}_n]\,.$$

Il sotto-anello di X generato da Y è l'insieme degli elementi $p(y_1, \ldots, y_n)$ dove $p(\mathsf{x}_1, \ldots, \mathsf{x}_n) \in R[\mathsf{x}_1, \ldots, \mathsf{x}_n]$ e $y_1, \ldots, y_n \in Y$. Queste costruzioni possono essere formulate in generale.

Definizione 6.3. Sia S un insieme non vuoto e sia $a\colon S \to \omega$ una funzione. L'insieme W 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

$$s \in S \ \wedge \ w_1, \dots, w_m \in W \ \wedge \ a(s) = m \ \Rightarrow \ \langle s \rangle^\frown w_1{}^\frown \dots {}^\frown w_m \in W\,.$$

Lemma 6.4. *L'insieme W delle parole su (S, a) è $\bigcup_n W_n$ dove*

$$W_0 = \{ \langle s \rangle \mid a(s) = 0 \}$$

$$W_{n+1} = W_n \cup \left\{ \langle s \rangle^\frown w_1{}^\frown \cdots {}^\frown w_m \mid s \in S \wedge w_1, \dots, w_m \in W \ \wedge \ a(s) = m \right\}.$$

Dimostrazione. Per induzione su n si dimostra che $W_n \subseteq W$ e $W_n \subseteq W_m$, se $n < m$. Quindi è sufficiente dimostrare che se $w_1, \dots, w_m \in \bigcup_n W_n$, $a(s) = m$ allora $z = \langle s \rangle^\frown w_1{}^\frown \dots {}^\frown w_m$ appartiene a $\bigcup_n W_n$: ma se k è sufficientemente grande per cui $w_1, \dots, w_m \in W_k$, allora $z \in W_{k+1} \subseteq \bigcup_n W_n$. □

Definizione 6.5. Sia W l'insieme delle parole su (S, a). L'**altezza** di una parola $w \in W$ è il più piccolo n tale che $w \in W_n$.

$$\mathrm{ht}\colon W \to \omega$$

è la funzione altezza.

Se dobbiamo dimostrare che ogni parola $w \in W$ gode si una certa propeirtà, è possibile dimostrare ciò procedendo per induzione su $\mathrm{ht}(w)$; o, equivalentemente, dimostrando che tutte le parole in W_0 godono di questa proprietà e che se tutte le parole in W_n godono di questa proprietà, allora ciò vale anche per W_{n+1}. Il risultato seguente ci garantisce che le parole su un insieme S possono essere lette in un unico modo.

Lemma 6.6. *Sia W l'insieme delle parole su (S, a). Allora*

$$\forall w, z \in W\, (w \subseteq z \Rightarrow w = z)\,.$$

Dimostrazione. Per induzione su $\mathrm{lh}(w)$. Se $\mathrm{lh}(w) = 1$, allora $w = \langle s \rangle$ e $a(s) = 0$; ma se $z = \langle s, \dots \rangle$ ha lunghezza > 1, allora $a(s) \geq 1$: contraddizione. Quindi possiamo supporre $\mathrm{lh}(w) > 1$, cioè $w = \langle s \rangle^\frown w_1{}^\frown \dots {}^\frown w_m$ e $a(s) = m$. Quindi $z = \langle s \rangle^\frown z_1{}^\frown \dots {}^\frown z_m$ e $w_1{}^\frown \dots {}^\frown w_m \subseteq z_1{}^\frown \dots {}^\frown z_m$, da cui

$$w_1 \subseteq z_1 \quad \vee \quad z_1 \subseteq w_1\,.$$

Se vale la prima possibilità, poiché $\mathrm{lh}(w_1) < \mathrm{lh}(w)$, l'ipotesi induttiva implica che $w_1 = z_1$; se vale la seconda possibilità, allora $\mathrm{lh}(z_1) \leq \mathrm{lh}(w_1) < \mathrm{lh}(w)$ e quindi per ipotesi induttiva $z_1 = w_1$. Quindi $w_2{}^\frown \dots {}^\frown w_m \subseteq z_2{}^\frown \dots {}^\frown z_m$. Ripetendo questo argomento si ricava $w_i = z_i$ per $1 \leq i \leq m$, cioè $w = z$. □

Definizione 6.7. Siano z e w parole su (S, a).

(i) z è una **sotto-parola** di w se $\mathrm{lh}(w) > 0$ e per qualche $n < \mathrm{lh}(w)$

$$\forall m < \mathrm{lh}(z)\,(z(m) = w(m \dotplus n))\,.$$

(ii) z è una **sillaba** di w se $\mathrm{lh}(w) > 0$ e $w = \langle s\rangle^\frown w_1{}^\frown \dots {}^\frown w_m$, con $m = a(s)$ e $z = w_i$ per qualche $i \leq m$.

Esercizio 6.8. Dimostrare che z è una sotto-parola di w se e solo se esistono parole $z_1, \dots, z_n \in W$ tali che $z = z_1$, $w = z_n$ e z_i è una sillaba di z_{i+1}.

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 6.4, osserviamo che $W_0 = Y \subseteq X$ e che se $w \in W_{n+1}$ allora esistono e sono unici $f \in \mathcal{F}$ e $w_1, \dots, w_m \in W_n$ tali che $w = \langle f\rangle^\frown w_1, \dots, w_m$, con $m = \mathrm{ar}(f)$. Definiamo una mappa

$$\Phi\colon W \to X$$

ponendo $\Phi \restriction W_0 =$ l'identità su Y e

$$\Phi(\langle f\rangle^\frown w_1, \dots, w_m) = f(\Phi(w_1), \dots, \Phi(w_m))\,.$$

Sia $Y_n = \Phi[W_n]$. È facile verificare che

$$\begin{aligned} Y_0 &= Y \\ Y_{k+1} &= Y_k \cup \{\, f(x_1, \dots, x_n) \mid f \in \mathcal{F} \wedge \mathrm{ar}(f) = n \wedge x_1, \dots, x_n \in Y_k \,\} \end{aligned}$$

e che $Y_0 \subseteq Y_1 \subseteq \dots$. Se $f \in \mathcal{F}$ è n-aria e $x_0, \dots, x_{n-1} \in \bigcup_{k\in\mathbb{N}} Y_k$, fissiamo un $\bar{k}$ sufficientemente grande tale che $x_0, \dots, x_{n-1} \in Y_{\bar{k}}$: allora $f(x_0, \dots, x_{n-1}) \in Y_{\bar{k}+1} \subseteq \bigcup_{k\in\mathbb{N}} Y_k$. 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 6.9. *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.

Esercizi

Esercizio 6.10. Dimostrare che $\operatorname{ht}(w) = \max\{\operatorname{ht}(z) \mid z \text{ è una sillaba di } w\}$.

7. Aritmetica cardinale

Un insieme X si dice **bene ordinabile** se esiste un buon ordine su X.

Esercizio 7.1. 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 7.2. 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 8 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 7.3. Se X e Y sono bene ordinabili, allora $|X| \leq |Y|$ se e solo se $\exists f(f\colon X \rightarrowtail Y)$.

La **somma** ed il **prodotto** di cardinali sono definiti come

$$\begin{aligned} \kappa + \lambda &= |\kappa \times \{0\} \cup \lambda \times \{1\}| \\ \kappa \cdot \lambda &= |\kappa \times \lambda|\ . \end{aligned}$$

È immediato verificare che la somma e il prodotto cardinale sono operazioni commutative e associative e per (22) e (23) la cardinalità della somma e del prodotto di due ordinali è, rispettivamente, la somma e prodotto cardinale delle loro cardinalità, cioè

$$|\alpha \dot{+} \beta| = |\alpha| + |\beta| \quad \text{e} \quad |\alpha \boldsymbol{\cdot} \beta| = |\alpha| \cdot |\beta|\ . \tag{24}$$

Lemma 7.4. (a) $\forall m, n \in \omega\,(m + n = m \dot{+} n \in \omega)$.

(b) $\forall m, n \in \omega\,(m \cdot n = m \boldsymbol{\cdot} n \in \omega)$.

Dimostrazione. Cominciamo col dimostrare per induzione su n che

$$\forall m \in \omega\, (m \dotplus n \in \omega) \quad \text{e} \quad \forall m \in \omega\, (m \cdot n \in \omega)\,.$$

Se $n = 0$ allora $m \dotplus n = n$; se $n = \boldsymbol{S}(k)$ allora $m \dotplus n = \boldsymbol{S}(m \dotplus k) \in \omega$, per ipotesi induttiva e poiché ω è chiuso per $\boldsymbol{S}$. Il caso del prodotto è lasciato per esercizio.

Per (24) e il Teorema 3.17 si ha

$$m \dotplus n = |m \dotplus n| = |m| + |n| = m + n$$

e, analogamente, $m \cdot n = m \cdot n$. $\square$

Esercizio 7.5. 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 7.6. Il buon-ordine di Gödel su $\mathrm{Ord} \times \mathrm{Ord}$ 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 $\mathrm{Ord} \times \mathrm{Ord}$ e che $\alpha \times \alpha$ è un segmento iniziale, per ogni $\alpha \in \mathrm{Ord}$.

Teorema 7.7. *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)

$$X(\alpha, \beta) = \left\{\, (\alpha', \beta') \in \kappa \times \kappa \mid (\alpha', \beta') <_{\mathrm{G}} (\alpha, \beta) \,\right\}$$

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 $|\kappa \times \kappa| = \kappa$. $\square$

È immediato verificare che $\max(\kappa, \lambda) \leq \kappa + \lambda \leq \kappa \cdot \lambda \leq \max(\kappa, \lambda) \cdot \max(\kappa, \lambda)$ e quindi, se almeno uno tra κ e λ è infinito, per il Teorema 7.7,

$$\max(\kappa, \lambda) = \kappa + \lambda = \kappa \cdot \lambda\,.$$

Quindi 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 7.8 (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 7.9. 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 7.10. *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 7.7 e la parte (II) dell'Esercizio precedente $\mathscr{P}(\lambda \times \lambda)$ 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

$$\begin{tikzcd}
{}^{n+1}\kappa \arrow[r] \arrow[rrr, bend left, "j_{n+1}"] & {}^n\kappa \times \kappa \arrow[r] & \kappa \times \kappa \arrow[r] & \kappa \\
s \arrow[r, mapsto] & (s \restriction n, s(n)) \arrow[r, mapsto] & (j_n(s \restriction n), s(n)) \arrow[r, mapsto] & f(j_n(s \restriction n), s(n))\,.
\end{tikzcd}$$

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 7.11. *Se X è bene ordinabile e infinito, allora $|{}^{<\omega}X| = |X|$. In particolare, l'insieme delle sequenze finite di naturali ${}^{<\omega}\omega$ è numerabile.*

Esercizio 7.12. Dimostrare che l'esponenziazione ordinale e cardinale coincidono sui naturali,

$$\forall n, m \in \omega \, (n^m = n^{\cdot m} \in \omega)\,.$$

Esercizi

Esercizio 7.13. Dimostrare che un cardinale $\kappa \geq \omega$ è chiuso sotto somma, prodotto ed esponenziazione ordinale, cioè

$$\alpha, \beta < \kappa \quad \Rightarrow \quad \alpha \dotplus \beta,\ \alpha \cdot \beta,\ \alpha^{\cdot \beta} < \kappa\,.$$

Se $\kappa \leq \lambda$ sono cardinali definiamo

$$[\lambda]^\kappa = \{\, X \subseteq \lambda \mid |X| = \kappa \,\}\,.$$

Dimostrare che $[\lambda]^\kappa$ è in bijezione con ${}^\kappa\lambda$.

