Elementi di Logica Matematica
Versione del 15 dicembre 2014

Alessandro Andretta
alessandro.andretta@unito.it

Indice

Preliminari

Notazione

La notazione $x \in A$ significa che l'elemento x **appartiene all'insieme** A. L'insieme degli x che hanno la proprietà P si indica con $\{x \mid P(x)\}$. Se ogni elemento di A è contenuto in B diremo che A **è incluso in** B e scriveremo $A \subseteq B$; questo non preclude che A e B coincidano — se invece vogliamo che A e B siano distinti, scriveremo $A \subset B$. L'**insieme vuoto** è denotato da $\emptyset$. L'**insieme dei sottoinsiemi di** X è $\mathscr{P}(X)$.

L'**unione** di due insiemi A e B è l'insieme $A \cup B$ degli enti che stanno in A o in B, l'**intersezione** è l'insieme $A \cap B$ degli enti che stanno tanto in A quanto in B, la **differenza** è l'insieme $A \setminus B$ degli enti che stanno in A ma non in B, la **differenza simmetrica** è l'insieme $A \triangle B$ degli enti che stanno in $A \cup B$ ma non in $A \cap B$.

L'**intersezione di una famiglia** $\{A_i \mid i \in I\}$ di insiemi si scrive $\bigcap_{i \in I} A_i$ o anche $\bigcap \{A_i \mid i \in I\}$ ed è la collezione degli enti che appartengono ad *ogni* A_i; analogamente, l'**unione della famiglia** $\{A_i \mid i \in I\}$ è l'insieme degli enti che appartengono a *qualche* A_i e lo si denota con $\bigcup_{i \in I} A_i$ o con $\bigcup \{A_i \mid i \in I\}$.

Il **prodotto cartesiano** di due insiemi A e B è l'insieme $A \times B$ formato da tutte le coppie ordinate (a, b) con $a \in A$ e $b \in B$.

Talvolta è necessario considerare l'**unione disgiunta** $A \cup B$ di due insiemi A, B: questa è usualmente definita da $\{0\} \times A \cup \{1\} \times B$. L'unione disgiunta $\cup_{i \in I} A_i$ degli insiemi A_i è definita come $\bigcup_{i \in I} \{i\} \times A_i$.

Una **relazione** è un insieme di coppie ordinate; se $f \subseteq A \times B$ è una relazione tale che per ogni $a \in A$ esiste un unico $b \in B$ tale che $(a, b) \in f$, diremo che f è una **funzione** da A in B, e useremo la notazione $f \colon A \to B$.

Se $f\colon A \to B$ e $a \in A$, l'unico elemento $b \in B$ per cui $(a,b) \in F$ lo si indica con $f(a)$. Una **funzione parziale** da A in B è una $f\colon A' \to B$ con $A' \subseteq A$. Quando si deve considerare una funzione (parziale) f da A in B come sottoinsieme del prodotto cartesiano $A \times B$, parleremo del suo **grafo** $\mathrm{Gr}(f) = \{(a,b) \in A \times B \mid (a,b) \in f\}$; resta il fatto che *non c'è differenza tra una funzione e il suo grafo*. L'insieme di tutte le funzioni da A in B è indicato con B^A. Diremo che $f \in B^A$ è iniettiva se $f(a_1) \neq f(a_2)$ per ogni scelta di $a_1, a_2 \in A$ distinti; f è suriettiva se per ogni $b \in B$ c'è un $a \in A$ tale che $f(a) = b$; f è biettiva se è tanto iniettiva quanto suriettiva. Talvolta useremo la notazione $f\colon A \rightarrowtail B$ per indicare che la funzione f è iniettiva, mentre $f\colon A \twoheadrightarrow B$ significa che è suriettiva. Se $f\colon A \to B$, e $A_0 \subseteq A$ e $B_0 \subseteq B$, allora $f[A_0] \stackrel{\text{def}}{=} \{f(x) \mid x \in A_0\}$ e $f^{-1}[B_0] \stackrel{\text{def}}{=} \{x \in A \mid f(x) \in B_0\}$. Se $f\colon A \to B$ e $A' \subseteq A$, indichiamo con $f \restriction A'$ la restrizione di f all'insieme A', con $\mathrm{ran}(f) = f[A]$ l'immagine di f, e con $\mathrm{dom}(f)$ il dominio di f. La **funzione identica** su un insieme A è la funzione $\mathrm{id}_A\colon A \to A$ definita da $\mathrm{id}_A(a) = a$ per ogni $a \in A$.

Se E è una **relazione di equivalenza** su un insieme A indichiamo con $[a]_E$ la classe di equivalenza dell'elemento $a \in A$; quando la relazione E è chiara dal contesto scriveremo semplicemente $[a]$. L'**insieme quoziente** è denotato con A/E.

La notazione per gli insiemi numerici è standard: $\mathbb{N}$ è l'insieme dei numeri naturali incluso lo 0, $\mathbb{Z}$ è l'insieme degli interi relativi, $\mathbb{Q}$ è l'insieme dei numeri razionali, $\mathbb{R}$ è l'insieme dei numeri reali, $\mathbb{C}$ è l'insieme dei numeri complessi. I simboli $\mathbb{R}_+$ e $\mathbb{R}_-$ denotano, rispettivamente, l'insieme dei reali positivi, cioè strettamente maggiori di 0, e l'insieme dei reali negativi, cioè strettamente minori di 0. Più in generale poniamo $\mathbb{R}_{<a} = \{x \in \mathbb{R} \mid a < x\}$ e $\mathbb{R}_{>a} = \{x \in \mathbb{R} \mid a > x\}$ e analogamente se al posto di $<$ usiamo la relazione $\leq$. Un analogo discorso vale se al posto di $\mathbb{R}$ usiamo gli insiemi $\mathbb{N}$, $\mathbb{Z}$ o $\mathbb{Q}$. Se a, b, c sono interi, diremo che a e b sono congruenti modulo c, in simboli $a \equiv b \mod c$, se $a - b$ è divisibile per c. L'anello delle classi di resto di $\mathbb{Z}$ modulo c è indicato con $\mathbb{Z}/c\mathbb{Z}$.

Un **insieme è finito** se è in biezione con $\{0, \ldots, n-1\}$ per qualche $n \in \mathbb{N}$; se $n = 0$ allora l'insieme in questione è $\emptyset$, l'insieme vuoto. Un insieme che non sia finito si dice **infinito**. Un insieme è **numerabile** se è finito, oppure è in biezione con $\mathbb{N}$.

Capitolo I

Introduzione alla logica matematica

1. Sistemi assiomatici

La matematica si differenzia dalle altre discipline scientifiche per il metodo con cui vengono stabiliti i nuovi risultati. Non è sufficiente — e, nella stragrande maggioranza dei casi, neppure necessario — effettuare misurazioni, esperimenti o simulazioni. Nessun esperimento può decidere se $\sqrt{2}$ sia o meno un numero razionale, dato che $\mathbb{Q}$ e $\mathbb{R} \setminus \mathbb{Q}$ sono densi nella retta reale. Per essere certi che $\sqrt{2}$ non è razionale, è necessario dimostrare che non esistono numeri interi n e m tali che $n^2 = 2m^2$. Naturalmente, in alcuni casi, gli esempi forniscono *indizi* sulla verità o meno di una congettura. Per esempio è stato verificato che nell'espansione decimale di lunghezza $3 \cdot 10^7$ di π, le cifre, le coppie di cifre, le triple di cifre, ecc. sono distribuite in modo molto uniforme [**Bai88**], e questi computi indubbiamente contribuiscono a rafforzare la congettura che π sia un numero normale, cioè ogni sequenza di cifre di lunghezza k compare con frequenza 10^{-k}, per ogni $k \geq 1$. Ma questi computi non ci consentono di stabilire la verità o la falsità della congettura (a tutt'oggi aperta) che π sia normale. Anzi: a volte, l'evidenza numerica può essere fuorviante, come mostrano i seguenti esempi.

- Fermat congetturò che tutti i numeri della forma $2^{2^n} + 1$ fossero primi, dopo aver verificato la congettura per $n \leq 4$, ma Eulero refutò questa congettura verificando che $2^{2^5} + 1 = 4292967297 = 641 \times 6700417$.
- Se $p < 1000$ è primo allora $2^{p-1} - 1$ non è divisibile per p^2, tuttavia 1093 è primo ma $2^{1092} - 1$ è divisibile per 1093^2.

- La proprietà $P(n)$ definita da "$n^2 - 79n + 1601$ è primo" è vera per $1 \leq n < 80$ ma è falsa per $n = 80$ dato che $80^2 - 79 \times 80 + 1601 = 1681 = 41^2$.
- L'equazione di Pell è un'equazione della forma $x^2 - ky^2 = 1$, con $k > 1$ numero naturale. Per un teorema di Lagrange l'equazione di Pell ha infinite soluzioni intere se k non è un quadrato. In particolare ci sono infiniti interi n per cui $991n^2 + 1$ è un quadrato perfetto, ma il minimo numero siffatto è

$$12055735790331359447442538767 \approx 10^{29}.$$

  Quindi l'evidenza numerica sembrerebbe corroborare la falsa congettura "$991n^2 + 1$ non è mai un quadrato".
- Littlewood dimostrò nel 1914 che la funzione $\pi(x) - \mathrm{Li}(x)$ cambia segno infinite volte, dove $\pi(x)$ è il numero di primi $\leq x$ e $\mathrm{Li}(x) = \int_2^x \frac{\mathrm{d}t}{\ln(t)}$. Tuttavia l'evidenza numerica sembrava suggerire che $\pi(x) < \mathrm{Li}(x)$ per ogni x; infatti il primo x per cui $\pi(x) > \mathrm{Li}(x)$ è immenso — si stima che x sia dell'ordine di 10^{316}.

Una **dimostrazione** è un ragionamento che a partire da alcune affermazioni iniziali ci permette di concludere il risultato desiderato. Le affermazioni iniziali si chiamano **assiomi** o **postulati**, e variano a seconda del settore della matematica in cui si lavora. I risultati ottenuti mediante dimostrazioni si dicono **teoremi** e questi devono essere dedotti dagli assiomi in modo assolutamente preciso, senza ricorrere a principi estranei. Per esempio, non possiamo dire di aver dimostrato un nuovo teorema in geometria Euclidea se nella dimostrazione usiamo argomentazioni basate sulla nostra intuizione delle figure, o su risultati di altre parti della matematica. Quindi le dimostrazioni sono delle successioni di affermazioni, ciascuna delle quali è un assioma oppure è ottenuta dalle affermazioni precedenti mediante le **regole logiche**. Queste, come vedremo nella Sezione 4.A e più diffusamente nel Capitolo VI, sono le stesse per tutte le teorie matematiche.

Vediamo alcuni esempi di assiomatizzazioni in matematica.

Geometria. Euclide nel III secolo avanti Cristo sviluppò la geometria a partire da alcune nozioni non definite (punto, retta, piano, ecc.) e da cinque assiomi, oggi noti come postulati di Euclide. Questo sistema assiomatico, che va sotto il nome di geometria euclidea, fu esposto da Euclide nella sua opera monumentale, gli *Elementi*. Questo libro è stato considerato per molti secoli l'archetipo del ragionamento matematico rigoroso, e soltanto nel diciannovesimo secolo è stato sottoposto ad una attenta analisi logica per opera di Hilbert.

Aritmetica e Analisi. Nella seconda metà dell'Ottocento, i fondamenti dell'analisi matematica furono riformulati in modo rigoroso. Questo lavoro noto come aritmetizzazione dell'analisi culminò con l'opera di Weierstraß.

Le proprietà elementari dei numeri naturali possono essere dedotte da degli assiomi introdotti da Dedekind e Peano alla fine dell' ottocento — il sistema assiomatico così ottenuto è noto come **aritmetica di Peano** (si veda la Sezione 7.E).

Insiemi. Anche la teoria degli insiemi, introdotta da Dedekind e Cantor alla fine dell'Ottocento, può (anzi: deve!) essere sviluppata a partire da dei postulati. L'assiomatizzazione più usata è dovuta a Zermelo e Frænkel. Nel Capitolo IV svilupperemo la teoria degli insiemi a partire da un sistema assiomatico leggermente differente, dovuto a Kelley e Morse.

Algebra e Topologia. Il metodo assiomatico è una caratteristica saliente dell'algebra e della topologia — i gruppi, gli anelli, i campi, gli spazi topologici ... sono definiti a partire da assiomi e le loro proprietà vengono stabilite in generale, senza considerare esempi specifici.

Questi esempi, piuttosto diversi tra loro, rientrano in due grandi famiglie:

- le assiomatizzazioni *classiche* (la geometria euclidea, l'aritmetica di Peano e la trattazione assiomatica degli insiemi), introdotte per descrivere certi mondi matematici specifici (il piano e lo spazio ordinario, i numeri naturali, la totalità degli insiemi), e
- le assiomatizzazioni *moderne* (le strutture algebriche, le strutture topologiche, ...) che ambiscono a caratterizzare mediante assiomi intere famiglie di enti tra loro non isomorfi.

Questa distinzione è in realtà solo apparente perché, come vedremo, tutte le teorie del prim'ordine sono del secondo tipo, vale a dire: nessuna delle teorie assiomatiche descritte qui sopra caratterizza univocamente una struttura.

2. Simboli

Quando facciamo matematica fissiamo sempre, in modo implicito o esplicito, un linguaggio in cui i teoremi, le congetture, le dimostrazioni, ecc. sono formulati. Se scorriamo un testo di analisi potremmo imbatterci in vari tipi di simboli.

- Le lettere x, y, z, ... in genere designano numeri reali arbitrari. Anche altre lettere dell'alfabeto possono essere usate per indicare un generico reale e a volte, per evitare ambiguità, si ricorre alle lettere dell'alfabeto greco.
- Invece certe lettere designano numeri ben specifici — per esempio $\pi = 3{,}14159\ldots$ è il rapporto tra la lunghezza del diametro e la lunghezza della circonferenza, mentre $e = 2{,}71828\ldots$ è la costante di Eulero.

- I simboli $+$, $\cdot$ denotano le operazioni binarie di somma e prodotto, che non sono altro che specifiche funzioni da coppie di reali a valori reali.
- Il simbolo $<$ denota la relazione d'ordine.

Naturalmente il significato dei simboli varia da disciplina a disciplina — per esempio in un testo di algebra il simbolo $+$ viene spesso usato per denotare l'operazione in un gruppo abeliano, e il simbolo 1 indica l'elemento neutro di un gruppo scritto in notazione moltiplicativa. Se c'è però un simbolo sulla cui interpretazione siamo tutti d'accordo è il simbolo di uguaglianza $=$ che asserisce che l'oggetto scritto a sinistra del segno di uguale coincide con l'oggetto scritto a destra.

Ci sono poi alcune espressioni che ricorrono in ogni testo matematico:

- "per ogni x..."
- "c'è almeno un x tale che ..."
- "se... allora ..."
- "... se e solo se ..."
- le particelle "non", "e", "o".

Per formalizzare in modo non ambiguo i ragionamenti e le dimostrazioni sono stati introdotti dei simboli noti come **connettivi logici**

$$\neg \qquad \vee \qquad \wedge \qquad \Rightarrow \qquad \Leftrightarrow$$

ed i simboli di **quantificatore**

$$\exists \qquad \forall.$$

I connettivi e i quantificatori si dicono **costanti logiche**, di cui ora vediamo il significato.

- $\neg$ denota la **negazione** e serve per affermare l'opposto di quanto asserisce l'affermazione a cui si applica. Per esempio

  $$\neg(x < y)$$

  significa che x non è minore di y.
- $\vee$ è la **disgiunzione** e corrisponde al *vel* latino: questo *o* quello *o* eventualmente entrambi. Se asseriamo che

  $$(x \text{ è pari}) \vee (x \text{ è un quadrato perfetto})$$

  intendiamo dire che il numero x può essere pari cioè un elemento di $\textsc{pari} = \{2n \mid n \in \mathbb{N}\}$, o un quadrato perfetto cioè un elemento di $\textsc{quadrati} = \{n^2 \mid n \in \mathbb{N}\}$, o di entrambi cioè un elemento dell'unione $\textsc{pari} \cup \textsc{quadrati}$.

- $\wedge$ è la **congiunzione** e serve per asserire che due fatti valgono contemporaneamente. Per esempio

$$(x > 2) \wedge (x < 3)$$

  significa che il numero x si trova nell'intervallo $(2; 3)$. Anche le particelle "ma" e "però" sono delle congiunzioni, a cui noi attribuiamo una connotazione avversativa. Resta il fatto che in matematica il significato di "A ma B" o di "A però B" è lo stesso di "A e B" e quindi si scrivono come "A $\wedge$ B".
- $\Rightarrow$ è l'**implicazione** e corrisponde all'espressione "se... allora ...". Quando in matematica asseriamo che "se A allora B", stiamo affermando che l'unico caso problematico è quando la premessa A vale e la conseguenza B non vale. In particolare, se la premessa è falsa possiamo concludere che l'implicazione vale. Per esempio se in un testo di analisi vediamo scritto

$$(x > 0) \Rightarrow (x = y^2 \text{ per qualche } y > 0)$$

  siamo d'accordo che questa implicazione vale, dato che o x è positivo e quindi ha una radice positiva, oppure è negativo o nullo e quindi non c'è nulla da dire. Un'implicazione non sottintende nessuna relazione di causalità tra la premessa e la conseguenza — l'unico significato di A $\Rightarrow$ B è che non è possibile che A valga e B no. Le espressioni "affinché valga A deve valere B" oppure "affinché valga A è necessario che valga B" significano che "se A allora B" e quindi si scrivono A $\Rightarrow$ B, mentre "affinché valga A è sufficiente che valga B" significa che A vale quando B vale, cioè B $\Rightarrow$ A.
- $\Leftrightarrow$ è il **bi-condizionale** o **bi-implicazione** e corrisponde all'espressione "se e solo se". Quando asseriamo che "A se e solo se B" intendiamo dire che "se A allora B, e se B allora A". Spesso in matematica "A se e solo se B" lo si scrive, in modo più ampolloso, come "condizione necessaria e sufficiente affinché valga A, è che valga B".
- $\exists$ è il **quantificatore esistenziale**. L'espressione $\exists x$A si legge: "c'è un x tale che A", ovvero "A vale, per qualche x" e asserisce che c'è *almeno un* ente che gode della proprietà A.
- $\forall$ è il **quantificatore universale**. L'espressione $\forall x$A si legge: "per ogni x vale A", ovvero "A vale, per tutti gli x" e asserisce che *ogni* ente gode della proprietà A.

2.A. Significato delle costanti logiche. È utile introdurre una notazione apposita per parlare di regole dimostrative. Scriveremo

$$\frac{\mathrm{A}_1 \qquad \mathrm{A}_2 \qquad \dots \qquad \mathrm{A}_n}{\mathrm{B}}$$

per dire che "B discende da $\mathrm{A}_1, \dots, \mathrm{A}_n$".

2.A.1. *Connettivi.* Per dimostrare $A \wedge B$ è sufficiente dimostrare A e dimostrare B. Possiamo esprimere graficamente questo così

$$\frac{A \qquad B}{A \wedge B}\,.$$

Viceversa, da $A \wedge B$ possiamo dedurre tanto A quanto B, cioè

$$\frac{A \wedge B}{A} \quad \text{e} \quad \frac{A \wedge B}{B}\,. \tag{2.1}$$

Il connettivo $\wedge$ è commutativo, nel senso che asserire $A \wedge B$ è come asserire $B \wedge A$: se assumiamo $A \wedge B$ ricaviamo prima B e poi A, da cui otteniamo $B \wedge A$; analogamente da $B \wedge A$ si ricava $A \wedge B$.

Dimostrato A, possiamo indebolire il nostro risultato asserendo $A \vee B$, dove B è un'affermazione qualsiasi. Analogamente, da B si deduce $A \vee B$, per qualsiasi A. In simboli

$$\frac{A}{A \vee B} \qquad \text{e} \qquad \frac{B}{A \vee B}\,.$$

Invece a partire da $A \vee B$ non possiamo né concludere A né concludere B (Esempio 2.1). D'altra parte, se sappiamo $A \vee B$ e se sappiamo negare una tra le due affermazioni A e B, allora possiamo concludere l'altra, cioè

$$\frac{A \vee B \qquad \neg A}{B} \qquad \text{e} \qquad \frac{A \vee B \qquad \neg B}{A}\,. \tag{2.2}$$

Il connettivo $\vee$ è commutativo, nel senso che asserire $A \vee B$ è come asserire $B \vee A$. La **disgiunzione esclusiva** (corrispondente al latino *aut* e usualmente chiamata in informatica *xor*) "A oppure B, ma non entrambe", è denotata con

$$A \veebar B$$

e non è altro che un'abbreviazione di $(A \vee B) \wedge \neg(A \wedge B)$.

Supponiamo ora che valga A. Allora non possiamo asserire $\neg A$, altrimenti avremmo una contraddizione, quindi possiamo concludere $\neg\neg A$. Viceversa supponiamo $\neg\neg A$: se, per assurdo, A non valesse, allora concluderemmo $\neg A$ da cui una contraddizione. Riassumendo: abbiamo la regola della doppia negazione che asserisce che da A si deduce $\neg\neg A$ e viceversa:

$$\frac{A}{\neg\neg A} \qquad \text{e} \qquad \frac{\neg\neg A}{A}\,. \tag{2.3}$$

Il ragionamento precedente è un esempio di dimostrazione per assurdo: se si vuole dedurre A da certe ipotesi è sufficiente aggiungere $\neg A$ alle ipotesi e dimostrare una contraddizione, cioè un'affermazione del tipo $B \wedge \neg B$. Analogamente, per dimostrare $\neg A$ a partire da certe ipotesi è sufficiente dimostrare che A assieme alle altre ipotesi porta ad una contraddizione ed usare la regola (2.3).

Possiamo ora dimostrare le leggi di De Morgan, vale a dire

$$\frac{\mathrm{A} \wedge \mathrm{B}}{\neg(\neg \mathrm{A} \vee \neg \mathrm{B})} \quad \text{e} \quad \frac{\mathrm{A} \vee \mathrm{B}}{\neg(\neg \mathrm{A} \wedge \neg \mathrm{B})} .$$

Dimostrazione. Supponiamo $\mathrm{A} \wedge \mathrm{B}$ e, per assurdo, assumiamo $\neg \mathrm{A} \vee \neg \mathrm{B}$. Per la regola (2.1) otteniamo A da $\mathrm{A} \wedge \mathrm{B}$ e applicando regola della doppia negazione (2.3) otteniamo $\neg\neg \mathrm{A}$. Quindi applicando la regola (2.2) a $\neg \mathrm{A} \vee \neg \mathrm{B}$ si ottiene $\neg \mathrm{B}$. Poiché B segue da $\mathrm{A} \wedge \mathrm{B}$ per la regola (2.1), otteniamo una contraddizione e possiamo quindi concludere che $\neg\,(\neg \mathrm{A} \vee \neg \mathrm{B})$ come richiesto.

L'altra legge — che ci permette di concludere $\neg(\neg \mathrm{A} \wedge \neg \mathrm{B})$ a partire da $\mathrm{A} \vee \mathrm{B}$ — è dimostrata in modo analogo. □

Per mezzo delle leggi di De Morgan possiamo dare esempi di affermazioni della forma $\mathrm{A} \vee \mathrm{B}$ da cui non possiamo concludere né A né B.

Esempio 2.1. Consideriamo le affermazioni:

$$\begin{aligned} \mathrm{A}: &\quad \pi + \mathrm{e} \notin \overline{\mathbb{Q}}, \\ \mathrm{B}: &\quad \pi \cdot \mathrm{e} \notin \overline{\mathbb{Q}}, \end{aligned}$$

dove $\overline{\mathbb{Q}}$ è il campo dei numeri algebrici. In altre parole A asserisce "$\pi + \mathrm{e}$ è trascendente" e B asserisce "$\pi \cdot \mathrm{e}$ è trascendente". (Si veda l'Appendice A per la definizione di numero algebrico e trascendente.) Poiché i numeri e, π sono le uniche soluzioni dell'equazione $x^2 - (\pi + \mathrm{e}) \cdot x + \pi \cdot \mathrm{e} = 0$ e sono entrambi numeri trascendenti, allora $\pi + \mathrm{e} \in \overline{\mathbb{Q}}$ e $\pi \cdot \mathrm{e} \in \overline{\mathbb{Q}}$ non possono valere simultaneamente, cioè vale $\neg\,(\neg \mathrm{A} \wedge \neg \mathrm{B})$ e per De Morgan possiamo asserire $\mathrm{A} \vee \mathrm{B}$. A tutt'oggi la trascendenza di $\mathrm{e} + \pi$ e di $\mathrm{e} \cdot \pi$ sono problemi aperti, cioè non c'è nessuna dimostrazione di A o di B.[1]

Esempio 2.2. Sia P l'insieme dei numeri primi e sia

$$W = \left\{ p \in P \mid p^2 \mid (2^{p-1} - 1) \right\}.$$

Consideriamo le affermazioni:

$$\begin{aligned} \mathrm{A}: &\quad W \text{ è infinito}, \\ \mathrm{B}: &\quad P \setminus W \text{ è infinito}. \end{aligned}$$

Poiché P è infinito, almeno uno tra W e $P \setminus W$ è infinito, cioè $\mathrm{A} \vee \mathrm{B}$ è vera. Tuttavia gli unici primi in W noti a tutt'oggi (15 dicembre 2014) sono 1093 e 3511, e anche l'esistenza di infiniti primi non in W è un problema aperto. In altre parole: tanto A quanto B sono problemi aperti.

[1] È opinione diffusa tra gli esperti di teoria dei numeri che entrambi i problemi abbiano una risposta affermativa, cioè che valgano tanto A quanto B e quindi valga $\mathrm{A} \wedge \mathrm{B}$.

Per quanto detto sull'implicazione, asserire $\neg(\mathrm{A} \Rightarrow \mathrm{B})$ significa dire che A vale ma B non vale. Quindi equivale a dire $\mathrm{A} \wedge \neg\mathrm{B}$ che, per le leggi di De Morgan, è equivalente a $\neg(\neg\mathrm{A} \vee \mathrm{B})$. Abbiamo quindi verificato che $\neg(\mathrm{A} \Rightarrow \mathrm{B})$ è equivalente a $\neg(\neg\mathrm{A} \vee \mathrm{B})$, cioè $\mathrm{A} \Rightarrow \mathrm{B}$ è equivalente a $\neg\mathrm{A} \vee \mathrm{B}$, in simboli

$$\frac{\mathrm{A} \Rightarrow \mathrm{B}}{\neg\mathrm{A} \vee \mathrm{B}} \qquad \text{e} \qquad \frac{\neg\mathrm{A} \vee \mathrm{B}}{\mathrm{A} \Rightarrow \mathrm{B}}.$$

La regola (2.2) può essere riformulata per l'implicazione così: da $\mathrm{A} \Rightarrow \mathrm{B}$ e A possiamo dedurre B. Questa regola prende il nome di *Modus Ponens*:

(MP) $$\frac{\mathrm{A} \Rightarrow \mathrm{B} \qquad \mathrm{A}}{\mathrm{B}}\,.$$

Infine utilizzando la regola della doppia negazione (2.3) è facile verificare che

$$\frac{\mathrm{A} \Rightarrow \mathrm{B}}{\neg\mathrm{B} \Rightarrow \neg\mathrm{A}}\,.$$

$\neg\mathrm{B} \Rightarrow \neg\mathrm{A}$ si dice il **contrappositivo** di $\mathrm{A} \Rightarrow \mathrm{B}$. Osserviamo che, a differenza della congiunzione e dalla disgiunzione, il connettivo $\Rightarrow$ non commuta, cioè $\mathrm{A} \Rightarrow \mathrm{B}$ non ha lo stesso significato di $\mathrm{B} \Rightarrow \mathrm{A}$.

Il bi-condizionale $\Leftrightarrow$ è definito come la congiunzione di due implicazioni, in simboli

$$\frac{\mathrm{A} \Leftrightarrow \mathrm{B}}{\mathrm{A} \Rightarrow \mathrm{B}} \qquad \text{e} \qquad \frac{\mathrm{A} \Leftrightarrow \mathrm{B}}{\mathrm{B} \Rightarrow \mathrm{A}}$$

e

$$\frac{\mathrm{A} \Rightarrow \mathrm{B} \qquad \mathrm{B} \Rightarrow \mathrm{A}}{\mathrm{A} \Leftrightarrow \mathrm{B}}\,.$$

Il bi-condizionale è commutativo, cioè asserire $\mathrm{A} \Leftrightarrow \mathrm{B}$ è come asserire $\mathrm{B} \Leftrightarrow \mathrm{A}$.

2.A.2. *Quantificatori.* Quando scriviamo un'affermazione del tipo $\exists x\mathrm{A}$ o $\forall x\mathrm{A}$ implicitamente intendiamo che A stia affermando qualche proprietà di x. Se, per esempio, A è l'equazione $x^2 + x = 0$, l'espressione $\exists x\mathrm{A}$ dice che l'equazione data ammette una soluzione — il che è vero in ogni campo. Invece $\forall x\mathrm{A}$ dice che ogni numero è soluzione di A — e questo vale solo nel campo $\mathbb{Z}/2\mathbb{Z}$. Se invece A non dice nulla della variabile x, il significato di $\exists x\mathrm{A}$ e di $\forall x\mathrm{A}$ coincide con quello di A — per esempio $\exists x \exists y\,(y^2 + y = 0)$ e $\forall x \exists y\,(y^2 + y = 0)$ sono entrambe equivalenti a $\exists y\,(y^2 + y = 0)$. Negare $\forall x\mathrm{A}$ significa dire che non tutti gli x godono della proprietà descritta da A, cioè c'è almeno un x per cui si può asserire $\neg\mathrm{A}$. Viceversa, se neghiamo $\exists x\mathrm{A}$ allora vuol dire che non si dà il caso che ci sia un x per cui vale A, cioè per ogni x deve valere $\neg\mathrm{A}$. In simboli

$$\frac{\neg\forall x\mathrm{A}}{\exists x\neg\mathrm{A}} \qquad \text{e} \qquad \frac{\neg\exists x\mathrm{A}}{\forall x\neg\mathrm{A}}\,.$$

Quando scriviamo $\forall x \forall y\mathrm{A}$ intendiamo dire che in qualsiasi modo si scelgano gli elementi x e y vale A, e questo è la stessa cosa che dire $\forall y \forall x\mathrm{A}$. Analogamente $\exists x \exists y\mathrm{A}$ ha lo stesso significato di $\exists y \exists x\mathrm{A}$. Quindi

$$\frac{\exists x \exists y\mathrm{A}}{\exists y \exists x\mathrm{A}} \qquad \text{e} \qquad \frac{\forall x \forall y\mathrm{A}}{\forall y \forall x\mathrm{A}}\,.$$

Supponiamo $\exists x \forall y \mathrm{A}$ valga: questo vuol dire che c'è un $\bar{x}$ tale che per ogni y vale A. Quindi se scegliamo un y arbitrario possiamo sempre trovare un x tale che A: basta prendere l'elemento $\bar{x}$ di prima. In altre parole

$$\frac{\exists x \forall y \mathrm{A}}{\forall y \exists x \mathrm{A}} \,.$$

Questa regola non può essere invertita: da $\forall y \exists x \mathrm{A}$ non possiamo concludere $\exists x \forall y \mathrm{A}$ — per convincersi di questo basta considerare le affermazioni $\forall y \exists x (y < x)$ e $\exists x \forall y (y < x)$ in $\mathbb{N}$.

Il quantificatore esistenziale si distribuisce rispetto alla disgiunzione nel seguente senso: dire che "c'è un x per cui A oppure c'è un x per cui B" è la stessa cosa che dire "c'è un x per cui A o B", in simboli

$$\frac{(\exists x \mathrm{A}) \vee (\exists x \mathrm{B})}{\exists x (\mathrm{A} \vee \mathrm{B})} \qquad \text{e} \qquad \frac{\exists x (\mathrm{A} \vee \mathrm{B})}{(\exists x \mathrm{A}) \vee (\exists x \mathrm{B})} \,.$$

Per quanto riguarda il quantificatore esistenziale e la congiunzione abbiamo solo una regola: se "c'è un x tale che A e B" allora "c'è un x tale che A, e c'è un x tale che B", cioè

$$\frac{\exists x (\mathrm{A} \wedge \mathrm{B})}{(\exists x \mathrm{A}) \wedge (\exists x \mathrm{B})} \,.$$

Il viceversa non vale: dal fatto che ci sia un numero pari e ci sia un numero dispari non possiamo concludere che esista un numero che è tanto pari quanto dispari.

Analogamente, il quantificatore universale si distribuisce rispetto alla congiunzione

$$\frac{(\forall x \mathrm{A}) \wedge (\forall x \mathrm{B})}{\forall x \, (\mathrm{A} \wedge \mathrm{B})} \qquad \text{e} \qquad \frac{\forall x \, (\mathrm{A} \wedge \mathrm{B})}{(\forall x \mathrm{A}) \wedge (\forall x \mathrm{B})} \,,$$

ma solo parzialmente rispetto alla disgiunzione

$$\frac{(\forall x \mathrm{A}) \vee (\forall x \mathrm{B})}{\forall x \, (\mathrm{A} \vee \mathrm{B})} \,.$$

Questo parallelismo tra il quantificatore esistenziale e la disgiunzione, da un lato, e il quantificatore universale e la congiunzione, dall'altro, non è così sorprendente, visto che i quantificatori possono essere visti come disgiunzioni e congiunzioni generalizzate: dire che vale $\exists x P(x)$ in $\mathbb{N}$ equivale ad asserire $P(0) \vee P(1) \vee P(2) \vee \ldots$ mentre dire che vale $\forall x P(x)$ in $\mathbb{N}$ equivale ad asserire $P(0) \wedge P(1) \wedge P(2) \wedge \ldots$

Per asserire un'affermazione del tipo $\exists x \mathrm{A}$ non si richiede di esibire esplicitamente un testimone x che renda vera A. Per esempio, per dimostrare $\exists x \mathrm{A}$ è possibile procedere per assurdo, cioè dimostrare che l'affermazione $\forall x \neg \mathrm{A}$ porta ad una contraddizione. Molti risultati di teoria dei numeri sono di questo tipo — si dimostra che deve esistere un numero che gode di una

certa proprietà, ma spesso non si riesce neppure a stabilire un limite superiore a tale numero. Un'affermazione esistenziale in cui non si riesce facilmente a determinare il testimone è data dal seguente

Esempio 2.3. L'affermazione $\exists x\,(P(x) \Rightarrow \forall x P(x))$ è sempre vera, indipendentemente dal significato della proprietà P.

Per verificare ciò procediamo per casi.

- La proprietà P vale per ogni individuo, cioè $\forall x P(x)$. Allora per le proprietà dell'implicazione vale $P(x) \Rightarrow \forall x P(x)$ e quindi un qualsiasi individuo testimonia $\exists x\,(P(x) \Rightarrow \forall x P(x))$.
- C'è un individuo che non gode della proprietà P: questo individuo testimonia $\exists x\,(P(x) \Rightarrow \forall x P(x))$, visto che non rende vera $P(x)$ e quindi rende vera l'implicazione $P(x) \Rightarrow \forall x P(x)$.

Quindi $\exists x\,(P(x) \Rightarrow \forall x P(x))$ vale in ogni caso.

Ci sono delle situazioni in cui si sa che il testimone di un'affermazione esistenziale $\exists x \mathrm{A}$ è uno tra una lista finita di individui $a_1, \ldots, a_k$, senza però essere in grado di specificare quale tra questi sia il testimone cercato, cioè senza essere in grado di trovare esplicitamente un indice i per cui a_i rende vera A.

Esempio 2.4. La **funzione di Möbius** $\mu\colon \mathbb{N} \to \{-1, 0, 1\}$ è definita da $\mu(0) = \mu(1) = 0$ e

$$\mu(n) = \begin{cases} 0 & \text{se } p^2 \mid n \text{ per qualche primo } p, \\ 1 & \text{se } n = p_1 \cdots p_k \text{ con } p_1 < \cdots < p_k \text{ primi e } k \text{ pari}, \\ -1 & \text{se } n = p_1 \cdots p_k \text{ con } p_1 < \cdots < p_k \text{ primi e } k \text{ dispari}. \end{cases}$$

È stato dimostrato che ci sono infiniti n tali che

$$\left|\textstyle\sum_{k=1}^{n} \mu(k)\right| > \sqrt{n}, \tag{2.4}$$

e quindi $\exists x\,(|\sum_{k=1}^{x} \mu(k)| > \sqrt{x})$. Tuttavia non si conosce nessun esempio esplicito di numero che soddisfi (2.4): il primo n siffatto si trova nell'intervallo $(10^{14}; \mathrm{e}^{1.59 \cdot 10^{40}})$.

Esempio 2.5. L'affermazione

$$\exists x \exists y\,(x \text{ e } y \text{ sono irrazionali e } x^y \text{ è razionale})$$

è vera. Infatti se l'affermazione

$$\mathrm{A}: \quad \sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$$

è vera, allora basta prendere $x = y = \sqrt{2}$; se invece vale $\neg$A, allora basta prendere $x = \sqrt{2}^{\sqrt{2}}$ e $y = \sqrt{2}$.

Osservazione 2.6. Decidere se un intero n soddisfa o meno la (2.4) è un problema risolubile in modo meccanico, per lo meno in linea di principio. Quindi per determinare il minimo n che rende vera la (2.4) basta esaminare lista finita di potenziali candidati. Ma quando i numeri diventano troppo grandi, come nel caso dell'Esempio 2.4, le difficoltà di calcolo diventano insormontabili.

L'Esempio 2.5 seguente mostra invece una situazione opposta: si sa che

$$(x, y) = (\sqrt{2}, \sqrt{2}) \quad \text{oppure} \quad (x, y) = (\sqrt{2}^{\sqrt{2}}, \sqrt{2})$$

ma poiché stabilire se un numero della forma a^b è razionale o meno è cosa non banale, il ragionamento qui sopra non ci consente di determinare se vale A oppure $\neg$A.

Indicando con B l'affermazione $\exists x \exists y\, (x, y \in \mathbb{R} \setminus \mathbb{Q} \wedge x^y \in \mathbb{Q})$, l'Esempio 2.5 mette in luce un'altra tecnica dimostrativa: il metodo della **dimostrazione per casi** asserisce che se B segue da A e da $\neg$A, allora B è dimostrata,

$$\frac{\mathrm{A} \Rightarrow \mathrm{B} \qquad \neg\mathrm{A} \Rightarrow \mathrm{B}}{\mathrm{B}}\,.$$

L'affermazione A si dice **ipotesi condizionale**.

2.B. Formalizzazione. Usando le costanti logiche è possibile trasformare in forma simbolica le affermazioni di matematica scritte nel linguaggio naturale — questa opera di traduzione si dice **formalizzazione** e le espressioni simboliche così ottenute si dicono **formule**. Le formule più semplici sono dette atomiche e corrispondono ad affermazioni che non possono essere ulteriormente analizzate mediante le costanti logiche. Le **formule atomiche** sono della forma

$$a = b$$

oppure

$$P(a_1, \ldots, a_n)$$

dove la lettera P indica un predicato n-ario, cioè un'affermazione elementare riguardante gli enti $a_1, \ldots, a_n$. Quando P è binario (vale a dire 2-ario) scriveremo $a_1\, P\, a_2$ invece di $P(a_1, a_2)$.

I teoremi della matematica elementare possono essere formulati senza usare i quantificatori, oppure facendo precedere l'affermazione da dei quantificatori universali — per esempio:

- "valgono la proprietà commutativa e la proprietà associativa" può essere formalizzato così

$$(x \cdot y = y \cdot x) \wedge ((x \cdot y) \cdot z = x \cdot (y \cdot z))\,,$$

oppure così

$$\forall x \forall y \forall z ((x \cdot y = y \cdot x) \wedge ((x \cdot y) \cdot z = x \cdot (y \cdot z))),$$

o anche così

$$\forall x \forall y \, (x \cdot y = y \cdot x) \; \wedge \; \forall x \forall y \forall z \, ((x \cdot y) \cdot z = x \cdot (y \cdot z)) \, ,$$

- "un triangolo è equilatero se e solo se è equiangolo" può essere formalizzato così

  $$T(x) \Rightarrow (L(x) \Leftrightarrow A(x))$$

  oppure così

  $$\forall x \, (T(x) \Rightarrow (L(x) \Leftrightarrow A(x))) \, ,$$

  dove T è il predicato "essere un triangolo", L è il predicato "essere un poligono con i lati tutti uguali" e A è il predicato "essere un poligono con gli angoli interni tutti uguali". Abbiamo messo le parentesi attorno alla bi-implicazione per indicare che il connettivo principale è l'implicazione: se x è un triangolo, allora ...,
- "il prodotto di due numeri è zero se e solo se almeno uno dei due è zero" può essere formalizzato così

  $$x \cdot y = 0 \Leftrightarrow (x = 0 \vee y = 0),$$

  oppure così

  $$\forall x \forall y \, (x \cdot y = 0 \Leftrightarrow (x = 0 \vee y = 0)) \, .$$

Notiamo come nel secondo esempio l'articolo indeterminativo "*un*" significhi "*un qualsiasi*".

Se vogliamo esprimere qualche concetto più avanzato dobbiamo usare alternanze di quantificatori. Per esempio

$$\forall x \, (x \neq 0 \; \Rightarrow \; \exists y \, (x \cdot y = 1))$$

formalizza

un elemento non nullo ha un inverso,

un'affermazione vera in ogni campo. La scrittura $x \neq 0$ è un'abbreviazione di $\neg(x = 0)$ — più in generale $a \neq b$ sta per $\neg(a = b)$.

Nell'esempio precedente le espressioni della forma

$$\text{ogni } x \text{ tale che } P(x) \; (\dots)$$

significano: "preso un x, se $P(x)$ allora $(\dots)$" da cui l'uso di $\Rightarrow$ nella formalizzazione. Un errore comune è usare $\wedge$ al posto di $\Rightarrow$ nella formalizzazione precedente — si otterrebbe un'affermazione che dice "ogni x gode della proprietà P e $(\dots)$"! Per esempio

$$\forall x (x \neq 0 \wedge \exists y (x \cdot y = 1))$$

dice che "ogni x è non nullo e ha un inverso", un'asserzione falsa in qualsiasi campo, dato che non vale quando x è 0. Invece le espressioni del tipo

$$\text{c'è un } x \text{ tale che } P(x) \text{ per cui } (\dots)$$

si formalizzano come

$$\exists x\,(P(x) \wedge (\dots))\,.$$

In particolare la scrittura $\exists x > 0(\dots)$ è un'abbreviazione di $\exists x(x > 0 \wedge (\dots))$ e non di $\exists x(x > 0 \Rightarrow (\dots))$.