Esercizio 7.14. Per il Teorema di Cantor 7.8 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.

8. L'Assioma di Scelta

A. Il principio del buon ordinamento e il Lemma di Zorn. 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 8.1. 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 assiomi di MK, vale a dire: non è possibile dimostrare o refutare AC a partire da MK.

Teorema 8.2. *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 quando $\beta < \alpha$. 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 $\alpha \in \mathrm{Ord}$, allora avremmo un'iniezione $\mathrm{Ord} \rightarrowtail X$, contro l'Esercizio 1.15. Quindi esiste un $\bar{\alpha}$ 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 8.2.1. *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 8.2.2. *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 α, altrimenti si avrebbe una relazione funzionale iniettiva $G\colon \mathrm{Ord} \rightarrowtail X$. 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 7.2 di cardinalità può essere estesa ad ogni insieme.

Esercizio 8.3. 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 8.2 "Ogni insieme è bene ordinabile" implica il AC.

Il seguente risultato, noto come Lemma di Zorn, è la più utile tra le riformulazioni di AC.

Teorema 8.4. *Assumiamo che ogni insieme sia bene-ordinabile. (Per il risultato precedente discende da AC.) Sia $\langle X, \preccurlyeq \rangle$ un insieme non-vuoto parzialmente ordinato tale che ogni $C \subseteq X$ linearmente ordinato da $\preccurlyeq$ ammette un maggiorante. Allora $\langle X, \preccurlyeq \rangle$ ha un elemento massimale.*

Dimostrazione. Sia $X = \{ x_\alpha \mid \alpha < \kappa \}$ e supponiamo per assurdo che nessun x_α sia massimale. Definiamo induttivamente una successione $\nu \mapsto \alpha_\nu \in \kappa$ tale che

$$\nu < \xi \Rightarrow x_{\alpha_\nu} \prec x_{\alpha_\xi} .$$

Poniamo $\alpha_0 = 0$, e dato α_ν scegliamo come $\alpha_{\nu+1}$ il più piccolo $\xi \in \kappa$ tale che $x_{\alpha_\nu} \prec x_\xi$. (Tale elemento esiste per la nostra assunzione.) Se gli α_ν sono definiti per ogni $\nu < \lambda$, con λ limite, allora $\{ x_{\alpha_\nu} \mid \nu < \lambda \}$ è una catena e quindi ammette dei maggioranti x_γ. Sia α_λ il più piccolo tra questi γ. Questo definisce una funzione iniettiva $\mathrm{Ord} \to \kappa$, $\nu \mapsto \alpha_\nu$, un assurdo. Ne segue che deve $\langle X, \preceq \rangle$ ammette un elemento massimale. □

Il Lemma di Zorn è equivalente ad AC nella teoria MK:

Teorema 8.5. *Assumiamo l'enunciato del Teorema 8.4. Allora vale* AC.

Dimostrazione. Sia $\mathcal{A}$ una famiglia non vuota di insiemi non vuoti e sia $I = \bigcup \mathcal{A}$ così che $\mathcal{A} \subseteq \mathscr{P}(I)$. L'insieme

$$X = \{ p \subseteq \mathcal{A} \times I \mid p \text{ è una funzione e } \forall A \in \mathrm{dom}(p)\, (p(A) \in A) \}$$

ordinato per inclusione soddisfa le ipotesi del Lemma di Zorn, quindi c'è una $f \in X$ massimale. Se $\mathrm{dom}(f) \neq \mathcal{A}$ e $\bar{A} \in \mathcal{A} \setminus \mathrm{dom}(f)$, allora fissiamo un $\bar{a} \in \bar{A}$. Ma $f \cup \{(\bar{A}, \bar{a})\} \in X$, contro la massimalità di f. Quindi $f \colon \mathcal{A} \to I$ è una funzione di scelta. □

Capitolo II

La formalizzazione della semantica

9. Sintassi

Le teorie Zermelo-Frænkel (ZF) e Morse-Kelly (MK) sono formulate nel linguaggio della teoria degli insiemi LST che ha il simbolo di appartenenza $\in$ come unico simbolo non-logico. Gli altri simboli di LST sono quelli standard, presenti in ogni linguaggio sintattico del prim'ordine, cioè

- il simbolo di uguaglianza $=$,
- i connettivi logici $\neg$, $\vee$, $\wedge$, $\Rightarrow$ e $\Leftrightarrow$,
- il quantificatore esistenziale $\exists$ e quello universale $\forall$,
- le variabili $\mathsf{v}_0, \mathsf{v}_1, \dots$.

Come al solito le lettere $\mathsf{x}, \mathsf{y}, \mathsf{z}, \dots$ variamente decorate variano sulle variabili. Le formule di LST sono denotate da lettere greche minuscole quali φ, ψ, χ,.... Useremo inoltre le parentesi "(" e ")" per garantire l'unicità della lettura delle formule.

Osservazione 9.1. L'uso delle parentesi potrebbe essere evitato mediante la notazione polacca. Analogamente potremmo limitarci all'uso di un solo quantificatore e di un sistema minimo di connettivi, per esempio $\neg$ e $\vee$, oppure il simbolo di Sheffer o quello di Pierce. Tuttavia questi cambiamenti non migliorerebbero la matematica mentre appesantirebbero inutilmente la notazione.

Gli oggetti sintattici, quali LST, le sue formule, le teorie e—più in generale—tutti gli oggetti della metateoria saranno denotati mediante un carattere $\mathsf{sans\text{-}serif}$, nel tentativo di distinguerli dalle loro controparti insiemistiche definite formalmente all'interno di una teoria assiomatica quale ZF, MK, etc., come vedremo nella prossima sezione. È utile introdurre dei simboli per le usuali costruzioni nella metateoria: per esempio $\in$ denota la relazione di appartenenza ed $\mathbb{N}$ è l'insieme dei numeri naturali. Naturalmente, quando si parla di *insieme* nella metateoria si intende un ente concreto, quale $\mathbb{N}$, oppure Vbl, l'insieme delle variabili, o Form l'insieme delle formule di LST. L'idea di base è che i ragionamenti, le argomentazioni nella metateoria debbono essere il più possibile concreti, finitistici. Naturalmente la metateoria può (o meglio: dovrebbe) essere sviluppata all'interno di un sistema formale sufficientemente debole, quale PA o $\mathsf{ZF} - \mathsf{Inf}$, ma preferiamo adottare uno stile più informale e lasciare al lettore l'onere di questa formalizzazione.

Una variabile $\mathsf{v_n}$ è sostituibile a $\mathsf{v_m}$ in φ se

- $\mathsf{v_m}$ non è libera in φ, oppure
- nessuna occorrenza libera di $\mathsf{v_m}$ in φ è sotto l'influsso di un quantificatore $\exists\,\mathsf{v_n}$ oppure $\forall\,\mathsf{v_n}$.

Un **assioma logico** è una formula φ di LST che è una tautologia, oppure è della forma

(LAx 1) $\forall \mathsf{v_n}\,(\varphi \Rightarrow \psi) \Rightarrow (\varphi \Rightarrow \forall \mathsf{v_n}\,\psi)$, se $\mathsf{v_n}$ non occorre libera in φ,

(LAx 2) $\forall \mathsf{v_n}\,\varphi \Rightarrow \varphi[\mathsf{v_m}/\mathsf{v_n}]$ se $\mathsf{v_m}$ è sostituibile in φ a $\mathsf{v_n}$.

(LAx 3) $\mathsf{v_n} = \mathsf{v_n}$, per ogni n.

(LAx 4) $\mathsf{v_n} = \mathsf{v_m} \Rightarrow \big(\varphi[\mathsf{v_n}/\mathsf{v_k}] \Leftrightarrow \varphi[\mathsf{v_m}/\mathsf{v_k}]\big)$, se $\mathsf{v_n}$ e $\mathsf{v_m}$ sono sostituibili a $\mathsf{v_k}$ in φ.

Sia Γ un insieme di formule di LST. Una **derivazione da** Γ è una sequenza finita di formule $\langle \varphi_0, \dots, \varphi_\mathsf{n} \rangle$ tali che per $i = 0, \dots, \mathsf{n}$:

- φ_i è in Γ, oppure
- φ_i è un assioma logico, oppure
- φ_i è $\forall \mathsf{x}\,\varphi_j$, per qualche $j < i$ (regola di *generalizzazione* (Gen)),
- esistono $j, k < i$ tali che φ_j è $\varphi_k \Rightarrow \varphi_i$ (regola del *modus ponens* (MP)).

Diremo che φ è **derivabile da** Γ (ovvero che φ è un **teorema** di Γ), in simboli

$$\Gamma \vdash \varphi\,,$$

se esiste $\langle \varphi_0, \dots, \varphi_\mathsf{n} \rangle$, derivazione da Γ, tale che φ è φ_n. Quando Γ è formato da una sola formula ψ o quando Γ è vuoto, scriveremo, rispettivamente, $\psi \vdash \varphi$ e $\vdash \varphi$. Osserviamo che se $\Gamma \vdash \varphi$ e $\Gamma \subseteq \Gamma'$ implicano $\Gamma' \vdash \varphi$.