Negare un'affermazione della forma

$$\text{ogni } x \text{ tale che } P(x)\ (\dots)$$

significa dire:

$$\text{c'è un } x \text{ tale che } P(x) \text{ e non } (\dots).$$

Infatti per le proprietà dei quantificatori $\neg\forall x\,(P(x) \Rightarrow (\dots))$ è equivalente a $\exists x \neg\,(P(x) \Rightarrow (\dots))$ e poiché $P(x) \Rightarrow (\dots)$ significa $\neg P(x) \vee (\dots)$, per le leggi di De Morgan otteniamo $\exists x\,(\neg\neg P(x) \wedge \neg(\dots))$ da cui $\exists x\,(P(x) \wedge \neg(\dots))$. Analogamente negare un'affermazione della forma

$$\text{c'è un } x \text{ per cui } P(x) \text{ e } (\dots)$$

significa dire

$$\text{per ogni } x \text{ tale che } P(x) \text{ non vale } (\dots),$$

in altre parole: $\neg\exists x\,(P(x) \wedge (\dots))$ è equivalente a $\forall x\,(P(x) \Rightarrow \neg(\dots))$.

Un'affermazione del tipo

$$\text{esiste un unico } x \text{ tale che } P(x) \tag{2.5}$$

significa che "c'è un x tale che $P(x)$ e tale che ogni altro y che gode della proprietà P è uguale a x", cioè

$$\exists x\,(P(x) \wedge \forall y\,(P(y) \Rightarrow y = x))\,,$$

o, equivalentemente,

$$\exists x\,(P(x) \wedge \forall y\,(y \neq x \Rightarrow \neg P(y)))\,.$$

Un altro modo equivalente per scrivere la frase qui sopra è che "$P(x)$ per qualche x, e due oggetti che godano della proprietà P devono coincidere", cioè

$$\exists x P(x) \wedge \forall x \forall y\,(P(x) \wedge P(y) \Rightarrow x = y)\,.$$

(Affermare solo $\forall x \forall y\,(P(x) \wedge P(y) \Rightarrow x = y)$ non è sufficiente, dato che la proprietà P potrebbe essere sempre falsa e quindi, banalmente, due elementi che soddisfano P coincidono!) Un ulteriore modo per formalizzare la (2.5) è

$$\exists x \forall y\,(P(y) \Leftrightarrow x = y)$$

cioè "c'è un x tale che $P(y)$ se e solo se $y = x$, per ogni y". Abbrevieremo una qualsiasi delle formule qui sopra con

$$\exists! x P(x).$$

Quindi $\exists!$ non è un nuovo tipo di quantificatore, ma semplicemente un'abbreviazione.

Le frasi del tipo "$P(x)$, per tutti gli x sufficientemente grandi" vanno formalizzate come

$$\exists y \forall x \left(y < x \Rightarrow P(x)\right).$$

Se stiamo parlando di numeri naturali, la frase precedente viene spesso formulata come "per tutti gli x, eccetto al più una quantità finita, vale $P(x)$", mentre la frase "per infiniti x vale $P(x)$" si formalizza come

$$\forall y \exists x \left(y < x \wedge P(x)\right).$$

2.C. Esempi di formalizzazione.

2.C.1. Dati i simboli di funzione f e g, la frase "$f \circ g$ ha un punto fisso" si formalizza come

$$\exists x \exists y \left(f(x) = y \wedge g(y) = x\right),$$

o anche

$$\exists x \left(f(g(x)) = x\right).$$

2.C.2. Dato il simbolo di predicato P, la frase "ci sono almeno tre elementi per cui vale P" si formalizza come

$$\exists x_1 \exists x_2 \exists x_3 \left(P(x_1) \wedge P(x_2) \wedge P(x_3) \wedge x_1 \neq x_2 \wedge x_2 \neq x_3 \wedge x_1 \neq x_3\right),$$

mentre "ci sono al più tre elementi per cui vale P" è equivalente alla negazione di "ci sono almeno quattro elementi per cui vale P" e quindi si formalizza come

$$\forall x_1 \forall x_2 \forall x_3 \forall x_4 \big(P(x_1) \wedge P(x_2) \wedge P(x_3) \wedge P(x_4) \Rightarrow \\ x_1 = x_2 \vee x_1 = x_3 \vee x_1 = x_4 \vee x_2 = x_3 \vee x_2 = x_4 \vee x_3 = x_4\big).$$

Per economia di scrittura abbrevieremo le congiunzioni $\varphi_1 \wedge \cdots \wedge \varphi_n$ con

$$\bigwedge_{1 \leq i \leq n} \varphi_i$$

e le disgiunzioni $\varphi_1 \vee \cdots \vee \varphi_n$ con

$$\bigvee_{1 \leq i \leq n} \varphi_i,$$

mentre i blocchi di quantificatori (dello stesso tipo) $\forall x_1 \dots \forall x_n$ e $\exists x_1 \dots \exists x_n$ li si abbreviano con $\forall x_1, \dots, x_n$ e $\exists x_1, \dots, x_n$. Quindi la formula qui sopra la si abbrevia

$$\forall x_1, \dots, x_4 \Big(\bigwedge_{1 \le i \le 4} P(x_i) \Rightarrow \bigvee_{1 \le i < j \le 4} x_i = x_j \Big).$$

È utile introdurre una notazione per la formalizzazione delle frasi "ci sono almeno n elementi",

$$(\boldsymbol{\varepsilon}_{\ge n}) \qquad \exists x_1, \dots, x_n \left(\textstyle\bigwedge_{1 \le i < j \le n} x_i \ne x_j \right)$$

"ci sono al più n elementi" cioè "non è vero che ci sono almeno $n+1$ elementi"

$$(\boldsymbol{\varepsilon}_{\le n}) \qquad \forall x_1, \dots, x_{n+1} \left(\textstyle\bigvee_{1 \le i < j \le n+1} x_i = x_j \right)$$

e "ci sono esattamente n elementi"

$$(\boldsymbol{\varepsilon}_{n}) \qquad \boldsymbol{\varepsilon}_{\le n} \wedge \boldsymbol{\varepsilon}_{\ge n}.$$

Le definizioni date valgono per $n \ge 2$. Quando $n = 1$ poniamo

$$(\boldsymbol{\varepsilon}_{\ge 1}) \qquad \exists x_1 \, (x_1 = x_1) \,,$$

$$(\boldsymbol{\varepsilon}_{\le 1}) \qquad \forall x_1, x_2 \, (x_1 = x_2) \,,$$

$$(\boldsymbol{\varepsilon}_{1}) \qquad \boldsymbol{\varepsilon}_{\le 1} \wedge \boldsymbol{\varepsilon}_{\ge 1}.$$

2.C.3. Supponiamo di imbatterci in una frase quale: "tra due razionali c'è un irrazionale, e viceversa" o più in generale, in una frase del tipo "tra due elementi che godono della proprietà P c'è un elemento che gode della proprietà Q, e viceversa". Qui "viceversa" significa che "tra due elementi che godono della proprietà Q c'è un elemento che gode della proprietà P". Per formalizzarla abbiamo bisogno di due predicati unari P e Q e del simbolo $<$ per l'ordinamento:

$$\begin{aligned} &\forall x \forall y \, ((x < y \wedge P(x) \wedge P(y)) \Rightarrow \exists z \, (x < z \wedge z < y \wedge Q(z))) \\ &\qquad \wedge \forall x \forall y \, ((x < y \wedge Q(x) \wedge Q(y)) \Rightarrow \exists z \, (x < z \wedge z < y \wedge P(z))) \end{aligned}$$

2.C.4. Un celebre teorema di Euclide asserisce che esistono infiniti numeri primi, cioè

$$\forall x \exists y \, (x < y \wedge \mathrm{Pr}(y))$$

dove Pr è il predicato unario "essere un numero primo". Se vogliamo formalizzare questo enunciato usando soltanto la relazione di divisibilità $\mid$ (oltre che la relazione d'ordine), trasformiamo $\mathrm{Pr}(y)$ in

$$1 < y \wedge \forall z \, (z \mid y \Rightarrow z = 1 \vee z = y)$$

e quindi il teorema di Euclide diventa

$$\forall x \exists y \, (x < y \wedge 1 < y \wedge \forall z \, (z \mid y \Rightarrow z = 1 \vee z = y)) \,.$$

Abbiamo così eliminato il predicato Pr, ma abbiamo introdotto la costante 1. Per sbarazzarci anche di questa basta osservare che 1 è l'unico numero naturale che divide ogni numero naturale, cioè $\exists! u \forall w (u \mid w)$, e quindi il teorema di Euclide si può formalizzare come

$$\exists u \forall w \Big(u \mid w \wedge \forall x \exists y \big(x < y \wedge u < y \wedge \forall z \, (z \mid y \Rightarrow z = u \vee z = y) \big) \Big).$$

Poiché $z \mid y$ se e solo se $\exists v \, (v \cdot z = y)$, è possibile anche formalizzare il tutto usando la relazione d'ordine e il prodotto (Esercizio 2.7).

2.C.5. Due naturali distinti x e y possono avere gli stessi fattori primi, ma se consideriamo anche $x+1, x+2, \ldots, x+k$ e $y+1, y+2, \ldots, y+k$ con k sufficientemente grande, è possibile trovare un primo p che divide uno ed uno solo tra $x+i$ e $y+i$, con $i \leq k$. La **congettura di Erdős-Woods** asserisce che esiste un k universale. In altre parole:

> C'è un intero $k > 0$ tale che ogni intero x è completamente determinato dai primi che dividono $x, x+1, \ldots, x+k$

La formalizzazione di questo problema è

$$\exists k \, \forall x, y \, \big[x \neq y \Rightarrow \exists i, p \, (i \leq k \wedge \mathrm{Pr}(p) \wedge (p \mid (x+i) \Leftrightarrow p \nmid (y+i))) \big].$$

Naturalmente possiamo eliminare il simbolo Pr come nell'esempio precedente, mentre la disuguaglianza $i \leq k$ può essere trasformata in $\exists z \, (i + z = k)$.

Esercizi

Esercizio 2.7. Formalizzare il teorema di Euclide sui numeri primi usando soltanto il prodotto $\cdot$ e la relazione d'ordine $<$.

Esercizio 2.8. Formalizzare i seguenti enunciati sui numeri naturali usando i simboli indicati:

(i) Il **postulato di Bertrand**: per ogni $n > 1$ c'è almeno un primo tra n e $2n$, usando l'ordinamento $<$, la somma $+$, la costante 1 e la relazione di divisibilità $|$. Ripetere l'esercizio usando solo $+$ e $|$.

(ii) La **congettura di Legendre**: per ogni $n > 1$ c'è un primo tra n^2 e $(n+1)^2$, usando $<$, 1 e il prodotto $\cdot$. Ripetere l'esercizio usando $<$ e $\cdot$.

(iii) La **congettura dei primi gemelli**: ci sono infiniti primi della forma p, $p+2$, usando $<$ e $|$.

(iv) La **congettura di Goldbach**: ogni numero pari maggiore di due è somma di due primi, usando $<$, la costante 2, $+$ e $|$. Ripetere l'esercizio usando $+$ e $|$.

(v) Il **teorema di Vinogradov**: ogni numero dispari sufficientemente grande è somma di tre primi, non necessariamente distinti, usando $<$, $+$ e $|$. Ripetere l'esercizio usando $+$ e $|$.

(vi) "Ogni numero naturale sufficientemente grande è somma di al più quattro cubi", usando $<$, $+$ e $\cdot$. Ripetere l'esercizio usando solo $+$ e $\cdot$.

(vii) L'**ultimo teorema di Fermat**: nessun cubo è somma di due cubi, nessuna quarta potenza è somma di due quarte potenze, e così via, usando $<$, 2, $+$ e la funzione esponenziale x^y. Ripetere l'esercizio usando solo $+$ e x^y.

(viii) Il **teorema di Dirichlet**: se a e b sono relativamente primi, allora ci sono infiniti numeri primi congruenti ad a modulo b, usando $<$, la somma $+$ e $\cdot$. Ripetere l'esercizio usando solo $+$ e $\cdot$.

(ix) Il **teorema di Green-Tao**: l'insieme dei primi contiene progressioni aritmetiche arbitrariamente lunghe, usando $<$, $+$ e $\cdot$. Ripetere l'esercizio usando $+$ e $\cdot$.

(x) La **congettura di Beal**: se a, b, c, x, y, z sono dei numeri naturali tali che $a^x + b^y = c^z$, con $a, b, c > 1$ e $x, y, z > 2$, allora a, b e c hanno un fattore primo in comune, usando $<$, 1, $+$, $\cdot$ e x^y. Ripetere l'esercizio usando $+$, $\cdot$ e x^y.

Esercizio 2.9. (i) Formalizzare le seguenti frasi usando il simbolo f:

- f è iniettiva,
- f è suriettiva,
- f è biettiva,
- f è un'involuzione, cioè $f \circ f$ è l'identità.
- le fibre di f hanno al più tre elementi, cioè la contro-immagine di un punto ha taglia ≤ 3.

(ii) Se $f, g \colon A \times A \to A$ sia $\langle f, g \rangle \colon A \times A \to A \times A$ la funzione definita da $(a_1, a_2) \mapsto (f(a_1, a_2), g(a_1, a_2))$. Ripetere la parte (i) dell'esercizio con $\langle f, g \rangle$ al posto di f, usando i simboli f e g.

Esercizio 2.10. Formalizzare la seguente frase:

> tra sei persone prese a caso ce ne sono almeno tre che si conoscono tra di loro, o che sono totalmente estranee

usando i predicati binari $C(x, y)$ per esprimere il fatto che x e y si conoscono e $E(x, y)$ per esprimere il fatto che x e y sono estranei. (Naturalmente è possibile usare solo il predicato C e definire $E(x, y)$ come $\neg C(x, y)$.)

Esercizio 2.11. Sia f una funzione reale di variabile reale. Usando i simboli f, $+$, $\cdot$ e $<$, formalizzare le frasi:

- f è continua,
- f è differenziabile.

Esercizio 2.12. Sia $f \colon \mathbb{R}^2 \to \mathbb{R}$. Usando i simboli f, $+$, $\cdot$, x_0 e y_0 formalizzare il Teorema della Funzione Implicita:

> Se f è differenziabile con continuità, si annulla in (x_0, y_0) e $\partial f / \partial y$ non si annulla in (x_0, y_0), allora c'è un intorno aperto U di x_0 e un intorno aperto V di y_0 tali che per ogni $x \in U$ c'è esattamente un $y \in V$ per cui $f(x, y) = 0$.

Esercizio 2.13. Formalizzare le seguenti affermazioni:

(i) dati due punti c'è una retta su cui i punti giacciono;

(ii) dati due punti distinti c'è un'unica retta su cui i punti giacciono;

(iii) dati tre punti che non giacciono su una retta, c'è un unico piano su cui giacciono;

usando i predicati unari $P(x)$, $Q(x)$, $R(x)$ per formalizzare "x è un punto", "x è una linea", "x è un piano" e il predicato binario $L(x, y)$ per formalizzare "x giace su y".

Note e osservazioni

La trascendenza della costante e di Eulero è stata dimostrata nel 1873 da Hermite, la trascendenza di π è stata dimostrata nel 1882 da Lindeman — si veda l'Esempio 2.1. I primi p che soddisfano $p^2 \mid (2^{p-1} - 1)$ (Esempio 2.2) si dicono **primi di Wieferich**, dal nome del matematico che per primo li ha definiti e studiati nel 1909.

L'Esempio 2.4 illustra come i teoremi possano contraddire le opinioni basate sugli esperimenti e le simulazioni numeriche. Stieltjes congetturò nel 1885 in una lettera ad Hermite e a Mertens che $\forall n \left(\left|\sum_{k=1}^{n} \mu(k)\right| < \sqrt{n}\right)$ e questa divenne nota come **congettura di Mertens**. La congettura è stata refutata nel 1985 da Odlyzko e te Riele [**OtR85**]. La funzione μ prende il nome da Möbius.

L'Esempio 2.5 illustra bene la potenza e la semplicità dei ragionamenti non costruttivi e del metodo della dimostrazione per casi, cioè dimostrare un'affermazione B a partire da un'ipotesi condizionale A e dalla sua negazione ¬A, sulla cui validità non sappiamo nulla. In realtà, l'esistenza di numeri irrazionali il cui esponenziale è razionale segue immediatamente dal seguente risultato[2] dimostrato nel 1934 da Gelfond e indipendentemente da Schneider: se $a \neq 0, 1$ è algebrico e b è irrazionale, allora a^b è trascendente. Quindi l'enunciato A nell'Esempio 2.5 è falso. Il metodo della dimostrazione per casi è stato usato in teoria dei numeri prendendo come ipotesi condizionale uno dei più importanti problemi aperti della matematica, l'Ipotesi di Riemann generalizzata [**IR90**, pp. 358–361].

La congettura di Erdős-Woods è stato formulata Erdős e studiata da Woods [**Woo81**] in collegamento a interessanti problemi di logica (si veda pag. 130). Su questa congettura non si sa molto, eccetto che discende dalla congettura *abc* (Esempio 3.3) e che $k \neq 1$, dato che le coppie $(2, 3)$ e $(8, 9)$ hanno gli stessi divisori primi; non è noto se $k \neq 2$. Per ulteriori informazioni si veda [**Guy04**, B29].

Gli enunciati nell'Esercizio 2.8 sono congetture aperte o risultati importanti di teoria dei numeri. Il postulato di Bertrand è stato congetturato nel 1845 da Bertrand e dimostrato nel 1850 da Chebyshev. Vinogradov dimostrò nel 1937 il teorema che porta il suo nome. (Si noti che la congettura di Goldbach implica questo risultato.) I teoremi in (viii) e (ix) sono stati dimostrati rispettivamente da Dirichlet nel 1837, e da Green e Tao nel 2004.

Le congetture di Legendre, di Goldbach, dei primi gemelli, di Beal e la parte (vi) dell'Esercizio 2.8 sono a tutt'oggi (15 dicembre 2014) problemi aperti. Le prime due portano il nome dei matematici che le hanno formulate, Goldbach e Legendre, mentre la congettura di Beal è stata formulata nel 1993 indipendentemente da Beal[3] e da Granville. La parte (vi) dell'Esercizio 2.8 è un teorema se al posto di quattro cubi si prendono sette cubi — vedi le Osservazioni a pagina 62.

Fermat circa nel 1637 scrisse sul margine del libro *Arithmetica* di Diofanto:

> Ho scoperto una dimostrazione davvero meravigliosa del fatto che è impossibile separare un cubo in due cubi, o una quarta potenza in due quarte potenze, e in generale nessun' altra potenza superiore alla seconda può essere divisa in due potenze del medesimo tipo. Questo margine è troppo piccolo per riportarla.[4]

Fermat non esibì mai una dimostrazione di questo enunciato (anche se diede una dimostrazione per il caso di esponente 4) che divenne noto come l'*ultimo teorema di Fermat* — Esercizio 2.8 parte (vii). Nel corso dei secoli questa congettura divenne uno dei più noti problemi aperti della

[2] L'enunciato di questo teorema era il settimo nella famosa lista dei problemi aperti in matematica redatta da Hilbert nel 1900.

[3] Andrew Beal è un magnate texano con l'hobby della teoria dei numeri e ha offerto $100.000 per la soluzione della congettura. In Italia, invece, i magnati (brianzoli e non) sembrano avere altri hobby.

[4] Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

matematica ed è stata finalmente dimostrata nel 1995 da Wiles e Taylor, guadagnandosi finalmente il titolo di teorema.

L'enunciato dell'Esercizio 2.10 è il caso particolare di un risultato generale di teoria dei grafi, noto come Teorema di Ramsey (si veda pagina 96), che può essere formulato come segue: per ogni n c'è un $m > n$ tale che prese m persone ce ne sono almeno n che si conoscono l'un l'altra, o che sono totalmente estranee.

Gli Esercizi 2.12 e 2.13 sono tratti da [**PD11**].

3. Linguaggi

3.A. Simboli, termini e formule.

Simboli. Un linguaggio L del prim'ordine consiste dei seguenti oggetti:

- la parentesi aperta (e la parentesi chiusa),
- i simboli $\neg$, $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$, $\exists$, $\forall$ e $=$,
- una lista infinita di simboli detti **variabili**

  $$v_0, v_1, v_2, \ldots$$

  Le lettere $x, y, z, \ldots$, eventualmente decorate con apici o pedici, indicano una generica variabile v_n,
- dei simboli di costante $c, d, e, \ldots$,
- dei simboli di funzione $f, g, h, \ldots$,
- dei simboli di predicato $P, Q, R, \ldots$

Ad ogni simbolo di funzione e di predicato è associato un numero intero positivo detto **arietà** del simbolo — i simboli di arietà 1, 2 e 3 si dicono, rispettivamente, simboli unari, binari e ternari.

I simboli di costante, di funzione e di predicato si dicono simboli non logici e caratterizzano il linguaggio in questione. Per il momento possiamo supporre che siano in quantità finita; per un esempio differente si vedano le Sezioni 5.D.6 e 5.D.7.

Termini. L'insieme dei **termini** di un linguaggio L è definito induttivamente dalle clausole:

- una variabile è un termine,
- un simbolo di costante è un termine,
- un'espressione del tipo $f(t_1, \ldots, t_n)$ è un termine, dove f è un simbolo di funzione n-ario e $t_1, \ldots, t_n$ sono termini.

Osservazione 3.1. Il lettore più attento avrà notato che nello scrivere $f(t_1, \ldots, t_n)$ oltre ai simboli ufficiali abbiamo anche usato la virgola — un simbolo che non era contemplato nella nostra lista ufficiale — per separare i termini t_i. L'uso della virgola è per motivi puramente tipografici (delimitare visivamente gli oggetti) e sarebbe indubbiamente più corretto scrivere

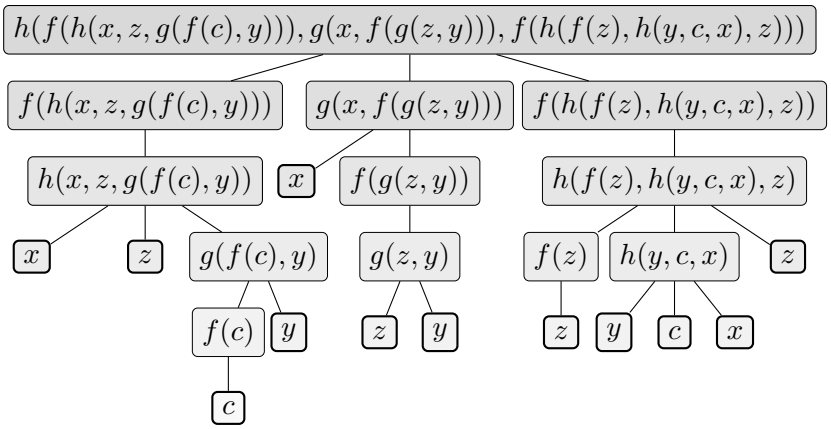


Figura 1. L'albero sintattico del termine descritto nella (3.1).

$f(t_1 \dots t_n)$ invece di $f(t_1, \dots, t_n)$. Questo però presuppone implicitamente la non ambiguità della lettura delle espressioni: se un termine di L può essere letto come $f(t_1 \dots t_n)$ e come $g(u_1 \dots u_m)$ allora $n = m$, $f = g$ e $t_i = u_i$ per $i = 1, \dots, n$. Dimostreremo questo risultato sulla non-ambiguità delle espressioni nella Sezione 20 dove vedremo che, in linea di principio, potremmo evitare anche l'uso delle parentesi. Ma all'inizio dello studio della logica una notazione leggermente ridondante è preferibile ad una notazione eccessivamente stringata.

Un termine t è una sequenza finita di simboli (ottenuta secondo un protocollo ben definito), ma può essere visualizzato meglio mediante il suo **albero sintattico**[5] in cui la radice è etichettata da t e gli altri nodi sono etichettati da termini che compongono t. Per esempio l'albero sintattico del termine

$$h(f(h(x,z,g(f(c),y))),g(x,f(g(z,y))),f(h(f(z),h(y,c,x),z))), \tag{3.1}$$

dove c è un simbolo di costante e f, g e h sono simboli di funzione di arietà 1, 2 e 3, è l'oggetto descritto nella Figura 1. I nodi terminali, cioè quelli che non hanno nessun nodo al di sotto di essi, sono etichettati con le variabili e coi simboli di costante e sono evidenziati da una cornice più spessa. Potremmo anche semplificare la notazione etichettando ogni nodo non terminale con il simbolo di funzione usata per costruire quel termine. In questo caso l'albero sintattico può essere disegnato come nella Figura 2. I nodi dell'albero sintattico di t sono i sottotermini di t.

[5]La botanica della logica e dell'informatica è un po' bizzarra, visto che gli alberi crescono all'ingiù. Forse *radici* sarebbe un nome più appropriato, ma a quel punto avremmo bisogno di un altro nome per il nodo che si trova più in alto.

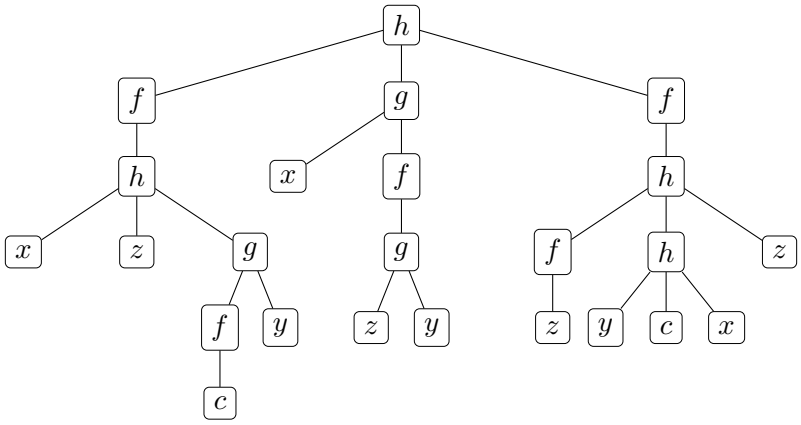


Figura 2. Una descrizione semplificata dell'albero sintattico della Figura 1.

Notazione. Se f è un simbolo di funzione binaria, si usa solitamente la notazione infissa $t_1\ f\ t_2$ invece di quella prefissa $f(t_1, t_2)$. In particolare scriveremo $t_1 + t_2$ e $t_1 \cdot t_2$ al posto di $+(t_1, t_2)$ e $\cdot(t_1, t_2)$.

Se f è un simbolo di funzione binaria, l'espressione $t_1\ f \dots f\ t_n$ è ambigua, dato che dipende da dove inseriamo le parentesi. Per esempio, le possibili definizioni di $t_1\ f\ t_2\ f\ t_3$ sono due: $t_1\ f\ (t_2\ f\ t_3)$ e $(t_1\ f\ t_2)\ f\ t_3$. In generale, il numero di modi possibili di mettere le parentesi tra $n+1$ oggetti è dato dal *numero di Catalan di ordine* n, $\binom{2n}{n} - \binom{2n}{n-1}$. Per questo motivo introduciamo la seguente:

Convenzione. Nell'espressione $t_1\ f \dots f\ t_n$ si intende sempre che si associa a destra, cioè $t_1\ f\ (t_2\ f\ (\dots (t_{n-1}\ f\ t_n) \dots))$. In particolare $t_1 + \dots + t_n$ sta per $t_1 + (\dots + (t_{n-1} + t_n) \dots)$ e $t_1 \cdot \dots \cdot t_n$ sta per $t_1 \cdot (\dots \cdot (t_{n-1} \cdot t_n) \dots)$. Utilizzeremo le abbreviazioni

$$nt \text{ al posto di } \underbrace{t + \dots + t}_{n} \quad \text{e} \quad t^n \text{ al posto di } \underbrace{t \cdot \dots \cdot t}_{n}.$$

Infine, se f è un simbolo di funzione unaria e t è un termine, la scrittura

$$f^{(n)}(t)$$

denota il termine

$$\underbrace{f(\dots f}_{n \text{ volte}}(t) \dots).$$

Una misura di complessità per i termini è una funzione dall'insieme dei termini a valore nei numeri naturali tale per cui la complessità di un termine t sia sempre maggiore della complessità dei termini che concorrono a costruire t. Abbiamo due misure naturali di complessità per un termine t:

- $\mathrm{lh}(t)$, la **lunghezza** (incluse le parentesi) della stringa t e
- $\mathrm{ht}(t)$, l'**altezza** di t, cioè la massima lunghezza di un cammino nell'albero sintattico di t che parta dalla radice ed arrivi ad un nodo terminale.

Quindi se t è il termine descritto in (3.1) a pagina 20, allora $\mathrm{lh}(t) = 48$ e $\mathrm{ht}(t) = 5$.

Osservazione 3.2. Le misure di complessità come lh e ht, sono utili per fare dimostrazioni per induzione sull'insieme dei termini. Per esempio, per verificare che ogni termine gode di una proprietà $\mathcal{P}$ si verifica che la proprietà $\mathcal{P}$ vale per i termini di complessità minima (caso base) e che se $\mathcal{P}$ vale per tutti i termini di complessità inferiore alla complessità di t, allora anche t gode della proprietà $\mathcal{P}$.

La scrittura $t(x_1, \ldots, x_n)$ indica che le variabili che compaiono in t sono tra le $x_1, \ldots, x_n$. (Non chiediamo che tutte le x_i occorrano in t.) In algebra, se $f(X)$ denota un polinomio nella variabile X, allora $f(Y)$ denota il polinomio f dove X è stata sostituita da Y. Analogamente, se x occorre in $t(x)$, il termine ottenuto sostituendo s al posto di x viene indicato con $t[s/x]$ o, se la variabile x è chiara dal contesto, semplicemente con $t(s)$. Un termine si dice **chiuso** se non contiene variabili, cioè se è stato costruito a partire dai simboli di costante e dai simboli di funzione. (Ovviamente se il linguaggio non contiene costanti, allora non ci sono termini chiusi.)

Formule. Una **formula atomica** è un'espressione della forma

$$P(t_1, \ldots, t_n)$$

oppure della forma

$$t_1 = t_2$$

dove $t_1, t_2, \ldots, t_n$ sono termini e P è un simbolo di predicato n-ario. L'insieme delle **formule** è definito induttivamente dalle clausole:

- una formula atomica è una formula,
- se φ è una formula, allora anche $(\neg\varphi)$ è una formula,
- se φ e ψ sono formule, allora anche $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \Rightarrow \psi)$ e $(\varphi \Leftrightarrow \psi)$ sono formule,
- se φ è una formula e x è una variabile, allora anche $\exists x\varphi$ e $\forall x\varphi$ sono formule.

Useremo le lettere greche φ, ψ, e χ, variamente decorate, per le formule.[6] Una formula della forma $(\neg\varphi)$ è detta negazione; analogamente, una formula della forma $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \Rightarrow \psi)$, $(\varphi \Leftrightarrow \psi)$, $\exists x\varphi$ e $\forall x\varphi$ è detta,

[6] Per le formule useremo talvolta anche le prime lettere dell'alfabeto in $\mathrm{A}, \mathrm{B}, \mathrm{C}, \ldots$ in carattere tondo, come del resto abbiamo già fatto implicitamente nella Sezione 2.A.

rispettivamente, congiunzione, disgiunzione, implicazione, bi-implicazione, **formula esistenziale** e **formula universale**.

Convenzioni. (i) Per evitare l'eccessivo proliferare di parentesi, le sopprimeremo quando ciò non comporti ambiguità. Per esempio scriveremo $\varphi \wedge \psi$, $\varphi \vee \psi$, $\varphi \Rightarrow \psi$ e $\varphi \Leftrightarrow \psi$ invece di $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, ...; ma se vogliamo prendere la negazione di una di queste formule reintrodurremo le parentesi. Seguiremo la convenzione che $\wedge$ e $\vee$ legano più fortemente di $\Rightarrow$ e $\Leftrightarrow$, e che $\neg$ lega più fortemente di tutti gli altri connettivi. Quindi

$$\varphi \wedge \psi \Rightarrow \chi, \quad \neg\varphi \vee \psi$$

sono abbreviazioni per

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

In analogia con quanto detto per i termini, se $\odot$ è un connettivo binario (cioè diverso da $\neg$) scriveremo $\varphi_1 \odot \cdots \odot \varphi_n$ al posto di $\varphi_1 \odot (\varphi_2 \odot (\cdots \odot \varphi_n) \dots)$.

(ii) Se P è un simbolo di relazione binario spesso useremo la notazione infissa $t_1\ P\ t_2$ al posto della notazione prefissa $P(t_1, t_2)$. In particolare, scriveremo $s < t$ invece di $<(s, t)$.

(iii) $t_1 \neq t_2$ è un'abbreviazione di $\neg(t_1 = t_2)$.

Le **sottoformule** di φ sono φ e le formule usate per costruire φ. Una sottoformula di φ che sia diversa da φ si dice **sottoformula propria**. In altre parole:

- se φ è atomica, allora non ha sottoformule proprie,
- se φ è $\neg\psi$, allora le sue sottoformule proprie sono ψ e le sottoformule proprie di ψ,
- se φ è $\psi \odot \chi$ dove $\odot$ è un connettivo binario, allora le sue sottoformule proprie sono: ψ, χ, le sottoformule proprie di ψ e le sottoformule proprie di χ,
- se φ è $\exists x\psi$ o $\forall x\psi$, allora le sottoformule proprie di φ sono ψ e tutte le sottoformule proprie di ψ.

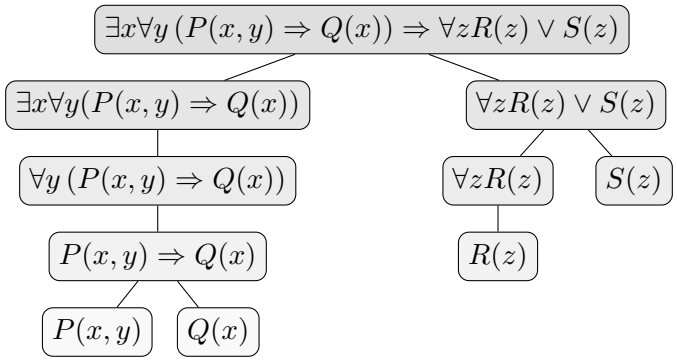
Per esempio, le sottoformule proprie della formula

$$\exists x \forall y\, (P(x, y) \Rightarrow Q(x)) \Rightarrow \forall z R(z) \vee S(z) \tag{3.2}$$

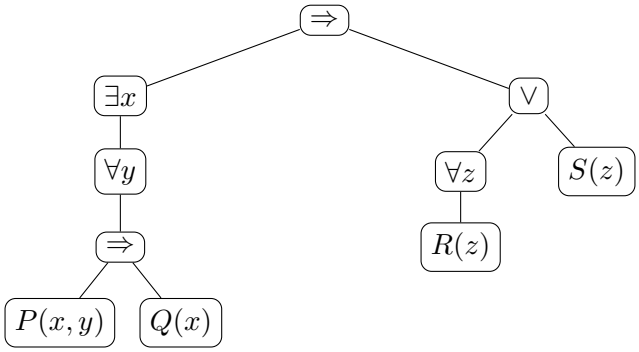
sono $\exists x \forall y\,(P(x,y) \Rightarrow Q(x))$, $\forall z R(z) \vee S(z)$ e tutte le sottoformule proprie di queste due. Quindi la lista completa delle sottoformule proprie di (3.2) è:

$$\begin{array}{rr} \exists x \forall y (P(x,y) \Rightarrow Q(x)) & \forall z R(z) \vee S(z) \\ \forall y (P(x,y) \Rightarrow Q(x)) & \forall z R(z) \\ P(x,y) \Rightarrow Q(x) & R(z) \\ P(x,y) & S(z) \\ Q(x) & \end{array}$$

Come per i termini, anche le formule possono essere descritte mediante alberi: l'albero sintattico della formula (3.2) è



o più semplicemente



I nodi dell'albero sintattico di φ sono le sottoformule di φ. Anche in questo caso abbiamo due nozioni di complessità : la lunghezza e l'altezza, definite in modo del tutto simile a quanto detto per i termini a pagina 22.

3.B. Ancora sulla formalizzazione. Nelle pagine precedenti abbiamo visto alcuni esempi di espressioni formalizzabili in un dato linguaggio L, ma ci capiterà spesso di imbatterci in frasi che *non* sono formalizzabili in L, anche se magari lo sono in un linguaggio più ricco. In matematica si fa spesso uso di espressioni contenenti quantificatori e connettivi che però non

sono delle formule secondo la nostra definizione ufficiale, quindi dovremo imparare a distinguere le formule ufficiali da quelle che potremmo chiamare **pseudo-formule**. Queste ultime sono semplicemente delle abbreviazioni stenografiche/simboliche di frasi matematiche espresse in un linguaggio naturale. Per esempio le espressioni contenenti prodotti non sono formalizzabili usando solo l'addizione. L'espressione $x \cdot y$ non può essere resa con

$$\underbrace{x + \cdots + x}_{y}$$

quando x, y sono numeri naturali: l'espressione qui sopra non è un termine, dato che la sua lunghezza non è un intero fissato, ma dipende da y. (Naturalmente, un'espressione del tipo $x \cdot 3$ può essere scritta come $x + (x + x)$, che è un termine.) Per esempio, nell'Esercizio 2.8 parte (vii) a pagina 16, non possiamo eliminare il simbolo per l'esponenziale rimpiazzandolo con

$$x^y = \underbrace{x \cdots x}_{y}$$

perché il membro di destra non è un termine. Come vedremo nella Sezione 6.B, l'esponenziale può essere scritto usando solo addizione e moltiplicazione, ma questo è un risultato per nulla banale.

In generale le espressioni contenenti delle ellissi possono presentare problemi per la formalizzazione. Per esempio il

Problema di Waring. *Per ogni $k > 1$ c'è un n tale per cui ogni naturale è somma di n numeri che sono delle potenze di esponente k.*

viene formalizzato così:

$$\forall k > 1 \exists n \forall x \exists y_1, \ldots, y_n \left(x = y_1^k + \cdots + y_n^k \right). \tag{3.3}$$

La scrittura qui sopra, benché perfettamente accettabile nell'uso quotidiano è una pseudo-formula, dato che il numero di quantificatori all'inizio dell'espressione non è fissato una volta per tutte. Ciò non significa che ci sia qualcosa di errato o sconveniente in quanto scritto in (3.3) — semplicemente non è una formula secondo la nostra definizione ufficiale. Non significa neppure che il problema di Waring non sia formalizzabile mediante una formula del prim'ordine — si veda l'Esercizio 6.51.

In alcuni casi può non essere evidente come formalizzare un enunciato in un dato linguaggio.

Esempio 3.3. La **congettura *abc*** asserisce che per ogni $\varepsilon > 0$ c'è una costante κ_ε tale che se a, b, c sono coprimi fra loro e $c = a + b$, allora $c \leq \kappa_\varepsilon d^{(1+\varepsilon)}$, dove d è il prodotto dei fattori primi distinti di a, b e c.

A prima vista la formalizzazione di questo enunciato nel linguaggio dell'aritmetica sembra improponibile, per via di numeri reali ε presente

nell'esponenziale $d^{(1+\varepsilon)}$. Tuttavia il reale ε può essere preso arbitrariamente piccolo, quindi della forma $1/n$, mentre κ_ε deve essere sufficientemente grande, per cui la disuguaglianza $c \leq \kappa_\varepsilon d^{(1+\varepsilon)}$ diventa $c^n \leq m d^{n+1}$. Quindi la congettura *abc* è formalizzabile così:

$$\forall n\, \exists m\, \forall a, b, c, d\, \big(n > 0 \wedge \boxed{d \text{ è il prodotto dei fattori primi distinti di } a,\ b \text{ e } c} \\ \wedge \boxed{a,\ b,\ c \text{ sono coprimi}} \wedge c = a + b \Rightarrow c^n \leq m d^{n+1}\big),$$

dove $\boxed{d \text{ è il prodotto dei fattori primi distinti di } a,\ b \text{ e } c}$ può essere resa come

$$\forall p \left(\Pr(p) \Rightarrow p^2 \nmid d \wedge (p \mid d \Leftrightarrow p \mid a \vee p \mid b \vee p \mid c)\right)$$

e $\boxed{a,\ b,\ c \text{ sono coprimi}}$ può essere resa come

$$\neg\exists p\, [\Pr(p) \wedge ((p \mid a \wedge p \mid b) \vee (p \mid a \wedge p \mid c) \vee (p \mid b \wedge p \mid c))]\,.$$

Naturalmente, possiamo sostituire i simboli 0, $<$, $\mid$ e Pr con le loro definizioni in termini di somma e prodotto, e per quanto detto poco sopra, un discorso analogo si potrebbe applicare all'esponenziale.

3.C. Strutture e validità. Le formule sono strumenti particolarmente utili per studiare le strutture algebriche o le strutture d'ordine, e sono usate in maniera più o meno esplicita nella matematica. In algebra si parte da una famiglia di strutture algebriche e selezionando le proprietà rilevanti della struttura si definiscono le nuove strutture algebriche. Naturalmente, per parlare delle proprietà della struttura abbiamo bisogno di un linguaggio opportuno — per esempio, per definire la nozione di semigruppo partiamo da un insieme non vuoto S dotato di un'operazione binaria $*$ e richiediamo che valga le proprietà associativa

$$\forall x, y, z \in S\, ((x * y) * z = x * (y * z)) \tag{3.4}$$

Esempi di semigruppi sono:

- i numeri naturali $\mathbb{N}$ con l'operazione di addizione $+$,
- l'insieme $M_{n,n}(R)$ delle matrici $n \times n$ su un anello R con l'operazione di prodotto matriciale,
- l'insieme F delle funzioni da un insieme X in sé stesso con l'operazione di composizione $\circ$,

e così via. L'espressione (3.4) è una pseudo-formula, dato che abbiamo seguito l'usanza solita di indicare che gli oggetti su cui si quantifica appartengono ad un dato insieme, allontanandoci dalla definizione ufficiale di formula. In logica si preferisce partire da un linguaggio (che in questo caso contiene soltanto il simbolo di operazione binaria $*$) e dire che la formula

$$\forall x, y, z\, ((x * y) * z = x * (y * z)) \tag{3.5}$$

è vera nelle strutture $(\mathbb{N}, +)$, $(M_{n,n}(R), \cdot)$, $(F, \circ)$, ... In altre parole: il simbolo di operazione $*$ viene interpretato di volta in volta come un'operazione diversa, a seconda della struttura specifica.

Il nostro obbiettivo è:

> trovare una procedura per verificare quando una formula φ è vera in una struttura.

Innanzitutto osserviamo che alcune formule risultano vere in ogni struttura, indipendentemente dal significato che attribuiamo ai simboli del linguaggio — formule di questo tipo si dicono **valide**. All'estremo opposto abbiamo le formule **insoddisfacibili** cioè che risultano sempre false in ogni struttura, indipendentemente dal significato dei simboli. Per esempio, se P e f sono simboli di predicato e di funzione n-ari, allora le formule

$$\begin{gathered} x = x \\ x = y \Rightarrow y = x \\ x = y \wedge y = z \Rightarrow x = z \\ x_1 = y_1 \wedge \cdots \wedge x_n = y_n \Rightarrow (P(x_1, \ldots, x_n) \Leftrightarrow P(y_1, \ldots, y_n)) \\ x_1 = y_1 \wedge \cdots \wedge x_n = y_n \Rightarrow f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n) \end{gathered} \tag{3.6}$$

sono valide, visto che abbiamo stabilito che il simbolo $=$ denota sempre l'usuale relazione di uguaglianza. Invece la formula

$$\forall x, y\, (x \cdot y = y \cdot x)$$

è **soddisfacibile** (vale a dire: non insoddisfacibile) ma non valida, dato che è vera o falsa a seconda che il simbolo $\cdot$ denoti un'operazione commutativa o meno, ad esempio, la moltiplicazione di numeri reali piuttosto che il prodotto di matrici. Analogamente

$$\forall x, y\, (x < y \Rightarrow \exists z\, (x < z \wedge z < y))$$

è un'affermazione vera nei razionali o nei reali, ma falsa negli interi, quindi è una formula soddisfacibile, ma non valida. Se vogliamo istituire una procedura per verificare se una formula è vera in una struttura, dobbiamo cominciare ad esaminare le formule più semplici, vale a dire le formule atomiche. Tuttavia già il caso delle formule atomiche è problematico. Per esempio, per verificare se la formula $x < y$ è vera in un insieme ordinato $(A, <)$ è necessario attribuire un valore alle variabili x e y. Viceversa, ci sono formule contenenti variabili libere che sono vere o false in una struttura, indipendentemente dal valore attribuito alle variabili. Per esempio, la formula $\neg(x < y) \vee (x < y)$ è vera in ogni struttura (in cui abbia senso interpretare il simbolo $<$) indipendentemente dal valore attribuito alle variabili. Infatti, in generale, ogni formula della forma $\varphi \Rightarrow \varphi$ ovvero $\neg\varphi \vee \varphi$ è valida,

indipendentemente da ciò che φ asserisce. Per i medesimi motivi, anche $\varphi \wedge \psi \Rightarrow \varphi$ è valida.

3.C.1. *Tautologie.* Dagli esempi qui sopra si vede come certe formule sono valide in virtù dei connettivi. Per studiare questo tipo di validità bisogna analizzare come una formula è costruita a partire da formule atomiche, esistenziali e universali. Diremo che una formula φ è **combinazione booleana**[7] di formule $\mathrm{A}_1, \ldots, \mathrm{A}_n$ se φ è ottenuta da queste senza l'uso di quantificatori. Se le A_i sono atomiche o esistenziali o universali (cioè non sono combinazioni booleane di loro sottoformule), allora diremo che $\mathrm{A}_1, \ldots, \mathrm{A}_n$ sono le **componenti primitive** di φ. In altre parole, sono i nodi dell'albero sintattico di φ al di sopra dei quali non compaiono formule quantificate. Per esempio le sottoformule primitive della formula in (3.2) a pagina 23 sono

$$\underbrace{\boxed{\exists x \forall y \, (P(x,y) \Rightarrow Q(x))}}_{\mathrm{A}} \qquad \underbrace{\boxed{\forall z R(z)}}_{\mathrm{B}} \qquad \underbrace{\boxed{S(z)}}_{\mathrm{C}}$$

quindi la formula $\exists x \forall y \, (P(x,y) \Rightarrow Q(x)) \Rightarrow \forall z R(z) \vee S(z)$ può essere scritta come $\mathrm{A} \Rightarrow \mathrm{B} \vee \mathrm{C}$.

Se fissiamo arbitrariamente dei valori di verità per le formule primitive, possiamo calcolare il valore di verità di una φ usando le proprietà dei connettivi. Più precisamente: una **valutazione** è una funzione

$$v \colon \{\varphi \mid \varphi \text{ è atomica o esistenziale o universale}\} \to \{0,1\},$$

dove 0 rappresenta il falso e 1 rappresenta il vero. Ogni valutazione v può essere estesa ad una funzione (che verrà indicata ancora con v) dall'insieme di tutte le formule a valori in $\{0,1\}$, ponendo

$$\begin{aligned} v(\neg\varphi) &= 1 - v(\varphi), \\ v(\varphi \wedge \psi) &= \min\{v(\varphi), v(\psi)\} = v(\varphi) \cdot v(\psi) \\ v(\varphi \vee \psi) &= \max\{v(\varphi), v(\psi)\}, \\ v(\varphi \Rightarrow \psi) &= 1 - (v(\varphi) \cdot (1 - v(\psi))) \\ v(\varphi \Leftrightarrow \psi) &= v(\varphi) + v(\psi) + 1 \pmod 2. \end{aligned}$$

Diremo che una formula è vera secondo v se e solo se $v(\varphi) = 1$, altrimenti diremo che è falsa secondo v. (Chiaramente la definizione di v qui sopra è imposta dal significato delle costanti logiche — Sezione 2.A.)

Una formula φ è

- una **tautologia** se $v(\varphi) = 1$ per ogni valutazione v,
- una **contraddizione proposizionale** se $v(\varphi) = 0$ per ogni valutazione v.

[7] Il motivo dell'aggettivo *booleano* risulterà chiaro nelle sezioni seguenti.

Quindi una tautologia è una formula valida e una contraddizione proposizionale è una formula insoddisfacibile. Non tutte le formule valide sono tautologie — per esempio, si vedano le formule in (3.6) a pagina 27.

Siamo ora in grado di rendere rigorosi i discorsi fatti nella Sezione 2.A quando asserivamo che due espressioni costruite a partire da connettivi (per esempio $A \Rightarrow B$ e $\neg A \vee B$) erano equivalenti. Diremo che

- φ è **tautologicamente equivalente** a ψ se $\psi \Leftrightarrow \varphi$ è una tautologia,
- φ è **conseguenza tautologica di** $\psi_1, \dots, \psi_n$ se $(\psi_1 \wedge \dots \wedge \psi_n) \Rightarrow \varphi$ è una tautologia.

Queste nozioni sono usate in matematica, spesso in modo implicito, quando invece di dimostrare un'affermazione del tipo $\varphi \Rightarrow \psi$ si dimostra una formula tautologicamente equivalente ad essa, per esempio $\neg\psi \Rightarrow \neg\varphi$ oppure $\neg\varphi \vee \psi$.

Per verificare se una formula φ, che è combinazione booleana di sue sottoformule primitive $A_1, \dots, A_n$, è una tautologia o meno, si utilizza una tabella nota come **tavola di verità** di φ. Si tratta di una tabella

A_1	A_2	$\dots$	A_n	φ
0	0	$\dots$	0	i_1
0	0	$\dots$	1	i_2
$\vdots$	$\vdots$		$\vdots$	$\vdots$
1	1	$\dots$	1	i_{2^n}

con $n+1$ colonne indicizzate da A_1, $A_2, \dots, A_n$ e φ, e 2^n righe: nelle prime n colonne scriviamo tutte le possibili valutazioni v di $A_1, \dots, A_n$ e nell'ultima colonna la valutazione di φ. Quindi φ è una tautologia se e solo se la colonna $n+1$-esima non contiene 0.

La tavola di verità della negazione è

A	$\neg$A
0	1
1	0

mentre quelle dei connettivi binari sono

A	B	A $\vee$ B	A $\wedge$ B	A $\Rightarrow$ B	A $\Leftrightarrow$ B
0	0	0	0	1	1
1	0	1	0	0	0
0	1	1	0	1	0
1	1	1	1	1	1

Osservazioni 3.4. (a) Mentre la nozione di *equivalenza tra formule* è stata presentata in modo informale — due formule sono equivalenti se dicono la stessa cosa — la nozione di *equivalenza tautologica* è una vera e propria definizione matematica. La definizione di *equivalenza logica* (che

formalizza l'idea intuitiva di equivalenza tra formule) verrà introdotta nel Capitolo VI.

(b) Se ogni connettivo può essere espresso in termini di una lista prefissata di connettivi, diremo che questa lista è un **insieme adeguato di connettivi**. In altre parole: per definire le formule avremmo potuto limitarci ai connettivi presenti nella lista specificata. Poiché $\mathrm{A} \vee \mathrm{B}$ e $\mathrm{A} \wedge \mathrm{B}$ sono tautologicamente equivalenti a $\neg(\neg\mathrm{A} \wedge \neg\mathrm{B})$ e $\neg(\neg\mathrm{A} \vee \neg\mathrm{B})$ rispettivamente, ne segue che $\{\neg, \wedge\}$ e $\{\neg, \vee\}$ sono insiemi adeguati di connettivi.

Supponiamo che φ sia combinazione booleana di sue sottoformule primitive $\mathrm{A}_1, \ldots, \mathrm{A}_n$. Poiché $\mathrm{B} \Rightarrow \mathrm{C}$ è tautologicamente equivalente a $\neg\mathrm{B} \vee \mathrm{C}$ e $\mathrm{B} \Leftrightarrow \mathrm{C}$ è tautologicamente equivalente a $(\neg\mathrm{B} \vee \mathrm{C}) \wedge (\neg\mathrm{C} \vee \mathrm{B})$ è possibile trasformare (cioè trovare una formula tautologicamente equivalente a) φ di modo che compaiano soltanto i connettivi $\neg$, $\vee$ e $\wedge$. Applicando ripetutamente le leggi di De Morgan e la regola della doppia negazione, possiamo trasformare la formula di modo che il simbolo di negazione $\neg$ risulti applicato soltanto a formule primitive. Infine applicando ripetutamente la mutua distributività della disgiunzione e congiunzione, possiamo trasformare φ in una disgiunzione

$$\mathrm{D}_1 \vee \cdots \vee \mathrm{D}_m$$

in cui ciascuna D_i è una congiunzione

$$\mathrm{C}_{i,1} \wedge \cdots \wedge \mathrm{C}_{i,k_i}$$

tale che ciascuna $\mathrm{C}_{i,j}$ è una formula primitiva o la negazione di una formula primitiva. Una formula siffatta si dice in **forma normale disgiuntiva**. Osserviamo che se φ è una contraddizione proposizionale, allora è tautologicamente equivalente a $(\neg\mathrm{A}_1 \wedge \mathrm{A}_1) \vee \cdots \vee (\neg\mathrm{A}_n \wedge \mathrm{A}_n)$. L'Esercizio 3.36 mostra come usare le tavole di verità per calcolare la forma normale disgiuntiva di una formula.

3.C.2. *Variabili libere e vincolate.* Ogni formula contiene una quantità finita di variabili e ogni volta che una variabile compare in una formula parleremo di **occorrenza della variabile nella formula**. Per esempio la variabile z occorre tre volte nella formula $\exists x \forall y\,(P(x,y) \Rightarrow Q(x)) \Rightarrow \forall z R(z) \vee S(z)$ dell'equazione (3.2) a pagina 23: nelle prime due occorrenze la z è muta dato che dire $\forall z R(z)$ ha lo stesso significato di $\forall u R(u)$, cioè ogni oggetto gode della proprietà R, mentre la terza occorrenza serve per asserire che z gode della proprietà S. Le occorrenze del primo tipo si dicono **vincolate**, quelle del secondo tipo si dicono **libere**.

Definizione 3.5. Sia φ una formula e x una variabile.

- Se φ è atomica allora ogni occorrenza di x in φ è libera.

- Se φ è della forma $\neg\psi$ allora le occorrenze libere di x in φ sono esattamente quelle di x in ψ.
- Se φ è della forma $\psi \odot \chi$, dove $\odot$ è un connettivo binario, allora le occorrenze libere di x in φ sono quelle di x in ψ e quelle di x in χ.
- Supponiamo φ sia della forma $\exists y\psi$ oppure $\forall y\psi$. Se y è la variabile x, allora tutte le occorrenze di x in φ sono vincolate. Se invece y è una variabile diversa da x, allora le occorrenze libere di x in φ sono esattamente le sue occorrenze libere di x in ψ.

Diremo che la variabile x occorre libera in φ (equivalentemente: x è una variabile libera di φ) se c'è almeno un'occorrenza libera di x in φ. In analogia con quanto detto per i termini a pagina 22, la notazione

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

serve per porre in evidenziare il fatto che le variabili che occorrono libere in φ sono alcune tra le $x_1, \ldots, x_n$. (Non richiediamo che *ogni* $x_1, \ldots, x_n$ compaia libera o compaia del tutto in φ ed è perfettamente possibile che la formula non contenga alcuna variabile libera, o addirittura nessuna variabile.) Un **enunciato** o **formula chiusa** è una formula che non contiene variabili libere. La **chiusura universale di una formula** φ è la formula $\varphi^\forall$ ottenuta quantificando universalmente tutte le variabili libere di φ; se invece quantificando esistenzialmente tutte le variabili libere si ottiene **chiusura esistenziale** $\varphi^\exists$. Come osservato a pagina 11, nell'uso comune le formule prive di quantificatori sono considerate equivalenti alla loro chiusura universale.

3.C.3. *Sostituibilità.* Un termine, può essere sostituito al posto di una variabile in un altro termine (vedi pag. 22), o in una formula. Se $t_1, \ldots, t_n$ sono termini, l'espressione

$$\varphi[t_1/x_1, \ldots, t_n/x_n]$$

ottenuta rimpiazzando *tutte le occorrenze* di x_i in φ con t_i, non denota necessariamente una formula: per esempio se φ è $\exists x(x < y) \wedge x = y$ e c è una costante, allora $\varphi[c/x]$ è $\exists c(c < y) \wedge c = y$ che non è una formula, visto che solo le variabili possono essere quantificate. Indicheremo con

$$\varphi[\![t_1/x_1, \ldots, t_n/x_n]\!]$$

la formula ottenuta rimpiazzando le *occorrenze libere* di x_i in φ con t_i, $(i = 1, \ldots, n)$. Chiaramente, se una delle variabili, per esempio x_1, non occorre libera in φ, allora la formula diventa $\varphi[\![t_2/x_2, \ldots, t_n/x_n]\!]$, quindi la definizione è di interesse quando tutte le $x_1, \ldots, x_n$ occorrono libere in φ. In questo caso la formula φ asserisce qualche cosa sugli oggetti $x_1, \ldots, x_n$ e $\varphi[\![t_1/x_1, \ldots, t_n/x_n]\!]$ dovrebbe asserire la medesima cosa su $t_1, \ldots, t_n$. Per essere sicuri che ciò avvenga, è però necessario che nessuna variabile di un t_i

risulti vincolata dopo che la sostituzione è avvenuta. Se ciò non accade il significato di $\varphi[\![t_1/x_1, \dots, t_n/x_n]\!]$ può cambiare completamente: per esempio la formula

$$\exists y\,(2 \cdot y + 1 = x) \tag{3.7}$$

dice che x è dispari, $\exists y\,(2 \cdot y + 1 = z + 2)$ dice che $z + 2$ è dispari, ma $\exists y\,(2 \cdot y + 1 = y)$ *non dice* che y è dispari! Un termine t è **sostituibile** per x in φ se nessuna delle variabili di t risulta vincolata da un quantificatore in $\varphi[\![t/x]\!]$. In particolare, se x non occorre libera in φ oppure t è un termine chiuso (cioè non contiene variabili), allora t è sostituibile per x in φ. D'ora in poi stipuliamo che:

Convenzione. Quando scriviamo $\varphi[\![t_1/x_1, \dots, t_n/x_n]\!]$ assumiamo sempre che i termini $t_1, \dots, t_n$ siano sostituibili per $x_1, \dots, x_n$ in φ.

Osservazioni 3.6. (a) È importante che la sostituzione delle $x_1, \dots, x_n$ con $t_1, \dots, t_n$ avvenga in simultanea: se φ è $x_1 < x_2$, allora $\varphi[\![x_2/x_1, x_1/x_2]\!]$ è $x_2 < x_1$, mentre $\varphi[\![x_2/x_1]\!]$ è $x_2 < x_2$ e $(\varphi[\![x_2/x_1]\!])[\![x_1/x_2]\!]$ è $x_1 < x_1$.

(b) Se nessuna delle variabili che occorrono quantificate in φ è tra le $x_1, \dots, x_n$ o tra le variabili dei termini $t_1, \dots, t_n$, allora $\varphi[\![t_1/x_1, \dots, t_n/x_n]\!]$ è la formula $\varphi[t_1/x_1, \dots, t_n/x_n]$ ottenuta sostituendo *ogni* occorrenza di x_i con t_i.

Le formule

$$\exists z\,(2 \cdot z + 1 = x)\,, \quad \exists w\,(2 \cdot w + 1 = x)\,, \quad \exists u\,(2 \cdot u + 1 = x)\,, \quad \dots$$

ottenute sostituendo ovunque la y con una nuova variabile, si dicono **varianti** della formula (3.7) e asseriscono tutte che x è dispari. Fa eccezione il caso in cui ad y venga sostituita x, dato che $\exists x\,(2 \cdot x + 1 = x)$ *non dice* che x è dispari. Ciò è del tutto analogo a quanto avviene in analisi: se f è integrabile le espressioni $\int_0^1 f(x, y)\,\mathrm{d}y$ e $\int_0^1 f(x, z)\,\mathrm{d}z$ sono del tutto equivalenti e denotano una funzione nella variabile x, mentre $\int_0^1 f(x, x)\,\mathrm{d}x$ denota un numero. In generale, una variante di $\varphi(x_1, \dots, x_n)$ è una formula $\varphi'(x_1, \dots, x_n)$ con le medesime variabili libere, ottenuta sostituendo alcune delle variabili quantificate con altre variabili di modo che nessuna occorrenza libera di una x_i in φ risulti vincolata in φ'. Se vogliamo asserire che "y è dispari" prendiamo una variante della (3.7) tale che la variabile quantificata non sia y (né ovviamente x), per esempio $\exists z\,(2z + 1 = x)$. Ciò è sempre possibile, visto che le variabili sono in quantità infinita. A questo punto possiamo sostituire x con y e ottenere $\exists z\,(2z + 1 = y)$.

Questo algoritmo è del tutto generale e ci permette di definire l'operazione di sostituzione in generale: data una formula $\varphi(x_1, \dots, x_n)$ e dei termini $t_1, \dots, t_n$, costruiamo una variante φ' di φ in cui nessuna delle variabili che occorrono vincolate occorrano anche in qualche t_i (così che i termini

$t_1, \ldots, t_n$ risultano essere sostituibili ad $x_1, \ldots, x_n$ in φ'): allora la formula $\varphi'[\![t_1/x_1, \ldots, t_n/x_n]\!]$ coincide con la formula $\varphi'[t_1/x_1, \ldots, t_n/x_n]$.

Se x non occorre libera nella formula φ, allora φ è equivalente a $\exists x\varphi$ e $\forall x\varphi$ — per esempio le formule $\exists x\,(y^2 - 3y + 2 = 0)$ e $\forall x\,(y^2 - 3y + 2 = 0)$ sono equivalenti a $y^2 - 3y + 2 = 0$. La nozione di variabile libera/vincolata ci permette di formulare nella piena generalità le manipolazioni sui quantificatori a cui si è accennato a pagina 8. Ricordiamo che

- $\forall x\,(\varphi \wedge \psi) \Leftrightarrow \forall x\varphi \wedge \forall x\psi$,
- $\exists x\,(\varphi \vee \psi) \Leftrightarrow \exists x\varphi \vee \exists x\psi$,
- $\forall x\varphi \vee \forall x\psi \Rightarrow \forall x\,(\varphi \vee \psi)$,
- $\exists x\,(\varphi \wedge \psi) \Rightarrow \exists x\varphi \wedge \exists x\psi$,

sono formule valide e che le due ultime implicazioni non possono essere trasformate in biimplicazioni. Supponiamo ora che x non occorra libera nella formula φ: se vale $\varphi \wedge \exists x\psi$ allora la x di cui asseriamo ψ è muta in φ e quindi si conclude che $\exists x\,(\varphi \wedge \psi)$. Analogamente, da $\forall x\,(\varphi \vee \psi)$ si ricava $\varphi \vee \forall x\psi$.

Quindi *se x non occorre libera in φ*, le formule

- $\varphi \wedge \exists x\psi \Leftrightarrow \exists x\,(\varphi \wedge \psi)$,
- $\varphi \vee \forall x\psi \Leftrightarrow \forall x\,(\varphi \vee \psi)$,

sono valide, e poiché φ è equivalente tanto a $\exists x\varphi$ quanto a $\forall x\varphi$, anche

- $\forall x\varphi \vee \forall x\psi \Leftrightarrow \forall x\,(\varphi \vee \psi)$,
- $\exists x\varphi \wedge \exists x\psi \Leftrightarrow \exists x\,(\varphi \wedge \psi)$,

sono valide.

Consideriamo per esempio la formula

$$\exists x\left(x^2 - 3x + 2 = 0\right) \wedge \exists x\left(x^2 + x - 12 = 0\right)$$

che asserisce che le due equazioni di secondo grado hanno una radice. Questa formula (che è vera quando x varia sui reali) è equivalente alla formula

$$\exists x\left(x^2 - 3x + 2 = 0 \wedge \exists x\left(x^2 + x - 12 = 0\right)\right)$$

e alla formula

$$\exists x\left(\exists x\left(x^2 - 3x + 2 = 0\right) \wedge x^2 + x - 12 = 0\right).$$

Se volessimo modificare quest'ultima formula, portando all'esterno il quantificatore più interno, dovremmo innanzitutto rimpiazzare $\exists x\,(x^2 - 3x + 2 = 0)$ con la sua variante $\exists y\,(y^2 - 3y + 2 = 0)$ per ottenere quindi

$$\exists x\exists y\left((y^2 - 3y + 2 = 0) \wedge (x^2 + x - 12 = 0)\right).$$

Se non effettuassimo questo cambiamento di variabile, commetteremmo un illecito e otterremmo la formula $\exists x \exists x((x^2-3x+2=0) \wedge (x^2+x-12=0))$ che è equivalente a $\exists x\,((x^2-3x+2=0) \wedge (x^2+x-12=0))$ e che asserisce che le due equazioni hanno una radice in comune (il che è falso quando x varia sui reali).

3.C.4. *Forma prenessa.* Le equivalenze qui sopra sono molto utili per trasformare una formula $\varphi(x_1,\dots,x_n)$ in un'altra formula equivalente $\varphi'(x_1,\dots,x_n)$ che abbia le stesse variabili libere e che sia in **forma prenessa** cioè della forma

$$\mathsf{Q}_1 y_1 \mathsf{Q}_2 y_2 \dots \mathsf{Q}_m y_m \psi,$$

dove $\mathsf{Q}_1,\dots,\mathsf{Q}_n$ sono quantificatori e ψ è **aperta** cioè priva di quantificatori. Il blocco di quantificatori $\mathsf{Q}_1 y_1 \mathsf{Q}_2 y_2 \dots \mathsf{Q}_m y_m$ si dice **prefisso** e la formula ψ si dice **matrice**.

Attenzione. Se una formula non è aperta, non significa che sia chiusa, e viceversa.

Mostriamo come ottenere una formula prenessa logicamente equivalente alla (3.2) a pagina 23

$$\forall x \exists y\,(\neg P(x,y) \vee Q(x)) \Rightarrow \forall z R(z) \vee S(z).$$

Innanzitutto trasformiamo le implicazioni in disgiunzioni

$$\neg\,(\exists x \forall y\,(\neg P(x,y) \vee Q(x))) \vee \forall z R(z) \vee S(z)$$

poi trasformiamo $\neg\,(\exists x \forall y\,(\neg P(x,y) \vee Q(x)))$ in $\forall x \exists y\,(P(x,y) \wedge \neg Q(x))$ e $\forall z R(z)$ in $\forall w R(w)$ così da ottenere

$$\forall x \exists y\,(P(x,y) \wedge \neg Q(x)) \vee \forall w R(w) \vee S(z)$$

quindi $\forall w R(w) \vee S(z)$ diventa $\forall w\,(R(w) \vee S(z))$

$$\forall x \exists y\,(P(x,y) \wedge \neg Q(x)) \vee \forall w\,(R(w) \vee S(z))$$

infine, dato che $(P(x,y) \wedge \neg Q(x)) \vee \forall w (R(w) \vee S(z))$ è equivalente a $\forall w((P(x,y) \wedge \neg Q(x)) \vee R(w) \vee S(z))$ si ottiene

$$\forall x \exists y \forall w\,((P(x,y) \wedge \neg Q(x)) \vee R(w) \vee S(z))\,.$$

Questo esempio suggerisce il seguente algoritmo per ottenere una formula $\varphi'(x_1,\dots,x_n)$ in forma prenessa a partire da $\varphi(x_1,\dots,x_n)$:

Passo 1: trasformare tutte le implicazioni $\mathrm{A} \Rightarrow \mathrm{B}$ in $\neg\mathrm{A} \vee \mathrm{B}$ e tutte le biimplicazioni $\mathrm{A} \Leftrightarrow \mathrm{B}$ in $(\neg\mathrm{A} \vee \mathrm{B}) \wedge (\neg\mathrm{B} \vee \mathrm{A})$,

Passo 2: mediante le leggi di De Morgan, la regola della doppia negazione, e le trasformazioni sui quantificatori viste nella Sezione 2, spostare le negazioni all'interno della formula, fino al livello delle sotto-formule atomiche,

Passo 3: applicare ripetutamente la seguente operazione: trasformare le sotto-formule del tipo $(\mathsf{Q}x\mathrm{A}) \odot (\mathsf{Q}'y\mathrm{B})$ dove Q, Q' sono quantificatori e $\odot$ è $\vee$ oppure $\wedge$, in $\mathsf{Q}z\mathsf{Q}'w\,(\mathrm{A}[\![z/x]\!] \odot \mathrm{B}[\![w/y]\!])$ dove z è sostituibile in A e non occorre libera in B e w è sostituibile in B e non occorre libera in A.

La forma prenessa equivalente ad una data formula è ben lungi dall'essere unica — per esempio, poiché $\mathrm{A} \odot \mathrm{B}$ è equivalente a $\mathrm{B} \odot \mathrm{A}$, nel Passo 3 possiamo trasformare $(\mathsf{Q}x\mathrm{A}) \odot (\mathsf{Q}'y\mathrm{B})$ in $\mathsf{Q}'w\mathsf{Q}z\,(\mathrm{A}[\![z/x]\!] \odot \mathrm{B}[\![w/y]\!])$. In particolare anche

$$\forall w \forall x \exists y\,((P(x,y) \wedge \neg Q(x)) \vee R(w) \vee S(z))$$

è una formula prenessa equivalente alla (3.2).

Se si trasforma in forma prenessa $\forall x \varphi \Rightarrow \psi$ oppure $\exists x \varphi \Rightarrow \psi$ dove x non occorre libera in ψ, si ottiene rispettivamente $\exists x\,(\varphi \Rightarrow \psi)$ e $\forall x\,(\varphi \Rightarrow \psi)$. In altre parole: se B non menziona x, un'affermazione del tipo

> se per qualche x vale A di x, allora è vero che B

è equivalente a

> per ogni x, se vale A di x, allora è vero che B.

Per esempio la frase

> se y è un quadrato, allora è maggiore o uguale a zero

si formalizza come

$$\exists x\,(y = x \cdot x) \Rightarrow y \geq 0$$

o equivalentemente come

$$\forall x\,(y = x \cdot x \Rightarrow y \geq 0)\,.$$

L'altra equivalenza tra

> se per ogni x vale A di x, allora è vero che B

e

> c'è un x per cui A di x implica che B

è più sorprendente (intuitivamente saremmo portati a pensare che $\forall x \varphi \Rightarrow \psi$ debba essere equivalente a $\forall x\,(\varphi \Rightarrow \psi)$) e mostra come l'uso disinvolto dei quantificatori nel linguaggio comune sia prono ad errori. Per esempio, consideriamo il seguente enunciato della teoria degli insiemi:[8]

> due insiemi sono uguali se hanno gli stessi elementi.

[8] Questo è noto come Assioma di Estensionalità — si veda il Capitolo IV, pag. 257–258.

Si formalizza così

$$\forall x \forall y \left(\forall z \left(z \in x \Leftrightarrow z \in y \right) \Rightarrow x = y \right),$$

che in forma prenessa diventa

$$\forall x \forall y \exists z \left(\left(z \in x \Leftrightarrow z \in y \right) \Rightarrow x = y \right),$$

e che si legge

> dati due insiemi x e y c'è un elemento z tale che: se z appartiene ad x se e solo se z appartiene ad y, allora x e y coincidono.

Viene naturale chiedersi chi sia questo elemento z! Per scoprirlo basta prendere il contrappositivo di quanto scritto tra le parentesi, cioè

$$\forall x \forall y \exists z \left(x \neq y \Rightarrow \left(\left(z \in x \wedge z \notin y \right) \vee \left(z \in y \wedge z \notin x \right) \right) \right)$$

che si legge:

> dati due insiemi x e y c'è un elemento z tale che: se x e y sono distinti, allora z appartiene ad uno dei due insiemi ma non all'altro.

Quindi, dati due insiemi x e y basta scegliere uno z che sta in uno dei due insiemi ma non nell'altro, nel caso in cui $x \neq y$, oppure z arbitrario nel caso in cui $x = y$.

È possibile dimostrare risultati sulle formule in forma prenessa procedendo per induzione sulla lunghezza del prefisso: si dimostra che una certa proprietà $\mathcal{P}$ vale per le formule prive di quantificatori, e che se $\mathcal{P}$ vale per una certa φ, allora vale anche per $\exists x \varphi$ e per $\forall x \varphi$. Poiché ogni formula è equivalente ad una in forma prenessa, questo metodo può essere usato per dimostrare che una proprietà $\mathcal{P}$ vale per tutte le formule.

La lunghezza del prefisso è una nozione di complessità per le formule in forma prenessa, analoga alla nozione di lunghezza e altezza introdotte alla fine della Sezione 3.A. Tuttavia, in molte applicazioni, è più utile utilizzare un'altra misura di complessità, basata sull'alternanza di blocchi di quantificatori nel prefisso:

- se il prefisso è costituito da un unico blocco di quantificatori universali si ha una $\forall$-formula; se è costituito da un unico blocco di quantificatori esistenziali si ha una $\exists$-formula,
- se il prefisso è costituito da un blocco di quantificatori universali seguito da un blocco di quantificatori esistenziali si ha una $\forall\exists$-formula; se è costituito da un blocco di quantificatori esistenziali seguito da un blocco di quantificatori universali si ha una $\exists\forall$-formula,

- se il prefisso è costituito da un blocco di quantificatori universali seguito da un blocco di quantificatori esistenziali seguito da un blocco di quantificatori universali si ha una $\forall\exists\forall$-formula; se è costituito da un blocco di quantificatori esistenziali seguito da un blocco di quantificatori universali seguito da un blocco di quantificatori esistenziali si ha una $\exists\forall\exists$-formula,

e così via. La negazione di una $\forall$-formula è equivalente ad una $\exists$-formula, e viceversa; la negazione di una $\forall\exists$-formula è equivalente ad una $\exists\forall$-formula, e viceversa; la negazione di una $\forall\exists\forall$-formula è equivalente ad una $\exists\forall\exists$-formula, e viceversa; ecc.

3.D. Soddisfazione di enunciati. Fissiamo un linguaggio del prim'ordine L. Chiaramente L verrà scelto in funzione del tipo di struttura che si intende studiare — per studiare i campi avremo bisogno di due simboli per le operazioni di somma $+$ e prodotto $\cdot$, un simbolo di operazione unaria $-$ per denotare l'opposto di un numero, più i simboli per lo zero 0 e per l'unità del campo 1; per studiare i gruppi abeliani ordinati dobbiamo usare un linguaggio con un simbolo $+$ per l'operazione di somma gruppale e un simbolo $\lhd$ per l'ordinamento, ecc. Una **struttura per** L o L**-struttura** consiste di:

- un insieme non vuoto M, detto **universo** o **dominio** della struttura,
- degli elementi privilegiati c^M di M, uno per ogni simbolo di costante c del linguaggio L,
- delle operazioni $*^M, +^M, \ldots$, una per ogni simbolo di operazione $*, +, \ldots$ del linguaggio L,
- dei sottoinsiemi $P^M \subseteq M^n$, uno per ogni simbolo P di predicato n-ario del linguaggio L.

Talvolta, al fine di uniformarci all'uso comune o se questo aiuta la leggibilità, useremo la lettera M come pedice invece che apice e scriveremo $c_M, *_M, +_M, P_M \ldots$ per indicare gli elementi privilegiati, le operazioni, i sottoinsiemi della struttura. Quando non c'è pericolo di confusione identificheremo la struttura con il suo domino, come avviene negli altri campi della matematica — in algebra si dice "dato un gruppo G" e raramente si deve ricorrere ad espressioni del tipo "dato un gruppo $(G, *)$". Se invece è necessario distinguere la struttura dal suo universo (per esempio quando abbiamo strutture distinte sullo stesso universo) utilizzeremo le lettere corsive $\mathcal{M}, \mathcal{N}, \ldots$ per le strutture.

Il linguaggio per i gruppi ha un simbolo di operazione binaria $\cdot$, un simbolo di operazione unaria f, e un simbolo di costante 1. Al fine di uniformarci con la notazione usuale in matematica, scriveremo x^{-1} invece di $f(x)$. Le formule atomiche sono della forma $t_1 = t_2$, con t_1 e t_2 termini.

Una struttura per questo linguaggio consiste di un insieme M con un elemento privilegiato 1^M, un'operazione binaria $(x, y) \mapsto x \cdot^M y$, ed un'operazione unaria $x \mapsto x^{-1_M}$. Diremo che M è un gruppo se soddisfa gli enunciati

$$\forall x \forall y \forall z \, (x \cdot (y \cdot z) = (x \cdot y) \cdot z) \tag{3.8a}$$

$$\forall x \, (x \cdot 1 = x \, \wedge \, 1 \cdot x = x) \tag{3.8b}$$

$$\forall x \left(x \cdot x^{-1} = 1 \, \wedge \, x^{-1} \cdot x = 1 \right). \tag{3.8c}$$

Volendo essere particolarmente stringati potremmo prendere come unico assioma per la teoria dei gruppi la congiunzione dei tre enunciati precedenti.[9]

Se L è il linguaggio per studiare i campi ordinati, allora una struttura per questo linguaggio è data da un insieme M con due elementi privilegiati 0^M e 1^M (non necessariamente distinti), due operazioni binarie $+^M$ e $\cdot^M$, un'operazione unaria $-^M$, e una relazione binaria $<^M$. Naturalmente M in generale non sarà un campo ordinato — per assicurarci che ciò avvenga dobbiamo richiedere che la struttura M soddisfi gli assiomi per i gruppi abeliani

$$\forall x \forall y \forall z \, ((x + y) + z = x + (y + z)) \tag{3.9a}$$

$$\forall x \forall y \, (x + y = y + x) \tag{3.9b}$$

$$\forall x \, (x + 0 = x \, \wedge \, 0 + x = x) \tag{3.9c}$$

$$\forall x \, (x + (-x) = 0 \, \wedge \, (-x) + x = 0), \tag{3.9d}$$

più quelli che servono per gli anelli unitari

$$\forall x \forall y \forall z \, ((x \cdot y) \cdot z = x \cdot (y \cdot z)) \tag{3.10a}$$

$$\forall x \, (x \cdot 1 = x \, \wedge \, 1 \cdot x = x) \tag{3.10b}$$

$$\forall x \forall y \forall z \, ((x + y) \cdot z = (x \cdot z) + (y \cdot z)), \tag{3.10c}$$

più la commutatività del prodotto

$$\forall x \forall y \, (x \cdot y = y \cdot x), \tag{3.11}$$

più gli assiomi per i campi

$$0 \neq 1 \tag{3.12a}$$

$$\forall x \, (x \neq 0 \Rightarrow \exists y \, (x \cdot y = 1)), \tag{3.12b}$$

più gli assiomi per gli ordini totali

$$\neg \exists x \, (x < x) \tag{3.13a}$$

$$\forall x \forall y \forall z (x < y \wedge y < z \Rightarrow x < z) \tag{3.13b}$$

$$\forall x \forall y \, (x < y \vee x = y \vee y < x). \tag{3.13c}$$

[9] Nella Sezione 5.A.2 vedremo altre assiomatizzazioni succinte del concetto di gruppo.

Infine dobbiamo avere degli assiomi che garantiscono la compatibilità dell'ordinamento con le operazioni algebriche

$$\forall x \forall y \forall z \, (x < y \Rightarrow x + z < y + z) \tag{3.14a}$$

$$\forall x \forall y \, (0 < x \wedge 0 < y \Rightarrow 0 < x \cdot y) \, . \tag{3.14b}$$

Dire che M **soddisfa un enunciato** σ di L significa che se sostituiamo i simboli $0, 1, +, \cdot, -, <$ con le costanti, le operazioni e la relazione binaria di M, e se restringiamo i quantificatori agli elementi di M, otteniamo un'affermazione vera in M. Per esempio, dire che la struttura

$$(M, +^M, \cdot^M, -^M, <^M, 0^M, 1^M)$$

soddisfa l'enunciato (3.12b) equivale ad asserire che

$$\forall x \in M \left(x \neq 0^M \Rightarrow \exists y \in M \left(x \cdot^M y = 1^M \right) \right)$$

mentre dire che M soddisfa l'enunciato (3.14b) significa che

$$\forall x, y \in M \, (0 <^M x \wedge 0 <^M y \Rightarrow 0 <^M x \cdot^M y).$$

Come si vede da questi esempi, gli apici per le operazioni, costanti e relazioni di M appesantiscono eccessivamente la scrittura, per cui verranno soppressi, quando questo non causa confusione.

Se M è una L-struttura e σ un enunciato di L, scriveremo

$$M \vDash \sigma$$

per dire che la struttura M soddisfa l'enunciato σ; equivalentemente diremo che σ è vero in M. Quando ciò non accade scriveremo $M \nvDash \sigma$. Osserviamo che

la scrittura...	equivale a dire...
$M \vDash \neg\sigma$	$M \nvDash \sigma$,
$M \vDash \sigma \wedge \tau$	$M \vDash \sigma$ e $M \vDash \tau$,
$M \vDash \sigma \vee \tau$	$M \vDash \sigma$ oppure $M \vDash \tau$,
$M \vDash \sigma \Rightarrow \tau$	se $M \vDash \sigma$ allora $M \vDash \tau$,
$M \vDash \sigma \Leftrightarrow \tau$	$M \vDash \sigma$ se e solo se $M \vDash \tau$.

Se M rende vero ogni σ appartenente ad un insieme Σ di enunciati, diremo che M è un **modello** di Σ, in simboli

$$M \vDash \Sigma.$$

Poiché una struttura soddisfa una congiunzione se e solo se soddisfa tutte le formule di cui la congiunzione è costituita, dire che M è un modello di un insieme finito di enunciati $\{\sigma_1, \ldots, \sigma_n\}$ equivale a dire che $M \vDash \bigwedge_{1 \leq i \leq n} \sigma_i$.

Ricapitolando, abbiamo visto alcuni linguaggi del prim'ordine utili per studiare alcune classi di strutture matematiche:

- L_{GRUPPI} ha un simbolo di operazione binaria $\cdot$, un simbolo di operazione unaria $^{-1}$ e un simbolo di costante 1. Una L_{GRUPPI}-struttura è un gruppo se e solo se soddisfa l'insieme Σ_{GRUPPI} formato dagli enunciati (3.8).
- $L_{\text{GRUPPI A.}}$ è ottenuto da L_{GRUPPI} rimpiazzando i simboli $\cdot$, $^{-1}$ e 1 con $+$, $-$ e 0. Una $L_{\text{GRUPPI A.}}$-struttura è un gruppo abeliano se e solo se soddisfa l'insieme $\Sigma_{\text{GRUPPI A.}}$ formato dagli enunciati (3.9).
- L_{ANELLI} è ottenuto aggiungendo ad $L_{\text{GRUPPI A.}}$ il simbolo $\cdot$ di operazione binaria. Una L_{ANELLI}-struttura è un anello se soddisfa l'insieme Σ_{ANELLI} ottenuto aggiungendo a $\Sigma_{\text{GRUPPI A.}}$ gli enunciati (3.10a) e (3.10c), ed è un anello commutativo se soddisfa $\Sigma_{\text{ANELLI C.}}$, l'insieme di enunciati ottenuto aggiungendo a Σ_{ANELLI} la (3.11).
- $L_{\text{ANELLI-1}}$ è ottenuto da L_{ANELLI} aggiungendo il simbolo di costante 1 e una sua struttura è un anello unitario se soddisfa l'insieme di enunciati $\Sigma_{\text{ANELLI-1}}$ dato da Σ_{ANELLI} con l'aggiunta di (3.10b). Se aggiungiamo anche la (3.11) otteniamo l'insieme di enunciati $\Sigma_{\text{ANELLI C.}}$, i cui modelli sono gli anelli commutativi unitari; aggiungendo anche gli enunciati (3.12) si ottiene Σ_{CAMPI} i cui modelli sono i campi.
- Aggiungendo a $L_{\text{ANELLI-1}}$ un simbolo di relazione binaria $<$ si ottiene il linguaggio $L_{\text{ANELLI O.}}$. Un campo ordinato è una $L_{\text{ANELLI O.}}$-struttura che soddisfa l'insieme di enunciati $\Sigma_{\text{CAMPI O.}}$, ottenuto aggiungendo a Σ_{CAMPI} gli enunciati (3.13) e (3.14).