10. La formalizzazione della sintassi

Ad ogni numero naturale $\mathsf{n} = 0, 1, 2 \ldots$ della metateoria associamo (ricorsivamente in n) un elemento $\ulcorner \mathsf{n} \urcorner$ di ω ed una formula di LST con un'unica variabile libera

$$\mathsf{num}_{\mathsf{n}}(\mathsf{v}_0) \tag{25}$$

che è vera esattamente per il valore $\ulcorner \mathsf{n} \urcorner$. Al fine di semplificare la notazione scriveremo $0, 1, 2, \ldots$ in vece di $\ulcorner 0 \urcorner, \ulcorner 1 \urcorner, \ulcorner 2 \urcorner, \ldots$. Quindi $\mathsf{3}$ è il numero naturale tre pensato nella metateoria, mentre 3 è l'insieme $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$, cioè l'unico insieme x che soddisfa $\mathsf{num}_3(x)$.

Osservazione 10.1. Verrebbe voglia di scrivere che

$$\omega = \{ \ulcorner \mathsf{n} \urcorner \mid \mathsf{n} \in \mathbb{N} \} .$$

Tuttavia dobbiamo resistere a questa tentazione in quanto questa espressione è priva di significato, in quanto la supposta caratterizzazione di ω sul lato destro dell'uguaglianza non è una formula di LST. In un modello malfondato $\mathfrak{M} = \langle M, E \rangle$ della teoria degli insiemi è possibile avere numeri naturali non-standard, cioè elementi di $\omega^{\mathfrak{M}}$, la versione di ω del modello $\mathfrak{M}$, che non sono della forma $\ulcorner \mathsf{n} \urcorner$, per nessun $\mathsf{n} \in \mathbb{N}$. Dato che la scrittura $\ulcorner \mathsf{n} \urcorner$ può risultare pesante, scriveremo n al suo posto, quando questo non ingenera troppa confusione.

Descriviamo ora una codifica di LST all'interno di V_ω. Questa codifica è ben lungi dall'essere unica, dal momento che c'è molta libertà nello scegliere quale codice associare ai vari simboli, ma l'idea di base è che vogliamo associare un elemento $\ulcorner \mathsf{x} \urcorner$ di V_ω ad ogni oggetto x della metateoria. La variabile v_n è codificata come

$$\ulcorner \mathsf{v}_\mathsf{n} \urcorner = (0, \ulcorner \mathsf{n} \urcorner)$$

e $\mathrm{Vbl} \stackrel{\text{def}}{=} \{0\} \times \omega$ è l'insieme dei codici per variabili. Poniamo:

$$\begin{aligned} \ulcorner \neg \urcorner &= (1,0) & \ulcorner \vee \urcorner &= (1,1) \\ \ulcorner \wedge \urcorner &= (1,2) & \ulcorner \Rightarrow \urcorner &= (1,3) \\ \ulcorner \Leftrightarrow \urcorner &= (1,4) & \ulcorner \exists \urcorner &= (1,5) \\ \ulcorner \forall \urcorner &= (1,6) & \ulcorner = \urcorner &= (1,7) \\ \ulcorner \in \urcorner &= (1,8). \end{aligned}$$

La codifica $\ulcorner \varphi \urcorner$ di una formula φ di LST è una sequenza finita di elementi di V_ω (e quindi è ancora un elemento di quest'insieme) definita per induzione sulla complessità di φ come segue:

- $\ulcorner \mathsf{v}_\mathsf{n} \in \mathsf{v}_\mathsf{m} \urcorner = \langle (0, \ulcorner \mathsf{n} \urcorner), (1,8), (0, \ulcorner \mathsf{m} \urcorner) \rangle$

- $\ulcorner \mathsf{v_n} = \mathsf{v_m} \urcorner = \langle (0, \ulcorner \mathsf{n} \urcorner), (1,7), (0, \ulcorner \mathsf{m} \urcorner) \rangle$
- $\ulcorner (\neg \varphi) \urcorner = \langle (1,0), \ulcorner \varphi \urcorner \rangle$
- $\ulcorner (\varphi \circ \psi) \urcorner = \langle \ulcorner \varphi \urcorner, \ulcorner \circ \urcorner, \ulcorner \psi \urcorner \rangle$, dove $\circ$ è uno tra: $\vee$, $\wedge$, $\Rightarrow$, $\Leftrightarrow$.
- $\ulcorner (\exists \mathsf{v_n}\, \varphi) \urcorner = \langle (1,5), (0, \ulcorner \mathsf{n} \urcorner), \ulcorner \varphi \urcorner) \rangle$
- $\ulcorner (\forall \mathsf{v_n}\, \varphi) \urcorner = \langle (1,6), (0, \ulcorner \mathsf{n} \urcorner), \ulcorner \varphi \urcorner) \rangle$

L'insieme dei codici per le formule atomiche è

$$\begin{aligned} \mathrm{AtForm} &= \{ \langle x, (1,7), y \rangle, \langle x, (1,8), y \rangle \mid x, y \in \mathrm{Vbl} \} \\ &= \{ \langle x, \ulcorner = \urcorner, y \rangle, \langle x, \ulcorner \in \urcorner, y \rangle \mid x, y \in \mathrm{Vbl} \} \end{aligned}$$

La sua chiusura sotto le operazioni binarie

$$\begin{aligned} (x,y) &\mapsto \langle x, (1,1), y \rangle = \langle x, \ulcorner \vee \urcorner, y \rangle \\ (x,y) &\mapsto \langle x, (1,2), y \rangle = \langle x, \ulcorner \wedge \urcorner, y \rangle \\ (x,y) &\mapsto \langle x, (1,3), y \rangle = \langle x, \ulcorner \Rightarrow \urcorner, y \rangle \\ (x,y) &\mapsto \langle x, (1,4), y \rangle = \langle x, \ulcorner \Leftrightarrow \urcorner, y \rangle \end{aligned} \tag{26}$$

e l'operazione unaria

$$x \mapsto \langle (1,0), x \rangle = \langle \ulcorner \neg \urcorner, x \rangle \tag{27}$$

è l'insieme QFForm dei codici per le formule prive di quantificatori. Chiudendo AtForm o, equivalentemente, QFForm sotto (26), (27) e

$$\begin{aligned} x &\mapsto \langle (1,5), (0,n), x \rangle = \langle \ulcorner \exists \urcorner, (0,n), x \rangle \\ x &\mapsto \langle (1,6), (0,n), x \rangle = \langle \ulcorner \forall \urcorner, (0,n), x \rangle \end{aligned} \tag{28}$$

otteniamo l'insieme Form i cui elementi sono denotati da lettere minuscole greche (in grassetto) come $\boldsymbol{\varphi}$, $\boldsymbol{\psi}$, $\boldsymbol{\chi}$,.... Se $\boldsymbol{\varphi} = \langle (1,0), \boldsymbol{\psi} \rangle$ oppure $\boldsymbol{\varphi} = \langle \boldsymbol{\psi}, (1,i), \boldsymbol{\chi} \rangle$ con $i = 1, \dots, 4$ diremo che $\boldsymbol{\psi}$ e $\boldsymbol{\chi}$ sono componenti booleane di $\boldsymbol{\varphi}$. Consideriamo la relazione R su Form definita da $\boldsymbol{\psi}\ R\ \boldsymbol{\varphi}$ se e solo se:

- $\boldsymbol{\psi}$ è una componente booleana di $\boldsymbol{\varphi}$, oppure
- $\boldsymbol{\varphi} = \langle \ulcorner \exists \urcorner, (0,n), \boldsymbol{\psi} \rangle$, oppure
- $\boldsymbol{\varphi} = \langle \ulcorner \forall \urcorner, (0,n), \boldsymbol{\psi} \rangle$,

e sia $<_{\mathrm{subform}}$ la chiusura transitiva di R: è un ordine stretto, ben-fondato, che formalizza nei codici la nozione di "essere una sotto-formula".

La funzione

$$\mathrm{Fv} \colon \mathrm{Form} \to [\mathrm{Vbl}]^{<\omega}$$

associa ad ogni $\boldsymbol{\varphi}$ l'insieme finito $\mathrm{Fv}(\boldsymbol{\varphi})$ dei (codici delle) variabili libere di $\boldsymbol{\varphi}$. L'insieme dei codici degli enunciati è

$$\mathrm{Sent} = \{ \boldsymbol{\varphi} \in \mathrm{Form} \mid \mathrm{Fv}(\boldsymbol{\varphi}) = \emptyset \}$$

e le lettere $\boldsymbol{\sigma}$, $\boldsymbol{\tau}$ variano su quest'insieme. Notiamo che AtForm, QFForm e Form sono sottoinsiemi di V_ω. Quando non c'è pericolo di confusione scriveremo $\neg\boldsymbol{\varphi}$, $\boldsymbol{\varphi} \vee \boldsymbol{\psi}$, $\exists v_n\, \boldsymbol{\varphi}$,... al posto dei più corretti, ma barocchi, $\langle \ulcorner\neg\urcorner, \boldsymbol{\varphi}\rangle$, $\langle \boldsymbol{\varphi}, \ulcorner\vee\urcorner, \boldsymbol{\psi}\rangle$, $\langle \ulcorner\exists\urcorner, (0, n), \boldsymbol{\varphi}\rangle$, ...

Chiaramente, se φ è una formula di LST, allora $\ulcorner\varphi\urcorner \in \mathrm{Form}$, e la tentazione è quella di scrivere che

$$\begin{aligned} \mathrm{Form} &= \{ \ulcorner\varphi\urcorner \mid \varphi \text{ è una } \mathsf{LST}\text{-formula} \} . \\ &= \{ \ulcorner\varphi\urcorner \mid \varphi \in \mathsf{Form} \} , \end{aligned}$$

ma, come abbiamo già detto nell'Osservazione 10.1, questo tipo di "uguaglianze" che mescolano teoria e metateoria sono prive di significato.

Un insieme X di oggetti della metateoria si dice *ricorsivo* se c'è un metodo effettivo per determinare se una dato ente y è in X o meno. Esempi di insiemi ricorsivi sono l'insieme delle variabili di LST, l'insieme delle formule e degli enunciati di LST, l'insieme degli assiomi di ZF e di MK, etc.

Definizione 10.2. Sia T un sistema di assiomi, come MK o ZF. Un insieme X della metateoria è **rappresentabile** in T se c'è una $\varphi_{\mathsf{X}}(v_0)$, formula di LST, tale che per ogni oggetto y della metateoria

- se y è in X allora $\mathsf{T} \vdash \varphi_{\mathsf{X}}(\ulcorner \mathsf{y} \urcorner)$
- se y non è in X allora $\mathsf{T} \vdash \neg\varphi_{\mathsf{X}}(\ulcorner \mathsf{y} \urcorner)$.

Si ha il seguente:

Teorema 10.3. *Ogni insieme ricorsivo* X *della metateoria è rappresentabile in* ZF *e in* MK.