Osservazioni 3.7. (a) Se $M \vDash \Sigma$ e Σ è un insieme infinito di enunciati infinito, per esempio $\Sigma = \{\sigma_n \mid n \in \mathbb{N}\}$, siamo tentati di dire che M soddisfa la congiunzione infinita $\bigwedge_{n\in\mathbb{N}} \sigma_n$. Tuttavia dobbiamo resistere stoicamente a questa tentazione, dato che $\bigwedge_{n\in\mathbb{N}} \sigma_n$ *non* è una formula di un linguaggio del prim'ordine. Ci sono sistemi formali, le **logiche infinitarie**, in cui è consentito formare congiunzioni e disgiunzioni di infinite formule, ma queste fanno parte di argomenti più avanzati e non verranno trattate in questo libro.

(b) Quando valutiamo se un enunciato σ è vero in una struttura M, la quantificazione avviene sugli *elementi* di M e non sui *sottoinsiemi* di M. Questo vincolo è ciò che caratterizza i linguaggi e la logica del prim'ordine. Per quantificare anche sui sottoinsiemi della struttura si deve introdurre una nuova lista di variabili per denotare i sottoinsiemi ed un simbolo $\in$ per specificare quando un elemento della struttura appartiene ad un sottoinsieme, e la relazione di soddisfazione deve essere modificata in modo da distinguere tra i due livelli di quantificazione (su elementi o su insiemi). Il sistema che si ottiene va sotto il nome di **logica del second'ordine**. Se si è più ambiziosi è possibile definire la logica del terz'ordine, in cui ci sono tre livelli di quantificazione (su

elementi, su sottoinsiemi, su famiglie di sottoinsiemi) o, più in generale, è possibile definire la logica di ordine n. Le logiche di ordine $n > 1$ si dicono logiche di ordine superiore è hanno un potere espressivo molto superiore rispetto alla logica del prim'ordine. Tuttavia, come spesso capita in matematica, la ricerca dell'eccessiva generalità va a scapito della profondità dei risultati, per cui in questo libro, come nella maggior parte dei manuali, ci concentreremo principalmente sulla logica del prim'ordine.

Diremo che un enunciato τ è **conseguenza logica** di un insieme Σ di enunciati (del medesimo linguaggio del prim'ordine), o che τ **discende logicamente** da Σ, in simboli

$$\Sigma \models \tau$$

se

$$M \vDash \Sigma \text{ implica che } M \vDash \tau, \text{ per ogni } L\text{-struttura } M.$$

Quando $\Sigma = \{\sigma\}$ è costituito da un unico enunciato identificheremo Σ con σ e diremo che τ è **conseguenza logica** di σ, in simboli $\sigma \models \tau$. Equivalentemente: τ è conseguenza logica di σ se $\sigma \Rightarrow \tau$ è un enunciato valido. Due enunciati σ e τ si dicono **logicamente equivalenti** se uno è conseguenza logica dell'altro, cioè se

$$\sigma \models \tau \quad \text{e} \quad \tau \models \sigma;$$

equivalentemente, se $\sigma \Leftrightarrow \tau$ è un enunciato valido.

Attenzione. Non si deve confondere $\vDash$ la relazione di soddisfazione, con $\models$ la relazione di conseguenza logica — sono nozioni distinte anche se usano simboli simili! La relazione di soddisfazione ($M \vDash \sigma$) è una relazione tra L-strutture ed enunciati (o insiemi di enunciati), mentre la relazione di conseguenza logica ($\Sigma \models \sigma$) è una relazione tra insiemi di enunciati e singoli enunciati. Nella maggioranza dei testi, le due nozioni sono denotate con il medesimo simbolo, ma noi abbiamo preferito, almeno per questo capitolo, adottare questa variante notazionale per aiutare il lettore a non confondere le due nozioni.

Definizione 3.8. (i) Una **teoria del prim'ordine** o semplicemente **teoria** è un insieme T di enunciati di un linguaggio del prim'ordine L, che si dice linguaggio di T.

(ii) Un **sistema di assiomi** per una teoria T è un insieme Σ di enunciati del linguaggio di T tale che per ogni enunciato σ

$$\Sigma \models \sigma \quad \text{se e solo se} \quad T \models \sigma.$$

(iii) Una teoria si dice **finitamente assiomatizzabile** se ammette un sistema finito di assiomi.

Le due espressioni "teoria" e "insieme di enunciati" denotano lo stesso concetto, ma la prima è particolarmente comoda per indicare delle assiomatizzazioni al prim'ordine di settori della matematica. Quindi parleremo di *teoria del prim'ordine dei gruppi abeliani*, *teoria del prim'ordine degli anelli*, *teoria del prim'ordine dei campi*, ... per indicare le teorie che hanno per sistemi di assiomi rispettivamente $\Sigma_{\text{GRUPPI A.}}$, Σ_{ANELLI}, Σ_{CAMPI} .... Invece riserveremo le locuzioni *teoria dei gruppi abeliani*, *teoria degli anelli*, *teoria dei campi*, ..., per indicare genericamente certe parti della matematica.

Osservazione 3.9. Ogni teoria T, in quanto insieme di enunciati, è un sistema di assiomi per sé stessa. Tuttavia non è detto che un sistema di assiomi per T sia un sottoinsieme di T. Per esempio gli enunciati (3.8a), $\forall x \forall y \exists z\,(x \cdot z = y)$ e $\forall x \forall y \exists z\,(z \cdot x = y)$ formano un sistema di assiomi per la teoria Σ_{GRUPPI} definita a pagina 40. (Nelle pagine seguenti vedremo degli esempi più significativi di questo fenomeno.)

Il seguente risultato, che dimostreremo nella Sezione 31.B del Capitolo VI (si veda il Teorema 31.9), è utilissimo per dimostrare che una teoria non è finitamente assiomatizzabile.

Teorema 3.10. *Sia T una teoria del prim'ordine in un linguaggio L e sia $\{\sigma_n \mid n \in \mathbb{N}\}$ un suo sistema di assiomi. Supponiamo che per ogni n ci sia un $m > n$ tale che*

$$\{\sigma_0, \dots, \sigma_n\} \not\models \sigma_m.$$

Allora T non è finitamente assiomatizzabile.

Osservazione 3.11. È ovvio che nessun sottoinsieme finito di $\{\sigma_n \mid n \in \mathbb{N}\}$ sia un sistema di assiomi per T. Il teorema asserisce che nessun insieme finito Δ di L-enunciati va bene.

Esempi 3.12. (a) Sia L il linguaggio privo di simboli non logici. Le L-strutture sono semplicemente gli insiemi non vuoti. La **teoria del prim'ordine degli insiemi infiniti** ha $\{\varepsilon_{\geq n} \mid n \geq 1\}$ come sistema di assiomi e non è finitamente assiomatizzabile.

(b) Analogamente, la **teoria del prim'ordine dei gruppi infiniti** che ha per assiomi gli enunciati (3.8) e gli $\{\varepsilon_{\geq n} \mid n \geq 1\}$ non è finitamente assiomatizzabile.

Diremo che Σ è un **sistema indipendente di enunciati** se nessuno dei suoi enunciati è conseguenza logica degli altri enunciati, cioè se $\Sigma \setminus \{\sigma\} \not\models \sigma$, per ogni $\sigma \in \Sigma$. Due insiemi di enunciati Σ e Δ sono **logicamente equivalenti** se e solo se sono un sistema di assiomi l'uno per l'altro, cioè se e solo se

$$\Sigma \models \sigma \quad \text{se e solo se} \quad \Delta \models \sigma$$

per ogni enunciato σ. Ogni insieme finito di enunciati Σ contiene un sottoinsieme indipendente di assiomi Δ, ma naturalmente l'insieme Δ è ben lungi dall'essere unico. Se abbiamo un insieme infinito di enunciati non possiamo sperare di trovare un sottoinsieme indipendente (Esercizio 3.57). Tuttavia

Teorema 3.13. *Ogni teoria del prim'ordine ha un sistema di assiomi indipendente.*

La dimostrazione (peraltro semplice) è rimandata al Capitolo VI.

Definizione 3.14. Fissiamo un linguaggio L.

(i) Una teoria di L si dice:
- **soddisfacibile** se ha almeno un modello, cioè se $M \vDash T$ per qualche L-struttura M,
- **completa** se è soddisfacibile e
$$T \models \sigma \quad \text{oppure} \quad T \models \neg\sigma$$
per ogni L-enunciato σ.

(ii) Due L-strutture M e M' si dicono **elementarmente equivalenti** se soddisfano esattamente gli stessi L-enunciati.

(iii) La **teoria di una L-struttura** M è l'insieme degli enunciati σ che valgono in M.

Proposizione 3.15. *Se T è una teoria soddisfacibile, le seguenti affermazioni sono equivalenti:*

(a) *T è completa,*

(b) *T è un sistema di assiomi per la teoria di un qualche suo modello,*

(c) *due modelli di T sono elementarmente equivalenti.*

Dimostrazione. (a)⇒(b) Sia M un modello di T e sia σ un L-enunciato: dalla definizione di teoria completa segue che $T \models \sigma$ se e solo se $M \vDash \sigma$ e quindi T è un sistema di assiomi per la teoria di M.

(b)⇒(c) Supponiamo T sia un sistema di assiomi per la teoria di M, vale a dire
$$T \models \sigma \quad \text{se e solo se} \quad M \vDash \sigma$$
per ogni L-enunciato σ. Supponiamo $N \vDash T$: se $M \vDash \sigma$ allora $T \models \sigma$ e quindi $N \vDash \sigma$; se $M \nvDash \sigma$ allora $M \vDash \neg\sigma$ e quindi $T \models \neg\sigma$ da cui$N \vDash \neg\sigma$ e $N \nvDash \sigma$. Abbiamo verificato che un modello N di T soddisfa gli stessi enunciati del modello M, quindi due modelli di T soddisfano esattamente gli stessi enunciati.

(c)⇒(a) Dimostriamo il contrappositivo: se T è soddisfacibile ma $T \not\models \sigma$ e $T \not\models \neg\sigma$ allora ci sono M e M' modelli di T tali che $M \vDash \sigma$ e $M' \vDash \neg\sigma$. □

3.E. Insiemi di verità. Abbiamo visto che cosa vuol dire che un enunciato è vero in una struttura, ma che dire delle formule che non sono enunciati? Per alcune di queste (per esempio se $\varphi(x_1, \dots, x_n)$ è una tautologia oppure se è una formula come in (3.6) a pagina 27) abbiamo visto che sono sempre vere in ogni struttura e quindi le loro negazioni sono sempre false. Ma in generale, una formula $\varphi(x_1, \dots, x_n)$ definisce un insieme di n-uple di elementi della struttura che, sostituiti al posto delle variabili $x_1, \dots, x_n$, rendono vera φ nella struttura. Più precisamente: data una L-struttura M ed una formula $\varphi(x_1, \dots, x_n)$ di L, l'**insieme di verità** di φ in M è l'insieme

$$\mathbf{T}_\varphi = \mathbf{T}^M_{\varphi(x_1,\dots,x_n)}$$

delle n-uple di elementi di M che soddisfano la formula $\varphi(x_1, \dots, x_n)$. Se $\mathbf{T}^M_{\varphi(x_1,\dots,x_n)} = M^n$ diremo che φ è **vera** in M. Osserviamo che quando φ è un enunciato questa terminologia è coerente con le precedenti definizioni, dato che

$$\begin{aligned} \mathbf{T}^M_{\varphi(x_1,\dots,x_n)} = M^n \quad &\text{se e solo se} \quad M \vDash \varphi \\ \mathbf{T}^M_{\varphi(x_1,\dots,x_n)} = \emptyset \quad &\text{se e solo se} \quad M \vDash \neg\varphi. \end{aligned}$$

Per comodità notazionale, definiamo

$$\begin{aligned} \mathbf{T}^M_\sigma = 1 \quad &\text{se e solo se} \quad M \vDash \sigma \\ \mathbf{T}^M_\sigma = 0 \quad &\text{se e solo se} \quad M \vDash \neg\sigma. \end{aligned}$$

quando σ è un enunciato. Allora

$$\begin{array}{c} M \text{ e } N \text{ sono elementarmente equivalenti} \\ \Updownarrow \\ \mathbf{T}^M_\sigma = \mathbf{T}^N_\sigma \text{ per ogni enunciato } \sigma. \end{array} \tag{3.15}$$

Esempi 3.16. (A) Se $\varphi(x_1, \dots, x_n)$ è valida allora $\mathbf{T}_\varphi = M^n$, se è insoddisfacibile, allora $\mathbf{T}_\varphi = \emptyset$,

(B) l'insieme di verità in $\mathbb{N}$ di $\exists y\,(y + y = x)$ è l'insieme dei numeri pari,

(C) l'insieme di verità in $\mathbb{N}$ di $1 < x \wedge \forall y\,(\exists z(z \cdot y = x) \Rightarrow y = 1 \vee y = x)$ è l'insieme dei numeri primi,

(D) l'insieme di verità di $x^2 < 1$ nella struttura $\mathbb{N}$ è il singoletto $\{0\}$, mentre nella struttura $\mathbb{R}$ è l'intervallo aperto $(-1; 1)$,

(E) l'insieme di verità in $\mathbb{R}$ di $y = x^2 - 3x + 2$ è una parabola, cioè un sottoinsieme di $\mathbb{R}^2$,

(F) nella struttura $\mathbb{R}$ l'insieme di verità di $x^2 + x + 1 = 0$ è l'insieme vuoto, mentre nella struttura $\mathbb{C}$ è una curva algebrica (l'unione di due rette), in particolare è un sottoinsieme non vuoto di $\mathbb{C}$,

(G) se $\varphi(x_1, x_2)$ è la formula $x_1 = x_2$, allora $\mathbf{T}_{\varphi(x_1,x_2)}$ è la diagonale di M^2,

(H) se $\varphi(x_1, \dots, x_n)$ è $P(x_1, \dots, x_n)$ dove P è un simbolo di predicato n-ario di L, allora $\mathbf{T}_{\varphi(x_1,\dots,x_n)} = P^M$, il sottoinsieme di M^n associato a P.

Osserviamo che la dimensione n di $\mathbf{T}_\varphi$ dipende non solo dalla formula φ, ma anche dalla lista $x_1, \dots, x_n$ delle variabili — per esempio se φ è $y = x^2 - 3x + 2$, allora l'insieme di verità di $\varphi(x, y, z)$ nella struttura $\mathbb{R}$ è il cilindro $\{(x, y, z) \in \mathbb{R}^3 \mid y = x^2 - 3x + 2\}$.

È immediato verificare che date le formule $\varphi(x_1, \dots, x_n)$ e $\psi(x_1, \dots, x_n)$ con insiemi di verità $\mathbf{T}_\varphi, \mathbf{T}_\psi \subseteq M^n$

$$\mathbf{T}_{\neg\varphi} = M^n \setminus \mathbf{T}_\varphi \tag{3.16a}$$

$$\mathbf{T}_{\varphi\wedge\psi} = \mathbf{T}_\varphi \cap \mathbf{T}_\psi \tag{3.16b}$$

$$\mathbf{T}_{\varphi\vee\psi} = \mathbf{T}_\varphi \cup \mathbf{T}_\psi \tag{3.16c}$$

$$\mathbf{T}_{\varphi\Rightarrow\psi} = (M^n \setminus \mathbf{T}_\varphi) \cup \mathbf{T}_\psi \tag{3.16d}$$

$$\mathbf{T}_{\varphi\Leftrightarrow\psi} = M^n \setminus (\mathbf{T}_\varphi \triangle \mathbf{T}_\psi). \tag{3.16e}$$

Se φ è $\exists y\psi$ e y non è una tra le $x_1, \dots, x_n$,

$$\mathbf{T}_{\varphi(x_1,\dots,x_n)} = p(\mathbf{T}_{\psi(y,x_1,\dots,x_n)}) \tag{3.17a}$$

dove $p\colon M^{n+1} \to M^n$ è la proiezione lungo la prima coordinata, cioè

$$p(y, x_1, \dots, x_n) = (x_1, \dots, x_n).$$

Quindi data una formula $\varphi(x_1, \dots, x_n)$ si ha

$$M \vDash \exists x_1 \dots x_n \varphi \quad \text{se e solo se} \quad \mathbf{T}_{\varphi(x_1,\dots,x_n)} \neq \emptyset, \tag{3.17b}$$

$$M \vDash \forall x_1 \dots x_n \varphi \quad \text{se e solo se} \quad \mathbf{T}_{\varphi(x_1,\dots,x_n)} = M^n. \tag{3.17c}$$

Usando queste equivalenze è facile stabilire quando una struttura M soddisfa un enunciato σ.

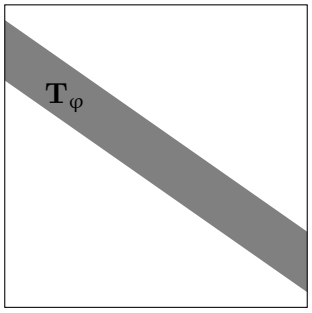
Esempi 3.17. (A) $M \vDash \forall x\,(\varphi(x) \Rightarrow \psi(x))$ se e solo se l'insieme di verità di $\varphi(x) \Rightarrow \psi(x)$ è M, vale a dire se $\mathbf{T}_\varphi \subseteq \mathbf{T}_\psi$.

(B) L'enunciato $\forall x\,(\varphi(x) \Rightarrow \psi(x)) \Rightarrow (\forall x\varphi(x) \Rightarrow \forall x\psi(x))$ è soddisfatto in ogni M. Per dimostrare ciò dobbiamo verificare che:

$$\text{se } M \vDash \forall x\,(\varphi(x) \Rightarrow \psi(x)) \text{ allora } M \vDash \forall x\varphi(x) \Rightarrow \forall x\psi(x).$$

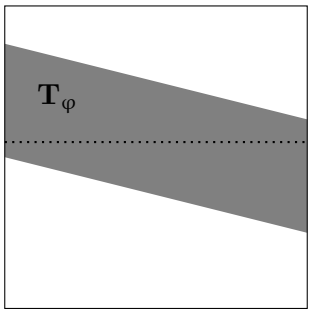
Quindi supponiamo che M sia una struttura che soddisfa $\forall x\,(\varphi(x) \Rightarrow \psi(x))$ e $\forall x\varphi(x)$, vale a dire $\mathbf{T}_\varphi \subseteq \mathbf{T}_\psi$ e $\mathbf{T}_\varphi = M$. Allora $\mathbf{T}_\psi = M$ e quindi $M \vDash \forall x\psi(x)$ come richiesto.

(C) L'enunciato $\forall x \exists y \varphi(x, y)$ vale in M se e solo se l'insieme $\mathbf{T}_\varphi \subseteq M^2$ ha tutte le sezioni verticali non vuote,



M^2

mentre dire che $M \vDash \exists y \forall x \varphi(x, y)$ significa che c'è una sezione orizzontale di $\mathbf{T}_\varphi$ che è tutto M



M^2

(D) Consideriamo l'enunciato

$$\forall x(P(x) \vee Q(x)) \Rightarrow \forall x\, P(x) \vee \forall x\, Q(x). \tag{3.18}$$

Fissiamo una struttura M. Per la (3.17c), asserire che $M \vDash \forall x(P(x) \vee Q(x))$ significa che $\mathbf{T}_{P(x)\vee Q(x)} = \mathbf{T}_{P(x)} \cup \mathbf{T}_{Q(x)} = M$, cioè $P^M \cup Q^M = M$; mentre asserire che $M \vDash \forall x\, P(x) \vee \forall x\, Q(x)$ significa che $P^M = M$ oppure $Q^M = M$. Quindi una struttura M soddisfa (3.18) se e solo se: ogni qual volta $P^M \cup Q^M = M$ necessariamente $P^M = M$ oppure $Q^M = M$. Per esempio, la struttura M che ha per dominio $\mathbb{N}$ e in cui $P^M = Q^M = \emptyset$ soddisfa l'enunciato, mentre la struttura N sempre con dominio $\mathbb{N}$ in cui P^N e Q^N sono, rispettivamente, l'insieme dei pari e l'insieme dei dispari, non lo soddisfa. Ne segue che l'enunciato (3.18) è soddisfacibile, ma non valido.

(E) Supponiamo che la formula $\varphi(x_1, \ldots, x_n)$ sia conseguenza tautologica di $\psi_1(x_1, \ldots, x_n), \ldots, \psi_k(x_1, \ldots, x_n)$; in altre parole: $\psi_1 \wedge \cdots \wedge \psi_k \Rightarrow \varphi$ è una tautologia (vedi pag. 28). Allora $\psi_1 \wedge \cdots \wedge \psi_k \Rightarrow \varphi$ è valida, quindi $\mathbf{T}^M_{\psi_1(x_1,\ldots,x_n)} \cap \cdots \cap \mathbf{T}^M_{\psi_k(x_1,\ldots,x_n)} \subseteq \mathbf{T}^M_{\varphi(x_1,\ldots,x_n)}$, per ogni struttura M.

In particolare, se $\varphi(x_1, \dots, x_n)$ e $\psi(x_1, \dots, x_n)$ sono tautologicamente equivalenti, allora $\mathbf{T}^M_{\varphi(x_1,\dots,x_n)} = \mathbf{T}^M_{\psi(x_1,\dots,x_n)}$.

La nozione di conseguenza logica, vista nella Sezione 3.D per gli enunciati, si generalizza a formule arbitrarie. Se Σ è un insieme di enunciati e $\varphi(x_1, \dots, x_n)$ è una formula, diremo che φ **è conseguenza logica di** Σ, in simboli $\Sigma \models \varphi$, se $\Sigma \models \varphi^\forall$, dove $\varphi^\forall$ è la chiusura universale di φ; equivalentemente, se

$$\mathbf{T}^M_{\varphi(x_1,\dots,x_n)} = M^n, \text{ per ogni struttura } M \text{ tale che } M \vDash \Sigma,$$

cioè se φ è vera in ogni modello di Σ. Due formule φ e ψ sono **logicamente equivalenti modulo** ovvero **su** Σ se e solo se $\varphi \Leftrightarrow \psi$ è conseguenza logica di Σ.

Osservazione 3.18. Il concetto di equivalenza di formule (con variabili libere) modulo un certo sistema di assiomi è una nozione piuttosto comune in matematica. Per esempio le formule

$$(xy)^2 = x^2y^2 \quad \text{e} \quad xy = yx$$

sono logicamente equivalenti modulo Σ_{GRUPPI}, e quindi sono logicamente equivalenti le loro chiusure universali, vale a dire $\forall x, y\,[(xy)^2 = x^2y^2]$ e la proprietà commutativa. Asserire che due formule sono logicamente equivalenti modulo Σ è più forte che asserire che le loro chiusure universali sono equivalenti modulo Σ (si veda l'Esercizio 3.45 e l'Osservazione 8.15).

3.F. Sottostrutture, morfismi e prodotti.

3.F.1. *Sottostrutture.* Un sottoinsieme di un insieme ordinato è a sua volta un insieme ordinato mediante la medesima relazione di ordine. Analogamente una relazione di equivalenza su un insieme induce una relazione di equivalenza su ogni sottoinsieme. Viceversa un sottoinsieme di un gruppo è un sottogruppo soltanto se contiene l'identità ed chiuso sotto le operazioni di prodotto e di inverso. Queste idee si generalizzano in modo ovvio alle L-strutture.

Dato un linguaggio L contenente soltanto simboli di predicato $R_1, R_2, \dots$ e una L-struttura

$$(M, R_1^M, R_2^M, \dots)$$

una **sottostruttura** è semplicemente un sottoinsieme non vuoto N di M su cui definiamo le relazioni nel modo ovvio: se R_i è k-aria poniamo

$$R_i^N = R_i^M \cap N^k.$$

Se L contiene anche simboli di costante $c_1, c_2, \dots$ o simboli di operazione $f_1, f_2, \dots$, una sottostruttura di

$$(M, R_1^M, R_2^M, \dots, c_1^M, c_2^M, \dots, f_1^M, f_2^M, \dots)$$

è un insieme non vuoto $N \subseteq M$ contenente gli elementi $c_1^M, c_2^M, \dots$ e chiuso sotto le funzioni $f_1^M, f_2^M, \dots$; quindi N è la struttura

$$(N, R_1^N, R_2^N, \dots, c_1^N, c_2^N, \dots, f_1^N, f_2^N, \dots)$$

dove $c_i^N = c_i^M$ e le f_i^N sono le restrizioni delle f_i^M ad N. Se $(N, \dots)$ è una sottostruttura di $(M, \dots)$, allora diremo che $(M, \dots)$ è una sovrastruttura di $(N, \dots)$. Per esempio, una sottostruttura di un campo ordinato

$$(F, <, +, -, \cdot, 0, 1)$$

è un sottoinsieme $R \subseteq F$ contenente 0 e 1 e chiuso per $+, \cdot$ e $-$, vale a dire è un anello ordinato (ma, in generale, non è un campo).

3.F.2. *Morfismi.* Un **morfismo** o **omomorfismo** dalla L-struttura M nella L-struttura N è una funzione $F\colon M \to N$ che rispetta tutte le relazioni, tutte le funzioni e tutte le costanti. In altre parole se R e g sono simboli di relazione e di funzione n-ari e c è un simbolo di costante, allora per ogni $a_1, \dots, a_n \in M$

(A) se $(a_1, \dots, a_n) \in R^M$ allora $(F(a_1), \dots, F(a_n)) \in R^N$,
(B) $F(g^M(a_1, \dots, a_n)) = g^N(F(a_1), \dots, F(a_n))$,
(C) $F(c^M) = c^N$.

Questa nozione generalizza simultaneamente la definizione di omomorfismo (di gruppi, anelli,...) e la definizione di funzione crescente tra insiemi ordinati. Se $F\colon M \to N$ è un morfismo biettivo e $F^{-1}\colon N \to M$ è anch'esso un morfismo, allora F e F^{-1} sono **isomorfismi** e diremo che le due strutture sono isomorfe, in simboli

$$M \cong N.$$

Se F è iniettivo e (A) si rafforza ad

(A′) $(a_1, \dots, a_n) \in R^M$ se e solo se $(F(a_1), \dots, F(a_n)) \in R^N$

diremo che F è un'**immersione**. Diremo che M si immerge in N se c'è un'immersione $F\colon M \to N$.

Osservazioni 3.19. (a) È importante che un morfismo preservi tutte le costanti. Per esempio $F\colon \mathbb{Z} \to \mathbb{Z}$, $k \mapsto 0$, è un morfismo della struttura $(\mathbb{Z}, +, \cdot, 0)$ in sé stessa (cioè è un morfismo di anelli), ma non è un morfismo di $(\mathbb{Z}, +, \cdot, 0, 1)$ in sé stessa (cioè non è un morfismo di anelli unitari).

(b) Un isomorfismo è un morfismo biettivo, ma non viceversa. Per esempio: se $<$ è l'usuale ordine sui naturali e $\prec$ è definito da $n \prec m \Leftrightarrow m = n+1$, allora $\mathrm{id}_{\mathbb{N}}\colon (\mathbb{N}, \prec) \to (\mathbb{N}, <)$ è un morfismo biettivo, ma non è un isomorfismo. Analogamente un'immersione è un morfismo iniettivo, ma non viceversa.

Se M è una L-struttura e $x_1, \dots, x_n$ sono le variabili che compaiono in un termine t, allora risulta definita una funzione n-aria

$$t^M \colon M^n \to M$$

che associa a $(a_1, \dots, a_n) \in M^n$ il valore $t^M(a_1, \dots, a_n)$ ottenuto rimpiazzando i simboli di funzione e di costante con le corrispettive funzioni e costanti di M. Per esempio il termine[10] $t(x, y, z)$

$$x \cdot (y \cdot y) + ((x \cdot y) + 1)$$

nel linguaggio degli anelli unitari[11] definisce una funzione polinomiale $R^3 \to R$ in ogni anello unitario R, che associa ad $(a, b, c) \in R^3$ l'elemento $ab^2 + ab + 1_R \in R$. Ogni morfismo $F \colon R_1 \to R_2$ di anelli unitari commuta con le funzioni polinomiali indotte da t, cioè per ogni $a, b \in R_1$

$$F(ab^2 + ab + 1_{R_1}) = F(a)F(b)^2 + F(a)F(b) + 1_{R_2}.$$

Più in generale, se $F \colon M \to N$ è un morfismo di L-strutture e t è un L-termine con variabili libere $x_1, \dots, x_n$, allora

$$\forall a_1, \dots a_n \in M\big(F(t^M(a_1, \dots, a_n)) = t^N(F(a_1), \dots, F(a_n))\big). \tag{3.19}$$

Ne segue che per ogni morfismo $F \colon M \to N$:

- se $\varphi(x_1, \dots, x_n)$ è $t_1(x_1, \dots, x_n) = t_2(x_1, \dots, x_n)$ allora

  $t_1^M(a_1, \dots, a_n) = t_2^M(a_1, \dots, a_n)$ implica che
  $$t_1^N(F(a_1), \dots, F(a_n)) = t_2^N(F(a_1), \dots, F(a_n)),$$

- se $\varphi(x_1, \dots, x_n)$ è $P(t_1(x_1, \dots, x_n), \dots, t_k(x_1, \dots, x_n))$ allora

  $\big(t_1^M(a_1, \dots, a_n), \dots, t_k^M(a_1, \dots, a_n)\big) \in P^M$ implica che
  $$\big(t_1^N(F(a_1), \dots, F(a_n)), \dots, t_k^N(F(a_1), \dots, F(a_n))\big) \in P^N.$$

Possiamo esprimere più sinteticamente tutto ciò dicendo che ogni morfismo preserva le formule atomiche.

Definizione 3.20. Un morfismo $F \colon M \to N$ di L-strutture **preserva una formula** $\varphi(x_1, \dots, x_n)$ se e solo se per ogni $a_1, \dots, a_n \in M$

$$\begin{aligned}(a_1, \dots, a_n) \in \mathbf{T}^M_{\varphi(x_1,\dots,x_n)} \text{ implica che} \\ (F(a_1), \dots, F(a_n)) \in \mathbf{T}^N_{\varphi(x_1,\dots,x_n)},\end{aligned} \tag{3.20}$$

[10] Ricordiamo la convenzione di pagina 22 per cui le variabili di $t(x, y, z)$ sono *tra* le x, y, z.

[11] Seguiremo la consuetudine in algebra e denoteremo l'identità moltiplicativa con 1_R invece che con 1^R.

cioè se l'immagine dell'insieme di verità di φ calcolato in M è incluso nell'insieme di verità di φ calcolato in N,

$$F[\mathbf{T}^M_{\varphi(x_1,\dots,x_n)}] \stackrel{\text{def}}{=} \{(F(a_1),\dots,F(a_n)) \mid (a_1,\dots,a_n) \in \mathbf{T}^M_{\varphi(x_1,\dots,x_n)}\} \subseteq \mathbf{T}^N_{\varphi(x_1,\dots,x_n)}.$$

Osservazioni 3.21. (a) Se F è un morfismo che preserva $\varphi(x_1,\dots,x_n)$ e $\neg\varphi(x_1,\dots,x_n)$, allora usando la (3.16a), la condizione (3.20) può essere rafforzata a

$(a_1,\dots,a_n) \in \mathbf{T}^M_{\varphi(x_1,\dots,x_n)}$ se e solo se $(F(a_1),\dots,F(a_n)) \in \mathbf{T}^N_{\varphi(x_1,\dots,x_n)}$,

cioè

$$F[\mathbf{T}^M_{\varphi(x_1,\dots,x_n)}] = \mathbf{T}^N_{\varphi(x_1,\dots,x_n)}.$$

(b) Ogni morfismo preserva la formula $x_1 = x_2$; un morfismo F preserva la formula $x_1 \neq x_2$ se e solo se F è iniettivo.

La dimostrazione del prossimo risultato è lasciata al lettore.

Proposizione 3.22. *Se $F\colon M \to N$ è un morfismo, allora*

(a) *se F preserva φ e ψ, allora preserva anche $\varphi \wedge \psi$ e $\varphi \vee \psi$,*

(b) *se F preserva φ, allora preserva anche $\exists x\varphi$,*

(c) *se F è suriettivo e preserva φ, allora preserva anche $\forall x\varphi$,*

(d) *se F è un isomorfismo, allora preserva ogni formula.*

Quindi i morfismi suriettivi preservano le **formule positive**, cioè quelle ottenute dalle formule atomiche mediante i quantificatori e i connettivi $\wedge$ e $\vee$. In particolare,

Proposizione 3.23. *Se $F\colon M \to N$ è un morfismo suriettivo e $M \vDash \sigma$, dove σ è un enunciato positivo, allora $N \vDash \sigma$.*

L'immagine omomorfa di un gruppo, di un gruppo abeliano, di un anello, ... è ancora un gruppo, un gruppo abeliano, un anello, ..., ma l'immagine omomorfa di un dominio di integrità non è necessariamente un dominio di integrità, visto che fra gli assiomi c'è $\forall x, y(x \neq 0 \wedge y \neq 0 \Rightarrow x \cdot y \neq 0)$ che non è una formula positiva. Quindi la Proposizione 3.22 non può essere estesa a tutte le formule.

Se M è una sottostruttura di N, allora l'inclusione $M \hookrightarrow N$ è un morfismo quindi per ogni formula atomica φ

$$\mathbf{T}^M_{\varphi(x_1,\dots,x_n)} = \mathbf{T}^N_{\varphi(x_1,\dots,x_n)} \cap M^n.$$

Utilizzando le identità (3.16) a pagina 45 e procedendo per induzione sulla complessità di φ, questa uguaglianza si generalizza a tutte le φ prive di quantificatori. Applicando le identità (3.17) otteniamo che

Proposizione 3.24. *Sia M è una sottostruttura di N e $\varphi(x_1, \dots, x_n)$ una formula priva di quantificatori. Allora*

- *se $N \vDash \forall x_1, \dots, x_n \varphi$ allora $M \vDash \forall x_1, \dots, x_n \varphi$ e*
- *se $M \vDash \exists x_1, \dots, x_n \varphi$ allora $N \vDash \exists x_1, \dots, x_n \varphi$.*

Quindi, se una teoria T è assiomatizzata da enunciati universali, allora si preserva per sottostrutture, cioè: se M è una sottostruttura di N e $N \vDash T$ allora $N \vDash T$. In particolare:

- se $M \subseteq N$ e $R \subseteq N \times N$ è un ordine (o un ordine lineare, o una relazione di equivalenza) su N, allora $R \cap M \times M$ è un ordine (o un ordine lineare, o una relazione di equivalenza) se M;
- se R_i è un ordine (o un ordine lineare, o una relazione di equivalenza) su M_i per tutti gli $i \in I$, allora $\bigcap_{i \in I} R_i$ è un ordine (o un ordine lineare, o una relazione di equivalenza) su $\bigcap_{i \in I} M_i$.

[leftmargin=1pc]

3.F.3. *Prodotti.* Il **prodotto di due strutture**

$$(M, R_1^M, R_2^M, \dots, f_1^M, f_2^M, \dots, c_1^M, c_2^M, \dots) \text{ e}$$
$$(N, R_1^N, R_2^N, \dots, f_1^N, f_2^N, \dots, c_1^N, c_2^N, \dots)$$

è la struttura che ha per dominio $M \times N$ così definita:

- se R_i è un simbolo di relazione n-ario, allora $R_i^{M \times N} \subseteq (M \times N)^n$ è definito da

$$((a_1, b_1), \dots, (a_n, b_n)) \in R_i^{M \times N} \quad \text{se e solo se} \quad (a_1, \dots, a_n) \in R_i^M \text{ e } (b_1, \dots, b_n) \in R_i^N,$$

- se f_i è un simbolo di funzione n-ario, allora $f_i^{M \times N} \colon (M \times N)^n \to M \times N$ è definita da

$$f_i^{M \times N}((a_1, b_1), \dots, (a_n, b_n)) = \big(f_i^M(a_1, \dots, a_n), f_i^N(b_1, \dots, b_n)\big),$$

- $c_i^{M \times N} = (c_i^M, c_i^N)$.

Per esempio il prodotto di $(\mathbb{Z}, \leq, +, 0)$ con sé stesso è la struttura $(\mathbb{Z} \times \mathbb{Z}, \trianglelefteq, \oplus, \mathbf{0})$ dove

$$(n_1, m_1) \trianglelefteq (n_2, m_2) \Leftrightarrow n_1 \leq n_2 \wedge m_1 \leq m_2,$$
$$(n_1, m_1) \oplus (n_2, m_2) = (n_1 + n_2, m_1 + m_2),$$
$$\mathbf{0} = (0, 0).$$

Gli enunciati positivi non sono preservati dalla costruzione del prodotto — per esempio $\forall x, y (x \leq y \vee y \leq x)$ è vera in $(\mathbb{Z}, \leq)$ ma non in $(\mathbb{Z} \times \mathbb{Z}, \trianglelefteq)$.

Invece sono preservati gli enunciati della forma

$$\forall x_1, \dots, x_n \, (t(x_1, \dots, x_n) = s(x_1, \dots, x_n)) \tag{3.21}$$

dove t e s sono termini. Infatti se M e N soddisfano un enunciato di questo tipo, allora per ogni $(a_1, b_1), \dots, (a_n, b_n) \in M \times N$

$$\begin{aligned} t^{M\times N}((a_1, b_1), \dots, (a_n, b_n)) &= (t^M(a_1, \dots, a_n), t^N(b_1, \dots, b_n)) \\ &= (s^M(a_1, \dots, a_n), s^N(b_1, \dots, b_n)) \\ &= s^{M\times N}((a_1, b_1), \dots, (a_n, b_n)). \end{aligned}$$

Una teoria del prim'ordine si dice **equazionale** se ha un sistema di assiomi costituito da enunciati della forma (3.21). Tenendo presente che una formula è equivalente alla sua chiusura universale (vedi pagina 31), una teoria è equazionale se ha un sistema di assiomi costituito da formule della forma

$$t(x_1, \dots, x_n) = s(x_1, \dots, x_n)$$

dove t e s sono termini. La teoria dei gruppi (pag. 38) e la teoria degli anelli (pag. 38) sono esempi di teorie equazionali.

Poiché le formule (3.21) sono universali, per quanto abbiamo appena detto, e per la (3.19), si ottiene:

Proposizione 3.25. *Una teoria equazionale T si preserva per sottostrutture, immagini omomorfe, e prodotti. In altre parole:*

(a) *se $M \vDash T$ e $N \subseteq M$ è una sottostruttura, allora $N \vDash T$,*

(b) *se $M \vDash T$ e $F\colon M \twoheadrightarrow N$ è un morfismo suriettivo, allora $N \vDash T$,*

(c) *se $M \vDash T$ e $N \vDash T$, allora $M \times N \vDash T$.*

3.F.4. *Immersioni elementari e teorie complete.*

Definizione 3.26. (i) Sia N una sottostruttura di una L-struttura M. Diremo che N è una **sottostruttura elementare di** M se

$$\mathbf{T}^N_{\varphi(x_1,\dots,x_n)} = \mathbf{T}^M_{\varphi(x_1,\dots,x_n)} \cap N^n$$

per ogni formula φ.

(ii) Se $f\colon N \to M$ è un'immersione e $\mathrm{ran}(f)$ è una sottostruttura elementare, diremo che f è un'**immersione elementare** e che N si immerge elementarmente in M.

Per la (3.15), se N si immerge elementarmente in M, allora M ed N sono elementarmente equivalenti. Un isomorfismo è un'immersione elementare, quindi due strutture isomorfe sono elementarmente equivalenti. Il viceversa non vale perché, come vedremo in seguito, ci possono essere strutture elementarmente equivalenti di cardinalità differente.

Due L-strutture hanno la stessa taglia se c'è una biezione tra di loro. In particolare, strutture isomorfe hanno la stessa cardinalità, ma non vale il viceversa. Nel Capitolo VI dimostreremo il seguente criterio per dimostrare la completezza di una teoria.

Teorema 3.27. *Sia L un linguaggio con una quantità al più numerabile di simboli non logici e sia T una L-teoria soddisfacibile che ha solo modelli infiniti. Supponiamo ci sia un modello M di T tale che ogni modello N di T di ugual taglia di M è isomorfo a M. Allora T è una teoria completa.*

Vediamo degli esempi di teorie complete.

Esempio 3.28. Consideriamo il linguaggio L privo di simboli non logici: i suoi modelli sono gli insiemi non vuoti. Se $\Sigma_\emptyset$ è la L-teoria priva di assiomi, allora $\Sigma_\emptyset$ è soddisfacibile, dato che è soddisfatta da un qualsiasi insieme non vuoto, ma non è completa, dato che né l'enunciato "ci sono esattamente n elementi" $\boldsymbol{\varepsilon}_n$ di pagina 15, né la sua negazione sono conseguenza logica di questa teoria. D'altro canto le teorie $\Sigma_n = \{\boldsymbol{\varepsilon}_n\}$ e $\Sigma_\infty = \{\boldsymbol{\varepsilon}_{\geq n} \mid n > 0\}$ sono complete. Ciò è immediato nel caso di Σ_n dato che due modelli di Σ_n sono semplicemente due insiemi di taglia n e quindi isomorfi. Ma M e N sono semplicemente due insiemi con n elementi, quindi sono in biezione, e quindi sono isomorfi. Per Σ_∞, osserviamo che due modelli numerabili sono isomorfi, quindi possiamo applicare il Teorema 3.27. Quindi le teorie Σ_n ($n = 1, 2, \ldots, \infty$) sono le uniche teorie complete che estendono $\Sigma_\emptyset$ (Esercizio 3.61).

Se T è una teoria completa che ha un modello finito di taglia n, allora $T \models \boldsymbol{\varepsilon}_n$ e quindi ogni modello di T è finito di taglia n. Quindi le teorie dei (semi)gruppi (abeliani o no), degli anelli, dei campi, ... non sono complete. Per ulteriori esempi di teorie complete si consideri la teoria di una struttura, oppure si vedano gli esempi della Sezione 5.B.

3.F.5. *Insiemi definibili.* Un sottoinsieme A di M^n si dice **definibile senza parametri** o più semplicemente **definibile** se è l'insieme di verità di una qualche formula φ e una lista di variabili $x_1, \ldots, x_n$, cioè se $A = \mathbf{T}^M_{\varphi(x_1,\ldots,x_n)}$. Quando l'insieme A è il singoletto $\{(a_1, \ldots, a_n)\}$ diremo che $(a_1, \ldots, a_n)$ è definibile. L'intero n si dice dimensione dell'insieme definibile A.

Diremo che $A \subseteq M^n$ è **definibile con parametri** $p_1, \ldots, p_k \in M$ se c'è una formula φ e una lista di variabili $(x_1, \ldots, x_n, y_1, \ldots, y_k)$ tali che

$$A = \{(a_1, \ldots, a_n) \in M^n \mid (a_1, \ldots, a_n, p_1, \ldots, p_k) \in \mathbf{T}^M_{\varphi(x_1,\ldots,x_n,y_1,\ldots,y_k)}\}.$$

In altre parole: A è la sezione di $\mathbf{T}^M_{\varphi(x_1,\ldots,x_n,y_1,\ldots,y_k)}$ determinata da $(p_1, \ldots, p_k)$.

Una funzione $f\colon X \to M$ con $X \subseteq M^n$ è definibile (con o senza parametri) se il suo grafo $\mathrm{Gr}(f)$ lo è. Ogni elemento $a \in M$ è definibile con parametro

a, mediante la formula $x_1 = y_1$. Al fine di evitare banalità, quando si considerano elementi (cioè singoletti) la nozione di definibilità è sempre da intendersi *senza* parametri. Ogni insieme definibile senza parametri può essere sempre visto come insieme definibile con parametri $p_1, \dots, p_k$ — basta congiungere la formula che definisce l'insieme con una formula valida con variabili libere $y_1, \dots, y_k$, per esempio $\bigwedge_{1\leq i\leq k} y_i = y_i$. Quindi la nozione di insieme definibile con parametri generalizza quella di insieme definibile senza parametri. Viceversa, se $A \subseteq M^n$ è definibile mediante $\varphi(x_1, \dots, x_n, y_1, \dots, y_k)$ e parametri $p_1, \dots, p_k$, e se ciascun p_i è definibile mediante $\psi_i(y_i)$, allora A è definibile senza parametri mediante la formula

$$\exists y_1, \dots, y_k \, (\bigwedge_{1\leq i\leq k} \psi_i(y_i) \wedge \varphi(x_1, \dots, x_n, y_1, \dots, y_k))$$

o, equivalentemente mediante la formula

$$\forall y_1, \dots, y_k \, (\bigwedge_{1\leq i\leq k} \psi_i(y_i) \Rightarrow \varphi(x_1, \dots, x_n, y_1, \dots, y_k)).$$

Quindi le nozioni di definibilità con e senza parametri coincidono nelle strutture in cui ogni elemento è definibile — questo avviene, per esempio, nella struttura dei numeri naturali (Sezione 6.A).

La famiglia degli insiemi definibili in M (con o senza parametri), di una dimensione fissata n contiene sempre l'insieme vuoto (definito dalla formula $\bigwedge_{1\leq i\leq n} x_i \neq x_i$ o anche dalla formula $\bigvee_{1\leq i\leq n} x_i \neq x_i$), l'insieme M^n (definito dalla formula $\bigwedge_{1\leq i\leq n} x_i = x_i$ o anche dalla formula $\bigvee_{1\leq i\leq n} x_i = x_i$) ed è chiusa per complementi, intersezioni, unioni e differenze: se $A, B \subseteq M^n$, sono definiti dalle formule $\varphi(x_1, \dots, x_n)$ e $\psi(x_1, \dots, x_n)$ allora

- $M^n \setminus A$ è definito da $\neg\varphi$,
- $A \cap B$ è definito da $\varphi \wedge \psi$,
- $A \cup B$ è definito da $\varphi \vee \psi$,
- $A \setminus B$ è definito da $\varphi \wedge \neg\psi$.

Definizione 3.29. Un'**algebra di sottoinsiemi** di un insieme X è una famiglia non vuota $\mathcal{A} \subseteq \mathscr{P}(X)$ che contiene X e l'insieme vuoto $\emptyset$, chiusa per intersezioni, unioni e differenze.

Quindi la famiglia degli insiemi definibili in M (con o senza parametri), di una dimensione fissata n è un'algebra di sottoinsiemi di M^n.

Osservazione 3.30. Un sottoinsieme $A \subseteq M^n$ definibile con parametri $p_1, \dots, p_k$ può essere identificato con un sottoinsieme $\hat{A} \subseteq M^{n+m}$ definibile con gli stessi parametri — per esempio se A è definito a partire da $\varphi(x_1, \dots, x_n, y_1, \dots, y_k)$ e parametri $p_1, \dots, p_k$, allora $\hat{A} = A \times M^m$, è definito da

$$\varphi(x_1, \dots, x_n, x_{n+1}, \dots, x_{n+m}, y_1, \dots, y_k)$$

e dai parametri $p_1, \ldots, p_k$. Inoltre la mappa $A \mapsto \hat{A}$ rispetta[12] le usuali operazioni insiemistiche di intersezione, unione, complementazione, ... quindi la famiglia dei sottoinsiemi definibili di dimensione n può essere vista come una sottofamiglia dei sottoinsiemi di dimensione $m > n$.

In generale, la complessità della famiglia aumenta al crescere della dimensione — come vedremo nella Sezione 6.A, i sottoinsiemi definibili di dimensione 1 di $(\mathbb{N}, S)$ dove S è l'operazione di successore, sono esattamente i sottoinsiemi finiti e cofiniti, mentre la diagonale $\{(n, n) \mid n \in \mathbb{N}\}$ è un sottoinsieme definibile di dimensione 2 che è infinito e il cui complemento è infinito.

In generale è molto più semplice verificare che un $A \subseteq M^n$ è definibile (con o senza parametri) piuttosto che dimostrare l'opposto: nel primo caso dobbiamo trovare una formula φ il cui insieme di verità è proprio A, mentre nel secondo caso dobbiamo dimostrare che *nessuna* formula φ va bene. Un metodo spesso efficace per dimostrare la non-definibilità di un insieme si basa sulla nozione di **automorfismo** di una struttura, cioè un isomorfismo della struttura in sé stessa. L'insieme degli automorfismi di una struttura M,

$$\mathrm{Aut}(M)$$

è un gruppo con l'operazione di composizione. Ogni struttura M ha almeno un automorfismo — la funzione identica id_M — e se questo è l'unico automorfismo, cioè se $\mathrm{Aut}(M)$ è il gruppo banale, diremo che M è **rigida**. Per la Proposizione 3.22(d), se $A \subseteq M^n$ è definibile, allora viene mandato su sé stesso da ogni automorfismo. Quindi per dimostrare che un $A \subseteq M^n$ non è definibile è sufficiente trovare un automorfismo che non manda A su sé stesso. Se c'è un automorfismo f tale che $f[A] \neq A$ e $f(p_i) = p_i$, per $i = 1, \ldots, k$, possiamo concludere che A non è definibile con parametri $p_1, \ldots, p_k$. Per esempio, $\{\mathrm{i}, -\mathrm{i}\}$ è definibile nel campo complesso mediante la formula $x \cdot x + 1 = 0$, ma né l'unità immaginaria né il suo coniugato sono definibili, visto che $z \mapsto \overline{z}$ è un automorfismo.

Osservazioni 3.31. (a) Non è detto che un insieme invariante per automorfismi sia definibile. (Un $A \subseteq M^n$ è **invariante per automorfismi** se per ogni automorfismo F e $a_1, \ldots, a_n \in M$ si ha che $(a_1, \ldots, a_n) \in A \Rightarrow (F(a_1), \ldots, F(a_n)) \in A$.) Per esempio l'unico automorfismo dei numeri naturali con l'operazione di successore è l'identità (Esercizio 3.52) e quindi ogni sottoinsieme di $\mathbb{N}$ è invariante per automorfismi. I sottoinsiemi definibili sono tanti quanti le formule del linguaggio contenente i simboli 0 e S quindi, come vedremo nel Capitolo VI, sono in quantità numerabile, mentre i sottoinsiemi di $\mathbb{N}$ sono molti di più.

[12] Una mappa siffatta si dice omomorfismo di algebre di Boole, vedi Sezione 8.F.

(b) Se M è rigida e $M \cong N$, allora anche N è rigida e l'isomorfismo tra M ed N è unico, dato che se $F, G\colon M \to N$ sono isomorfismi allora $G^{-1} \circ F$ è un automorfismo di M e quindi è l'identità. Quindi se $\mathcal{C}$ è una famiglia di L-strutture tra loro isomorfe e se una di queste è rigida (equivalentemente: sono tutte rigide), allora le strutture in $\mathcal{C}$ sono isomorfe in modo canonico e quindi completamente identificabili tra di loro.

3.F.6. *Interpretabilità in strutture.* Fissiamo un campo $\Bbbk$. L'insieme $\mathrm{GL}_2(\Bbbk)$ delle matrici invertibili 2×2 su $\Bbbk$ può essere identificato con il sottoinsieme di $\Bbbk^4$

$$\{(x_{11}, x_{12}, x_{21}, x_{22}) \mid x_{11} \cdot x_{22} \neq x_{12} \cdot x_{21}\},$$

e l'operazione di moltiplicazione di matrici può essere vista come un'operazione binaria su $\Bbbk^4$. Quindi il gruppo $\mathrm{GL}_2(\Bbbk)$ può essere definito nel campo $\Bbbk$, e diremo che la struttura $(\mathrm{GL}_2(\Bbbk), \cdot)$ è definibilmente interpretabile nella struttura $(\Bbbk, +, \cdot, 0, 1)$. Più in generale, una L-struttura M è **definibilmente interpretabile** in una L'-struttura M' se c'è un isomorfismo $F\colon M \to N$ tale che N è un sottoinsieme definibile (di opportuna dimensione) di M' e se tutte le relazioni, le funzioni, le costanti di N possono essere definite in M'. (Le operazioni k-arie di N possono essere viste come relazioni $k+1$-arie su N.)

Un'estensione della nozione di interpretazione definibile è ottenuta codificando la struttura M come quoziente di M'. Più precisamente, richiediamo che N sia della forma X/E con X sottoinsieme definibile (di opportuna dimensione) di M' e E una relazione di equivalenza definibile su X. In questo caso diremo che M è **definibilmente interpretabile in un quoziente** di M'. Prendendo $E = \mathrm{id}_M$ si ricade nella definizione precedente.

Per esempio consideriamo lo spazio proiettivo di dimensione n su un campo $\Bbbk$

$$\mathbb{P}_n(\Bbbk) \stackrel{\text{def}}{=} (\Bbbk^{n+1} \setminus \{\mathbf{0}\})/E$$

dove E è la relazione di collinearità su $\Bbbk^{n+1}$,

$$\mathbf{x}\, E\, \mathbf{y} \Leftrightarrow \exists \lambda \in \Bbbk \setminus \{0\}\, (\lambda \mathbf{x} = \mathbf{y}).$$

Se $f \in \Bbbk[X_1, \ldots, X_n]$ è un polinomio omogeneo di grado d, cioè $f(\lambda \mathbf{x}) = \lambda^d f(\mathbf{x})$ per ogni $\mathbf{x} \in \Bbbk^{n+1}$ e ogni $\lambda \in \Bbbk$, la varietà proiettiva definita da f è

$$V = \{[\mathbf{x}] \in \mathbb{P}_n(\Bbbk) \mid f(\mathbf{x}) = 0\}.$$

Quindi, la struttura $(\mathbb{P}_n(\Bbbk), V)$ è definibilmente interpretabile in $\Bbbk$.

3.G. Assiomatizzabilità. Nella Sezione 3.C abbiamo visto che cosa significa dire che una L-struttura M soddisfa una teoria T del linguaggio L. La classe dei modelli di T è

$$\mathrm{Mod}(T) = \{M \mid M \text{ è una } L\text{-struttura tale che } M \vDash T\}\,.$$

Chiaramente $\mathrm{Mod}(T) = \emptyset$ se e solo se T è insoddisfacibile e $\mathrm{Mod}(T)$ è la totalità delle L-strutture se e solo se T consiste di enunciati validi.

Viceversa, data una classe $\mathcal{C}$ di L-strutture, possiamo chiederci se esista qualche teoria T del linguaggio L tale che $\mathcal{C} = \mathrm{Mod}(T)$. Per la Proposizione 3.22(d) se $M \in \mathrm{Mod}(T)$ e $N \cong M$, allora $N \in \mathrm{Mod}(T)$, quindi il problema è sensato soltanto quando $\mathcal{C}$ è chiusa per isomorfismi.

Definizione 3.32. Una classe $\mathcal{C}$ di L-strutture si dice **assiomatizzabile** se $\mathcal{C} = \mathrm{Mod}(T)$ per qualche teoria T. Se T può essere presa finita, diremo che $\mathcal{C}$ è **finitamente assiomatizzabile**.

Per quanto detto a pagina 38 e seguenti:

- la classe dei gruppi è finitamente assiomatizzabile nel linguaggio L_{GRUPPI} mediante gli assiomi Σ_{GRUPPI},
- la classe degli anelli è finitamente assiomatizzabile nel linguaggio L_{ANELLI} mediante gli assiomi Σ_{ANELLI},
- la classe dei campi ordinati è finitamente assiomatizzabile nel linguaggio $L_{\text{ANELLI O.}}$ mediante gli assiomi $\Sigma_{\text{CAMPI O.}}$.

Nelle prossime sezioni vedremo altri esempi di classi di strutture che sono finitamente assiomatizzabili, ed anche esempi di classi di strutture che sono assiomatizzabili, ma non finitamente, ed esempi di classi di strutture che non sono assiomatizzabili del tutto. Come per la definibilità, è molto più semplice mostrare che una classe è (finitamente) assiomatizzabile, piuttosto che mostrare l'opposto: nel primo caso è sufficiente esibire un sistema (finito) di enunciati che assiomatizza la classe data, nel secondo bisogna dimostrare che nessun insieme (finito) di enunciati è in grado di assiomatizzare la classe di strutture in questione. In certi casi, il problema della (finita) assiomatizzabilità o meno di una classe di strutture dipende dal linguaggio del prim'ordine. Nella Sezione 5.H del Capitolo II vedremo che la classe dei grafi bipartiti è assiomatizzabile, ma non finitamente, nel linguaggio dei grafi (Esercizio 5.42), mentre la medesima classe risulta essere finitamente assiomatizzabile in un opportuno linguaggio ampliato. Un discorso analogo vale per la classe dei gruppi abeliani privi di torsione (Esempio 5.2). Un altro esempio interessante è costituito dalla classe degli **ordini lineari omogenei**, cioè ordini lineari tali che per ogni coppia di intervalli aperti $(a; b)$ e $(c; d)$ c'è sempre un automorfismo F (cioè una biezione crescente) tale che $F(a) = c$ e $F(b) = d$. Come vedremo nell'Esercizio 33.10 del Capitolo VI, gli ordini

lineari omogenei non sono assiomatizzabili nel linguaggio contenente solo $<$, mentre sono finitamente assiomatizzabili in un linguaggio opportunamente ampliato (Esercizio 3.59).

Il prossimo risultato, che dimostreremo nella Sezione 31.B del Capitolo VI, fornisce un metodo per dimostrare la non-assiomatizzabilità di una classe di strutture.

Teorema 3.33. *Siano $\mathcal{C}_0 \subseteq \mathcal{C}_1$ delle classi assiomatizzabili e supponiamo che $\mathcal{C}_1$ sia finitamente assiomatizzabile mentre $\mathcal{C}_0$ no, relativamente ad un fissato linguaggio del prim'ordine L. Allora $\mathcal{C}_1 \setminus \mathcal{C}_0$ non è assiomatizzabile, neanche ampliando il linguaggio L.*

In particolare, per gli Esempi 3.12, la classe degli insiemi finiti e la classe dei gruppi finiti non sono assiomatizzabili al prim'ordine.

Esercizi

Esercizio 3.34. Dimostrare la Proposizione 3.22.

Esercizio 3.35. Verificare che le seguenti formule sono tautologicamente equivalenti:

(i) $\varphi \wedge (\psi \vee \chi)$ e $(\varphi \wedge \psi) \vee (\varphi \wedge \chi)$,

(ii) $\varphi \vee (\psi \wedge \chi)$ e $(\varphi \vee \psi) \wedge (\varphi \vee \chi)$,

(iii) $\neg(\varphi \wedge \psi)$ e $\neg\varphi \vee \neg\psi$,

(iv) $\neg(\varphi \vee \psi)$ e $\neg\varphi \wedge \neg\psi$,

(v) $\varphi \vee \psi$ e $\neg(\varphi \Leftrightarrow \psi)$.

Esercizio 3.36. Supponiamo che φ non sia una contraddizione proposizionale e che sia combinazione booleana di sottoformule primitive $\mathrm{A}_1, \ldots, \mathrm{A}_n$. Siano $i_1, \ldots, i_m$ le righe della tavola di verità di φ in cui nella colonna di φ compare il valore 1. Verificare che φ è tautologicamente equivalente alla disgiunzione $\mathrm{D}_{i_1} \vee \cdots \vee \mathrm{D}_{i_m}$ dove ogni D_i è la congiunzione $\mathrm{C}_{i,1} \wedge \cdots \wedge \mathrm{C}_{i,n}$, in cui $\mathrm{C}_{i,j}$ è A_j se nel posto di coordinate della tavola di verità (i, j) c'è un 1, oppure $\neg\mathrm{A}_j$ se c'è uno 0.

Esercizio 3.37. Per ogni sottoformula della formula (3.2) di pagina 23, trovare le occorrenze libere e vincolate delle variabili.

Esercizio 3.38. Mettere in forma prenessa le seguenti formule:

(i) $\exists y R(y, x) \Rightarrow \exists y\,(R(y, x) \wedge \neg\exists z\,(R(z, y) \wedge R(z, x)))$,

(ii) $\exists x \forall y \exists z P(x, y, z) \vee (\exists x \forall y Q(x, y) \wedge \neg\forall x \exists y R(x, y))$,

(iii) $\forall x \forall y\,(E(x, y) \Leftrightarrow \forall z\,(R(z, x) \Leftrightarrow R(z, y)))$.

Per ciascuna formula calcolare la complessità del prefisso basata sull'alternanza di quantificatori, come indicato a pagina 36.

Esercizio 3.39. Verificare che l'enunciato "f è una funzione continua da $\mathbb{R}$ in $\mathbb{R}$" è formalizzabile come una $\forall\exists\forall$-formula nel linguaggio contenente i simboli f, $+$ e $<$.

Esercizio 3.40. Supponiamo che φ sia combinazione booleana di sue sottoformule primitive $\psi_1, \ldots, \psi_n$, e sia φ' la formula ottenuta da φ rimpiazzando $\psi_1, \ldots, \psi_n$, con $\psi'_1, \ldots, \psi'_n$. Dimostrare che se ψ_i è tautologicamente equivalente a ψ'_i $(i = 1, \ldots, n)$ allora φ è tautologicamente equivalente a φ'.

Esercizio 3.41. Dimostrare che

(i) $\{\neg, \Rightarrow\}$, $\{\forall, \Rightarrow\}$ e $\{\vee, \Leftrightarrow, \forall\}$ sono insiemi adeguati di connettivi;

(ii) $\{\neg, \Leftrightarrow, \forall\}$, $\{\vee, \wedge, \forall\}$ e $\{\neg, \forall, \Leftrightarrow\}$ non sono adeguati;

(iii) il **tratto di Sheffer** $\mid$ e la **freccia di Peirce** $\uparrow$ definiti da

$$\mathrm{P} \mid \mathrm{Q} \text{ se e solo se } \neg(\mathrm{P} \wedge \mathrm{Q})$$
$$\mathrm{P} \uparrow \mathrm{Q} \text{ se e solo se } \neg(\mathrm{P} \vee \mathrm{Q}).$$

sono gli unici connettivi binari $\odot$ tali che $\{\odot\}$ è adeguato.

Esercizio 3.42. Sia L il linguaggio contenente un simbolo di relazione binaria R. Stabilire quali dei seguenti enunciati:

(σ_0) $\forall x, y, z\,(x\ R\ y \wedge y\ R\ z \Rightarrow x\ R\ z)$

(σ_1) $\forall x, y\,(x\ R\ y \Rightarrow \exists z\,(x\ R\ z \wedge z\ R\ y))$

(σ_2) $\forall x \exists y\,(x\ R\ y \wedge \neg\exists z\,(x\ R\ z \wedge z\ R\ y))$

(σ_3) $\exists x \forall y\,(y \neq x \Rightarrow x\ R\ y)$

(σ_4) $\exists x \forall y \neg(y\ R\ x)$

(σ_5) $\exists x \forall y \neg(x\ R\ y)$

valgono nelle strutture:

(a) $(\mathbb{N}, <)$,

(b) $(\mathbb{N}, \leq)$,

(c) $(\mathbb{N}, |)$, dove $|$ è la relazione di divisibilità,

(d) $(\mathbb{N}, \perp)$, dove $\perp$ è la relazione di coprimalità,

(e) $(\mathbb{Z}, <)$,

(f) $(\mathbb{Q}, <)$,

(g) $((0;1] \cup [2;3], <)$,

(h) $(\mathscr{P}(\mathbb{N}) \setminus \{\emptyset, \mathbb{N}\}, \subset)$,

(i) $(\mathbb{S}^2, \perp)$, dove $\mathbb{S}^2 = \left\{\mathbf{x} \in \mathbb{R}^3 \mid \|\mathbf{x}\| = 1\right\}$ è l'insieme dei vettori unitari dello spazio e $\perp$ è la relazione di ortogonalità.

Esercizio 3.43. Trovare gli insiemi di verità nella struttura $(\mathbb{N}, \cdot)$ delle formule

(i) $\psi(x)$: $\exists u \forall v\,(v = v \cdot u \wedge x \neq u \wedge \forall y \forall z\,(x = y \cdot z \Rightarrow y = u \vee z = u))$,

(ii) $\varphi(x)$: $\forall y \forall z\,(\psi(y) \wedge \psi(z) \wedge \exists u\,(y \cdot u = x) \wedge \exists u\,(z \cdot u = x) \Rightarrow y = z)$,

(iii) $\varphi_2(x)$: $\exists y\,(x = y \cdot y \wedge \psi(y))$,

(iv) $\chi(x)$: $\exists y \exists z\,(x = y \cdot z \wedge \psi(y) \wedge \psi(z))$.

Esercizio 3.44. Stabilire quali dei seguenti enunciati sono soddisfacibili, validi o insoddisfacibili:

(i) $\forall x\,(P(x) \Rightarrow Q(x)) \wedge \exists x\,(Q(x) \Rightarrow R(x)) \Rightarrow \forall x\,(P(x) \Rightarrow R(x))$,

(ii) $\forall x\,(P(x) \Rightarrow Q(x)) \wedge \forall x\,(Q(x) \Rightarrow R(x)) \Rightarrow \forall x\,(P(x) \Rightarrow R(x))$,

(iii) $\exists x \exists y\,(P(x) \Rightarrow Q(y)) \Leftrightarrow \exists x\,(P(x) \Rightarrow Q(x))$,

(iv) $\exists x\,P(x) \Rightarrow \exists x\,Q(x) \Rightarrow \exists x\,(P(x) \Rightarrow Q(x))$,

(v) $(\exists x\,P(x) \Rightarrow \exists x\,Q(x)) \Rightarrow \exists x\,(P(x) \Rightarrow Q(x))$,

(vi) $\exists x\,(P(x) \Rightarrow Q(x)) \Rightarrow (\exists x\,P(x) \Rightarrow \exists x\,Q(x))$,

(vii) $(\exists x\,P(x) \Rightarrow \forall x\,\neg Q(x)) \wedge \exists x\,(P(x) \wedge Q(x))$.

Esercizio 3.45. (i) Dimostrare che

$$\forall \vec{x}\ (\varphi(\vec{x}) \Leftrightarrow \psi(\vec{x})) \Rightarrow (\forall \vec{x}\,\varphi(\vec{x}) \Leftrightarrow \forall \vec{x}\,\psi(\vec{x}))$$

è valida.

(ii) Dimostrare con un controesempio che l'implicazione inversa non vale, cioè

$$(\forall \vec{x}\, \varphi(\vec{x}) \Leftrightarrow \forall \vec{x}\, \psi(\vec{x})) \Rightarrow \forall \vec{x}\, (\varphi(\vec{x}) \Leftrightarrow \psi(\vec{x}))$$

è soddisfacibile, ma non valida.

Esercizio 3.46. Dati un insieme $M \neq \emptyset$, due funzioni $f, g\colon M \to M$ e due sottoinsiemi $P, Q \subseteq M$, consideriamo il linguaggio L del prim'ordine contenente due simboli di funzione unaria e due simboli di predicato unario. Per semplicità notazione denoteremo questi simboli con f, g, P, Q e considereremo M come una L-struttura. Verificare che i seguenti insiemi sono definibili in M:

(i) $f[P]$;
(ii) $g[M \setminus f^{-1}[P]]$;
(iii) $f^{-1}[P] \setminus g[Q]$;
(iv) $f[P] \times g[Q]$.

Esercizio 3.47. Verificare che:

(i) se $F\colon M \to N$ è un morfismo di strutture, allora $\mathrm{ran}(F)$ è una sottostruttura di N e $F\colon M \to \mathrm{ran}(F)$ è un morfismo di strutture;
(ii) se L non contiene simboli di relazione, allora un morfismo biettivo $F\colon M \to N$ è un isomorfismo;
(iii) M si immerge in N se e solo se M è isomorfa ad una sottostruttura di N;
(iv) se $F\colon M \to N$ è biettiva e valgono (A′), (B) e (C) di pagina 48, allora F è un isomorfismo.

Esercizio 3.48. Per ciascuna coppia di gruppi

$$(\mathbb{R}_+, \cdot), \quad (\mathbb{Q}_+, \cdot), \quad (\mathbb{R} \setminus \{0\}, \cdot), \quad (\mathbb{Q} \setminus \{0\}, \cdot), \quad (\mathbb{R}, +), \quad (\mathbb{Q}, +)$$

stabilire se sono isomorfi, se sono elementarmente equivalenti, se uno si immerge nell'altro.

Esercizio 3.49. Per ciascuna coppia di strutture, stabilire se sono isomorfe, se sono elementarmente equivalenti, se una si immerge (elementarmente) nell'altra o se c'è un morfismo da una nell'altra:

- $(\mathbb{N}, +, 0, \leq)$ e $(\mathbb{N}, \cdot, 1, \leq)$,
- $(\mathbb{N}, +)$ e $(\mathbb{N}, \cdot)$,
- $(\mathbb{N}, +, 0, \leq)$ e $(\mathbb{N} \setminus \{0\}, \cdot, 1, \leq)$,
- $([0; 1), \leq)$ e $((0; 1], \leq)$,
- $([0; 1], \leq)$ e $((0; 1), \leq)$.

Esercizio 3.50. Dimostrare che

(i) se $f\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ è tale che per ogni $a, b, c, d \in \mathbb{N}$

$$f(a + c, b + d) = f(a, b) + f(c, d)$$

oppure

$$f(a, b + d) = f(a, b) + f(a, d) \quad \text{e} \quad f(a + c, b) = f(a, b) + f(c, b),$$

allora f non è iniettiva. In particolare, $(\mathbb{N} \times \mathbb{N}, +)$ non si immerge in $(\mathbb{N}, +)$;
(ii) $(\mathbb{Z}_+, \cdot)$ è isomorfo a $(\mathbb{N}[X], +)$. Concludere che $(\mathbb{Z}_+ \times \mathbb{Z}_+, \cdot)$ è isomorfo a $(\mathbb{Z}_+, \cdot)$, dove il prodotto su $\mathbb{Z}_+ \times \mathbb{Z}_+$ è definito componente per componente, cioè $(a, b) \cdot (c, d) = (a \cdot c, b \cdot d)$;
(iii) non c'è nessuna funzione iniettiva $f\colon \mathbb{Z}_+ \times \mathbb{Z}_+ \to \mathbb{Z}_+$ tale che per ogni $a, b, c, d \in \mathbb{Z}_+$

$$f(a, b \cdot d) = f(a, b) \cdot f(a, d) \quad \text{o} \quad f(a \cdot c, b) = f(a, b) \cdot f(c, b).$$

Esercizio 3.51. Sia M una L-struttura e $p_1, \ldots, p_k \in M$. Dimostrare che

(i) se $f_1, \ldots, f_n$ sono funzioni parziali da M^m in M e g è una funzione parziale da M^n in M e sono definibili in M con parametri $p_1, \ldots, p_k$, allora la funzione parziale h da M^m in M definita da $h(\vec{x}) = g(f_1(\vec{x}), \ldots, f_n(\vec{x}))$ è definibile con parametri $p_1, \ldots, p_k$;

(ii) se f è una funzione parziale iniettiva da M in sé stesso ed è definibile con parametri $p_1, \ldots, p_k$, allora anche la funzione parziale f^{-1} lo è.

Esercizio 3.52. Dimostrare che $\mathbb{N}$ con l'operazione di successore è un esempio di struttura rigida.

Esercizio 3.53. Dimostrare che $\mathbb{N}$ e $<$ non sono definibili senza parametri né in $(\mathbb{Z}, +)$ né in $(\mathbb{R}, +)$.

Esercizio 3.54. Dimostrare che:

(i) ogni elemento è definibile in $(\mathbb{N}, +)$,

(ii) ogni elemento è definibile in $(\mathbb{Z}, +, \cdot)$,

(iii) ogni elemento è definibile in $(\mathbb{Q}, +, \cdot)$.

(iv) Concludere che $(\mathbb{N}, +)$, $(\mathbb{Z}, +, \cdot)$ e $(\mathbb{Q}, +, \cdot)$ sono strutture rigide, cioè ammettono solo l'identità come automorfismo (vedi pag. 55).

(v) Dimostrare che nella struttura $(\mathbb{Z}, +)$, 0 è l'unico elemento definibile.

Esercizio 3.55. Dimostrare che i seguenti insiemi sono definibili in $(\mathbb{N}, |)$, dove $|$ è la relazione di divisibilità :

(i) $\{0\}$ e $\{1\}$;

(ii) $\{n \mid n \text{ non è primo}\}$;

(iii) $\{p^n \mid p \text{ è primo e } n > 0\}$;

(iv) $\left\{p^2 \mid p \text{ è primo}\right\}$;

(v) $\{pq \mid p \text{ e } q \text{ sono primi distinti}\}$;

(vi) $\left\{(n, m) \in \mathbb{N}^2 \mid n \perp m\right\}$, dove $n \perp m$ significa che n e m sono relativamente primi;

(vii) $\left\{(n, m, k) \in \mathbb{N}^3 \mid k = \text{mcm}(n, m)\right\}$, dove $\text{mcm}(n, m)$ è il minimo comune multiplo tra n ed m;

(viii) $\left\{(n, m, k) \in \mathbb{N}^3 \mid k = \text{mcd}(n, m)\right\}$, dove $\text{mcd}(n, m)$ è il massimo comun denominatore tra n ed m.

Esercizio 3.56. Per ciascuna delle seguenti classi di L-strutture, dove L è il linguaggio con un simbolo R di relazione binaria, stabilire se si tratta di una classe assiomatizzabile, e in caso affermativo se si tratta di una classe finitamente assiomatizzabile:

(i) la classe delle relazioni d'equivalenza che hanno esattamente n classi di equivalenza,

(ii) la classe delle relazioni d'equivalenza che hanno infinite classi di equivalenza,

(iii) la classe delle relazioni d'equivalenza che hanno finite classi di equivalenza,

(iv) la classe delle relazioni d'equivalenza con classi di equivalenza con esattamente n elementi,

(v) la classe delle relazioni d'equivalenza con classi di equivalenza con infiniti elementi,

(vi) la classe delle relazioni d'equivalenza con classi di equivalenza finite.

Esercizio 3.57. (i) Se $\sigma \in \Sigma$ e σ è valido, allora Σ e $\Sigma \setminus \{\sigma\}$ sono logicamente equivalenti.

(ii) Se per ogni n, l'enunciato $\sigma_{n+1} \Rightarrow \sigma_n$ è valido, ma $\sigma_n \Rightarrow \sigma_{n+1}$ non lo è, allora $\{\sigma_0, \sigma_1, \ldots\}$ non ha nessun sottoinsieme indipendente di assiomi.

Esercizio 3.58. Supponiamo che $\Sigma = \{\sigma_n \mid n \in \omega\}$ sia un insieme di enunciati tali che $\sigma_m \Rightarrow \sigma_n$ se e solo se $n < m$. Dimostrare che Σ non è finitamente assiomatizzabile.

Esercizio 3.59. Dimostrare che gli ordini lineari omogenei sono finitamente assiomatizzabili in un linguaggio contenente il simbolo $<$ e un predicato 6-ario $F(x, y, a, b, c, d)$.

Esercizio 3.60. Dimostrare che il campo complesso e il gruppo $\{z \in \mathbb{C} \mid |z| = 1\}$ sono definibilmente interpretabili in $(\mathbb{R}; +, \cdot)$.

Esercizio 3.61. Usando la notazione dell'Esempio 3.28, dimostrare che le teorie Σ_n $(n \in \mathbb{N})$ e Σ_∞ sono le uniche estensioni complete di $\Sigma_\emptyset$.

Esercizio 3.62. (i) Fissiamo un linguaggio L con un simbolo di funzione binario $*$. La proprietà associativa di $*$ è espressa dall'enunciato (3.5) a pagina 26 in cui il simbolo $*$ compare 4 volte. Dimostrare che è possibile trovare una formulazione della proprietà associativa che utilizza meno di 4 occorrenze del simbolo $*$, vale a dire: c'è un enunciato di L equivalente a (3.5) in cui il simbolo $*$ compare meno di 4 volte e calcolare il minimo numero di occorrenze di $*$ necessarie per esprimere la proprietà associativa.

(ii) Fissiamo un linguaggio L con un simbolo di relazione binaria R. Dimostrare che è possibile trovare una formulazione della proprietà transitiva

$$\forall x \forall y \forall z \, (x \; R \; y \wedge y \; R \; z \Rightarrow x \; R \; z)$$

che utilizza meno di 3 occorrenze del simbolo R e calcolare il minimo numero di occorrenze di R necessarie per esprimere la proprietà transitiva.

Note e osservazioni

Il problema di Waring (la formula (3.3) a pagina 25) è stato posto nel 1770 da Waring e dimostrato nel 1909 da Hilbert. Quindi si definisce $g(k)$ per $k > 1$ come il più piccolo n tale che ogni naturale x è somma di n potenze di esponente k. I primi valori della funzione g sono 1, 4 (Lagrange), 9, 19, ... [**HW79**]. In teoria dei numeri più che $g(k)$ è importante considerare la quantità $G(k)$, cioè il più piccolo n tale che ogni naturale sufficientemente grande x è somma di n potenze di esponente k. Chiaramente $G(k) \leq g(k)$ e si verifica che $G(2) = g(2) = 4$. Il valore esatto di $G(k)$ per $k \geq 3$ non è noto — per esempio si sa soltanto che $4 \leq G(3) \leq 7$, cioè ogni numero naturale sufficientemente grande è somma di al più sette cubi e che esistono numeri arbitrariamente grandi che non sono somma di tre cubi.

La congettura *abc* (Esempio 3.3) è stata formulata nel 1988 da Oesterlé e, indipendentemente, nel 1985 da Masser; per questo motivo è anche nota come **congettura di Oesterlé–Masser** [**GT02**]. Questa congettura, considerata "il problema aperto più importante in analisi diofantea" [**Gol96**], implica numerosi risultati in teoria dei numeri, tra cui: l'ultimo teorema di Fermat (Esercizio (vii)), l'esistenza di infiniti primi che non sono di Wiefeirich (Esempio 2.2), la congettura di Erdős-Woods (Sezione 2.C.5) con l'eccezione di al più un numero finito di controesempi.

Il Teorema 3.13 è dovuto a Tarski.

I connettivi $|$ e $\uparrow$ prendono il nome dai logici Sheffer e Peirce; in informatica sono comunemente noti come *nand* e *nor*.

4. Che cos'è la logica matematica?

Una sezione con un titolo come questo forse sarebbe stato più saggio collocarla alla fine del libro, quando il lettore avrà acquisito le nozioni di base della materia. Ma anche dopo aver relegato questa sezione ad epilogo del libro, questo titolo risulterebbe sempre un po' impegnativo, visto che questo testo non si propone di insegnare tutta la logica matematica (impresa palesemente impossibile), ma solo di insegnare le basi di quella parte della logica matematica che, a giudizio di che scrive, ha più stretta attinenza con altre parti della matematica. Forse questa sezione la si dovrebbe intitolare *Che cos'è quella parte della logica matematica trattata in questo libro?* o qualcosa del genere... Comunque il desiderio di dare una fugace panoramica di quanto verrà studiato in dettaglio nelle pagine successive è troppo forte.

La logica matematica nasce dal tentativo di dare delle risposte matematicamente precise a domande generali quali:

(1) *Che cos'è una dimostrazione?*
(2) *Che cos'è un procedimento effettivo?*
(3) *Che cosa vuol dire che una certa affermazione è vera?*
(4) *Che cos'è un insieme?*
(5) *La logica è un'area della matematica, o è in qualche modo precedente alla matematica?*

I tentativi di rispondere a queste domande hanno generato una vasta mole di teorie matematiche.

4.A. Teoria della dimostrazione. La nozione informale di dimostrazione può essere formalizzata in modo adeguato per i linguaggi del prim'ordine: si parte da un insieme Γ di formule di L detti postulati o assiomi e mediante una catena di ragionamenti si giunge ad una formula che chiamiamo teorema. Per effettuare questi ragionamenti abbiamo bisogno di metodi per dedurre una formula dalle precedenti — le regole logiche — e di un insieme fissato di formule detti **assiomi logici**:

- le tautologie (definite a pagina 28),
- le formule del tipo $\varphi[\![t/x]\!] \Rightarrow \exists x \varphi$, e
- le formule del tipo

$$(x_1 = y_1 \wedge x_2 = y_2 \wedge x_1 = x_2) \Rightarrow y_1 = y_2$$
$$(x_1 = y_1 \wedge \cdots \wedge x_n = y_n) \Rightarrow f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n)$$
$$(x_1 = y_1 \wedge \cdots \wedge x_n = y_n \wedge P(x_1, \ldots, x_n)) \Rightarrow P(y_1, \ldots, y_n)$$

Le **regole logiche** sono il *modus ponens* (pag. 8) e la regola di **introduzione del quantificatore esistenziale**: se x non occorre libera in ψ, allora da $\varphi \Rightarrow \psi$ possiamo dedurre $(\exists x \varphi) \Rightarrow \psi$.

Fissato un insieme Γ di formule di un linguaggio del prim'ordine L, una **derivazione da** Γ è una stringa finita di formule

$$\varphi_0, \varphi_1, \ldots, \varphi_n$$

tali che per ogni $i \leq n$:

- φ_i è in Γ, oppure
- φ_i è un assioma logico, oppure
- φ_i è ottenuta dalle φ_j con $j < i$ mediante una delle due regole logiche.

Una formula φ è un **teorema di** Γ, in simboli

$$\Gamma \vdash \varphi$$

se c'è una derivazione da Γ tale che l'ultima formula della derivazione φ_n è proprio φ.

La nozione di derivazione ha un carattere sintattico, mentre nell'usuale argomentazione matematica si basa sul concetto di conseguenza logica (vedi pagina 41) che è una nozione semantica, cioè che tratta di modelli. Per esempio, se si vuole dimostrare l'affermazione

ogni gruppo con 49 elementi è abeliano

si considera un gruppo di ordine 49 (o più in generale di ordine p^2 con p primo) e si argomenta che il gruppo è isomorfo a $\mathbb{Z}/49\mathbb{Z}$ oppure a $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$, che sono entrambi abeliani. La derivazione della sua versione formalizzata

$$\boldsymbol{\varepsilon}_{49} \Rightarrow \forall x \forall y \, (x \cdot y = y \cdot x)$$

a partire dagli assiomi per i gruppi (gli enunciati (3.8) a pagina 38), è invece assai laboriosa.[13] Tuttavia la nozione formale, sintattica di dimostrazione (codificata dalle definizione di derivazione) e quella semantica (in uso nella pratica matematica) sono strettamente collegate. Supponiamo, per semplicità, che tanto φ quanto le formule di Γ siano degli enunciati: se $\Gamma \vdash \varphi$ allora ogni modello di Γ è un modello di φ (Teorema di Correttezza 34.2) e, viceversa, se ogni modello che soddisfa Γ soddisfa anche φ allora $\Gamma \vdash \varphi$ (Teorema di Completezza 35.2). Quindi le derivazioni sono la controparte formale della nozione intuitiva di dimostrazione — φ è dimostrabile (nell'accezione comune del termine) a partire da Γ, se e solo se φ è derivabile da Γ, in simboli $\Gamma \vdash \varphi$.

Attenzione. La parola "completezza" ha due significati distinti in logica, e questa spiacevole situazione può causare confusione. La "Completezza" nel Teorema 35.2 si riferisce al fatto che le regole logiche sono *complete*, cioè sono sufficientemente potenti per derivare ogni risultato dimostrato semanticamente, per mezzo di modelli. Questo non significa che l'insieme degli enunciati veri in ogni struttura sia una *teoria completa*, come l'Esempio 3.28 mostra.

Un sistema di assiomi Σ si dice **coerente** se non è contraddittorio, cioè se non è in grado di derivare una formula e la sua negazione. Chiaramente se Σ ha un modello allora è coerente, dato che una struttura non può soddisfare tanto un enunciato quanto la sua negazione. Ma vale anche il viceversa (Teorema di Esistenza di Modelli 35.3): se Σ è coerente, allora ha un modello.

Il calcolo logico che abbiamo descritto qui sopra (essenzialmente dovuto ad Hilbert e Ackermann) è molto utile per dimostrare i Teoremi di Correttezza e Completezza, ma è piuttosto distante dal modo informale con cui si argomenta in matematica. La **deduzione naturale**, inventata da Gentzen proprio per ovviare a questo inconveniente, permette un'analisi più

[13] Gli enunciati $\boldsymbol{\varepsilon}_n$ sono stati definiti a pagina 15.

incisiva della struttura delle dimostrazioni. L'idea di base del calcolo della deduzione naturale consiste nel privilegiare la nozione di regola: per ogni connettivo e quantificatore vengono introdotte delle regole simili a quelle della Sezione 2.A mediante le quali si definisce un'adeguata nozione di derivazione. Si dimostra che la deduzione naturale è equivalente al calcolo logico alla Hilbert-Ackermann nel senso che i teoremi derivabili da un insieme Σ di formule è lo stesso per i due calcoli logici. Questi argomenti verranno affrontati nel Capitolo **??**.