Se T è un sistema ricorsivo di assiomi,

$$\ulcorner \mathsf{T} \urcorner = \{ \boldsymbol{\sigma} \in \mathrm{Sent} \mid \varphi_{\mathsf{T}}(\boldsymbol{\sigma}) \} .$$

Osservazioni 10.4. (i) La definizione di $\ulcorner \mathsf{T} \urcorner$ dipende dalla definizione ricorsiva di T.

(ii) Se σ è in T allora $\ulcorner\sigma\urcorner \in \ulcorner \mathsf{T} \urcorner$, ma non è possibile dimostrare (o addirittura formulare correttamente) che $\ulcorner \mathsf{T} \urcorner = \{ \ulcorner\sigma\urcorner \mid \sigma \text{ è un enunciato di } \mathsf{T} \}$.

11. La verità in MK

Definizione 11.1. Se $M \neq \emptyset$ sia

$$\mathcal{A}^{(M)} = \{(\boldsymbol{\varphi}, f) \mid \boldsymbol{\varphi} \in \mathrm{Form} \ \wedge f \text{ è una funzione} \\ \mathrm{Fv}(\boldsymbol{\varphi}) \subseteq \mathrm{dom}\, f \in [\mathrm{Vbl}]^{<\omega} \ \wedge \mathrm{ran}\, f \subseteq M\}$$

e siano $\mathcal{A}^{(M)}_{\mathrm{At}}$ e $\mathcal{A}^{(M)}_{\mathrm{QF}}$ gli oggetti corrispondenti con $\boldsymbol{\varphi}$ in AtForm e QFForm, rispettivamente.

Osservazione 11.2. $\mathcal{A}^{(M)}$ è una classe propria se e solo se M è una classe propria. In ZF, se M è la classe definita dalla formula $\varphi(\mathsf{v_0}, \mathsf{v_1}, \ldots, \mathsf{v_n})$ e parametri $p_1, \ldots, p_n$, cioè,

$$M = \{\, x \mid \varphi(x, p_1, \ldots, p_n)\,\}$$

allora $\mathcal{A}^{(M)}$ è definita da una $\psi(\mathsf{v_0}, \mathsf{v_1}, \ldots, \mathsf{v_n})$ e parametri $p_1, \ldots, p_n$, e ψ è ottenuta in modo effettivo da φ. In MK la classe $\mathcal{A}^{(M)}$ è definita da una formula $\varphi(\mathsf{v_0}, \mathsf{v_1})$, usando M come parametro, cioè

$$\mathcal{A}^{(M)} = \{\, x \mid \varphi(x, M)\,\}\,.$$

Un discorso analogo vale per $\mathcal{A}^{(M)}_{\mathrm{At}}$ e per $\mathcal{A}^{(M)}_{\mathrm{QF}}$.

Supponiamo $E \subseteq M \times M$. Vogliamo definire la funzione

$$\mathrm{Sat} = \mathrm{Sat}^{\langle M,E\rangle} \colon \mathcal{A}^{(M)} \to 2$$

che formalizza la relazione di soddisfazione, cioè tale che

$$\mathrm{Sat}(\varphi, f) = 1 \quad \Leftrightarrow \quad \langle M, E\rangle \models \varphi[f]\,.$$

Cominciamo col definire Sat per sotto-classi di Form. La funzione di verità per AtForm è la mappa

$$T \colon \mathcal{A}^{(M)}_{\mathrm{At}} \to 2$$

definita da

$$\begin{aligned} T(\langle x, \ulcorner{=}\urcorner, y\rangle, f) = 1 \quad &\Leftrightarrow \quad f(y) = f(y) \\ T(\langle x, \ulcorner{\in}\urcorner, y\rangle, f) = 1 &\Leftrightarrow (f(x), f(y)) \in E \end{aligned} \tag{29}$$

Tale funzione T è solitamente indicata con $\mathrm{Sat}_{\mathrm{At}} = \mathrm{Sat}^{\langle M,E\rangle}_{\mathrm{At}}$.

Osservazione 11.3. Se M e E sono classi proprie, allora $\mathrm{Sat}_{\mathrm{At}}$ è una classe-funzione che non è un insieme. In MK è definita esplicitamente da una formula con parametri M ed E, mentre in ZF, $\mathrm{Sat}_{\mathrm{At}}$ è una classe definibile.

La funzione di verità per formule prive di quantificatori

$$\mathrm{Sat}_{\mathrm{QF}} = \mathrm{Sat}^{\langle M,E\rangle}_{\mathrm{QF}} \colon \mathcal{A}^{(M)}_{\mathrm{QF}} \to 2$$

è la mappa T che soddisfa (29) per le formule atomiche e

$$\begin{aligned} T(\neg\boldsymbol{\varphi}, f) &= 1 - T(\boldsymbol{\varphi}, f) \\ T(\boldsymbol{\varphi} \vee \boldsymbol{\psi}, f) &= \max\left(T(\boldsymbol{\varphi}, f), T(\boldsymbol{\psi}, f)\right) \\ T(\boldsymbol{\varphi} \wedge \boldsymbol{\psi}, f) &= \min\left(T(\boldsymbol{\varphi}, f), T(\boldsymbol{\psi}, f)\right) \\ T(\boldsymbol{\varphi} \Rightarrow \boldsymbol{\psi}, f) &= 1 \quad \text{se e solo se} \quad T(\boldsymbol{\varphi}, f) \leq T(\boldsymbol{\psi}, f) \\ T(\boldsymbol{\varphi} \Leftrightarrow \boldsymbol{\psi}, f) &= 1 \quad \text{se e solo se} \quad T(\boldsymbol{\varphi}, f) = T(\boldsymbol{\psi}, f) \end{aligned} \tag{30}$$

Questa definizione è basata su una ricorsione che ora andiamo ad esaminare: definiamo la relazione $\prec$ su $\mathcal{A}^{(M)}_{\mathrm{QF}}$

$$(\boldsymbol{\psi}, g) \prec (\boldsymbol{\varphi}, f)$$

se e solo se $\boldsymbol{\psi} <_{\mathrm{subform}} \boldsymbol{\varphi}$ e $g = f$ e $\boldsymbol{\varphi} \notin \mathrm{AtForm}$. La relazione $\prec$ è un ordine stretto, ben-fondato, regolare e $\mathcal{A}^{(M)}_{\mathrm{At}}$ è la classe degli elementi minimali. La funzione $\mathrm{Sat}^{\langle M,E\rangle}_{\mathrm{QF}}$ è definita per ricorsione su $\prec$ a partire da $\mathrm{Sat}^{\langle M,E\rangle}_{\mathrm{At}}$.

Definizione 11.4. Una funzione di verità è una mappa T con $\mathrm{dom}(T) \subseteq \mathcal{A}^{(M)}$ e $\mathrm{ran}(T) = 2$ che soddisfa:

(i) se $(\boldsymbol{\varphi}, f) \in \mathrm{dom}\, T$ e $\boldsymbol{\psi} <_{\mathrm{subform}} \boldsymbol{\varphi}$, allora $(\boldsymbol{\psi}, f) \in \mathrm{dom}\, T$;

(ii) se $(\boldsymbol{\varphi}, f) \in \mathrm{dom}\, T$, allora $(\boldsymbol{\varphi}, g) \in \mathrm{dom}\, T$ per ogni g tale che $(\boldsymbol{\varphi}, g) \in \mathcal{A}^{(M)}$;

(iii) $\mathrm{Sat}_{\mathrm{At}} \subseteq T$, e se $(\boldsymbol{\varphi}, f) \in \mathrm{dom}\, T$ e $\boldsymbol{\varphi} \notin \mathrm{AtForm}$ allora soddisfa (30) e
  (a) se $\boldsymbol{\varphi} = \exists v \boldsymbol{\psi}$, allora $T(\boldsymbol{\varphi}, f) = \sup_{a \in M} T(\boldsymbol{\psi}, f_{a/v})$,
  (b) se $\boldsymbol{\varphi} = \forall v \boldsymbol{\psi}$, allora $T(\boldsymbol{\varphi}, f) = \inf_{a \in M} T(\boldsymbol{\psi}, f_{a/v})$.

$\mathrm{Sat}_{\mathrm{At}}$ è la più piccola funzione di verità, quindi tutte le funzione di verità sono classi proprie, se M è una classe propria. Una facile induzione sulla complessità d $\boldsymbol{\varphi}$ dimostra che

Lemma 11.5. *Siano T e S funzioni di verità. Se $(\boldsymbol{\varphi}, f) \in \mathrm{dom}(T) \cap \mathrm{dom}(S)$ allora $T(\boldsymbol{\varphi}, f) = S(\boldsymbol{\varphi}, f)$. In particolare $T \cup S$ è una funzione di verità.*

Adotteremo la seguente notazione: se f è una funzione da un sottoinsieme finito di Vbl a valori in M, per $a \in M$ e $x \in \mathrm{Vbl}$ sia $f_{a/x}$ la funzione di dominio $\mathrm{dom}(f) \cup \{x\}$ definita da

$$f_{a/x}(v) = \begin{cases} a & \text{se } v = x, \\ f(v) & \text{altrimenti.} \end{cases}$$