4.B. Calcolabilità. Ogni funzione calcolabile risulta appartenere ad un insieme di funzioni note come **funzioni ricorsive**. Poiché ogni funzione ricorsiva è calcolabile, useremo il termine "ricorsivo" come sinonimo di "calcolabile". Un insieme $A \subseteq \mathbb{N}$ è ricorsivo se la sua funzione caratteristica lo è. Per verificare se un certo numero n appartiene a $\mathrm{ran}(f)$, dove $f\colon \mathbb{N} \to \mathbb{N}$ è ricorsiva, è sufficiente calcolare i valori $f(0), f(1), \ldots$: se n compare in questa lista, allora in un numero finito di passi saremo in grado di asserire che $n \in \mathrm{ran}(f)$, se invece n non compare, dovremo effettuare un numero infinito di computi per essere sicuri che $n \notin \mathrm{ran}(f)$. Un insieme della forma $\mathrm{ran}(f)$ con f calcolabile si dice **semiricorsivo** o **ricorsivamente enumerabile**. Ogni insieme ricorsivo è ricorsivamente enumerabile, ma non viceversa. I sottoinsiemi ricorsivamente enumerabili di $\mathbb{N}$ sono esattamente gli **insiemi diofantei** cioè quelli della forma

$$\mathbb{N} \cap \{f(n_1, \ldots, n_k) \mid n_1, \ldots, n_k \in \mathbb{Z}\} \tag{4.1}$$

dove f è un polinomio in k variabili a coefficienti in $\mathbb{Z}$.

Se consideriamo un linguaggio che ha un numero finito di simboli non logici — e tutti i linguaggi del prim'ordine sin qui considerati rientrano in questa tipologia — è possibile associare ad ogni formula e, più in generale, ad ogni stringa di formule un numero naturale. Se Σ è un insieme ricorsivo di assiomi, allora

(4.2) l'insieme delle derivazioni a partire da Σ è ricorsivo,

in altre parole: dimostrare che una stringa di formule costituisca o meno una derivazione è una verifica meccanica, mentre

> se Σ è *sufficientemente potente*, allora l'insieme dei teoremi di Σ è ricorsivamente enumerabile, ma non ricorsivo.

L'espressione "sufficientemente potente" significa che gli assiomi di Σ dimostrano certi fatti elementari sui numeri naturali — per esempio, l'**aritmetica di Peano** (Sezione 7.E del Capitolo II) rientra tra questi sistemi assiomatici.

Un ulteriore sviluppo di queste idee porta al celebre **Primo Teorema di Incompletezza**[14] di Gödel:

> Ogni sistema Σ di assiomi sufficientemente potente, ricorsivo e coerente è **incompleto**, cioè c'è un enunciato σ tale che $\Sigma \nvdash \sigma$ e $\Sigma \nvdash \neg\sigma$.

L'ipotesi di coerenza di Σ è necessaria, dato che un sistema di assiomi incoerente deriva qualsiasi formula.

4.C. Modelli. Per la logica matematica, i termini e le formule di un linguaggio L sono oggetti matematici a tutti gli effetti (al pari dei numeri naturali, dei grafi, degli spazi vettoriali, ...). Invece nell'uso corrente le (pseudo-)formule non hanno un vero *status* in matematica, la loro funzione è quella di descrivere proprietà delle strutture, che sono il vero oggetto di interesse per i matematici che non si occupano di logica. Quindi uno dei primi e principali ostacoli che si incontra all'inizio dello studio della logica è accettare che le formule e le strutture siano entrambi oggetti di studio. Questo cambiamento di punto di vista consente non solo di studiare tutte le formule che valgono in una data struttura, o in una classe di strutture, come già avviene nell'algebra, ma anche di seguire il percorso opposto: partire da un insieme di formule e andare a studiare le strutture che soddisfano questo insieme. La teoria dei modelli, cioè lo studio delle interazioni tra formule e strutture dello stesso linguaggio, già intrapreso nelle Sezioni 3 e 5 sarà sviluppato in modo sistematico nel Capitolo VI. Vedremo come lo studio dei modelli delle teorie del prim'ordine sia in grado di risolvere problemi provenienti da altre parti della matematica, e di gettare nuova luce su oggetti ben noti. Per esempio, vedremo come sia possibile costruire delle strutture $(M, +, \cdot, <)$ che sono elementarmente equivalenti, ma non isomorfe, a $(\mathbb{N}, +, \cdot, <)$. Queste strutture si dicono modelli non-standard dell'aritmetica e sono essenziali per poter comprendere appieno i teoremi di Incompletezza di Gödel.

Infine osserviamo che nelle pagine precedenti abbiamo detto che cosa significa che un enunciato di L è vero in una struttura M, cioè abbiamo dato una funzione

$$(\text{Enunciati di } L) \times (\text{Strutture di } L) \to \{0, 1\}$$

che associa ad una coppia (σ, M) il valore 1 se e solo se $M \vDash \sigma$. Ad una osservazione più attenta si vede però che la definizione data, benché rassicurante per via della sua naturalezza, non è molto soddisfacente dal punto di vista del rigore in quanto si passa con troppa disinvoltura dal linguaggio

[14] I teoremi di incompletezza sono tra i risultati più profondi della logica e verranno dimostrati nel Capitolo **??**.

formale L al linguaggio informale con cui solitamente si descrivono le verità matematiche. Per convincersi della necessità di un'adeguata formalizzazione della nozione di verità e conseguentemente di definibilità, basta considerare il seguente ragionamento, noto come **paradosso di Berry**:

> Sia n il più piccolo numero naturale che non è definibile con meno di 1000 simboli.

Ma la frase qui sopra ha meno di 1000 simboli ed è quindi una definizione di n. Nel Capitolo VI formalizzeremo in modo rigoroso la nozione di soddisfazione e il paradosso di Berry si scioglierà come neve al sole.

L'aritmetica di Peano e la teoria degli insiemi sono teorie in cui è possibile trovare enunciati che non sono né dimostrabili né refutabili a partire da tale teoria. Tuttavia ci sono molti esempi di teorie del prim'ordine, matematicamente interessanti, che non sono soggette al fenomeno dell'incompletezza. Per esempio, la teoria dei campi algebricamente chiusi di caratteristica zero (Sezione 5.D.4) è una teoria completa, quindi è la teoria di $(\mathbb{C}, +, \cdot)$, per la Proposizione 3.15. Ogni teoria completa T in un linguaggio ricorsivo è **decidibile**, nel senso che esiste un algoritmo in grado di determinare se un enunciato è dimostrabile o meno a partire da T, e lo studio delle teorie complete e decidibili è uno degli argomenti centrali nella teoria dei modelli. La teoria di $(\mathbb{N}, +, \cdot)$ è completa, ma indecidibile, e quindi non è ricorsivamente assiomatizzabile. Quindi ogni qual volta si interpreta definibilmente $(\mathbb{N}, +, \cdot)$ in una struttura, si ottiene che questa struttura è indecidibile.

4.D. Insiemi. 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. Nella Sezione 10 del Capitolo III e più diffusamente nel Capitolo V mostreremo come ricostruire in termini insiemistici gli enti fondamentali della matematica — l'aritmetica, i numeri reali, la teoria della misura, ecc. Per via di questa propedeuticità, studieremo la teoria degli insiemi nel Capitolo IV.

Oltre a fornire un linguaggio comodo ed elastico per la matematica, la teoria degli insiemi ha una vita sua propria, incentrata sull'analisi della nozione di infinito, con problemi, tecniche, metodologie specifiche, che la rendono una delle parti più affascinanti della logica matematica. Prima di addentrarci in questi argomenti osserviamo che la teoria degli insiemi può essere formalizzata come una teoria del prim'ordine — anzi la formalizzazione è una scelta necessaria, visto che Russell nel 1901 mostrò che la teoria ingenua degli insiemi è contraddittoria. Nei primi anni del XX secolo sono state introdotte alcune assiomatizzazioni (essenzialmente equivalenti) della nozione di insieme che evitano queste antinomie, e in questo libro svilupperemo la teoria degli insiemi come una teoria del prim'ordine. Torniamo al concetto di

infinito. L'idea rivoluzionaria di Cantor, l'inventore della teoria degli insiemi, è che è possibile confrontare la taglia degli insiemi infiniti mediante biezioni. In particolare, il tipo di infinito della retta reale è maggiore del tipo di infinito dei numeri naturali (Teorema 10.23 a pagina 231). Cantor congetturò che non ci fosse nessun tipo di infinità intermedia, cioè che ogni sottoinsieme infinito della retta fosse in biezione con i naturali o con la retta stessa e questa congettura prese il nome di **Ipotesi del Continuo**. Nel 1938 Gödel dimostrò che l'Ipotesi del Continuo non è refutabile a partire dal sistema di assiomi della teoria degli insiemi, e nel 1963 Cohen dimostrò che non è neppure dimostrabile. Quindi la teoria degli insiemi è incompleta e l'Ipotesi del Continuo è un esempio di tale incompletezza. Negli ultimi decenni sono stati individuati moltissimi altri esempi di enunciati indipendenti, alcuni dei quali provenienti da altre aree della matematica. Ma questi sono argomenti troppo avanzati per questo libro.

4.E. Metamatematica. In questo libro la teoria degli insiemi è presa come base fondante per la costruzione degli altri oggetti matematici. In particolare, le nozioni logiche quali linguaggio, derivazione, struttura, verità, ..., sono formalizzate all'interno della teoria assiomatica degli insiemi, che per brevità indicheremo con TI.[15] D'altra parte, come abbiamo osservato, anche la teoria degli insiemi è una teoria del prim'ordine e quindi il suo studio andrebbe posposto dopo il Capitolo VI dove si danno i risultati sulle teorie del prim'ordine. Ci troviamo davanti a una situazione paradossale: da un lato abbiamo bisogno della teoria degli insiemi per definire il concetto di struttura di un linguaggio del prim'ordine (e quindi per poter parlare di validità di una formula), dall'altro dobbiamo usare un linguaggio del prim'ordine per sviluppare in modo rigoroso la nozione di insieme, cioè la teoria TI. Più in generale: se la logica è una parte della matematica, come può essere fondamento di tutta la matematica (e quindi di sé stessa)? Questo circolo vizioso, che ricorda il problema della primogenitura tra galline e uova, è in realtà solo apparente. Vediamo come uscirne.

4.E.1. *Sintassi.* Consideriamo un linguaggio del prim'ordine L contenente una quantità finita di simboli non logici (cioè simboli di funzione, di relazione e di costante) — tutti gli esempi delle Sezioni 3 e 5 sono di questo tipo, così come è LST, il **linguaggio della teoria degli insiemi** che ha un unico simbolo di relazione binaria $\in$. I termini e le formule di L sono oggetti concreti, segni che scriviamo sulla lavagna o sul foglio di carta. Quindi è possibile determinare in modo meccanico se una certa stringa di simboli è un termine o una formula di L. Supponiamo Σ sia un insieme effettivo di enunciati di L, cioè tale che si possa stabilire in modo algoritmico se un

[15] TI è soltanto un simbolo per denotare una delle possibili assiomatizzazioni della teoria degli insiemi: ZF, GB, MK, ...

enunciato σ di L appartiene a Σ. Per brevità chiameremo gli L e Σ come sopra **finitistici**. Tutti gli esempi di sistemi di assiomi visti nelle Sezioni 3 e 5, così come i sistemi di assiomi per la teoria degli insiemi che vedremo nel Capitolo IV, sono esempi di teorie finitistiche. Come spiegato nella Sezione 4.A una **derivazione di σ a partire da** Σ è una stringa finita di formule di L, ciascuna delle quali è un assioma logico, oppure è in Σ, oppure è ottenuto dalle formule precedenti mediante una regola di inferenza, e come già osservato a pagina 65 la nozione "essere una dimostrazione in Σ" è effettiva. In altre parole: data una stringa $\varphi_0, \ldots, \varphi_n$ di formule di L possiamo stabilire in modo meccanico se questa è una derivazione in Σ.[16]

Le formule di LST e le derivazioni in questo linguaggio sono enti *pre-insiemistici*, oggetti concreti che ci servono per parlare di insiemi arbitrari. L'ambiente matematico in cui si effettuano questi ragionamenti costruttivi e finitistici sulle formule si dice **metateoria** o **metamatematica**. Tentando un'analogia un po' azzardata con il mondo dell'informatica, potremmo dire che la metamatematica sta alla matematica come i linguaggi-macchina stanno ai programmi in generale.

Diremo che Σ è **coerente** se da esso non è possibile derivare *ogni* formula o, equivalentemente, se da esso non si deriva una formula logicamente falsa, per esempio $\exists x(x \neq x)$. Quindi l'asserzione della coerenza di Σ è un enunciato universale e può essere visto come una previsione ottimistica: non riusciremo mai a derivare una contraddizione da Σ. Viceversa, per affermare che Σ è incoerente (cioè non è coerente) dobbiamo esplicitamente esibire una derivazione di una contraddizione da Σ.

4.E.2. *Semantica.* Le nozioni di struttura, verità di una formula in una struttura, ecc., sono tutte nozioni essenzialmente insiemistiche e che quindi sono formulabili all'interno di TI, ma non sono formalizzabili a livello di metateoria. Invece, tutti i ragionamenti della metateoria possono essere codificati all'interno di una teoria sufficientemente potente, quale, per esempio, la teoria TI. In particolare, le nozioni di derivazione e coerenza possono essere codificate nella teoria degli insiemi, quindi TI è in grado di formulare (e dimostrare) il Teorema di Completezza 35.2

> Sia T una teoria del prim'ordine in un linguaggio L e sia σ un L-enunciato. Allora $T \models \sigma$ se e solo se $T \vdash \sigma$.

e il Teorema di Esistenza di Modelli 35.3

> Una teoria del prim'ordine coerente è soddisfacibile.

[16] Osserviamo che quando in matematica asseriamo di aver dimostrato un certo teorema, stiamo essenzialmente affermando (modulo un'operazione di traduzione dell'enunciato nel linguaggio insiemistico LST) che un certo enunciato σ è derivabile a partire dagli assiomi della teoria degli insiemi.

Osserviamo che i risultati qui sopra si applicano a *tutte* le teorie del prim'ordine, e non solo quelle finitistiche.

4.E.3. *Codifica della sintassi.* Se L e Σ sono finitistici, allora sono rappresentabili all'interno della teoria degli insiemi mediante numeri naturali. Ogni formula φ è codificata mediante un numero naturale $\ulcorner\varphi\urcorner$, mentre Σ è codificato mediante un insieme calcolabile di numeri naturali $\ulcorner\Sigma\urcorner$. Quindi una derivazione a partire da Σ può essere codificata come una successione finita di naturali, e questa a sua volta può essere vista come un numero naturale.

Se nella metateoria abbiamo dimostrato che

$$\Sigma \vdash \sigma \tag{4.3}$$

allora il fatto che tale derivazione esiste è dimostrabile all'interno di TI, e scriveremo

$$\mathsf{TI} \vdash \ulcorner\Sigma \vdash \sigma\urcorner. \tag{4.4}$$

Quindi (4.4) segue da (4.3). L'implicazione inversa, in generale, non vale: per dimostrare la formula (4.3) bisogna *esibire esplicitamente una derivazione* $\varphi_0, \dots, \varphi_n$ di σ, mentre per dimostrare la (4.4) è sufficiente dimostrare che *c'è una qualche derivazione* di σ a partire da Σ, per esempio dimostrando per assurdo che la non-esistenza di una dimostrazione siffatta porta ad una contraddizione in TI. La situazione è analoga a quanto avviene in teoria dei numeri quando si dimostrano affermazioni del tipo $\exists n\, \varphi(n)$ con φ una proprietà calcolabile: se gli argomenti usati per la dimostrazione sono costruttivi, allora possiamo (sperare di) esibire esplicitamente un numero n per cui vale la proprietà φ, ma se si sono usati metodi astratti, in generale non si ha idea di quanto valga n.

L'affermazione "Σ è coerente" è formalizzabile in TI e indicheremo la sua formalizzazione con Con_Σ. Asserire che

$$\mathsf{TI} \vdash \neg\, \mathrm{Con}_\Sigma$$

significa che abbiamo dimostrato (in teoria degli insiemi) l'*esistenza* di una dimostrazione di una contraddizione in Σ, ma non è detto che abbiamo idea di come sia fatta tale dimostrazione. Per (4.2) e (4.1), asserire $\neg\, \mathrm{Con}_\Sigma$ è equivalente ad affermare che certo polinomio a coefficienti interi (esplicitamente calcolabile a partire da Σ) ha una soluzione negli interi.

Il **Secondo Teorema di Incompletezza** di Gödel asserisce che nessuna teoria sintattica Σ coerente e sufficientemente potente è in grado di dimostrare la propria coerenza. Sufficientemente potente significa che la teoria in questione è in grado di codificare la sintassi di un linguaggio finitistico, quindi TI è sufficientemente potente. Inoltre la vasta mole di risultati di matematica dimostrati nella teoria degli insiemi ci inducono a ritenere che

TI sia scevra da contraddizioni. Quindi, per il Teorema di Gödel,

$$\mathsf{TI} \nvdash \mathrm{Con}_{\mathsf{TI}} .$$

La coerenza è ovviamente un requisito essenziale per una teoria sintattica Σ, ma non è l'unico requisito importante. Consideriamo, per esempio la teoria Σ ottenuta aggiungendo a TI l'enunciato $\neg\,\mathrm{Con}_{\mathsf{TI}}$. Poiché TI è coerente e non dimostra $\mathrm{Con}_{\mathsf{TI}}$, ne segue che Σ è coerente. Inoltre una dimostrazione a partire da TI è anche una dimostrazione a partire da Σ, quindi $\neg\,\mathrm{Con}_{\mathsf{TI}} \Rightarrow \neg\,\mathrm{Con}_{\Sigma}$, da cui

$$\Sigma \vdash \neg\,\mathrm{Con}_{\Sigma} .$$

Cioè Σ dimostra l'esistenza di (un numero naturale che codifica) una derivazione di una contraddizione a partire da Σ, anche se noi non saremo mai in grado di esibire una dimostrazione siffatta. In altre parole: la teoria Σ è coerente, ma asserisce la propria incoerenza!

Lo studio della dialettica tra teoria e metateoria è uno degli aspetti più affascinanti della logica e verrà studiato nel Capitolo **??**.

Capitolo II

Definibilità in algebra e teoria dei numeri

5. Definibilità in algebra e in combinatorica

5.A. Gruppi.

5.A.1. *Linguaggi e assiomatizzazioni per i gruppi.* Per studiare la teoria del prim'ordine dei gruppi possiamo utilizzare il linguaggio L_{GRUPPI} introdotto a pagina 38. Una L_{GRUPPI}-struttura è un gruppo se e solo se soddisfa gli assiomi (3.8).

La scelta del linguaggio per formalizzare la nozione di gruppo è ben lungi dall'essere unica: se si rimuove il simbolo di inverso si ottiene il linguaggio L_{MONOIDI}; una struttura per questo linguaggio è un monoide se soddisfa (3.8a) e (3.8b), ed è un gruppo se soddisfa anche

$$\forall x \exists y \, (x \cdot y = 1 \, \wedge \, y \cdot x = 1) \, .$$

I termini e le formule di L_{MONOIDI} sono termini e formule di L_{GRUPPI}, ma non viceversa. Volendo essere ancora più parsimoniosi, potremmo rinunciare anche alla costante 1 limitandoci al linguaggio $L_{\text{SEMIGRUPPI}}$ che ha un solo simbolo $\cdot$ di operazione binaria (Esercizio 5.28).

Nel caso dei gruppi abeliani si usa di solito la notazione additiva al posto di quella moltiplicativa e si utilizza il linguaggio $L_{\text{GRUPPI A.}}$ introdotto a pagina 40.

In algebra una $L_{\text{SEMIGRUPPI}}$-struttura si dice **magma**; si tratta cioè di un insieme non vuoto dotato di un'operazione binaria. La nozione di magma è troppo generale per essere di qualche utilità. Per ottenere strutture matematicamente più interessanti dobbiamo imporre delle condizioni sull'operazione.

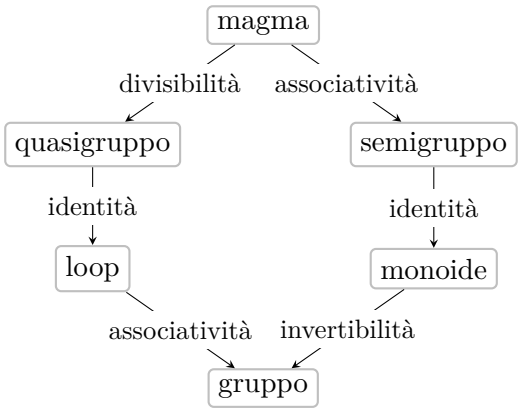


Figura 1. Alcune strutture algebriche con una operazione binaria

Ecco una breve lista delle strutture più comuni: un **quasigruppo** è una magma divisibile, cioè soddisfa $\forall x, y \exists z(y \cdot z = x)$ e $\forall x, y \exists z(z \cdot y = x)$, un quasigruppo con identità è un **loop**, un loop associativo è un gruppo. Alternativamente: una magma associativa è un semigruppo, un semigruppo con identità è un monoide, e un monoide che ammetta inversi, cioè che soddisfi $\forall x \exists y(x \cdot y = 1)$ e $\forall x \exists y(x \cdot y = 1)$, è un gruppo (Figura 1).

5.A.2. *Assiomatizzazioni equazionali*.* La teoria dei gruppi è equazionale ed è finitamente assiomatizzabile, quindi è assiomatizzabile mediante un unico assioma. Infatti questo assioma può essere un'equazione. Una teoria equazionale che sia assiomatizzabile mediante un'unica equazione si dice 1**-basata**.

È stato dimostrato che l'equazione nel linguaggio L_{GRUPPI}

$$((z \cdot (x \cdot y)^{-1})^{-1} \cdot (z \cdot y^{-1})) \cdot (y^{-1} \cdot y)^{-1} = x,$$

definisce un gruppo, mentre se vogliamo assiomatizzare i gruppi abeliani si può usare

$$((x + y) + z) + (-(x + z)) = y$$

dove $-$ è il simbolo dell'operazione unaria di opposto additivo. Se invece usiamo $-$ per denotare il simbolo di operazione binaria per la differenza, un singolo assioma per i gruppi abeliani è dato da

$$x - (y - (z - (x - y))) = z,$$

mentre un'assiomatizzazione dei gruppi mediante il simbolo / per la divisione, dove x/y sta per $x \cdot y^{-1}$, è dato dal singolo assioma

$$x/((((x/x)/y)/z)/(((x/x)/x)/z)) = y.$$

5.A.3. *Sottogruppi.* Per parlare di sottogruppi possiamo utilizzare il seguente trucco. Aggiungiamo un nuovo simbolo di predicato unario H al linguaggio dei gruppi, ottenendo così un linguaggio L_H. Le L_H-strutture hanno la forma $(G, \cdot, ^{-1}, 1, H)$: se queste soddisfano gli assiomi per i gruppi e anche l'enunciato

$$H(1) \wedge \forall x, y \left(H(x) \wedge H(y) \Rightarrow H(x \cdot y^{-1}) \right)$$

allora stiamo considerando dei gruppi dotati di un sottogruppo privilegiato. Se vogliamo dire che questo sottogruppo è normale e non banale utilizziamo l'enunciato

$$\forall x, y \left(H(x) \Rightarrow H(y \cdot x \cdot y^{-1}) \right) \wedge \exists x \left(x \neq 1 \wedge H(x) \right) \wedge \exists x \neg H(x).$$

Un gruppo G si dice **semplice** se non ha sottogruppi normali propri, cioè se

$$\forall H \left(H \text{ sottogruppo normale} \wedge \exists x \left(H(x) \wedge x \neq 1 \right) \Rightarrow \forall x \; H(x) \right).$$

Questa è una formula della logica del second'ordine (vedi l'Osservazione 3.7) dato che si quantifica su sottoinsiemi e quindi viene relegata nel limbo delle pseudo-formule. Infatti non c'è nessun sistema di assiomi del prim'ordine i cui modelli siano tutti e soli i gruppi semplici (Esercizio 32.24, della Sezione 32).

5.A.4. *Definibilità.* Un elemento g di un gruppo G ha **torsione** se $g^n = 1$ per qualche $n > 0$ e il più piccolo n siffatto si dice **ordine** di g e si indica con $o(g)$. Se g non ha torsione, si dice che g ha ordine infinito, $o(g) = \infty$.

Vediamo qualche esempio di formula e suo significato:

La formula...	significa che...
$\exists z \left(z \cdot x = y \cdot z \right)$	x e y sono coniugati
$x^n = 1$	$o(x)$ divide n
$\forall x \left(x^n = 1 \right)$	l'ordine di un qualsiasi elemento divide n.

Esempi di sottoinsiemi definibili senza parametri sono:

- il **centro** $C(G)$, definito dalla formula $\varphi(x)$: $\forall y (y \cdot x = x \cdot y)$. Più in generale, se $A \subseteq G$ è definibile in G con parametri $p_1, \ldots, p_n$, allora il suo centralizzante $C_G(A) \stackrel{\text{def}}{=} \{g \in G \mid \forall x \in A \left(g \cdot x = x \cdot g \right)\}$ è definibile in G con parametri $p_1, \ldots, p_n$;
- il sottogruppo banale $\{1\}$, definito dalla formula $\varphi(x)$: $x = x \cdot x$,
- il grafo della funzione inversa $\left\{(x, y) \mid y = x^{-1}\right\}$, definito dalla formula $\varphi(x, y)$: $y \cdot x = (y \cdot x) \cdot (y \cdot x)$.

Vediamo due esempi di insiemi non definibili.

5.A.5. *Torsione.* L'espressione

$$\exists n \in \mathbb{N} \left(x^n = 1 \right)$$

che afferma che x ha torsione finita, è una pseudo-formula, e non è una formula del nostro linguaggio, per via della quantificazione sui naturali. Se

tentassimo di sostituire $\exists n \in \mathbb{N}$ con una disgiunzione del tipo

$$\left(x^2 = 1\right) \vee \left(x^3 = 1\right) \vee \dots$$

otterremmo una stringa infinita di simboli, che non può essere una formula. A questo punto non possiamo ancora concludere che

$$\mathrm{Tor}(G) = \{x \in G \mid \exists n \in \mathbb{N}\,(x^n = 1)\}\,,$$

l'insieme degli elementi di torsione di G, sia indefinibile nel nostro linguaggio. L'Esercizio 32.32(i) del Capitolo VI mostra che le cose stanno proprio così.

5.A.6. *Divisibilità.* La parte n-divisibile di un gruppo è l'insieme degli elementi della forma y^n, ed è definita dalla formula $\exists y\,(x = y^n)$. Nel caso dei gruppi abeliani si utilizza solitamente la notazione additiva $(G, +)$ e la parte n-divisibile

$$nG = \{nx \mid x \in G\}$$

è un sottogruppo. Un gruppo abeliano si dice n-**divisibile** ($n \geq 2$) se coincide con la sua parte n-divisibile, cioè se $G = nG$. Una $L_{\text{GRUPPI A.}}$-struttura $(G, +, -, 0)$ è un gruppo n-divisibile ($n \geq 2$) se e solo se soddisfa $\Sigma_{\text{GRUPPI A.}}$ (vedi pagina 40) e l'enunciato

$$(\delta_n) \qquad \forall x \exists y (ny = x).$$

La parte divisibile di un gruppo abeliano è il sottogruppo ottenuto intersecando tutte le sue parti n-divisibili o, equivalentemente, tutte le sue parti p^k-divisibili, con p primo. Un gruppo abeliano è **divisibile** se e solo se coincide con la sua parte divisibile. Esempi di gruppi abeliani n-divisibili sono

$$\mathbb{Z}[1/n] = \left\{x \in \mathbb{Q} \mid \exists k (n^k x \in \mathbb{Z})\right\}$$

e $\mathbb{Z}[1/n]/\mathbb{Z}$, che può essere identificato con un sottogruppo del gruppo moltiplicativo $\{z \in \mathbb{C} \mid |z| = 1\} \cong \mathbb{R}/\mathbb{Z}$. Esempi di gruppi abeliani divisibili sono $\mathbb{Q} = \bigcup_{n \geq 1} \mathbb{Z}[1/n]$, $\mathbb{R}$, $\mathbb{Q}/\mathbb{Z}$ e $\mathbb{R}/\mathbb{Z}$.

L'espressione

$$\forall n > 0\, \exists y (ny = x)$$

non è una formula e quindi non può esser usata per definire la parte divisibile di un gruppo. Infatti non c'è nessuna formula $\varphi(x)$ che definisca la parte divisibile di un gruppo abeliano (Capitolo VI Esercizio 32.32(ii)).

5.B. Esempi di teorie del prim'ordine dei gruppi. I gruppi abeliani divisibili sono caratterizzabili mediante enunciati del nostro linguaggio: basta aggiungere agli usuali assiomi per i gruppi abeliani $\Sigma_{\text{GRUPPI A.}}$ gli enunciati δ_n per ogni $n \geq 2$. Fissato n prendiamo un primo p sufficientemente grande, diciamo $n! < p$. Il gruppo $\mathbb{Z}[1/n!]$ è k-divisibile, per ogni $k \leq n$, ma non è p-divisibile. Per il Teorema 3.10 abbiamo quindi

Proposizione 5.1. *La teoria dei gruppi abeliani divisibili non è finitamente assiomatizzabile.*

Analogamente i gruppi privi di torsione sono assiomatizzabili mediante Σ_{GRUPPI} con l'aggiunta degli L_{GRUPPI}-enunciati

$$(\tau_n) \qquad \forall x\,(x \neq 1 \Rightarrow x^n \neq 1)$$

con $n \geq 1$. (Naturalmente se decidessimo di usare il linguaggio $L_{\text{GRUPPI A.}}$ la definizione di τ_n diventa $\forall x\,(x \neq 0 \Rightarrow nx \neq 0)$ — vedi Esercizio 5.28.) La teoria del prim'ordine dei gruppi (abeliani o meno) privi di torsione non è finitamente assiomatizzabile (Esercizio 5.29). Poiché un gruppo abeliano divisibile privo di torsione G è uno spazio vettoriale su $\mathbb{Q}$ (Esercizio 5.22), la sua dimensione come spazio vettoriale si dice **rango** di G. Nel Capitolo VI (Esercizio 33.7(ii)) vedremo che la teoria del prim'ordine dei gruppi abeliani divisibili, privi di torsione è completa, quindi ogni gruppo siffatto è elementarmente equivalente tanto a $(\mathbb{Q}, +)$ quanto a $(\mathbb{R}, +)$.

Se espandiamo il linguaggio $L_{\text{GRUPPI A.}}$ con un simbolo di predicato binario $<$ e aggiungiamo a $\Sigma_{\text{GRUPPI A.}}$

- l'enunciato $\exists x\,(x \neq 0)$ (per garantire che il gruppo non sia banale),
- gli assiomi per gli ordini lineari stretti (3.13) di pagina 38, e
- l'enunciato $\forall x, y, z\,(x < y \Rightarrow x + z < y + z)$

otteniamo la teoria del prim'ordine dei **gruppi abeliani ordinati** $\Sigma_{\text{GR.A.O.}}$. Un gruppo abeliano è ordinabile se c'è un ordine stretto $<$ che lo rende un gruppo abeliano ordinato. Un gruppo abeliano ordinato è privo di torsione, e vale il converso.

Esempio 5.2. Nell'Esercizio 32.13 del Capitolo VI vedremo che un gruppo abeliano è ordinabile se e solo se è privo di torsione. Questa è un esempio di una teoria del prim'ordine che non è finitamente assiomatizzabile in un certo linguaggio L, ma lo diventa se si passa ad un linguaggio $L' \supseteq L$.

Fissiamo un gruppo abeliano ordinato $(G, +, 0_G, <)$. Se $G \neq \{0_G\}$, allora l'ordinamento è **privo di massimo o minimo**, cioè vale $\forall x\,\exists y, z\,(y < x \wedge x < z)$. Le traslazioni $x \mapsto x + z$ $(z \in G)$ mostrano che l'ordinamento è uniforme su G, nel senso che due intervalli $(a; b)$ e $(c; d)$ con $b + c = d + a$ sono isomorfi. In particolare si hanno due possibilità mutualmente esclusive:

- l'ordinamento è **discreto** cioè $\forall x\,\exists y\ (x < y \wedge \neg\exists z\,(x < z \wedge z < y))$ o, equivalentemente, c'è un elemento $1_G \in G$ tale che $0_G < 1_G \wedge \neg\exists z\,(0_G < z \wedge z < 1_G)$; oppure
- l'ordinamento è **denso**, cioè $\forall x, y\,(x < y \Rightarrow \exists z\,(x < z \wedge z < y))$.

In un gruppo divisibile ordinato l'ordinamento è denso, ma non vale il converso Esercizio 5.27. Se a $\Sigma_{\text{GR.A.O.}}$ aggiungiamo gli assiomi δ_n per la divisibilità, otteniamo la teoria dei **gruppi abeliani divisibili ordinati**. Si tratta di una teoria non finitamente assiomatizzabile (Esercizio 5.29(ii)) e nel Capitolo VI (Esercizio 33.7(iv)) vedremo che è una teoria completa. Quindi ogni gruppo abeliano divisibile ordinato è elementarmente equivalente a $(\mathbb{Q}, +, <)$ o, equivalentemente, a $(\mathbb{R}, +, <)$.

Esercizio 5.3. Dimostrare che

(i) $\mathbb{Z} \times \mathbb{Z}$ con l'ordinamento lessicografico

$$(n, m) <_{\text{lex}} (n', m') \quad \text{se e solo se} \quad n < n' \vee (n = n' \wedge m < m')$$

è un gruppo abeliano ordinato discreto, in cui $1_{\mathbb{Z}\times\mathbb{Z}} = (0, 1)$;

(ii) l'elemento $(1, 0)$ non è né pari né dispari, cioè non esiste alcun $(n, m) \in \mathbb{Z} \times \mathbb{Z}$ tale che $(n, m) + (n, m) = (1, 0)$ oppure $(n, m) + (n, m) = (1, 0) + 1_{\mathbb{Z}\times\mathbb{Z}}$.

Fissato un $n \geq 2$, ogni intero x è congruo modulo n ad un $1 \leq m \leq n$, cioè $\mathbb{Z}$ soddisfa gli enunciati

$$(\pi_n) \qquad \forall x \, \exists y \, (\bigvee_{1 \leq m \leq n} x + m1 = ny).$$

Per la parte (ii) dell'Esercizio 5.3, $\mathbb{Z} \times \mathbb{Z}$ non soddisfa π_2, quindi la teoria dei gruppi abeliani ordinati discreti non è completa.

Un gruppo abeliano ordinato discreto che soddisfi gli assiomi π_n per $n \geq 2$, si dice uno **$\mathbb{Z}$-gruppo**. La teoria degli $\mathbb{Z}$-gruppi non è finitamente assiomatizzabile (Esercizio 5.29(iii)) e nel Capitolo VI (Esercizio 33.7(v)) vedremo che è completa. Quindi ogni $\mathbb{Z}$-gruppo è elementarmente equivalente a $(\mathbb{Z}, +, -, 0, 1, <)$.

Se G è un gruppo abeliano ordinato, allora $G \times \mathbb{Z}$ è un gruppo abeliano ordinato discreto con l'ordinamento lessicografico

$$(g, n) < (h, m) \Leftrightarrow g < h \wedge (g = h \vee n < m).$$

Se inoltre G è divisibile, allora $G \times \mathbb{Z}$ è uno $\mathbb{Z}$-gruppo.

Se G è abeliano ordinato discreto, allora $Z = \{k1_G \mid k \in \mathbb{Z}\}$ è un sottogruppo di G isomorfo a $\mathbb{Z}$ e G/Z è abeliano. Inoltre se $a + Z \neq b + Z$, allora $a+Z < b+Z$, cioè $\forall g \in a + Z \, \forall h \in b + Z \ (g < h)$ oppure $b+Z < a+Z$, cioè $\forall g \in a + Z \, \forall h \in b + Z \ (h < g)$. Ne segue che G/Z un gruppo abeliano ordinato. Se inoltre G è uno $\mathbb{Z}$-gruppo, allora G/Z è divisibile.

5.C. Anelli.

5.C.1. Il linguaggio L per gli anelli con unità consiste di due simboli di funzione binari $+$ e $\cdot$, un simbolo di funzione unario $-$, e due simboli di costante 0 e 1. Una L-struttura $(R, +, -, \cdot, 0, 1)$ che soddisfa (3.9) e (3.10) di pagina 38 è un anello, ma una generica L-struttura si guarda bene dall'essere un anello. Ogni intero $n \in \mathbb{Z}$ può essere identificato con un termine chiuso in modo ovvio:

$$\text{a } n \in \mathbb{N} \text{ associamo il termine } \underbrace{1 + \cdots + 1}_{n}$$

e poi estendiamo questa identificazione a tutto $\mathbb{Z}$. Osserviamo che i termini chiusi

$$2 + 2, \quad 2 \cdot 2, \quad 4$$

sono tutti distinti: in una generica L-struttura possono denotare elementi distinti, ma in un anello denotano lo stesso elemento, cioè l'identità moltiplicativa sommata a sé stessa quattro volte. Analogamente, ad ogni polinomio $a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \in \mathbb{Z}[X]$ possiamo associare il termine

$$a_0 + (a_1 \cdot x) + (a_2 \cdot x^2) + \cdots + (a_n \cdot x^n).$$

Questo esempio è piuttosto generale, nel senso che ogni termine del nostro linguaggio può essere visto come un polinomio in più variabili con coefficienti interi.

Dato un anello R, ogni elemento del sottoanello primo è definibile mediante la formula $x = n$, per qualche $n \in \mathbb{Z}$. Se R ha caratteristica finita m, il sottoanello primo $\mathbb{Z}/m\mathbb{Z}$ è definibile in R mediante la formula $x = 0 \vee x = 1 \vee \cdots \vee x = m - 1$. Se R ha caratteristica zero, la definibilità del sottoanello primo $\mathbb{Z}$ dipende da R. Per esempio, $\mathbb{Z}$ è definibile in $\mathbb{Q}$, ma non in $\mathbb{R}$ o in $\mathbb{C}$ (Sezione 6).

Teorema 5.4. *Sia R un dominio di integrità di caratteristica zero.*

(a) *$\mathbb{Z}$ è definibile senza parametri in $(R[X], +, \cdot, R)$, cioè nella struttura ottenuta espandendo l'anello dei polinomi con un predicato unario per gli elementi di R.*

(b) *Se R è un campo, allora $\mathbb{Z}$ è definibile senza parametri in $(R[X], +, \cdot)$.*

Dimostrazione. È sufficiente costruire una formula $\varphi_{\mathbb{N}}(x)$ che definisce $\mathbb{N}$ per concludere che $\mathbb{Z}$ è definibile mediante la formula $\varphi_{\mathbb{N}}(x) \vee \varphi_{\mathbb{N}}(-x)$. Il predicato di divisibilità $x \mid y$ è definibile nel linguaggio degli anelli mediante la formula $\exists z\,(x \cdot z = y)$, quindi può essere utilizzato senza problemi.

(a) Usando il fatto che $R[X]$ è un dominio a fattorizzazione unica, dati due polinomi non costanti f e g tali che $f \mid g$, possiamo associare il massimo naturale n tale che $(f + k) \mid g$ per ogni $k \leq n$. Ogni $n \in \mathbb{N}$ può essere ottenuto

in questo modo — basta prendere $f = X$ e $g = X \cdot (X+1) \cdots (X+n)$. Consideriamo la formula $\varphi(x)$

$$\exists u, v \Big(\neg R(u) \wedge v \neq 0 \wedge u \mid v \wedge \forall y \big[(R(y) \wedge (u+y) \mid v) \Rightarrow ((u+y+1) \mid v \vee y = x) \big] \Big).$$

Ogni $n \in \mathbb{N}$ soddisfa $\varphi(x)$. Viceversa, supponiamo che un elemento $a \in R[X]$ soddisfi $\varphi(x)$: vogliamo verificare che $a \in \mathbb{N}$. Fissiamo $u, v \in R[X]$ che testimoniano φ per a: se per assurdo $a \notin \mathbb{N}$, allora $(u+n) \mid v$ per ogni n, contro l'unicità della fattorizzazione unica.

(b) È sufficiente osservare che R è definito in $R[X]$ da $x = 0 \vee x \mid 1$, e poi applicare la parte (a). □

Quindi $\mathbb{Z}$ è definibile in $R[X]$ se R è definibile in $R[X]$. Mediante un ragionamento più elaborato si dimostra che $\mathbb{Z}$ è definibile in $\mathbb{Z}[X]$ [**Rob51**].

5.C.2. *Ideali.* Formulare nel linguaggio degli anelli delle proprietà che coinvolgono gli ideali presenta lo stesso tipo di difficoltà che abbiamo incontrato nel formulare nel linguaggio dei gruppi la nozione di sottogruppo. Anche in questo caso si considera il linguaggio degli anelli con un ulteriore predicato unario I e si aggiunge come assioma l'enunciato

$$\exists x I(x) \wedge \neg I(1) \wedge \forall x, y, z \, (I(x) \wedge I(y) \Rightarrow I(x-y) \wedge I(x \cdot z) \wedge I(z \cdot x)) \tag{5.1}$$

che afferma l'insieme di verità di $I(x)$ è un ideale proprio (bilatero). Le nozioni di ideale primo e massimale sono formulate come

$$\forall x, y \, (I(x \cdot y) \Rightarrow I(x) \vee I(y))$$

e

$$\forall x \, (\neg I(x) \Rightarrow \exists y \, I(x \cdot y - 1))$$

rispettivamente. Le nozioni che coinvolgono quantificazioni su ideali arbitrari non sono, in generale, nozioni del prim'ordine. Per esempio, il **radicale** di un ideale $\mathfrak{a}$ di un anello commutativo unitario R è l'ideale

$$\sqrt{\mathfrak{a}} = \{x \in R \mid \exists n \in \mathbb{N} \, (x^n \in \mathfrak{a})\}.$$

Quando $\mathfrak{a} = \{0_R\}$ è l'ideale nullo si ottiene il **nilradicale** $\mathrm{Nil}(R)$ di R. Il nilradicale non è, in generale, un sottoinsieme definibile di R, visto che l'espressione che lo definisce è una pseudo-formula. Similmente, anche quando $\mathfrak{a}$ è definibile, può capitare che $\sqrt{\mathfrak{a}}$ non sia definibile. Una formulazione equivalente[1] è data da [**AM69**, Prop. 1.8, Capitolo 1]

$$\sqrt{\mathfrak{a}} = \bigcap \{\mathfrak{p} \mid \mathfrak{p} \text{ ideale primo e } \mathfrak{p} \supseteq \mathfrak{a}\},$$

[1] L'equivalenza delle due definizioni dipende dall'assioma di scelta, si veda pag. 420.

ma in questo caso la definizione utilizza una quantificazione su sottoinsiemi. Il **radicale di Jacobson**

$$\mathrm{Jac}(R) = \bigcap \{\mathfrak{m} \mid \mathfrak{m} \text{ ideale massimale}\}$$

è invece definibile, dato che è l'insieme degli x tali che $1 - x \cdot y$ è invertibile, per ogni y [**AM69**, Prop. 1.9, Capitolo 1], cioè è l'insieme di verità della formula

$$\forall y \exists z \left((1 - x \cdot y) \cdot z = 1\right).$$

5.C.3. *Semianelli.* Talvolta è necessario lavorare con strutture più semplici degli anelli.