Più in generale, se $a_1, \ldots, a_n \in M$ e $x_1, \ldots, x_n \in \mathrm{Vbl}$ allora $f_{a_1/x_1,\ldots,a_n/x_n}$ è la funzione di dominio $\mathrm{dom}(f) \cup \{x_1, \ldots, x_n\}$ definita induttivamente da

$$f_{a_1/x_1,\ldots,a_n/x_n} = (f_{a_1/x_1,\ldots,a_{n-1}/x_{n-1}})_{a_n/x_n}$$

Se T è una funzione di verità poniamo

$$
\begin{aligned}
T^{(\neg)} &= T \cup \{((\neg\boldsymbol{\varphi}, f), i) \mid (\boldsymbol{\varphi}, f) \in \operatorname{dom} T \text{ e } T(\boldsymbol{\varphi}, f) = 1 - i\} \\
T^{(\vee)} &= T \cup \{((\boldsymbol{\varphi} \vee \boldsymbol{\psi}, f), i) \mid (\boldsymbol{\varphi}, f), (\boldsymbol{\psi}, f) \in \operatorname{dom} T \text{ e} \\
&\qquad\qquad i = \max(T(\boldsymbol{\varphi}, f), T(\boldsymbol{\psi}, f))\} \\
T^{(\wedge)} &= T \cup \{((\boldsymbol{\varphi} \wedge \boldsymbol{\psi}, f), i) \mid (\boldsymbol{\varphi}, f), (\boldsymbol{\psi}, f) \in \operatorname{dom} T \text{ e} \\
&\qquad\qquad i = \min(T(\boldsymbol{\varphi}, f), T(\boldsymbol{\psi}, f))\} \\
T^{(\Rightarrow)} &= T \cup \{((\boldsymbol{\varphi} \Rightarrow \boldsymbol{\psi}, f), 1) \mid (\boldsymbol{\varphi}, f), (\boldsymbol{\psi}, f) \in \operatorname{dom} T \text{ e} \\
&\qquad\qquad T(\boldsymbol{\varphi}, f) \leq T(\boldsymbol{\psi}, f)\} \\
&\qquad \cup \{((\boldsymbol{\varphi} \Rightarrow \boldsymbol{\psi}, f), 0) \mid (\boldsymbol{\varphi}, f), (\boldsymbol{\psi}, f) \in \operatorname{dom} T \text{ e} \\
&\qquad\qquad T(\boldsymbol{\varphi}, f) > T(\boldsymbol{\psi}, f)\} \\
T^{(\Leftrightarrow)} &= T \cup \{((\boldsymbol{\varphi} \Leftrightarrow \boldsymbol{\psi}, f), 1) \mid (\boldsymbol{\varphi}, f), (\boldsymbol{\psi}, f) \in \operatorname{dom} T \text{ e} \\
&\qquad\qquad T(\boldsymbol{\varphi}, f) = T(\boldsymbol{\psi}, f)\} \\
&\qquad \cup \{((\boldsymbol{\varphi} \Leftrightarrow \boldsymbol{\psi}, f), 0) \mid (\boldsymbol{\varphi}, f), (\boldsymbol{\psi}, f) \in \operatorname{dom} T \text{ e} \\
&\qquad\qquad T(\boldsymbol{\varphi}, f) \neq T(\boldsymbol{\psi}, f)\} \\
T^{(\exists)} &= T \cup \big\{((\exists v \boldsymbol{\varphi}, f), i) \mid \exists g \supseteq f \big[(\boldsymbol{\varphi}, g) \in \operatorname{dom} T \text{ e} \\
&\qquad\qquad i = \sup\nolimits_{a \in M} T(\boldsymbol{\varphi}, g_{a/v})\big]\big\} \\
T^{(\forall)} &= T \cup \big\{((\forall v \boldsymbol{\varphi}, f), i) \mid \exists g \supseteq f \big[(\boldsymbol{\varphi}, g) \in \operatorname{dom} T \text{ e} \\
&\qquad\qquad i = \inf\nolimits_{a \in M} T(\boldsymbol{\varphi}, g_{a/v})\big]\big\}.
\end{aligned}
$$

È facile controllare che $T^{(\neg)}, \ldots, T^{(\forall)}$ sono funzioni di verità che estendono T. Infine sia $\mathrm{Sat}^{\langle M,E\rangle} \subseteq \mathcal{A}^{(M)} \times 2$ la classe

$$
\mathrm{Sat}^{\langle M,E\rangle} = \Big\{ \big((\boldsymbol{\varphi}, f), i\big) \mid \exists T \,\big[T \text{ una funzione di verità}, \\
(\boldsymbol{\varphi}, f) \in \operatorname{dom}(T) \text{ e } T(\boldsymbol{\varphi}, f) = i\big] \Big\}.
$$

La classe è ben-definita per l'assioma di comprensione, contiene ogni funzione di verità e, per il Lemma 11.5, è una funzione di verità. Osserviamo anche che Sat è la più grande funzione di verità e quindi coincide con $\mathrm{Sat}^{(\neg)}, \ldots, \mathrm{Sat}^{(\forall)}$. Una conseguenza immediata è che $\operatorname{dom} \mathrm{Sat} = \mathcal{A}^{\langle M,E\rangle}$.

Se $\boldsymbol{\varphi}(x_1, \ldots, x_n) \in \mathrm{Form}$ e $a_1, \ldots, a_n \in M$, allora $(\boldsymbol{\varphi}, f) \in \mathcal{A}^{(M)}$, dove $f = \{(x_1, a_1), \ldots, (x_n, a_n)\}$. Poniamo

$$\langle M, E\rangle \models \boldsymbol{\varphi}[a_1, \ldots, a_n]$$

se $\mathrm{Sat}^{\langle M,E\rangle}(\boldsymbol{\varphi}, f) = 1$. Se $\boldsymbol{\varphi} \in \mathrm{Sent}$, il valore $\mathrm{Sat}^{\langle M,E\rangle}(\boldsymbol{\varphi}, f)$ non dipende da f, quindi scriveremo $\mathrm{Sat}^{\langle M,E\rangle}(\boldsymbol{\varphi})$ e

$$\langle M, E\rangle \models \boldsymbol{\varphi} \qquad \text{se e solo se} \qquad \mathrm{Sat}^{\langle M,E\rangle}(\boldsymbol{\varphi}) = 1\,.$$

Se $S \subseteq \text{Sent}$ diremo che $\langle M, E\rangle$ è un modello di S, in simboli: $\langle M, E\rangle \models S$, se e solo se

$$\forall \boldsymbol{\sigma} \in S\,(\langle M, E\rangle \models \boldsymbol{\sigma})\,.$$

Teorema 11.6 (MK)**.** $\langle \mathrm{V}, \in\rangle \models \ulcorner \mathsf{ZF} \urcorner$.

La dimostrazione è una facile, ma noiosa verifica che viene lasciata al lettore.

Sia

$$\text{Prov}(\Gamma, \boldsymbol{\varphi}, p)$$

la formula di LST che asserisce che $p \in {}^{<\omega}\text{Form}$ è una derivazione di $\boldsymbol{\varphi}$ a partire da $\Gamma \subseteq \text{Form}$.

Proposizione 11.7. *Se* $S \subseteq \text{Form}$ *e* $\langle M, E\rangle \models S$*, allora*

$$\forall \boldsymbol{\sigma} \in \text{Sent}\ \exists p\,(\text{Prov}(S, \boldsymbol{\sigma}, p) \Rightarrow \langle M, E\rangle \models \boldsymbol{\sigma})\,.$$

Quindi, in particolare, ogni sistema di assiomi che ha un modello (insieme o classe) è consistente.

Corollario 11.8. $\mathsf{MK} \vdash \mathsf{CON}(\ulcorner \mathsf{ZF} \urcorner)$.

Quindi MK dimostra enunciati sui numeri naturali che non sono dimostrabili in ZF.

12. La gerarchia di Lévy

Una formula di LST è Δ_0, se tutti i suoi quantificatori (ammesso ne abbia) sono limitati, cioè della forma

$$\exists \mathsf{x}\,(\mathsf{x} \in \mathsf{y} \wedge \cdots) \qquad \text{o} \qquad \forall \mathsf{x}\,(\mathsf{x} \in \mathsf{y} \Rightarrow \cdots)\,.$$

Scriveremo $\exists \mathsf{x} \in \mathsf{y}\,\varphi$ e $\forall \mathsf{x} \in \mathsf{y}\,\varphi$ invece di $\exists \mathsf{x}\,(\mathsf{x} \in \mathsf{y} \wedge \varphi)$ e $\forall \mathsf{x}\,(\mathsf{x} \in \mathsf{y} \Rightarrow \varphi)$, rispettivamente. Ogni formula priva di quantificatori è quindi Δ_0 e l'insieme delle Δ_0 formule è chiuso sotto i connettivi e le quantificazioni limitate. Le formule Δ_0 si dicono anche Π_0 o Σ_0.

Le formule $\mathsf{s}\text{-}\Sigma_\mathsf{n}$ e $\mathsf{s}\text{-}\Pi_\mathsf{n}$ sono quelle che si costruiscono induttivamente dalle Δ_0 applicando un'opportuna alternanza di quantificatori:

- φ è $\mathsf{s}\text{-}\Sigma_\mathsf{n}$ se è della forma

$$\exists \mathsf{x}_1\, \forall \mathsf{x}_2 \ldots \mathsf{Q}_\mathsf{n} \mathsf{x}_\mathsf{n}\, \psi$$

  dove ψ è Δ_0 e Q_n è $\exists$ se n è dispari ed è $\forall$ se n è pari.
- φ è $\mathsf{s}\text{-}\Pi_\mathsf{n}$ se è della forma

$$\forall \mathsf{x}_1\, \exists \mathsf{x}_2 \ldots \mathsf{Q}_\mathsf{n} \mathsf{x}_\mathsf{n}\, \psi$$

  dove ψ è Δ_0 e Q_n è $\forall$ se n è dispari ed è $\exists$ se n è pari.

La lettera s nella definizione sopra sta a ricordarci che una formula è in $\mathsf{s}\text{-}\Sigma_n$ se e solo se ha una certa forma *sintattica*. Per esempio la negazione di una formula $\mathsf{s}\text{-}\Sigma_1$ *non è* in $\mathsf{s}\text{-}\Pi_1$ anche se è logicamente equivalente ad una formula in quella classe. È opportuno quindi considerare una classe più ampia di formule che sono logicamente equivalenti a formule $\mathsf{s}\text{-}\Sigma_n$. Più precisamente, possiamo definire un algoritmo che ad ogni φ di LST associa un'altra formula $\tilde{\varphi}$, tale che

$$(31)\qquad \begin{cases} \text{se } \varphi \text{ è } \Delta_0 \text{ allora } \tilde{\varphi} \text{ è } \varphi, \\ \tilde{\varphi} \text{ è in } \mathsf{s}\text{-}\Sigma_n, \\ \text{le variabili libere di } \tilde{\varphi} \text{ sono le stesse di } \varphi, \\ \text{la formula } \tilde{\varphi} \Leftrightarrow \varphi \text{ è derivabile nel calcolo dei predicati.} \end{cases}$$

La costruzione di $\tilde{\varphi}$ a partire da φ è essenzialmente l'algoritmo per trasformare una formula in forma normale prenessa con tre varianti:

(1) Innanzitutto non è necessario che la matrice della formula sia priva di quantificatori, ma basta che sia Δ_0.

(2) La formula $\tilde{\varphi}$ deve iniziare con un quantificatore esistenziale: questo può essere sempre ottenuto aggiungendo eventualmente un $\exists \mathsf{z}$ con z una variabile e che non compare nella formula.

(3) Infine richiediamo che i quantificatori si alternino—in altre parole si devono eliminare le espressioni del tipo "$\exists \mathsf{x}\, \exists \mathsf{y}$" e "$\forall \mathsf{x}\, \forall \mathsf{y}$". Ciò può essere fatto considerando che le formule

$$\exists \mathsf{x}\, \exists \mathsf{y}\, \psi \qquad \text{e} \qquad \forall \mathsf{x}\, \forall \mathsf{y}\, \psi$$

sono logicamente equivalenti a

$$\exists \mathsf{x}\, \forall \mathsf{z}\, \exists \mathsf{y}\, \psi \qquad \text{e} \qquad \forall \mathsf{x}\, \exists \mathsf{z}\, \forall \mathsf{y}\, \psi$$

dove z è una variabile diversa da x e y e che non compare in ψ.[1]

Esercizio 12.1. (i) Se φ è $\mathsf{s}\text{-}\Sigma_n$, allora $\tilde{\varphi}$ è φ.

(ii) Se φ è $\mathsf{s}\text{-}\Pi_n$, allora $\tilde{\varphi}$ è $\mathsf{s}\text{-}\Sigma_{n+1}$.

(iii) Se φ è $\mathsf{s}\text{-}\Sigma_n$, allora $\widetilde{\neg\varphi}$ è $\mathsf{s}\text{-}\Sigma_{n+1}$.

Definizione 12.2. Una formula φ si dirà Σ_n se e solo se $\tilde{\varphi}$ è in $\mathsf{s}\text{-}\Sigma_n$.

Osservazioni 12.3. (a) Le definizioni qui sopra possono sembrare un po' bizzarre—perché trasformare le formule in $\mathsf{s}\text{-}\Sigma_n$ e non in $\mathsf{s}\text{-}\Pi_n$? Il motivo, come vedremo, è che le formule $\mathsf{s}\text{-}\Sigma_n$ sono più maneggevoli delle $\mathsf{s}\text{-}\Pi_n$.

(b) Ogni formula di LST è in Σ_n, per qualche intero n calcolabile a partire dalla formula.

[1] Vedremo in seguito (Proposizione 12.8) che due quantificatori consecutivi dello stesso tipo possono essere trasformati in un singolo quantificatore.

Le classi $\mathsf{\Sigma_n}$ non sono chiuse per equivalenza logica—per esempio, una $\mathsf{\Sigma_1}$-formula φ è logicamente equivalente a $\varphi \wedge \exists \mathsf{x}\,(x = x)$, ma questa formula è $\mathsf{\Sigma_3}$. Per ovviare a questo inconveniente introduciamo un'ulteriore classificazione di formule.

Definizione 12.4. (a) Sia T un sistema ricorsivo di assiomi come, per esempio, ZF, MK,.... Diremo che una formula φ è $\mathsf{\Sigma_n^{(T)}}$ se è equivalente in T ad una s-$\mathsf{\Sigma_n}$-formula ψ, cioè

$$\mathsf{T} \vdash \varphi \Leftrightarrow \psi\,.$$

Equivalentemente, ψ può essere presa in $\mathsf{\Sigma_n}$.

Analogamente, una formula è $\mathsf{\Pi_n^{(T)}}$ se e solo se è equivalente in T ad una s-$\mathsf{\Pi_n}$-formula e solo se è equivalente in T ad una $\mathsf{\Pi_n}$-formula.

(b) Una formula è $\mathsf{\Delta_n^T}$ se è tanto $\mathsf{\Sigma_n^{(T)}}$ quanto $\mathsf{\Pi_n^{(T)}}$.

(c) Se T è vuoto scriveremo $\mathsf{\Sigma_n^{(\varnothing)}}$, $\mathsf{\Pi_n^{(\varnothing)}}$ e $\mathsf{\Delta_n^{(\varnothing)}}$.

Osservazioni 12.5. (i) Asserire che una formula φ di LST è in $\mathsf{\Sigma_n^{(T)}}$ (o in $\mathsf{\Pi_n^{(T)}}$) significa produrre una ψ in s-$\mathsf{\Sigma_n}$ (o in s-$\mathsf{\Pi_n}$) ed una derivazione $\mathsf{T} \vdash \varphi \Leftrightarrow \psi$.

(ii) Una formula è $\mathsf{\Sigma_n^{(\varnothing)}}$ se è logicamente equivalente ad una s-$\mathsf{\Sigma_n}$-formula.

(iii) Ogni s-$\mathsf{\Sigma_n}$-formula è $\mathsf{\Sigma_n}$-formula e ogni $\mathsf{\Sigma_n}$-formula è una $\mathsf{\Sigma_n^{(\varnothing)}}$-formula.

(iv) Le nozioni di $\mathsf{\Sigma_n}$-formula e $\mathsf{\Sigma_n^{(\varnothing)}}$-formula sono simili, ma ben distinte: la prima è ricorsiva, mentre la seconda è ricorsivamente enumerabile.

(v) φ è $\mathsf{\Sigma_n^{(T)}}$ se e solo se $\neg\varphi$ è $\mathsf{\Pi_n^{(T)}}$; φ è $\mathsf{\Pi_n^{(T)}}$ se e solo se $\neg\varphi$ è $\mathsf{\Sigma_n^{(T)}}$.

Spesso è utile considerare una generalizzazione dell'assioma del rimpiazzamento, nota come **Assioma di Collezione**. Come per il rimpiazzamento, ci sono due versioni: la prima è un singolo enunciato per MK (detto anche **Collezione Forte**) la seconda è uno schema di assiomi per ZF.

Assioma di Collezione (MK)**.** *Se R è una classe-relazione e A è un insieme, allora c'è un insieme B tale che*

$$\forall x \in A\, \exists y \in B\ (x, y) \in R\,.$$

Schema di Assiomi di Collezione (ZF)**.** *Per ogni formula di* LST

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

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

$$\forall A\, \forall z_1 \dots \forall z_n\, (\forall x\, (x \in A \Rightarrow \exists y\, \varphi(x, y, A, z_1, \dots, z_n)) \Rightarrow \\ \exists B\, \forall x \in A\, \exists y \in B\ \varphi(x, y, A, z_1, \dots, z_n).$$

Teorema 12.6. MK *dimostra l'Assioma di Collezione e* ZF *dimostra lo Schema di Assiomi di Collezione.*

Dimostrazione. Consideriamo solo il caso in MK, in quanto quello per ZF è simile. Sia $f\colon A \to \mathrm{Ord}$ definita da

$$f(x) = \min\{\alpha \mid \exists y \in \mathrm{V}_\alpha\ (x,y) \in R\}.$$

Per il Rimpiazzamento $\operatorname{ran} f$ è un insieme e sia $\beta = \sup \operatorname{ran} f$. Allora V_β è il B cercato. □

Corollario 12.7. *In* MK *l'Assioma di Rimpiazzamento può essere sostituito dall'Assioma di Collezione. In* ZF *lo Schema di Assiomi di Rimpiazzamento può essere sostituito dallo Schema di Assiomi di Collezione.*

Proposizione 12.8. (a) *Supponiamo che* T *contenga l'assioma della coppia.*
Se φ *e* ψ *sono* $\Sigma_n^{(\mathsf{T})}$*-formule allora* $\varphi \wedge \psi$ *e* $\varphi \vee \psi$ *sono* $\Sigma_n^{(\mathsf{T})}$*-formule.*
Se φ *e* ψ *sono* $\Pi_n^{(\mathsf{T})}$*-formule allora* $\varphi \wedge \psi$ *e* $\varphi \vee \psi$ *sono* $\Pi_n^{(\mathsf{T})}$*-formule.*

(b) *Supponiamo che* T *contenga l'assioma della coppia.*
Se φ *è in* $\Sigma_n^{(\mathsf{T})}$*, allora* $\exists x \in y\, \varphi$ *è in* $\Sigma_n^{(\mathsf{T})}$.
Se φ *è in* $\Pi_n^{(\mathsf{T})}$*, allora* $\forall x \in y\, \varphi$ *è in* $\Pi_n^{(\mathsf{T})}$.

(c) *Supponiamo che* T *contenga gli assiomi di estensionalità, della coppia e della collezione.*
Se φ *è una* $\Sigma_n^{(\mathsf{T})}$*-formula allora* $\forall x \in y\, \varphi$ *è una* $\Sigma_n^{(\mathsf{T})}$*-formula.*
Se φ *è una* $\Pi_n^{(\mathsf{T})}$*-formula allora* $\exists x \in y\, \varphi$ *è una* $\Pi_n^{(\mathsf{T})}$*-formula.*

Dimostrazione. (a) È sufficiente dimostrare il risultato per $\Sigma_n^{(\mathsf{T})}$, dato che il caso di $\Pi_n^{(\mathsf{T})}$ discende dall'Osservazione 12.5 Inoltre è sufficiente dimostrare che

(32) Se φ e ψ sono $\mathsf{s}\text{-}\Sigma_n$, allora $\varphi \wedge \psi$ è $\Sigma_n^{(\mathsf{T})}$.

Infatti, se φ' e ψ' sono $\Sigma_n^{(\mathsf{T})}$ prendiamo φ e ψ in $\mathsf{s}\text{-}\Sigma_n$ tali che $\mathsf{T} \vdash \varphi \Leftrightarrow \varphi'$ e $\mathsf{T} \vdash \psi \Leftrightarrow \psi'$: allora $\mathsf{T} \vdash (\varphi \wedge \psi) \Leftrightarrow (\psi' \wedge \varphi')$, per (32) $\varphi \wedge \psi$ è in $\Sigma_n^{(\mathsf{T})}$, da cui $\varphi' \wedge \psi'$ è in $\Sigma_n^{(\mathsf{T})}$

Dimostriamo (32) per induzione su n. Se $n = 0$, allora φ e ψ sono in Δ_0 e quindi $\varphi \wedge \psi$ è in Δ_0. Possiamo quindi supporre che $n > 0$ e che (32) valga per $n - 1$. Consideriamo due formule in $\mathsf{s}\text{-}\Sigma_n$

$$\begin{aligned} \varphi &: \quad \exists x_1\, \forall x_2 \dots Q_n\, x_n\, \alpha \\ \psi &: \quad \exists y_1\, \forall y_2 \dots Q_n\, y_n\, \beta \end{aligned}$$

con α e β in Δ_0. Possiamo supporre che le x_i siano distinte dalle y_j. Chiaramente

$$\varphi \land \psi \quad \Leftrightarrow \quad \exists x_1 \, \exists y_1 \, (\forall x_2 \ldots Q_n \, x_n \, \alpha \;\land\; \forall y_2 \ldots Q_n \, y_n \, \beta)$$

e per ipotesi induttiva e l'Osservazione 12.5(v),

$$\forall x_2 \ldots Q_n \, x_n \, \alpha \;\land\; \forall y_2 \ldots Q_n \, y_n \, \beta \quad \Leftrightarrow \quad \forall z_2 \ldots Q_n \, z_n \, \gamma$$

con γ in Δ_0. Per l'assioma della coppia

$$\begin{aligned} \varphi \land \psi \quad &\Leftrightarrow \quad \exists x_1 \, \exists y_1 \, (\forall z_2 \ldots Q_n \, z_n \, \gamma) \\ &\Leftrightarrow \quad \exists z_1 \, \forall z_2 \ldots Q_n \, z_n \, (\gamma \land x_1 \in z_1 \land y_1 \in z_1) \end{aligned}$$

Il caso della disgiunzione è lasciato al lettore.