Definizione 5.5. Un semianello è una struttura algebrica $(R, +, \cdot, 0)$ tale che $(R, +, 0)$ è un monoide commutativo, $(R, \cdot)$ è un semigruppo, l'operazione $\cdot$ è distributiva rispetto a $+$ e $0 \cdot x = x \cdot 0 = 0$ per tutti gli $x \in R$.

Se c'è un elemento $1 \in R$ che è elemento neutro per $\cdot$ parleremo di semianello unitario, e se l'operazione $\cdot$ è commutativa parleremo di semianello commutativo.

Ogni anello è un semianello. Esempi di semianelli che non sono anelli sono

- $\mathbb{N}$ con le operazioni usuali,
- $\mathbb{R} \cup \{+\infty\}$ con le operazioni di somma $x \oplus y \stackrel{\text{def}}{=} \min x, y$ e prodotto $x \otimes y \stackrel{\text{def}}{=} x + y$, con l'ovvia convenzione che $x + y = +\infty$ quando almeno uno tra x e y è $+\infty$,[2]
- l'insieme degli ideali di un anello,
- l'insieme dei polinomi $R[X]$ a coefficienti in un semianello R,
- una famiglia di insiemi contenente l'insieme vuoto e chiusa per unioni e intersezioni, o più in generale, un reticolo distributivo con minimo (si veda la Sezione 8.C).

Il linguaggio per i semianelli è ottenuto rimuovendo il simbolo $-$ dal linguaggio L_{ANELLI}.

5.D. Assiomatizzabilità. Ricordiamo che una collezione $\mathcal{C}$ di L-strutture si dice assiomatizzabile (al prim'ordine) se è della forma $\mathrm{Mod}(\Sigma)$ per qualche insieme Σ di L-enunciati. Se Σ può essere preso finito diremo che $\mathcal{C}$ è **finitamente assiomatizzabile (al prim'ordine)**. Equivalentemente: una collezione $\mathcal{C}$ di L-strutture è finitamente assiomatizzabile se e solo se è la collezione di tutti i modelli di un singolo enunciato σ, cioè $\mathcal{C} = \mathrm{Mod}(\sigma)$. Per quanto visto, i gruppi, gli anelli, i campi, sono finitamente assiomatizzabili.

[2] Questo semianello è di centrale importanza in un'area della matematica nota come *geometria tropicale* e per questo motivo $\mathbb{R} \cup \{+\infty\}$ è noto come *semianello tropicale*.

Aggiungendo a ciascuno di questi sistemi di assiomi tutti gli enunciati $\boldsymbol{\varepsilon}_{\geq n}$ definiti a pagina 15 otteniamo l'assiomatizzabilità dei gruppi infiniti, degli anelli infiniti, dei campi infiniti. Per il Teorema 3.10 nessuna di queste classi di strutture è finitamente assiomatizzabile, quindi per il Teorema 3.33 le classi complementari (i gruppi finiti, gli anelli finiti, i campi finiti) non sono assiomatizzabili al prim'ordine (Esercizio 5.29).

Nelle prossime pagine (così come nel caso della distributività infinitaria nei reticoli — pagina 387 del Capitolo V) vedremo ulteriori esempi di classi assiomatizzabili al prim'ordine. Per gli esempi più sofisticati ricorreremo a qualche risultato non banale di algebra.

5.D.1. *Anelli locali.* Un anello commutativo unitario in cui $0 \neq 1$ e che ha un unico ideale massimale si dice **anello locale**. Questa nozione non sembrerebbe essere formalizzabile nel linguaggio ampliato della Sezione 5.C.2, dato che stiamo quantificando su sottoinsiemi. Tuttavia un anello commutativo unitario R in cui $0 \neq 1$ è locale se e solo se x o $1 + x$ è invertibile per ogni $x \in R$ [**AM69**, Prop. 1.6, Capitolo 1]. Quindi gli anelli locali sono finitamente assiomatizzabili: basta prendere gli assiomi per gli anelli commutativi unitari $\Sigma_{\text{ANELLI C.}}$ (vedi pagina 40) con gli ulteriori assiomi (3.12a) a pagina 38 e

$$\forall x \exists y \, (x \cdot y = 1 \vee (1 + x) \cdot y = 1) \, .$$

5.D.2. *Anelli regolari di von Neumann.* Un anello con unità è **regolare di von Neumann** se $\forall x \, \exists y \, (x = xyx)$, quindi si tratta di una classe assiomatizzabile. Esempi di anelli regolari di von Neumann sono: i corpi, l'anello degli endomorfismi di uno spazio vettoriale su un corpo, gli anelli booleani (pag. 174). Ci sono molte formulazioni equivalenti di questo tipo di anelli [**Kap95, Goo91**] e alcune di queste non sono formulate al prim'ordine. Per esempio, R è regolare di von Neumann se e solo se ogni suo ideale sinistro finitamente generato è generato da un elemento idempotente. Un'altra formulazione equivalente nel lessico dell'algebra omologica è che ogni R-modulo sia *piatto*, e per questo motivo gli anelli regolari di von Neumann sono anche noti come **anelli assolutamente piatti**.

5.D.3. *Anelli Noetheriani.* Un anello commutativo unitario in cui $0 \neq 1$ si dice **Noetheriano** se ogni successione ascendente di ideali propri

$$J_0 \subseteq J_1 \subseteq J_2 \subseteq \dots$$

si stabilizza, cioè $J_n = J_{n+1}$ per ogni n sufficientemente grande. Equivalentemente: un anello è Noetheriano se ogni suo ideale proprio è finitamente generato. Gli anelli Noetheriani non sono assiomatizzabili al prim'ordine, ma gli anelli che *non* sono Noetheriani lo sono, a patto di aggiungere al linguaggio degli anelli un predicato unario I. Infatti basta assumere $\Sigma_{\text{ANELLI C.}}$ più l'enunciato (5.1) che certifica che l'insieme definito da I è un ideale, più

tutti gli enunciati

$$\forall x_1, \dots, x_n \left(\bigwedge_{1 \leq i \leq n} I(x_i) \Rightarrow \exists y \, (I(y) \wedge \forall z_1, \dots, z_n \, (\sum_{i=1}^{n} z_i \cdot x_i \neq y)) \right)$$

per ogni $n \geq 1$.

5.D.4. *Campi algebricamente chiusi e di caratteristica fissata.* I campi di caratteristica p sono finitamente assiomatizzabili — basta aggiungere l'enunciato $p1 = 0$ a Σ_{CAMPI}, il sistema di assiomi per i campi (vedi pag. 40).

Se aggiungiamo a Σ_{CAMPI} tutti gli enunciati $n1 \neq 0$ per ogni $n > 0$, otteniamo un sistema di assiomi per i campi di caratteristica 0.

Per il Teorema 3.10 i campi di caratteristica 0 non sono finitamente assiomatizzabili e quindi i campi di caratteristica finita non sono assiomatizzabili (Esercizio 5.29).

Un campo $\Bbbk$ si dice **algebricamente chiuso** se ogni polinomio non costante $f \in \Bbbk[X]$ ha una radice in $\Bbbk$ (Sezione 5.E). Una $L_{\text{ANELLI-1}}$-struttura è un campo algebricamente chiuso se soddisfa Σ_{CAMPI} e tutti gli enunciati

$$\forall a_0, \dots, a_n \, (a_n \neq 0 \Rightarrow \exists x \, (a_n \cdot x^n + \dots + a_1 \cdot x + a_0 = 0))$$

per ogni $n > 0$. La teoria dei campi algebricamente chiusi è denotata da ACF, mentre ACF_0 e ACF_p sono le teorie dei campi algebricamente chiusi di caratteristica fissata. Per il Teorema 3.10 i campi algebricamente chiusi non sono finitamente assiomatizzabili (Esercizio 5.29).

5.D.5. *Campi ordinati.* Come abbiamo detto a pagina 40 un campo ordinato è una $L_{\text{ANELLI O.}}$-struttura che soddisfa $\Sigma_{\text{CAMPI O.}}$ cioè gli assiomi per i campi e la compatibilità dell'ordinamento con le operazioni. Equivalentemente (Esercizio 5.35) è una struttura per il linguaggio che estende $L_{\text{ANELLI-1}}$ mediante un predicato unario P e che soddisfa

$$\forall x \ (P(x) \vee P(-x) \vee x = 0)$$
$$\forall x, y \, (P(x) \wedge P(y) \Rightarrow P(x + y) \wedge P(x \cdot y))$$

In altre parole: un campo ordinato è un campo F con un sottoinsieme privilegiato P, detto **cono degli elementi positivi**, che è chiuso per somma e prodotto, e tale che F è ripartito nei tre insiemi disgiunti P, $-P$ e $\{0\}$.

Un campo ordinato si dice **archimedeo** se soddisfa il **principio di Archimede**

$$\forall x \exists n \in \mathbb{N} \big(0 < x \Rightarrow x < \underbrace{1 + \dots + 1}_{n} \big).$$

Questa non è una formula del prim'ordine, ma soltanto una pseudo-formula. L'esempio tipico di un campo ordinato archimedeo è $\mathbb{R}$ e nella Sezione 31 costruiremo campi non archimedei elementarmente equivalenti ad $\mathbb{R}$. Quindi la proprietà di essere archimedeo, non è esprimibile al prim'ordine.

Definizione 5.6. Un campo ordinato si dice **reale chiuso** se ogni elemento positivo è un quadrato e ogni polinomio di grado dispari ha una radice.

$\mathbb{R}$ e $\overline{\mathbb{Q}} \cap \mathbb{R}$, il campo dei numeri algebrici reali, sono esempi di campi reali chiusi archimedei. I campi reali chiusi sono assiomatizzabili aggiungendo a $\Sigma_{\text{CAMPI O.}}$ l'esistenza della radice quadrata per gli elementi positivi

$$\forall x \left(x \geq 0 \Rightarrow \exists y (y^2 = x) \right)$$

e gli infiniti enunciati

$$(\rho_n) \quad \forall a_0, \ldots, a_{2n+1} \exists x \left(a_0 + a_1 \cdot x + a_2 \cdot x^2 + \cdots + a_{2n+1} \cdot x^{2n+1} = 0 \right).$$

Nel Capitolo **??** dimostreremo che la teoria del prim'ordine dei campi reali chiusi è completa, e quindi ogni campo reale chiuso è elementarmente equivalente al campo reale $\mathbb{R}$. Dimostreremo anche che nessuna sotto-lista finita delle ρ_n è sufficiente per definire l'essere un campo reale chiuso, quindi per il Teorema 3.10 la teoria dei campi reali chiusi non è finitamente assiomatizzabile.

5.D.6. *Spazi vettoriali.* Finora abbiamo considerato linguaggi del prim'ordine con una quantità finita di simboli non logici, ma è facile imbattersi in linguaggi che non rientrano in questa tipologia. Per esempio, possiamo considerare uno spazio vettoriale su un campo $\Bbbk$ come una struttura $(V, +, \{f_x \mid x \in \Bbbk\}, \mathbf{0})$ dove $+ \colon V \times V \to V$ è l'operazione di somma di vettori, $\mathbf{0} \in V$ è il vettore nullo e $f_x \colon V \to V$, $f_x(\mathbf{v}) = x\mathbf{v}$ è il prodotto per scalare. Il linguaggio utilizzato $L_\Bbbk$ ha quindi tante operazioni unarie quanti sono gli elementi di $\Bbbk$. Più in generale, un R-modulo sinistro (dove R è un anello unitario) può essere visto come una struttura $(M, +, \{f_x \mid x \in R\}, \mathbf{0})$, dove $f_x \colon M \to M$, $f_x(m) = xm$, è il prodotto per l'elemento $x \in R$. (Naturalmente, se $\Bbbk$ e R sono finiti, i linguaggi $L_\Bbbk$ e L_R sono anch'essi finiti.) Mediante il linguaggio $L_\Bbbk$ è possibile assiomatizzare al prim'ordine anche le algebre di Lie, cioè spazi vettoriali su $\Bbbk$ dotati di un'operazione binaria $(x, y) \mapsto [x, y]$ che è bilineare, soddisfa $[x, x] = 0$ e l'identità di Jacobi $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$ (Esercizio 5.37).

Similmente è possibile formalizzare la nozione di G-insieme, vale a dire un insieme non vuoto X con un'azione del gruppo G su X, cioè una mappa $G \times X \to X$, $(g, x) \mapsto g.x$, tale che $1_G.x = x$ e $g.(h.x) = (gh).x$ per ogni $g, h \in G$ e $x \in X$. La struttura risultante sarà della forma $(X, \{f_g \mid g \in G\})$ dove $f_g(x) = g.x$.

5.D.7. *Spazi metrici.* Un altro esempio di linguaggio con infiniti simboli non logici proviene dalla nozione di distanza: in questo caso, invece di avere infiniti simboli di funzione, avremo infiniti simboli di relazione. Più precisamente, uno spazio metrico (M, d) può essere visto come una struttura

con infiniti predicati binari S_r con $r \in \mathbb{R}_+ \cup \{0\}$ definiti da

$$S_r(x, y) \Leftrightarrow d(x, y) = r.$$

Il linguaggio risultante ha tanti simboli quanti sono i numeri reali strettamente positivi, e questo insieme, come vedremo nella Sezione 10.C è più che numerabile, cioè non può essere messo in biezione con l'insieme dei numeri naturali. Se si passa dall'uguaglianza ad una disuguaglianza è possibile essere un po' più parsimoniosi ed usare solo una quantità numerabile di predicati binari. Più precisamente fissiamo il linguaggio L contenente i predicati R_q con $q \in \mathbb{Q}_+$: dato uno spazio metrico (M, d) consideriamo la L-struttura su M definita mediante

$$R_q(x, y) \Leftrightarrow d(x, y) < q.$$

Una struttura siffatta soddisfa gli enunciati

$$\forall x\, R_q(x, x)$$
$$\forall x, y\ (R_q(x, y) \Rightarrow R_q(y, x))$$
$$\forall x, y, z\ (R_q(x, y) \wedge R_p(y, z) \Rightarrow R_{p+q}(x, z))\,.$$

Viceversa ogni L-struttura che soddisfi gli enunciati qui sopra induce una metrica

$$d(x, y) = \inf\{q \mid R_q(x, y)\}$$

che genera proprio la struttura in questione.

Osservazione 5.7. Dopo aver visto questi esempi, il lettore potrebbe chiedersi quale sia il motivo per limitarsi ai linguaggi del prim'ordine, visto che molti concetti provenienti da varie parti della matematica sembrano richiedere quantificazioni sui numeri naturali o su sottoinsiemi arbitrari della struttura. Il motivo è semplice: la logica del prim'ordine permette di dimostrare risultati sui modelli che non sarebbero ottenibili in contesti più generali. L'esempio forse più importante di questo fenomeno è la *compattezza della logica del prim'ordine* (Teorema 31.1 del Capitolo VI): se Σ è un insieme di enunciati di un linguaggio del prim'ordine tale che ogni suo sottoinsieme finito è soddisfacibile, allora anche Σ è soddisfacibile.

5.E. Intermezzo: campi algebricamente chiusi e chiusura algebrica. I campi algebricamente chiusi e la nozione di chiusura algebrica sono molto importanti in logica.

Questa sezione verrà scritta in seguito.

5.F. Strutture e linguaggi a più sorte. Le strutture del prim'ordine viste finora (gruppi, anelli, ...) hanno la particolarità Â che i loro elementi sono tutti della stessa natura. Ci sono tuttavia delle situazioni in matematica in cui enti di natura diversa concorrono alla definizione di un oggetto.

5.F.1. *Spazi vettoriali come strutture a due sorte.* La definizione di spazio vettoriale su un campo $\Bbbk$ (o più ingenerale nella definizione di R-modulo) utilizza due tipi di enti, i vettori e gli scalari. Nella trattazione della Sezione 5.D.6, il campo degli scalari viene occultato mediante le funzioni unarie f_x, con $x \in \Bbbk$, ma che fare se vogliamo formalizzare come strutture al prim'ordine gli spazi vettoriali al variare del campo $\Bbbk$? Una soluzione consiste nel considerare strutture M il cui universo è della forma $W \cup \Bbbk$, dotate di due predicati unari $V(x)$ e $S(x)$ per formalizzare le frasi "x è un vettore" e "x è uno scalare", così che la struttura soddisfa l'enunciato

$$\forall x \ (V(x) \Leftrightarrow \neg S(x)) \, .$$

Vale a dire: ogni elemento è un vettore o uno scalare, ma non entrambi. Usiamo i simboli $\oplus$ e $\otimes$ per le operazioni di somma di vettori e di prodotto per scalare e $\boxplus$ e $\boxtimes$ per le operazioni sul campo $\Bbbk$. Il problema è che $\oplus, \otimes, \boxplus, \boxtimes$ sono operazioni parziali, definite solo su certe coppie, e quindi questi simboli devono essere considerati come predicati ternari. In altre parole, tra gli assiomi dovremo aggiungere enunciati del tipo

$$\forall x, y \ (V(x) \wedge V(y) \Rightarrow \exists z \, (\oplus(x, y, z)))$$
$$\forall x, y, z, w \, (V(x) \wedge V(y) \Rightarrow (\oplus(x, y, z) \wedge \oplus(x, y, w) \Rightarrow z = w \wedge V(z)))$$

e analogamente per $\otimes$, $\boxplus$ e $\boxtimes$. Per esempio, la commutatività dell'addizione di vettori è formulata come

$$\forall x, y, z \ (V(x) \wedge V(y) \wedge V(z) \wedge \oplus(x, y, z) \Rightarrow \oplus(y, x, z))$$

e la distributività del prodotto per scalare rispetto all'addizione di vettori può essere formulato come

$$\forall x, y, z, x', y', z', w \, [V(x) \wedge V(y) \wedge V(z) \wedge V(x') \wedge V(y') \wedge V(z') \wedge$$
$$S(w) \wedge \otimes(w, x, x') \wedge \otimes(w, y, y') \wedge \otimes(w, z, z') \wedge \oplus(x, y, z) \Rightarrow \oplus(x', y', z')] .$$

Esercizio 5.8. Completare la verifica che la nozione di spazio vettoriale su un campo arbitrario è finitamente assiomatizzabile nel linguaggio contenente i simboli $V, S, \oplus, \otimes, \boxplus$ e $\boxtimes$.

La formalizzazione che abbiamo appena visto è piuttosto barocca, dato che dobbiamo specificare se una variabile varia sui vettori o sugli scalari. La pratica matematica suggerisce di introdurre due sorte di variabili: quelle per i vettori, denotate con lettere in neretto $\mathbf{u}, \mathbf{v}, \mathbf{w}, \ldots$, e quelle per gli scalari, denotate con lettere greche $\alpha, \beta, \gamma, \ldots$. A partire dalle variabili per scalari si costruiscono mediante $\boxplus$ e $\boxtimes$ i termini scalari; un termine vettoriale è ottenuto a partire dalle variabili vettoriali mediante applicazioni del simbolo $+$ e mediante il prodotto $\cdot$ di un termine scalare con un termine vettoriale.

Quindi la distributività del prodotto per scalare rispetto all'addizione diventa

$$\forall \mathbf{u}, \mathbf{v}, \alpha \left[\alpha \cdot (\mathbf{u} + \mathbf{v}) = \alpha \cdot \mathbf{u} + \alpha \cdot \mathbf{v}\right].$$

5.F.2. *L'insieme potenza come struttura a due sorte.* Un altro esempio di struttura a due sorte è dato da $\mathscr{P}(A)$, la famiglia dei sottoinsiemi di un insieme A: fissiamo due predicati unari, U per gli elementi di A e S per i sottoinsiemi di A, più un predicato binario E per specificare quando un punto appartiene ad un sottoinsieme. Possiamo quindi considerare $\mathscr{P}(A)$ come una struttura (M, U^M, S^M, E^M) dove

$$\begin{aligned} M &= A \cup \mathscr{P}(A) \\ U^M &= A \\ S^M &= \mathscr{P}(A) \\ E^M &= \{(x, X) \in A \times \mathscr{P}(A) \mid x \in X\}. \end{aligned}$$

Come nel caso degli spazi vettoriali distinguiamo tra variabili per elementi di A (indicate con lettere minuscole $x, y, z, \ldots$) e variabili per sottoinsiemi di A (indicate con lettere maiuscole $X, Y, Z, \ldots$). È immediato verificare che i seguenti enunciati valgono in M:

$$\begin{gathered} \forall X, Y \ [\forall z \ (E(z, X) \Leftrightarrow E(z, Y)) \Rightarrow X = Y], \\ \exists X \ (\neg \exists x \, E(x, X)), \\ \forall X \, \exists Y \, \forall z \ (E(z, X) \Leftrightarrow \neg E(z, Y)), \\ \forall X, Y \, \exists Z \, \forall w \ [E(w, Z) \Leftrightarrow (E(w, X) \wedge E(w, Y))]. \end{gathered}$$

Il primo dice che due insiemi che abbiano gli stessi elementi coincidono, il secondo che l'insieme vuoto esiste, il terzo che il complementare di un insieme esiste, il quarto che l'intersezione di due insiemi esiste.

Viceversa, una struttura M a due sorte che soddisfi gli enunciati qui sopra, è della forma $\mathcal{S} \subseteq \mathscr{P}(A)$ dove $\mathcal{S}$ è una famiglia contenente l'insieme vuoto e chiusa per complementi e intersezioni (e quindi contenente A e chiusa per unioni), ma non è detto che $\mathcal{S} = \mathscr{P}(A)$. Le famiglie $\mathcal{S}$ siffatte si dicono algebre di Boole e verranno studiate in dettaglio nelle Sezioni 8 e 23.

5.G. L'algebra dei termini. Una **congruenza** su una L-struttura M è una relazione di equivalenza $\sim$ su M tale che per ogni $a_1, \ldots, a_n, b_1, \ldots, b_n \in M$ e ogni simbolo di funzione n-ario f e ogni simbolo di relazione n-aria R, se $a_1 \sim b_1$, …, $a_n \sim b_n$ allora

$$f(a_1, \ldots, a_n) \sim f(b_1, \ldots, b_n) \wedge (R(a_1, \ldots, a_n) \Leftrightarrow R(b_1, \ldots, b_n)).$$

Quindi $M/\!\sim$ diventa una L-struttura. L'identità e la relazione banale $M \times M$ sono congruenze e l'intersezione di una famiglia di congruenze è una

congruenza. Se R è una relazione binaria su M, allora

$$\bigcap\{E \mid R \subseteq E \wedge E \text{ è una congruenza}\}$$

è la **congruenza generata** da R. Per semplicità tipografica tenderemo ad utilizzare il medesimo simbolo per la relazione e per la congruenza che essa genera.

L'insieme dei termini di un linguaggio L è denotato con Term_L, o con Term se non c'è pericolo di confusione, e può essere visto come una struttura algebrica dove le operazioni sono date dai simboli di funzione — più precisamente, se f è un simbolo di funzione n-ario, allora $f(t_1, \ldots, t_n)$ è il risultato dell'operazione f applicata agli elementi $t_1, \ldots, t_n \in \mathrm{Term}$. Un discorso analogo vale se l'insieme dei termini Term è sostituito da $\mathrm{Term}(x_0, \ldots, x_{n-1})$, l'insieme dei termini le cui variabili sono tra le $x_0, \ldots, x_{n-1}$, oppure dall'insieme dei termini chiusi $\mathrm{ClTerm}_L = \mathrm{ClTerm}$. Se $\sim$ è una congruenza su Term allora $\mathrm{Term}(x_1, \ldots, x_n)/{\sim}$ è isomorfo a $\mathrm{Term}/{\approx}$ dove $\approx$ è la congruenza generata dalla relazione $\sim \cup \{x_n \approx x_m \mid n < m\}$. Sia L_∞ il linguaggio ottenuto da L aggiungendo nuovi simbolo di costante $\{d_n \mid n \in \mathbb{N}\}$. La mappa

$$\mathrm{Term}_L \to \mathrm{ClTerm}_{L_\infty}, \qquad t \mapsto t[d_0/x_0, d_1/x_1, \ldots]$$

è una biezione, e se $\sim$ è una congruenza su Term_L allora

$$t \sim s \Leftrightarrow t[d_0/x_0, d_1/x_1, \ldots] \sim s[d_0/x_0, d_1/x_1, \ldots].$$

Allora $\mathrm{Term}_L/{\sim}$ e $\mathrm{ClTerm}_{L_\infty}/{\sim}$ sono L-strutture isomorfe, come lo sono $\mathrm{Term}_L(x_0, \ldots, x_{n-1})$ e ClTerm_{L_n}, dove L_n è il linguaggio ottenuto aggiungendo $d_0, \ldots, d_{n-1}$ to L.

da finire!

Se T è una teoria equazionale in un linguaggio L ... Vediamo qualche esempio.

Esempio 5.9. Sia $\sim$ la congruenza generata dalla proprietà associativa, cioè

$$(t * s) * u \sim t * (s * u),$$

per ogni scelta di termini t, s, u. L'algebra quoziente è un semigruppo.

Esercizio 5.10. Come abbiamo già osservato a pagina 21, applicando $*$ ai termini $t_1, \ldots, t_n$ possiamo formare $\binom{2n}{n} - \binom{2n}{n-1}$ termini distinti. Dimostrare che questi prodotti sono tutti $\sim$ equivalenti.

In altre parole: in un semigruppo $(A, *)$ l'espressione $a_1 * a_2 * \cdots * a_n$ non è ambigua.

Quindi gli elementi dell'algebra quoziente possono essere identificati con le espressioni della forma

$$x_1^{n_1} * x_2^{n_2} * \cdots * x_k^{n_k},$$

dove $x_1, \ldots, x_k$ sono variabili non necessariamente distinte e $n_1, \ldots, n_k > 0$ — se oltre alla proprietà associativa si richiede anche la proprietà commutativa, cioè che $t*s \sim s*t$ per ogni coppia di termini t e s, allora le variabili possono essere prese distinte.

Se partiamo dal sottoinsieme $\mathrm{Term}(x_1, \ldots, x_k)$ dei termini contenenti soltanto le variabili $x_1, \ldots, x_k$, allora $\mathrm{Term}(x_1, \ldots, x_k)/\sim$ risulta essere una sottostruttura di $\mathrm{Term}\,/\sim$. In particolare, se $\sim$ è la congruenza generata dalla proprietà associativa, allora gli elementi di $\mathrm{Term}(x)/\sim$ sono (o meglio: possono essere identificati con) espressioni della forma x^n con $n > 0$.

Esempio 5.11. Se $\sim$ è la congruenza che garantisce la proprietà associativa e commutativa, allora $\mathrm{Term}(x)/\sim$ è isomorfo a $(\mathbb{N} \setminus \{0\}, +)$.

Esempio 5.12. Se $\sim$ è la congruenza generata da $(s * t) * u \sim t$, allora l'algebra quoziente $\mathrm{Term}\,/\sim$ ha un solo elemento, vale a dire $s \sim t$ per ogni $s, t \in \mathrm{Term}$.

Per vedere ciò è sufficiente verificare che se $(A, *)$ è una struttura algebrica che soddisfa

$$(x * y) * z = y$$

per ogni x, y, z, soddisfa anche $\forall x, y, z\,((x * y) = z)$. Infatti ponendo $x = y$ si ottiene $(x * x) * z = x$ e quindi $((x * x) * z) * y = x * y$. Sostituendo $x * x$, z e y al posto di x, y e z, si ottiene $((x * x) * z) * y = z$. Quindi $x * y = z$ come richiesto.

Esempio 5.13. L'algebra quoziente ottenuta mediante la congruenza

$$s * (t * u) \sim (s * t) * (s * u)$$

si dice algebra distributiva a sinistra, ed è un oggetto molto importante nello studio del gruppo delle trecce.

5.G.1. Consideriamo il linguaggio L_{GRUPPI} della Sezione 5.A.1 ma con l'operazione binaria denotata con $*$. Consideriamo la congruenza $\sim$ generata da

- la proprietà associativa per $*$, cioè $t * (s * u) \sim (t * s) * u$
- $1 * t \sim t$,
- $t^{-1} * t \sim 1$.

La struttura quoziente $\mathrm{Term}\,/\sim$ è un gruppo (Esercizio 5.28) i cui elementi sono classi di equivalenza di termini costruiti a partire dalla costante 1 e dalle variabili, che, come abbiamo convenuto a pagina 19, sono una lista infinita $v_0, v_1, \ldots$ di oggetti. Essenzialmente è il gruppo più generale che può essere costruito a partire dalle variabili v_n; un gruppo di questo tipo si dice **gruppo libero di rango** ω e verrà studiato nella Sezione 14.E.1. Se

si considera $\mathrm{Term}(v_1,\dots,v_n)/\sim$ si ottiene il **gruppo libero di rango** n, il gruppo più generale con n generatori.

Gli elementi di $\mathrm{Term}(x)/\sim$ sono identificabili con espressioni della forma x^n con $n\in\mathbb{Z}$, quindi il gruppo libero su un generatore è isomorfo a $(\mathbb{Z},+)$.

Gli elementi di $\mathrm{Term}(x,y)/\sim$ sono identificabili con le espressioni della forma

$$x^{n_1} * y^{m_1} * x^{n_2} * y^{m_2} * \cdots * x^{n_k} * y^{m_k}$$

dove $k\geq 1$, $m_1,n_2,\dots,n_k\in\mathbb{Z}\setminus\{0\}$ e $n_1,m_k\in\mathbb{Z}$, con la convenzione che se $k=1$ e $n_1=m_k=0$ l'espressione risultante sta per la classe di equivalenza del termine 1. Se $\equiv$ è una congruenza che estende $\sim$, la struttura $\mathrm{Term}(x,y)/\equiv$ è un gruppo generato da due elementi $[x]$ e $[y]$ che è immagine suriettiva di $\mathrm{Term}(x,y)/\sim$, e ogni gruppo generato da due elementi è ottenibile come quoziente del gruppo libero di rango 2. Per esempio:

- se $\equiv$ garantisce la proprietà commutativa, allora le espressioni si riducono alla forma $x^n * y^m$ con $n,m\in\mathbb{Z}$, quindi $\mathrm{Term}/\equiv$ è isomorfo a $\mathbb{Z}\times\mathbb{Z}$
- se $\equiv$ garantisce la proprietà commutativa e richiede $x^n\equiv 1$ e $y^m\equiv 1$, allora $\mathrm{Term}/\equiv$ è isomorfo a $(\mathbb{Z}/n\mathbb{Z})\times(\mathbb{Z}/m\mathbb{Z})$,
- se si richiede che $x^4\equiv 1$ e $(x*y)^2\equiv 1$, allora $\mathrm{Term}/\equiv$ è isomorfo al gruppo diedrale D_4 delle isometrie del quadrato — per esempio x rappresenta una rotazione di $\pi/2$ e y la riflessione lungo una diagonale.

5.G.2. Se L è il linguaggio dei semianelli unitari (vedi Sezione 5.C.3), cioè il linguaggio contenente $+,\cdot,0$ e 1, e se $\sim$ è la congruenza generata da

- $(t+s)+u\sim t+(s+u)$ e $t+s\sim s+t$, cioè le proprietà associativa e commutativa per $+$,
- $(t\cdot s)\cdot u\sim t\cdot(s\cdot u)$ e $t\cdot s\sim s\cdot t$, cioè le proprietà associativa e commutativa per $\cdot$,
- $0+t\sim t$,
- $1\cdot t\sim t$,
- $0\cdot t\sim 0$,

allora $\mathrm{Term}(x_1,\dots,x_n)/\sim$ è il semigruppo libero su n generatori ed è isomorfo a $\mathbb{N}[X_1,\dots,X_n]$, il semianello dei polinomi in n variabili a coefficienti in $\mathbb{N}$.
5.G.3.

5.H. Grafi. Un **grafo** è costituito da un insieme non vuoto V di oggetti detti **vertici** variamente collegati fra loro.[3] Un vertice v non è mai collegato a sé stesso e se v e w sono collegati, il collegamento è unico. I collegamenti si dicono **spigoli**. Formalmente un grafo è una coppia (V,E) dove V è l'insieme

[3]Questo concetto non deve essere confuso con la nozione di *grafo di una funzione* $\mathrm{Gr}(f)$.

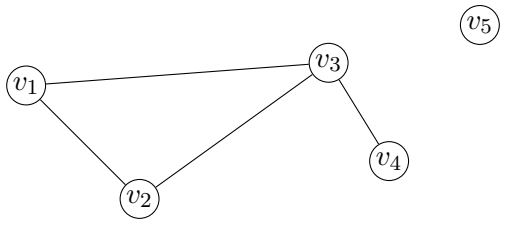


Figura 2. Un grafo finito.

dei vertici ed E è un sottoinsieme di

$$\{\{v, w\} \mid v, w \in V \wedge v \neq w\}.$$

$\{v, w\} \in E$ significa che v e w sono collegati da uno spigolo. Viceversa, due vertici x e y di un grafo sono collegati se $\{x, y\}$ è uno spigolo. Chiaramente l'insieme di coppie non ordinate di vertici E può essere identificato con il sottoinsieme simmetrico di $V \times V \setminus \{(v, v) \mid v \in V\}$ dato da $\tilde{E} = \{(v, w) \mid \{v, w\} \in E\}$. I **grafi finiti** (cioè in cui l'insieme dei vertici è finito) possono essere visualizzati come punti del piano uniti da line (eventualmente curve): i punti rappresentano i vertici, le linee gli spigoli. La **valenza** di un vertice v è il numero di vertici a cui v è collegato mediante uno spigolo. Nella Figura 2 è disegnato un grafo in cui i vertici v_1, v_2, v_3 sono mutualmente collegati, v_4 è solo collegato con v_3 e v_5 non è collegato con nessun altro vertice, cioè è un vertice isolato, cioè è il grafo (V, E) con $V = \{v_1, v_2, v_3, v_4, v_5\}$ ed $E = \{\{v_1.v_2\}, \{v_1, v_3\}, \{v_2, v_3\}, \{v_3, v_4\}\}$. I vertici v_1 e v_2 hanno valenza 2, il vertice v_3 ha valenza 3, il vertice v_4 ha valenza 1 e il vertice v_5 ha valenza 0. Due grafi (V, E) e (V', E') sono isomorfi se c'è una biezione $F\colon V \to V'$ tale che $\{v, w\} \in E \Leftrightarrow \{F(v), F(w)\} \in E'$ per ogni $v, w \in V$. Identificheremo sempre due grafi isomorfi.

Dato un grafo $G = (V, E)$ ed uno spigolo $e = \{x, y\} \in E$ la contrazione di G mediante lo spigolo e è il grafo $G/e = (V', E')$ ottenuto identificando i vertici x e y, vale a dire $V' = V \setminus \{x, y\} \cup \{v_e\}$ dove v_e è un nuovo vertice e

$$E' = \{\{v, w\} \in E \mid \{v, w\} \cap \{x, y\} = \emptyset\} \cup \{\{v_e, w\} \mid \{x, w\} \in E \setminus \{e\} \vee \{y, w\} \in E \setminus \{e\}\}$$

H è un **minore** di G, in simboli $H \leq G$, se H è ottenibile da un $H' \subseteq G$ mediante una successione finita di contrazioni, cioè se esistono $H_0, H_1, \ldots, H_n$ tali che $H = H_0$, $H_n = H'$ e H_i è H_{i+1}/e_{i+1} dove e_{i+1} è uno spigolo di H_{i+1}.

5.H.1. *Assiomi per i grafi.* Gli assiomi per i grafi sono formulati in un linguaggio L_{GRAFI} con un simbolo di relazione binaria E e asseriscono che

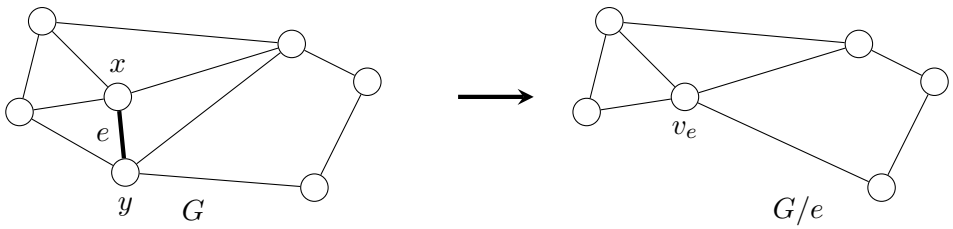


Figura 3. Contrazione dello spigolo $e = \{x, y\}$

questa relazione è irriflessiva e simmetrica cioè

$$\Sigma_{\text{GRAFI}} \begin{cases} \forall x \neg E(x, x) \\ \forall x, y \, (E(x, y) \Rightarrow E(y, x)) \, . \end{cases}$$

Diremo che $G' = (V', E')$ è un sottografo di un grafo $G = (V, E)$, in simboli $G' \subseteq G$, se $V' \subseteq V$ e $E' \subseteq E \cap V' \times V'$.

Osservazione 5.14. La nozione di sottografo non coincide con quella di sottostruttura perché non si richiede che $E' = E \cap V' \times V'$. Quando $V' \subseteq V$ e $E' = E \cap V' \times V'$ diremo che (V', E') è il **sottografo indotto** da (V, E) su V'.

Un grafo è **completo** se ogni coppia di vertici è collegata da uno spigolo, cioè se soddisfa l'enunciato

$$\forall x, y \, (x \neq y \Rightarrow E(x, y)) \, .$$

Due grafi completi con lo stesso numero di vertici sono chiaramente isomorfi e K_n denota il grafo completo con n vertici (Figura 4). Se il sottografo indotto su $X \subseteq V$ è completo, diremo che X è una **clique**.[4] All'estremo opposto, un insieme di vertici X si dice **indipendente** se due vertici in X non sono mai collegati da uno spigolo. Un grafo è indipendente se l'insieme dei vertici è indipendente, cioè se non ha spigoli.

L'enunciato dell'Esercizio 2.10 a pagina 17 può essere riformulato come un'affermazione sui grafi: in ogni grafo con sei vertici ci sono tre vertici che sono mutualmente collegati o mutualmente scollegati. Questo è un caso particolare del seguente risultato:

Teorema 5.15. *$\forall n \exists m \geq n$ tale che ogni grafo con m vertici contiene il grafo completo K_n come sottografo, oppure ha n vertici mutualmente scollegati.*

Un grafo è **bipartito** se l'insieme dei vertici V può essere ripartito in due sottoinsiemi disgiunti non vuoti A_0 e A_1 e se non ci sono spigoli tra vertici della stessa partizione. Il grafo bipartito in cui A_0 ha taglia n e

[4] In alcuni testi italiani, *clique* è stato tradotto con l'orripilante *cricca*.

A_1 ha taglia m e ogni vertice in A_i è collegato ad ogni vertice in A_{1-i} è indicato con $\mathrm{K}_{n,m}$ (Figura 4). Per formulare al prim'ordine il concetto di grafo bipartito si utilizza un linguaggio a due sorte, cioè si introducono due simboli di predicato 1-ario A_0 e A_1 con gli assiomi:

$$\exists x\, A_0(x) \;\wedge\; \exists x\, A_1(x)$$
$$\forall x\, (A_0(x) \vee A_1(x))$$
$$\forall x, y\, \left[(A_0(x) \wedge A_0(y)) \vee (A_1(x) \wedge A_1(y)) \Rightarrow \neg E(x,y)\right].$$

Se nella definizione di grafo bipartito usiamo una partizione dell'insieme dei vertici in k parti, invece che in due parti, si ottiene la nozione di grafo k-partito. Come vedremo nella Sezione 5.H.4 anche i grafi k-partiti possono essere finitamente assiomatizzati.

Un grafo si dice **planare** se può essere disegnato nel piano in modo che gli spigoli si intersechino solo nei vertici. I grafi K_4 e $\mathrm{K}_{2,3}$ sono planari,

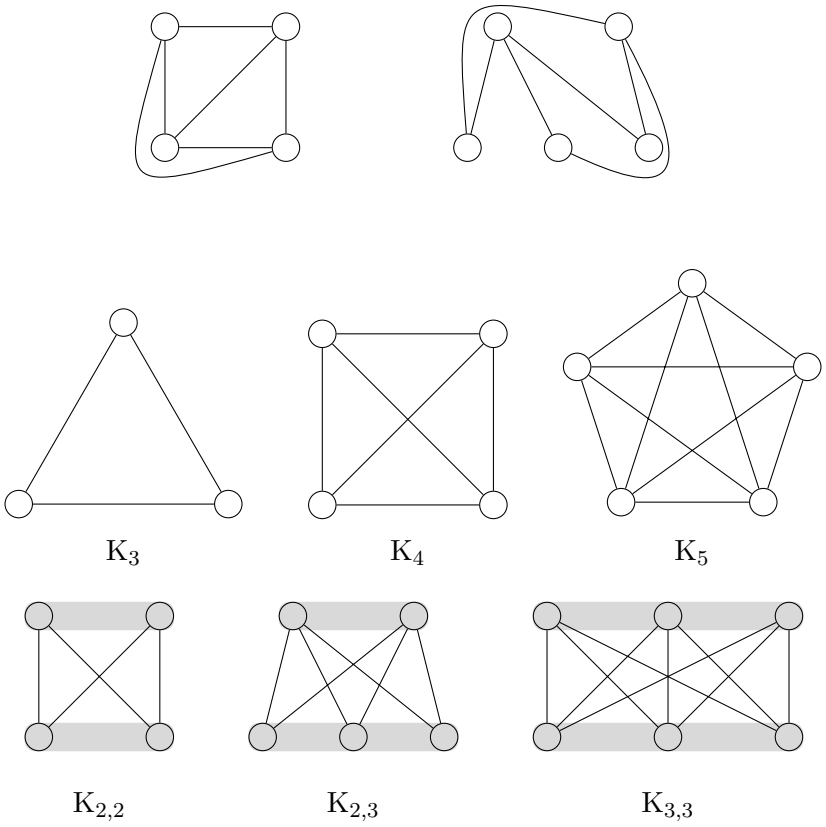


Figura 4. Grafi completi e bipartiti

mentre si dimostra che né K_5 né $\mathrm{K}_{3,3}$ lo sono — questi sono essenzialmente i controesempi minimali, dato che un grafo G è planare se e solo se non contiene K_5 o $\mathrm{K}_{3,3}$ come minore.