(b) Se $n = 0$ non c'è nulla da dimostrare, quindi possiamo supporre che φ sia della forma $\exists z \, \psi$, con ψ in Π_{n-1}. Allora $\exists x \in y \, \varphi$ è equivalente a $\exists x \, \exists z \, (x \in y \land \psi)$, che è in $\Sigma_n^{(T)}$ per la parte (a). La chiusura di $\Pi_n^{(T)}$ sotto quantificazione universale limitata si dimostra in modo analogo.

(c) Per l'Osservazione 12.5 è sufficiente verificare che $\Sigma_n^{(T)}$ è chiuso per quantificazione universale limitata. Se $n = 0$ il risultato è banale, quindi possiamo supporre che φ sia $\exists z \, \psi$ con ψ in Π_{n-1}. Allora $\forall x \in y \, \exists z \, \psi$ è equivalente per collezione a $\exists w \, \forall x \in y \, \exists z \in w \, \psi$. Per ipotesi induttiva e la parte (b), $\forall x \in y \, \exists z \in w \, \psi$ è in $\Pi_{n-1}^{(T)}$, da cui segue il risultato. □

13. Formule codificate

Nella sezione 10 abbiamo introdotto AtForm, QFForm e Form, gli insiemi dei codici per la collezione delle formule atomiche, delle formule prive di quantificatori e di tutte le formule. Estendiamo ora questa codifica alle altre classi di formule che abbiamo visto.

Definizione 13.1. (a) L'insieme Δ_0- Form è la chiusura di AtForm o, equivalentemente, di QFForm sotto le funzioni (26), (27) e

$$\begin{aligned} &x \mapsto \left\langle \ulcorner\exists\urcorner, v, \left\langle \langle v, \ulcorner\in\urcorner, w\rangle, \ulcorner\land\urcorner, x\right\rangle\right\rangle \\ &x \mapsto \left\langle \ulcorner\forall\urcorner, v, \left\langle \langle v, \ulcorner\in\urcorner, w\rangle, \ulcorner\Rightarrow\urcorner, x\right\rangle\right\rangle \end{aligned} \tag{33}$$

con $v, w \in \mathrm{Vbl}$.

(b) Gli insiemi s-Σ_n- Form e s-Π_n- Form ($n > 0$) sono definiti simultaneamente per ricorsione:

$$\begin{aligned} \text{s-}\Sigma_n\text{- Form} &= \{ \langle \ulcorner\exists\urcorner, v, x\rangle \mid v \in \mathrm{Vbl} \;\land\; x \in \text{s-}\Pi_{n-1}\text{- Form} \} \\ \text{s-}\Pi_n\text{- Form} &= \{ \langle \ulcorner\forall\urcorner, v, x\rangle \mid v \in \mathrm{Vbl} \;\land\; x \in \text{s-}\Sigma_{n-1}\text{- Form} \} \end{aligned}$$

dove s-Σ_0- Form $=$ s-Π_0- Form $= \Delta_0$- Form.

(c) In analogia con la trasformazione $\varphi \mapsto \tilde{\varphi}$ (pag.70), è possibile definire una funzione

$$\mathrm{Form} \to \bigcup_{n\in\omega} \text{s-}\Sigma_n\text{- Form} \qquad \boldsymbol{\varphi} \mapsto \tilde{\boldsymbol{\varphi}}$$

che soddisfa gli analoghi di (31). Secondo la falsariga della Definizione 12.2 poniamo

$$\Sigma_n\text{- Form} = \{\, \boldsymbol{\varphi} \in \mathrm{Form} \mid \tilde{\boldsymbol{\varphi}} \in \text{s-}\Sigma_n\text{- Form} \,\}\,.$$

Osserviamo che c'è una formula di LST, $\vartheta(\mathsf{v}_0, \mathsf{v}_1)$, tale che

$$\text{s-}\Sigma_n\text{- Form} = \{\, x \in \mathrm{V}_\omega \mid \vartheta(n, x) \,\}\,,$$

uniformemente in $n \in \omega$. In particolare, per ogni n fissato della metateoria, possiamo definire l'insieme

$$\text{s-}\Sigma_{\mathsf{n}}\text{- Form} = \{\, x \in \mathrm{V}_\omega \mid \exists \mathsf{v}_0(\mathsf{num}_{\mathsf{n}}(\mathsf{v}_0) \wedge \vartheta(\mathsf{v}_0, x)) \,\}$$

dove $\mathsf{num}_{\mathsf{n}}$ è come in (25).

Sia

$$\mathrm{Prov}(\Gamma, \boldsymbol{\varphi}, p)$$

la formula di LST che asserisce che $p \in {}^{<\omega}\mathrm{Form}$ è una derivazione di $\boldsymbol{\varphi}$ a partire da $\Gamma \subseteq \mathrm{Form}$. Per ogni $T \subseteq \mathrm{Sent}$ sia

$$(34) \quad \Sigma_n^T\text{- Form} = \{\, \boldsymbol{\varphi} \in \mathrm{Form} \mid \exists \boldsymbol{\psi} \in \text{s-}\Sigma_n\text{- Form}\ \exists p\, \mathrm{Prov}(T, \boldsymbol{\varphi} \Leftrightarrow \boldsymbol{\psi}, p) \,\}$$

Osserviamo che la definizione è uniforme in n e T. Se nella formula (34) sostituiamo $\ulcorner \mathsf{T} \urcorner$ al posto di T, dove T è ricorsiva, allora l'insieme risultante Σ_n^{T}- Form è definito da una formula che ha soltanto n come parametro.

14. Verità in ZF

In questa sezione definiamo (in ZF) le funzioni di verità per Σ_{n}- Form, per ogni $\mathsf{n} = 1, 2, \ldots$. Innanzitutto estendiamo la Definizione 11.1 al caso in cui si usa s-Σ_{n}- Form al posto di Form. La classe corrispondente viene indicata con $\mathcal{A}_n^{(M)}$.

Una classe si dice $\Sigma_{\mathsf{n}}^{(\mathsf{ZF})}$ o $\Pi_{\mathsf{n}}^{(\mathsf{ZF})}$ con parametri se è definita da una formula $\Sigma_{\mathsf{n}}^{(\mathsf{ZF})}$ o $\Pi_{\mathsf{n}}^{(\mathsf{ZF})}$ con parametri. Una classe è $\Delta_{\mathsf{n}}^{(\mathsf{ZF})}$ con parametri se è tanto $\Sigma_{\mathsf{n}}^{(\mathsf{ZF})}$ quanto $\Pi_{\mathsf{n}}^{(\mathsf{ZF})}$ con parametri. Se non ci sono parametri, diremo semplicemente che la classe è $\Sigma_{\mathsf{n}}^{(\mathsf{ZF})}$ o $\Pi_{\mathsf{n}}^{(\mathsf{ZF})}$.

Esercizio 14.1. Verificare che "z è una coppia ordinata" è $\Delta_0^{(\mathsf{ZF})}$

Spesso scriveremo una classe come un predicato: per esempio la scrittura $A(x_1, \ldots, x_n)$ significa che $A \subseteq \mathrm{V}^{\mathsf{n}}$ e che $(x_1, \ldots, x_n) \in A$. Questa notazione è particolarmente utile quando si lavora con controimmagini di classi. Per esempio se F è una funzione e A una relazione $n+1$-aria, $A(F(x), y_1, \dots, y_n)$ denota la classe

$$\{ (z, y) \mid \exists x \, (z = F(x) \wedge (z, y) \in A) \}$$

Se F e A sono $\Delta_1^{(\mathsf{ZF})}$, allora anche $A(F(x), y_1, \dots, y_n)$ lo è, dato che

$$\begin{aligned} A(F(x), y_1, \dots, y_n) &\Leftrightarrow \exists z \, ((x, z) \in F \wedge (z, y_1, \dots, y_n) \in A) \\ &\Leftrightarrow \forall z \, ((x, z) \in F \Rightarrow (z, y_1, \dots, y_n) \in A) \, , \end{aligned}$$

dove nella prima equazione si usa che F e A sono $\Sigma_1^{(\mathsf{ZF})}$, nella seconda equazione si usa che F e A sono $\Pi_1^{(\mathsf{ZF})}$. Come corollario si ottiene:

Corollario 14.2. *La composizione di funzioni* $\Delta_1^{(\mathsf{ZF})}$ *è* $\Delta_1^{(\mathsf{ZF})}$.

Lemma 14.3. *Supponiamo* $F \colon D \to \mathrm{V}$ *sia una classe-funzione* $\Sigma_i^{(\mathsf{ZF})}$ *(con parametri) e* D *una classe* $\Delta_1^{(\mathsf{ZF})}$ *(con parametri). Allora* F *è* $\Delta_1^{(\mathsf{ZF})}$ *(con parametri).*

Dimostrazione. Se $\mathsf{n} = \mathsf{0}$ non c'è nulla da dimostrare, quindi supponiamo $\mathsf{n} > \mathsf{0}$. Dobbiamo verificare che la classe complemento $\mathrm{V} \setminus F$ è $\Sigma_{\mathsf{n}}^{(\mathsf{ZF})}$ (con parametri). Ma $z \in \mathrm{V} \setminus F$ se e solo se

(1) z non è una coppia ordinata, oppure
(2) $\exists x \, \exists y \, (z = (x, y) \wedge x \notin D)$, oppure
(3) $\exists x \, \exists y \, \exists y' \, \exists z' \, (z = (x, y) \wedge x \in D \wedge (x, y') = z' \wedge z' \in F \wedge y \neq y')$,

quindi $\mathrm{V} \setminus F$ è definita dalla disgiunzione delle formule in (1), (2) e (3). La formula in (1) è $\Delta_0^{(\mathsf{ZF})}$ per l'Esercizio 14.1. La formula "$x \notin D$" è $\Delta_{\mathsf{n}}^{(\mathsf{ZF})}$ (con parametri), quindi la formula in (2) è $\Sigma_{\mathsf{n}}^{(\mathsf{ZF})}$ (con parametri). La formula in (3) è anche $\Sigma_{\mathsf{n}}^{(\mathsf{ZF})}$ (con parametri). Questo dimostra il Lemma. □

A. Soddisfazione per formule Δ_0. Supponiamo d'ora in poi che E sia regolare, vale a dire: per ogni $x \in M$ la sua **estensione**

$$\mathrm{ext}(x) = \mathrm{ext}^{M,E}(x) = \{ y \in M \mid (y, x) \in E \}$$

è un insieme. Chiaramente, se E è la relazione $\in$ e M è transitiva, allora $\mathrm{ext}(x) = x$. Possiamo anche definire un analogo della chiusura transitiva: per $x \in M$, sia

$$\begin{aligned} \mathrm{ext}_0(x) &= \mathrm{ext}(x) \\ \mathrm{ext}_{n+1}(x) &= \bigcup \{ \mathrm{ext}(y) \mid y \in \mathrm{ext}_n(x) \} \\ \mathrm{ext}_\omega(x) &= \bigcup_n \mathrm{ext}_n(x) \, . \end{aligned}$$

Fissiamo $(\varphi, f) \in \mathcal{A}_0^{(M)}$. Sia

$$\mathcal{E}(\varphi, f) = \bigcup \{ \operatorname{ext}_\omega(f(v)) \mid v \in \operatorname{Fv}(\varphi) \} .$$

È un insieme, dato che E è regolare. Sia $\lhd$ la relazione su $\mathcal{A}_0^{(M)}$ definita come segue: $(\psi, g) \lhd (\varphi, f)$ se e solo se

- φ è $\exists v\,(v \in x \wedge \psi)$ o $\forall v\,(v \in x \Rightarrow \psi)$ e $g = f_{a/v}$ per qualche $a \in \mathcal{E}(\varphi, f)$, oppure
- ψ è una componente booleana di φ e $f = g$.

Allora $\lhd$ è ben-fondata, e poiché $(\psi, g) \lhd (\varphi, f)$ implica che $\operatorname{ran} g \subseteq \mathcal{E}(\varphi, f)$, ne segue che $\lhd$ è regolare. Possiamo quindi applicare il teorema di ricorsione e definire la funzione di verità

$$\operatorname{Sat}_0^{\langle M,E\rangle} \colon \mathcal{A}_0^{(M)} \to 2$$

come l'unica funzione $T \colon \mathcal{A}_0^{(M)} \to 2$ che soddisfa (29), (30) e

$$\begin{aligned} &T\big(\exists v\,(v \in x \wedge \varphi)\,, f\big) = \\ &\qquad \max\big\{T\big(v \in x \wedge \varphi, f_{a/v}\big) \mid a \in \mathcal{E}\big(\exists v\,(v \in x \wedge \varphi)\,, f\big)\big\} \\ &T\big(\forall v\,(v \in x \Rightarrow \varphi)\,, f\big) = \\ &\qquad \min\big\{T\big(v \in x \Rightarrow \varphi, f_{a/v}\big) \mid a \in \mathcal{E}\big(\forall v\,(v \in x \Rightarrow \varphi)\,, f\big)\big\} \end{aligned} \tag{35}$$

Poiché $\operatorname{Sat}_{\mathrm{QF}}^{\langle M,E\rangle}$ e $\operatorname{Sat}_0^{\langle M,E\rangle}$ sono definite tramite una ricorsione, dal Lemma 14.3 discende il

Corollario 14.4. *Se M ed E sono $\Delta_1^{(\mathsf{ZF})}$, allora anche $\operatorname{Sat}_{\mathrm{QF}}^{\langle M,E\rangle}$ e $\operatorname{Sat}_0^{\langle M,E\rangle}$ sono $\Delta_1^{(\mathsf{ZF})}$.*

B. Soddisfazione per formule Σ_{n} in ZF. Nella metateoria fissiamo un naturale $\mathsf{n} \in \mathbb{N}$. Definiremo in ZF la funzione di verità per s-Σ_{n}-Form. Sia $\varphi \in$ s-Σ_{n}-Form, cioè

$$\varphi = \exists v_1\, \forall v_2 \, \dots \mathsf{Q} v_{\mathsf{n}} \psi$$

con $\psi \in \Delta_0$-Form e

$$\mathsf{Q} = \begin{cases} \exists & \text{se } \mathsf{n} \text{ è dispari,} \\ \forall & \text{se } \mathsf{n} \text{ è pari.} \end{cases}$$

Per ogni φ come sopra, la n-upla $(v_1, \dots, v_{\mathsf{n}})$ di elementi di Vbl e la $\psi \in \Delta_0$-Form sono univocamente determinati. Definiamo la funzione

$$\Phi_{\mathsf{n}} \colon \mathcal{A}_{\mathsf{n}}^{(M)} \times \underbrace{M \times \cdots \times M}_{\mathsf{n}\ \text{volte}} \to \mathcal{A}_0^{(M)}$$

ponendo $\Phi_{\mathsf{n}}((\boldsymbol{\varphi}, f), a_1, \dots, a_{\mathsf{n}}) = (\boldsymbol{\psi}, f_{a_1/v_1,\dots,a_{\mathsf{n}}/v_{\mathsf{n}}})$, dove $v_1, \dots, v_{\mathsf{n}}$ e $\boldsymbol{\psi}$ sono come sopra. Siamo quindi in grado di definire la funzione $\mathrm{Sat}_{\mathsf{n}}^{\langle M,E\rangle} : \mathcal{A}_{\mathsf{n}}^{(M)} \to 2$

$$
\begin{aligned}
&\mathrm{Sat}_{\mathsf{n}}^{\langle M,E\rangle}(\boldsymbol{\varphi}, f) = 1 \quad \text{se e solo se} \\
&\quad \exists a_1 \in M \, \forall a_2 \in M \dots \mathsf{Q} a_{\mathsf{n}} \in M \left(\mathrm{Sat}_0^{\langle M,E\rangle}(\Phi_{\mathsf{n}}((\boldsymbol{\varphi}, f), a_1, \dots, a_{\mathsf{n}})) = 1 \right) \\
&\qquad \exists a_1 \in M \, \forall a_2 \in M \dots \mathsf{Q} a_{\mathsf{n}} \in M \left(\mathrm{Sat}_0^{\langle M,E\rangle}(\boldsymbol{\psi}, f_{a_1/v_1,\dots,a_{\mathsf{n}}/v_{\mathsf{n}}}) = 1 \right).
\end{aligned}
$$

Ricordiamo che la funzione $\mathrm{Form} \to \bigcup_n \text{s-}\Sigma_n\text{-}\mathrm{Form}$, $\boldsymbol{\varphi} \mapsto \tilde{\boldsymbol{\varphi}}$, è stata introdotta nella Definizione 13.1(c). Sia

$$
\tilde{\mathcal{A}}_n^{(M)} = \left\{ (\boldsymbol{\varphi}, f) \mid (\tilde{\boldsymbol{\varphi}}, f) \in \mathcal{A}_n^{(M)} \right\}.
$$

Definizione 14.5. Se $(\boldsymbol{\varphi}, f) \in \mathcal{A}_{\mathsf{n}}^{(M)}$, poniamo

$$
\langle M, E\rangle \models_{\mathsf{n}} \boldsymbol{\varphi}[f] \qquad \text{se e solo se} \qquad \mathrm{Sat}_{\mathsf{n}}^{\langle M,E\rangle}(\tilde{\boldsymbol{\varphi}}, f) = 1 .
$$

Se $\boldsymbol{\varphi}(x_1, \dots, x_{\mathsf{m}}) \in \Sigma_{\mathsf{n}}\text{-}\mathrm{Form}$ e $a_1, \dots, a_{\mathsf{m}} \in M$, sia $f \colon \{x_1, \dots, x_{\mathsf{m}}\} \to \{a_1, \dots, a_{\mathsf{m}}\}$, $f(x_i) = a_i$ $(i = 1, \dots, \mathsf{m})$ e poniamo

$$
\langle M, E\rangle \models_{\mathsf{n}} \boldsymbol{\varphi}[a_1, \dots, a_{\mathsf{m}}]
$$

se $\langle M, E\rangle \models_{\mathsf{n}} \boldsymbol{\varphi}[f]$.

Lemma 14.6. *Supponiamo* $\mathsf{n} = 1, 2, \dots$. *Se M e E sono* $\Delta_1^{(\mathsf{ZF})}$, *la classe*

$$
\left\{ (\boldsymbol{\varphi}, f) \in \tilde{\mathcal{A}}_{\mathsf{n}}^{(M)} \mid \langle M, E\rangle \models_{\mathsf{n}} \boldsymbol{\varphi}[f] \right\}
$$

è $\Sigma_{\mathsf{n}}^{(\mathsf{ZF})}$.

Dimostrazione. Si verifica facilmente che $\tilde{\mathcal{A}}_{\mathsf{n}}^{(M)}$ è $\Delta_1^{(\mathsf{ZF})}$ e quindi per i Corollari 14.2 e 14.4, la funzione $\tilde{\mathcal{A}}_{\mathsf{n}}^{(M)} \times M \times \cdots \times M \to 2$

$$
((\boldsymbol{\varphi}, f), a_1, \dots, a_{\mathsf{n}}) \mapsto \mathrm{Sat}_0^{\langle M,E\rangle} \left(\Phi_{\mathsf{n}}((\tilde{\boldsymbol{\varphi}}, f), a_1, \dots, a_{\mathsf{n}})\right)
$$

è $\Delta_1^{(\mathsf{ZF})}$. Il risultato discende immediatamente dalla definizione di $\mathrm{Sat}_{\mathsf{n}}^{\langle M,E\rangle}$. □

L'insieme degli enunciati Σ_{n} veri in V

$$
\mathrm{True}_{\mathsf{n}} \stackrel{\text{def}}{=} \{ \boldsymbol{\sigma} \in \mathrm{Sent} \mid \langle \mathrm{V}, \in\rangle \models_{\mathsf{n}} \boldsymbol{\sigma} \}
$$

è Σ_{n}-completo.

Usando la nozione di soddisfazione per formule Σ_{n} è possibile definire rigorosamente che cosa significa che una classe transitiva M è una Σ_{n}-sottostruttura di V:

$$
\forall \boldsymbol{\sigma} \in \Sigma_{\mathsf{n}}\text{-}\mathrm{Form}\, (\langle M, \in\rangle \models_{\mathsf{n}} \boldsymbol{\sigma} \;\Leftrightarrow\; \langle \mathrm{V}, \in\rangle \models_{\mathsf{n}} \boldsymbol{\sigma}) .
$$

Indice analitico