5.H.2. *Cicli.* Un n-**ciclo** ($n \geq 3$) in un grafo è una successione di vertici distinti $x_1, \ldots, x_n$ tali che x_i è collegato a x_{i+1} e x_n è collegato a x_1. Un ciclo è un n-ciclo per qualche n e un grafo si dice **aciclico** se non contiene cicli, cioè se vale $\forall n \geq 3\, \chi_n$ dove χ_n è la formula

$$(\chi_n) \quad \neg\exists x_1, \ldots, x_n \left(\textstyle\bigwedge_{1 \leq i < j \leq n} x_i \neq x_j \wedge E(x_1, x_n) \wedge \bigwedge_{1 \leq i < n} E(x_i, x_{i+1}) \right).$$

Purtroppo $\forall n \geq 3\, \chi_n$ è soltanto una pseudo-formula — per assiomatizzare la classe dei grafi aciclici al prim'ordine bisogna aggiungere agli assiomi per i grafi tutti gli enunciati χ_n. La classe dei grafi aciclici è assiomatizzabile, ma non è finitamente assiomatizzabile e la classe dei grafi che contengono un ciclo non è neppure assiomatizzabile (Esercizio 5.41).

5.H.3. *Connessione.* Un k-**cammino** da v a w è una successione finita di vertici

$$v = z_0, z_1, \ldots, z_k = w$$

tale che ogni z_i è collegato a z_{i+1} e $k \geq 1$. Un cammino è un k-cammino per qualche k. Un grafo si dice **connesso** se ogni coppia di vertici è collegata da un cammino, altrimenti si dice sconnesso — il grafo della Figura 2 è sconnesso, dato che v_5 è isolato, mentre i grafi delle Figure 3 e 4 sono connessi. Una **componente connessa** di un grafo è un sottografo indotto connesso e massimale rispetto all'inclusione tra i sottografi indotti e connessi. Ogni grafo (V, E) è l'unione disgiunta delle sue componenti connesse, cioè c'è una partizione $\bigcup_{i \in I} V_i = V$ dell'insieme dei vertici tale che il sottografo indotto su ciascun V_i è una componente connessa.

La connessione è usualmente formulata come

$$\forall x, y\, \exists k \geq 1\, \exists z_0, \ldots, z_k\, (x = z_0 \wedge y = z_k \wedge \bigwedge_{i<k} E(z_i, z_{i+1})).$$

Questa è una pseudo-formula dato che

- in "$\exists k \geq 1$" si quantifica sui naturali positivi e non sull'insieme dei vertici e
- la quantificazione $\exists z_1, \ldots, z_k$ e la congiunzione $\bigwedge_{i<k} E(z_i, z_{i+1})$ non sono fissate una volta per tutte, ma dipendono da k.

La famiglia dei grafi connessi non è assiomatizzabile al prim'ordine (Esercizio 32.25 a pagina 470).

5.H.4. *Colorabilità.* Dato un grafo $G = (V, E)$, una k-**colorazione dei vertici di** G è una funzione $F\colon V \to \{0, \ldots, k-1\}$ tale che $v\ E\ w \Rightarrow F(v) \neq F(w)$. Equivalentemente: è un morfismo di strutture $F\colon G \to \mathrm{K}_k$. I numeri $0, \ldots, k-1$ si dicono **colori** di F. Un grafo si dice k-**colorabile** se ammette

una k-colorazione dei vertici. La k-colorabilità di un grafo è esprimibile al prim'ordine — basta introdurre nuovi predicati unari $A_0, \dots, A_{k-1}$ con gli assiomi

$$\forall x\,(A_0(x) \vee \cdots \vee A_{k-1}(x))$$
$$\neg\exists x \bigvee_{i<j<k} (A_i(x) \wedge A_j(x))$$
$$\forall x, y(E(x,y) \Rightarrow \neg \bigvee_{i<k} A_i(x) \wedge A_i(y)).$$

Infatti dire che un grafo è k-colorabile è solo un altro modo per dire che un grafo è k-partito. In particolare: un grafo è bipartito se e solo se è 2-colorabile. Se G è un grafo finito con vertici $\{v_0, \dots, v_{n-1}\}$, allora la mappa $v_i \mapsto i$ testimonia che G è n-colorabile. Il più piccolo naturale k tale che un grafo finito G è k-colorabile è il **numero cromatico** di G e lo si indica con $\boldsymbol{\chi}(G)$. Quindi $\boldsymbol{\chi}(\mathrm{K}_n) = n$ mentre un grafo privo di spigoli è 1-colorabile.

Teorema 5.16. *Per $G = (V, E)$ un grafo finito, le seguenti affermazioni sono equivalenti:*

(a) *G è 2-colorabile*

(b) *G non contiene cicli di lunghezza dispari.*

Dimostrazione. (a)⇒(b) Se $x_1, \dots, x_n$ è un ciclo e F è una 2-colorazione, allora

$$\forall i \leq n\ (F(x_1) \neq F(x_i) \Leftrightarrow i \text{ pari})$$

e poiché $F(x_1) \neq F(x_n)$, l'asserto segue.

(b)⇒(a) Sia $\bigcup_{i\in I} V_i = V$ la partizione dell'insieme dei vertici di G in componenti connesse. Poiché V è finito, anche I è finito, per cui possiamo scegliere $v_i \in V_i$ e definire $F\colon V \to \{0, 1\}$

$$F(v) = 1 \Leftrightarrow \text{ c'è un } k\text{-cammino da un qualche } v_i \text{ a } v, \text{ con } k \text{ pari.}$$

L'assunzione (b) garantisce che F è proprio una 2-colorazione. □

Osservazione 5.17. La dimostrazione che (a)⇒(b) non richiede che il grafo sia finito. Nella parte (a)⇒(b), se G è infinito, può avvenire che I, l'insieme degli indici nella partizione del grafo nelle sue componenti connesse, sia infinito, e per selezionare i vertici $v_i \in V_i$ si deve ricorrere ad un principio insiemistico, noto come Assioma della Scelta.

Il seguente risultato, noto come Teorema dei Quattro Colori, è uno dei risultati centrali della teoria.

Teorema 5.18. *Ogni grafo planare finito è 4-colorabile.*

Il Teorema 5.18 è generalmente formulato così: ogni carta geografica può essere colorata con quattro colori in modo che regioni adiacenti siano

colorate in modo diverso. (Per verificare l'equivalenza basta associare ad ogni territorio un vertice v e considerare lo spigolo $\{v, w\}$ soltanto quando v e w rappresentano territori confinanti.)

La nozione duale di colorazione dei vertici è quella di colorazione degli spigoli: dato un grafo $G = (V, E)$, una funzione $F\colon E \to \{1, \dots, k\}$ si dice **k-colorazione degli spigoli** di G e i numeri $1, \dots, k$ si dicono colori. Un sottoinsieme $H \subseteq V$ si dice **monocromatico** per una k-colorazione F se gli spigoli del sottografo indotto da H hanno tutti lo stesso colore, cioè se c'è un $1 \leq i \leq k$ tale che $F(\{x, y\}) = i$ per ogni $x, y \in H$ distinti. Poiché ogni grafo con m vertici è un sottografo di K_m, il Teorema 5.15 è il caso particolare quando $k = 2$ del seguente risultato, noto come Teorema di Ramsey.

Teorema 5.19. *$\forall n, k\, \exists m \geq n$ tale che per ogni k-colorazione di K_m c'è un sottografo indotto isomorfo a K_n e monocromatico.*

5.H.5. *Grafi infiniti.* Vediamo due esempi di grafi il cui insieme dei vertici è $\mathbb{N}$.

Il **grafo completo numerabile** è $\mathrm{K}_\omega = (\mathbb{N}, E)$ dove $E = \{\{n, m\} \mid n \neq m\}$, cioè ogni coppia di vertici distinti è collegata da uno spigolo. Ogni grafo numerabile può essere identificato con un sottografo di K_ω. Il Teorema di Ramsey 5.19 vale anche per K_ω: per ogni $k > 0$ e ogni k-colorazione degli spigoli di K_ω, c'è un $H \subseteq \mathbb{N}$ infinito tale che il sottografo indotto su H (che è ovviamente isomorfo a K_ω) è monocromatico. Dimostreremo questo risultato nella Sezione 26.

Il **grafo aleatorio numerabile** $\mathrm{R}_\omega = (\mathbb{N}, E)$ è il grafo così definito:

$$n\ E\ m \Leftrightarrow \mathbf{p}_n \mid m \vee \mathbf{p}_m \mid n$$

dove $(\mathbf{p}_n)_n$ è l'enumerazione crescente dei numeri primi. La relazione E è chiaramente simmetrica e la irriflessività segue da $n < \mathbf{p}_n$, quindi R_ω è davvero un grafo.

Definizione 5.20. Un grafo $G = (V, E)$ soddisfa la proprietà ρ se presi due sottoinsiemi finiti e disgiunti di vertici A, B c'è sempre x che ha uno spigolo con ogni vertice in A e nessuno spigolo con alcun vertice in B, cioè

$$\forall y \in A\ (x\ E\ y) \wedge \neg\exists z \in B\ (x\ E\ z)\,.$$

Proposizione 5.21. *R_ω ha la proprietà ρ.*

Dimostrazione. Basta prendere $x = (\prod_{n \in A} \mathbf{p}_n)^k$ con k sufficientemente grande per cui $\forall m \in B\ (x \nmid \mathbf{p}_m)$. □

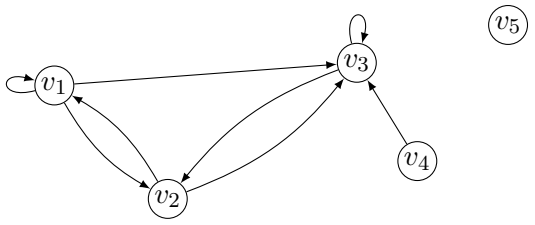


Figura 5. Un grafo diretto finito.

La proprietà ρ può essere riformulata mediante gli infiniti enunciati

$$(\rho_n) \quad \forall y_1, \dots, y_n, z_1, \dots, z_n \Big[\bigwedge_{1 \le i,j \le n} y_i \neq z_j \Rightarrow \exists x \, (\bigwedge_{1 \le i \le n} E(x, y_i) \wedge \neg E(x, z_i)) \Big],$$

quindi un sistema di assiomi per R_ω nel linguaggio L_{GRAFI} è $\Sigma_{\text{GRAFO ALEATORIO}}$ i cui assiomi sono Σ_{GRAFI}, l'enunciato $\boldsymbol{\varepsilon}_{\ge 3}$ "ci sono almeno tre vertici distinti", e gli enunciati ρ_n. Il Teorema 10.35 nella Sezione 10.I mostra che ogni grafo numerabile che soddisfi $\Sigma_{\text{GRAFO ALEATORIO}}$ è isomorfo a R_ω, e per questo motivo ogni grafo siffatto si dice grafo aleatorio (si veda l'Esempio 10.36 e l'Esercizio 19.18). Per il Teorema 3.27 la teoria $\Sigma_{\text{GRAFO ALEATORIO}}$ è completa.

5.H.6. *Grafi diretti.* Se nella definizione di grafo ammettiamo che un vertice possa essere collegato a sé stesso, e che i collegamenti tra i vertici ammettano un orientamento, otteniamo la nozione di **grafo diretto** o **digrafo**. Formalmente un grafo diretto è un insieme non vuoto V di vertici ed un sottoinsieme $R \subseteq V \times V$ di spigoli orientati, e ogni relazione binaria R su un insieme non vuoto V può essere vista come un grafo diretto. Per esempio, se

$$V = \{v_1, v_2, v_3, v_4, v_5\}$$

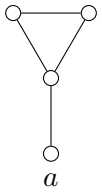
e

$$R = \{(v_1, v_1), (v_1, v_2), (v_1, v_3), (v_2, v_1), (v_2, v_3), (v_3, v_3), (v_4, v_3)\},$$

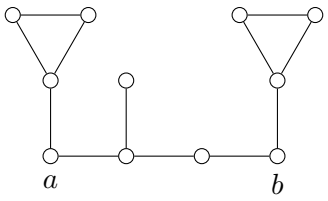
allora il grafo diretto (V, R) è rappresentato dalla Figura 5. Notare che vertici v_1, v_2 sono collegati in entrambe le direzioni, e così pure i vertici v_2, v_3.

5.H.7. *Interpretabilità nei grafi.* I grafi sono in grado di interpretare ogni struttura che possiamo considerare. Qui ci limitiamo a vedere come ogni struttura della forma $\mathcal{M} = (M, R)$ con $R \subseteq M \times M$ si può interpretare in un

grafo opportuno $G_{\mathcal{M}}$. Per ogni $a \in M$ consideriamo il grafo H_a



uno per ogni $a \in M$. Se $a\ R\ b$ e $a, b \in M$, allora l'R-collegamento da H_a a H_b è definito così:



(L'asimmetria del cammino da a a b è necessaria per codificare che a è in relazione R con b.) Il grafo $G_{\mathcal{M}}$ è ottenuto prendendo tutti gli H_a e gli R-collegamenti da H_a a H_b, quando $a\ R\ b$.

Verifichiamo che $\mathcal{M}$ è proprio interpretabile in $G_{\mathcal{M}}$. L'universo della struttura $\mathcal{M}$, cioè l'insieme M, è identificato con l'insieme dei vertici definito dalla formula

$$\psi_U(x) \Leftrightarrow \exists z_1, z_2, z_3\, \psi_H(x, z_1, z_2, z_3)$$

dove $\psi_H(x, z_1, z_2, z_3)$ è

$$\begin{aligned}(x\ E\ z_1 \wedge z_1\ E\ z_2 \wedge z_2\ E\ z_3 \wedge z_3\ E\ z_1 \wedge x \neq z_2 \wedge x \neq z_3)\\ \wedge \forall w\ (w\ E\ z_1 \Rightarrow w = x \vee w = z_2 \vee w = z_3)\\ \wedge \forall w\ (w\ E\ z_2 \Rightarrow w = z_1 \vee w = z_3)\\ \wedge \forall w\ (w\ E\ z_3 \Rightarrow w = z_1 \vee w = z_2)\,.\end{aligned}$$

La relazione R è identificata con l'insieme delle coppie ordinate di vertici definito dalla formula

$$\psi_R(x, y) \Leftrightarrow \psi_U(x) \wedge \psi_U(y) \wedge \exists u_1, u_2, u_3\, \psi_L(x, u_1, u_2, u_3, y),$$

dove $\psi_L(x, u_1, u_2, u_3, y)$ è

$$\begin{aligned}\big[x\ E\ u_1 \wedge u_1\ E\ u_2 \wedge u_1\ E\ u_3 \wedge u_3\ E\ y \wedge x \neq u_2 \wedge x \neq u_3 \wedge y \neq u_1\\ \wedge \forall w\ (w\ E\ u_1 \Rightarrow w = x \vee w = u_2 \vee w = u_3)\\ \wedge \forall w\ (w\ E\ u_3 \Rightarrow w = u_1 \vee w = y)\\ \wedge \forall w\ (w\ E\ u_2 \Rightarrow w = u_1)\big]\end{aligned}$$

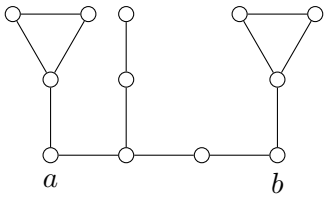
Un vertice di $G_{\mathcal{M}}$ o appartiene a qualche H_a, e quindi soddisfa $\varphi_H(x)$

$$\exists a, z_1, z_2, z_3\ [\psi_H(a, z_1, z_2, z_3) \wedge (x = a \vee x = z_1 \vee x = z_2 \vee x = z_3)]$$

oppure appartiene a qualche collegamento e quindi soddisfa $\varphi_L(x)$

$$\exists a, u_1, u_2, u_3, b \left[\psi_L(a, u_1, u_2, u_3, b) \wedge (x = u_1 \vee x = u_2 \vee x = u_3)\right].$$

Ne segue che la famiglia dei grafi della forma $G_{\mathcal{M}}$, vale a dire: la famiglia di tutti i grafi che codificano una struttura nel linguaggio con un'unica relazione binaria, è assiomatizzato da $\forall x\,(\varphi_H(x) \veebar \varphi_L(x))$, dove $\veebar$ è la disgiunzione esclusiva. La costruzione qui sopra si applica a linguaggi con più di una relazione binaria. Per esempio, nel caso di due relazioni binarie R ed S si definiscono gli H_a e gli R-collegamenti come sopra, mentre gli S-collegamenti da H_a a H_b sono definiti da:



Esercizi

Esercizio 5.22. Dimostrare i gruppi abeliani divisibili privi di torsione sono tutti e soli gli spazi vettoriali su $\mathbb{Q}$ e che gli omomorfismi tra gruppi abeliani divisibili privi di torsione sono applicazioni lineari tra gli spazi corrispondenti.

Esercizio 5.23. Sia $n > 1$. Dimostrare che in $\mathbb{Z}/n\mathbb{Z}$ ogni sottogruppo è definibile senza parametri. Quali sono gli elementi definibili di $\mathbb{Z}/n\mathbb{Z}$?

Esercizio 5.24. Dimostrare che:

(i) Se G è un gruppo divisibile privo di torsione di rango finito, allora gli unici sottoinsiemi definibili senza parametri sono $\emptyset$, G, $\{0_G\}$, e $G \setminus \{0_G\}$. In particolare, 0_G è l'unico elemento definibile.

(ii) Ogni groppo $\mathbb{Z}/n\mathbb{Z}$ è definibile in $\mathbb{R}/\mathbb{Z}$, con le identificazioni $\mathbb{Z}/n\mathbb{Z} \cong \{e^{2i\pi k/n} \mid 0 \leq k < n\}$ and $\mathbb{R}/\mathbb{Z} \cong \{z \in \mathbb{C} \mid |z| = 1\}$.

Esercizio 5.25. Sia $\Bbbk$ un campo e $n > 1$. Dimostrare che le :

(i) l'anello $M_{n,n}(\Bbbk)$ delle matrici $n \times n$ è definibilmente interpretabile in $\Bbbk$;

(ii) i gruppi $\mathrm{GL}_n(\Bbbk)$ delle matrici $n \times n$ invertibili, e $\mathrm{SL}_n(\Bbbk)$ delle matrici $n \times n$ con determinante 1 sono definibilmente interpretabili in $\Bbbk$;

(iii) l'insieme delle matrici $n \times n$ nilpotenti, cioè le $A \in M_{n,n}(\Bbbk)$ tali che $A^m = \mathbf{0}$ per qualche $m \in \mathbb{N}$, e l'insieme delle matrici $n \times n$ diagonalizzabili sono definibili in $\Bbbk$;

(iv) i gruppi $\mathrm{PGL}_n(\Bbbk) \stackrel{\text{def}}{=} \mathrm{GL}_n(\Bbbk)/C(\mathrm{GL}_n(\Bbbk))$, e $\mathrm{PSL}_n(\Bbbk) \stackrel{\text{def}}{=} \mathrm{SL}_n(\Bbbk)/C(\mathrm{SL}_n(\Bbbk))$, dove C è il centro, sono definibilmente interpretabili in un quoziente di $\Bbbk$.

Esercizio 5.26. Sia R un anello. Dimostrare che:

(i) R non è definibile nel gruppo $(R[X], +)$;

(ii) l'indeterminata X non è definibile nell'anello $(R[X], +, \cdot)$.

Esercizio 5.27. Sia $\{\xi_n \mid n \in \mathbb{N}\} \subseteq (0;1)$ un insieme $\mathbb{Q}$-linearmente indipendente, e sia $G = \bigcup_n \mathbb{Z}[\xi_0, \ldots, \xi_n]$ dove $\mathbb{Z}[\xi_0, \ldots, \xi_n] = \{\sum_{i=0}^{n} k_i \xi_i \mid k_i \in \mathbb{Z}\}$. Dimostrare che G è un gruppo abeliano densamente ordinato che non è 2-divisibile.

Esercizio 5.28. (i) Dimostrare che un semigruppo $(S, \cdot)$ è un gruppo se e solo se c'è un $e \in S$ che è un'**identità sinistra**, cioè $e \cdot x = x$ per ogni $x \in S$, e per ogni $x \in S$ c'è un $y \in S$ che è un **inverso sinistro relativamente ad** e, cioè $y \cdot x = e$. Analogamente se assumiamo identità e inversi destri.

(ii) Se S ha almeno due elementi e $\forall x, y \in S\ (y \cdot x = x)$ allora $(S, \cdot)$ è un esempio di semigruppo che ha un'identità sinistra, ogni elemento ha un'inverso destro, ma non è un gruppo.

(iii) Trovare un sistema di assiomi per i gruppi, e per i gruppi privi di torsione, nel linguaggio $L_{\text{SEMIGRUPPI}}$.

Esercizio 5.29. Dimostrare che le seguenti teorie del prim'ordine non sono finitamente assiomatizzabili:

(i) la teoria dei gruppi privi di torsione,

(ii) la teoria dei gruppi divisibili abeliani ordinati,

(iii) la teoria degli $\mathbb{Z}$-gruppi,

(iv) la teoria dei gruppi infiniti, degli anelli infiniti, dei campi infiniti, ecc.

(v) la teoria dei campi di caratteristica zero,

(vi) la teoria ACF_p con $p > 0$,

(vii) la teoria ACF_0,

(viii) la teoria ACF.

Concludere che le classi dei

- gruppi di torsione,
- gruppi abeliani ordinati non divisibili,
- gruppi finiti, anelli finiti, campi finiti, ecc.,
- campi di caratteristica positiva,
- campi non algebricamente chiusi di caratteristica fissata o meno,

non sono assiomatizzabili.

Esercizio 5.30. Sia G un gruppo, H un suo sottogruppo, e A un sottoinsieme di G. Il **centralizzante di** A **in** G è

$$C_G(A) = \{g \in G \mid \forall x \in A\,(xg = gx)\}$$

e il **normalizzante di** H **in** G è

$$N_G(H) = \left\{g \in G \mid gHg^{-1} = H\right\}.$$

Dimostrare che se A e H sono definibili con parametri $p_1, \ldots, p_n$, allora anche $C_G(A)$ e $N_G(H)$ sono definibili con i medesimi parametri in G.

Esercizio 5.31. Sia G un gruppo e H un suo sottogruppo. Supponiamo che un qualche laterale sinistro aH sia definibile senza parametri in G. Dimostrare che H è definibile senza parametri.

Esercizio 5.32. Sia L_H il linguaggio introdotto nella Sezione 5.A.3. Trovare un enunciato σ di L_H tale che

$$(G, \cdot, ^{-1}, e, H) \vDash \sigma \quad \text{se e solo se} \quad G/H \text{ è un gruppo abeliano.}$$

Esercizio 5.33. Trovare degli enunciati σ_n nel linguaggio dei gruppi additivi tale che $G \vDash \sigma_n$ se e solo se $G/2G$ ha n elementi. Concludere che $\mathbb{Z}^n$ e $\mathbb{Z}^m$ sono elementarmente equivalenti se e solo se $n = m$.

Esercizio 5.34. Dimostrare che in un anello locale, l'ideale massimale è definibile senza parametri.

Esercizio 5.35. Sia $\Bbbk$ un campo. Dimostrare che:

(i) Se $<$ è un ordinamento che rende $\Bbbk$ un campo ordinato allora $P = \{x \in \Bbbk \mid 0 < x\}$ è il cono degli elementi positivi; viceversa dato un P come sopra, la relazione $x < y \Leftrightarrow y - x \in P$ rende $\Bbbk$ campo ordinato.

(ii) In un campo ordinato valgono le seguenti proprietà
- $\forall x \neq 0 \ \big(x^2 \in P\big)$;
- $1 \in P$ e la caratteristica del campo è 0;
- $x \in P \Rightarrow x^{-1} \in P$;
- $0 < x < y \Rightarrow 0 < y^{-1} < x^{-1}$.

Esercizio 5.36. Supponiamo $\sim$ sia la congruenza su $\mathrm{Term}(L_{\text{GRUPPI A.}})$ che garantisce la struttura di gruppo abeliano. Dimostrare che $\mathrm{Term}/{\sim}$ è isomorfo a $(\mathbb{Z}[X], +)$.

Esercizio 5.37. (i) Verificare in dettaglio che le strutture descritte nella Sezione 5.D.6, cioè i moduli su un anello R, gli spazi vettoriali e le algebre di Lie su un campo $\Bbbk$, sono assiomatizzabili al prim'ordine nel linguaggio L_R e $L_\Bbbk$.

(ii) Dimostrare che la teoria degli spazi vettoriali su $\Bbbk$ è finitamente assiomatizzabile se e solo se $\Bbbk$ è finito. È vero l'analogo enunciato per gli R-moduli?

Esercizio 5.38. Dimostrare che se $\Bbbk$ è finito, allora "i vettori $\mathbf{v}_1, \ldots, \mathbf{v}_n$ sono linearmente indipendenti" è formalizzabile al prim'ordine nel linguaggio $L_\Bbbk$ della Sezione 5.D.6. Concludere che la teoria degli spazi vettoriali su $\Bbbk$ di dimensione fissata n è finitamente assiomatizzabile e che la teoria degli spazi vettoriali su $\Bbbk$ di dimensione infinita è assiomatizzabile, ma non finitamente assiomatizzabile.

Esercizio 5.39. Sia $A \subseteq \mathbb{R}^n$ definibile con parametri $p_1, \ldots, p_k \in \mathbb{R}$, nella struttura $(\mathbb{R}, +, \cdot)$. Dimostrare che $\mathrm{Cl}(A)$ e $\mathrm{Int}(A)$, la chiusura e l'interno di A, sono definibili con i medesimi parametri.

Esercizio 5.40. Sia $\Bbbk$ un campo con almeno tre elementi, sia

$$G = \left\{ \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \mid x, y \in \Bbbk \wedge x \neq 0 \right\},$$

sia $b \in \Bbbk \setminus \{0, 1\}$, e siano

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{e} \quad B = \begin{pmatrix} b & 0 \\ 0 & 1 \end{pmatrix}.$$

Lo scopo di questo esercizio è dimostrare che che il campo $\Bbbk$ è definibilmente interpretabile nel gruppo G mediante i parametri A e B.

Dimostrare che:

(i) i centralizzatori di A e B sono

$$C_G(A) = \left\{ \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \mid y \in \Bbbk \right\} \qquad C_G(B) = \left\{ \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} \mid x \in \Bbbk \setminus \{0\} \right\}$$

e che $C_G(B)$ agisce su $C_G(A)$ per coniugio:

$$\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & y/x \\ 0 & 1 \end{pmatrix};$$

(ii) la funzione

$$j \colon C_G(A) \setminus \{I\} \to C_G(B) \qquad j(M) = N \Leftrightarrow N^{-1}MN = A$$

dove $I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, è definibile in G mediante i parametri A e B, e

$$j \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}$$

(iii) l'operazione $*\colon C_G(A) \times C_G(A) \to C_G(A)$

$$M * N = \begin{cases} j(N)M\,(j(N))^{-1} & \text{se } N \neq I \\ I & \text{altrimenti} \end{cases}$$

è ben definita, commutativa e associativa, ed è definibile in G mediante i parametri A e B;

(iv) $(\Bbbk, +, \cdot, 0, 1)$ è isomorfo a $(C_G(A), \cdot, *, I, A)$. Concludere che il campo $\Bbbk$ è definibilmente interpretabile nel gruppo G mediante i parametri A e B.

Esercizio 5.41. Dimostrare che la classe dei grafi aciclici (vedi pag. 94) non è finitamente assiomatizzabile nel linguaggio dei grafi e che la classe dei grafi che contengono un ciclo non è assiomatizzabile.

Esercizio 5.42. Dimostrare che la classe dei grafi bipartiti è assiomatizzabile, ma non finitamente assiomatizzabile nel linguaggio dei grafi L_{GRAFI}. Concludere che la classe dei grafi che non sono bipartiti non è assiomatizzabile in questo linguaggio.

Esercizio 5.43. Dimostrare che:

(i) se $(V, E) \vDash \Sigma_{\text{GRAFO ALEATORIO}}$, allora V è infinito,

(ii) se $(V, E) \vDash \Sigma_{\text{GRAFO ALEATORIO}}$, allora

$\forall A, B \subseteq V\,(A, B \text{ finiti e disgiunti} \Rightarrow \{v \in V \mid \forall a \in A\,(a\ E\ v) \wedge \forall b \in B\,\neg(b\ E\ v)\} \text{ è infinito})$,

(iii) K_2 soddisfa tutti gli assiomi di $\Sigma_{\text{GRAFO ALEATORIO}}$ eccetto $\boldsymbol{\varepsilon}_{\geq 3}$.

Esercizio 5.44. Il **prodotto tensoriale** $G \times H$ di due grafi $G = (V_G, E_G)$ e $H = (V_H, E_H)$ è il grafo che ha per vertici $V_G \times V_H$ e per spigoli

$$(v_1, w_1)\ E_{G\times H}\ (v_2, w_2) \Leftrightarrow (v_1\ E_G\ v_2 \wedge w_1\ E_H\ w_2)\,.$$

In altre parole, $G \times H$ è il prodotto delle strutture (V_G, E_G) e (V_H, E_H). Dimostrare che $\boldsymbol{\chi}(G \times H) \leq \min(\boldsymbol{\chi}(G), \boldsymbol{\chi}(H))$, dove $\boldsymbol{\chi}$ è il numero cromatico.

Note e osservazioni

Le prime assiomatizzazioni dei gruppi (abeliani e no) mediante una singola equazione, come descritto nella Sezione 5.A.2, sono state individuate da Tarski nel 1938 e da Higman e Neumann nel 1952 — si veda [**MS96**] per un'interessante panoramica di questi risultati classici e degli sviluppi recenti. Il Teorema 5.4 è tratto da [**Rob51**].

Nel 1936, motivato da problemi di teoria dei reticoli (si veda l'Osservazione 8.27), von Neumann introdusse il concetto di anello regolare (Sezione 5.D.2). Poiché il termine *anello regolare* è anche usato per indicare una nozione completamente differente, oggi si preferisce includere *von Neumann* nella loro definizione.

La teoria dei grafi è un'importante ramo della combinatorica e rimandiamo il lettore al libro [**Die05**] per una trattazione esauriente. Il teorema sulla planarità dei grafi che non contengono come minore K_5 o $\mathrm{K}_{3,3}$ è stato dimostrato da Kuratowski e Wagner negli anni 30 del secolo scorso. Il Teorema dei Quattro Colori 5.18 è stato dimostrato nel 1976 da Appel e Haken [**AH76**]. Il grafo aleatorio numerabile è stato inventato nel 1959 da Erdős e Rényi, e indipendentemente da Gilbert. Il Teorema 5.19, dimostrato nel 1930 da Ramsey, è la pietra angolare di una vasta area della combinatorica nota come teoria di Ramsey. Il minimo m che soddisfa l'enunciato del teorema, cioè tale che ogni k-colorazione di K_m ha un sottografo indotto monocromatico isomorfo a K_n si denota con $R(n, k)$, o semplicemente $R(n)$ quando $k = 2$. Si dimostra che $R(2) = 3$, $R(3) = 6$ e $R(4) = 18$. Per valori più grandi di n si conoscono solo delle stime di $R(n)$ — per esempio $43 \leq R(5) \leq 49$ e $102 \leq R(6) \leq 165$. Questa è una situazione simile a quella dell'Esempio 2.5 — se $\mathrm{A}(n)$ è l'affermazione che prese n persone ce ne sono almeno 5 che si conoscono o che sono estranee, allora $\mathrm{A}(43) \vee \mathrm{A}(44) \vee \cdots \vee \mathrm{A}(49)$ e quindi in particolare $\exists n \mathrm{A}(n)$, ma tuttavia non

sappiamo quali delle disgiunzioni sono vere. Il problema di determinare l'esatto valore di $R(n)$ è estremamente difficile e molti esperti di combinatorica ritengono che il valore di $R(6)$ non verrà mai individuato. Dimostreremo il Teorema di Ramsey a pagina 468 nella Sezione 31. L'affermazione che la disuguaglianza nell'Esercizio 5.44 può essere rafforzata in un'uguaglianza, è un problema aperto in teoria dei grafi, noto come congettura di Hedetniemi.

L'Esercizio 5.40 e la Sezione 5.H.7 sono tratti da [**Mar02**].

6. Definibilità negli interi, nei reali e nei complessi

6.A. I numeri naturali.

6.A.1. *L'operazione di successore.* La struttura che consideriamo è $(\mathbb{N}, S)$ dove $S(n) = n + 1$ è il successore di n. Il linguaggio che si usa contiene soltanto un simbolo di funzione unaria, che per semplicità verrà indicata di nuovo con S.

L'elemento 0 è definibile in $(\mathbb{N}, S)$ dato che è l'unico numero che rende vera la formula

$$(\varphi_0(x)) \qquad \forall y\,(S(y) \neq x)\,.$$

Inoltre la funzione S è iniettiva, e per quanto la si iteri non ci riporta mai all'elemento di partenza. In altre parole, la struttura $(\mathbb{N}, S)$ soddisfa l'insieme di enunciati

$$\Sigma_{(\mathbb{N},S)} \quad \begin{cases} \exists! x\, \forall y\,(S(y) \neq x) \\ \forall x, y\,(x \neq y \Rightarrow S(x) \neq S(y)) \\ \forall x (S^{(n)}(x) \neq x) \qquad\qquad (\sigma_n, n \geq 1). \end{cases}$$

Notiamo che σ_m è conseguenza di σ_{mk}, quindi $\Sigma_{(\mathbb{N},S)}$ non è un insieme di assiomi indipendenti. L'insieme dei σ_n non può essere ricondotto ad una lista finita, dato che la struttura

$$\mathbb{N} \cup (\mathbb{Z}/n\mathbb{Z})$$

con l'operazione di successore $x \mapsto x + 1$ soddisfa i primi due enunciati di $\Sigma_{(\mathbb{N},S)}$ e σ_i per $1 \leq i \leq n$, ma non soddisfa σ_n. Quindi per il Teorema 3.10 abbiamo che

Proposizione 6.1. *La teoria $\Sigma_{(\mathbb{N},S)}$ non è finitamente assiomatizzabile.*

Il numero naturale $k > 0$ è l'unico elemento di $(\mathbb{N}, S)$ che soddisfa

$$(\varphi_k(x)) \qquad \exists y(\varphi_0(y) \wedge S^{(k)}(y) = x),$$

dove φ_0 è la formula che definisce l'elemento 0. Quindi ogni insieme finito $\{k_1, \ldots, k_n\} \subseteq \mathbb{N}$ è definibile mediante la formula

$$\varphi_{k_1}(x) \vee \varphi_{k_2}(x) \vee \cdots \vee \varphi_{k_n}(x).$$

Di conseguenza ogni insieme co-finito di naturali (cioè della forma $\mathbb{N} \setminus F$ con F finito) è definibile. Come vedremo nella Sezione 6.A.2, questi sono gli unici insiemi di naturali definibili nella struttura $(\mathbb{N}, S)$.

Sia (M, S_M) un modello di $\Sigma_{(\mathbb{N},S)}$ e sia 0_M l'elemento di M definito dalla $\varphi_0(x)$ qui sopra. La teoria $\Sigma_{(\mathbb{N},S)}$ implica che gli elementi 0_M, $S_M(0_M)$, $S_M(S_M(0_M)), \ldots$ sono tutti distinti, quindi la mappa $F\colon \mathbb{N} \to M$,

$$F(0) = 0_M$$
$$F(n+1) = S_M(F(n))$$

è un monomorfismo $(\mathbb{N}, S) \to (M, S_M)$. Infatti F è suriettiva se e solo se $(\mathbb{N}, S)$ e (M, S_M) sono isomorfi. Un modello (M, S_M) che non sia isomorfo a $(\mathbb{N}, S)$ si dice **non-standard**.

Supponiamo che (M, S_M) sia non-standard. La relazione di equivalenza $\sim$ su $M \setminus \mathrm{ran}(F)$ definita da

$$x \sim y \Leftrightarrow \exists n \in \mathbb{N}\,[x = \underbrace{S_M \circ \cdots \circ S_M}_{n \text{ volte}}(y) \vee y = \underbrace{S_M \circ \cdots \circ S_M}_{n \text{ volte}}(x)]$$

partiziona $M \setminus \mathrm{ran}(F)$ in classi di equivalenza, e dato che 0_M è l'unico elemento non in $\mathrm{ran}(S_M)$, ogni classe di equivalenza è isomorfa a $\mathbb{Z}$. Abbiamo quindi dimostrato:

Proposizione 6.2. *I modelli non standard (M, S_M) di $\Sigma_{(\mathbb{N},S)}$ sono, a meno di isomorfismo, della forma*

$$M = \mathbb{N} \cup (I \times \mathbb{Z})$$

con $I \neq \emptyset$ un insieme arbitrario e $S^M\colon M \to M$ è definita da

$$S^M(x) = \begin{cases} k+1 & \text{se } x = k \in \mathbb{N}, \\ (i, k+1) & \text{se } x = (i,k) \in I \times \mathbb{Z}. \end{cases}$$

Quindi la teoria $\Sigma_{(\mathbb{N},S)}$ non caratterizza $(\mathbb{N}, S)$ meno di isomorfismo.

Osservazioni 6.3. (a) La funzione F qui sopra è definita per ricorsione, e una definizione rigorosa della sua esistenza sarà data nel Teorema 7.3 nella Sezione 7.

(b) La formula che definisce $\sim$ non è una formula del linguaggio di $\Sigma_{(\mathbb{N},S)}$, dato che $S_M^{(n)}(x) \stackrel{\text{def}}{=} S_M \circ \cdots \circ S_M(x)$ è un termine solo quando n è un numero naturale fissato. In altre parole, la relazione $\sim$ non è definibile in $\Sigma_{(\mathbb{N},S)}$.

6.A.2. *Eliminazione dei quantificatori.* Per studiare la struttura della famiglia dei sottoinsiemi definibili di $(\mathbb{N}, S)$ è utile ampliare il linguaggio[5] con un

[5]Il linguaggio così ampliato sarà denotato con L_{D} nella Sezione 7.A.

simbolo di costante 0. Poiché 0 è definibile in $(\mathbb{N}, S)$ ne segue che $X \subseteq \mathbb{N}^k$ è definibile in $(\mathbb{N}, S)$ se e solo se è definibile in $(\mathbb{N}, S, 0)$.

I termini del linguaggio ampliato sono quelli del linguaggio originale, cioè della forma $S^{(n)}(x)$, più quelli contenenti il nuovo simbolo di costante, cioè della forma $S^{(n)}(0)$. Una formula $\varphi(x_1, \ldots, x_n)$ del linguaggio ampliato può essere trasformata in una formula del linguaggio originale $\varphi'(x_1, \ldots, x_n, y)$ rimpiazzando i termini della forma $S^{(k)}(0)$ con $S^{(k)}(y)$. Ne segue che

$$\varphi(x_1, \ldots, x_n) \quad \text{e} \quad \exists y \, (\varphi_0(y) \wedge \varphi'(x_1, \ldots, x_n, y))$$

sono equivalenti modulo $\Sigma_{\mathbb{N},S}$. La struttura ampliata $(\mathbb{N}, S, 0)$ ha gli stessi sottoinsiemi definibili di $(\mathbb{N}, S)$.

D'ora in poi, il linguaggio usato sarà quello ampliato e la teoria $\Sigma_{(\mathbb{N},S)}$ del linguaggio originario contenente solo il simbolo S, è rimpiazzata dalla sua analoga

$$\Sigma_{(\mathbb{N},S,0)} \quad \begin{cases} \forall x \, (S(x) \neq 0) \\ \forall x \, (x \neq 0 \Rightarrow \exists y (S(y) = x)) \\ \forall x, y \, (x \neq y \Rightarrow S(x) \neq S(y)) \\ \forall x (S^{(n)}(x) \neq x) \qquad\qquad (\sigma_n, n \geq 1). \end{cases}$$

Definizione 6.4. Sia T una teoria in un linguaggio contenente costanti. Diremo che T **ammette l'eliminazione debole dei quantificatori** se ad ogni formula φ possiamo associare una formula φ' priva di quantificatori e con le medesime variabili libere, così che φ e φ' sono logicamente equivalenti modulo T. Se questa assegnazione $\varphi \rightsquigarrow \varphi'$ può essere effettuata in modo meccanico, diremo che T **ammette l'eliminazione dei quantificatori**.

Definizione 6.5. Una teoria T per cui esista un algoritmo in grado di stabilire in modo meccanico se un dato enunciato σ sia conseguenza logica di T, si dice **decidibile**.

Le nozioni di *procedimento meccanico* e di *teoria decidibile* sottendono implicitamente che la teoria sia **ricorsivamente assiomatizzata**, cioè che ci siano metodi effettivi per verificare se una stringa di simboli sia una formula del linguaggio in questione e per stabilire se una data formula sia un assioma della teoria.

Proposizione 6.6. *Sia T una teoria ricorsivamente assiomatizzata.*

Se T ammette l'eliminazione (debole) dei quantificatori, e se T è completa per enunciati atomici, cioè se per ogni enunciato atomico σ

$$T \models \sigma \text{ oppure } T \models \neg\sigma,$$

allora T è completa.

Se T ammette l'eliminazione dei quantificatori, e se $\hat{A}$ T è decidibile per enunciati atomici, cioè se per ogni enunciato atomico σ è possibile stabilire in modo meccanico se $T \models \sigma$ oppure $T \models \neg\sigma$, allora T è decidibile.

Dimostrazione. Dato un enunciato σ, sia θ un enunciato privo di quantificatori logicamente equivalente modulo T a σ. Poiché θ è combinazione booleana di formule atomiche il risultato segue. □

Osservazioni 6.7. (a) La richiesta nella Definzione 6.4 che il linguaggio di T contenga costanti è necessaria per poter associare ad un enunciato un enunciato privo di quantificatori.

(b) La richiesta nella Proposizione 6.6 che $T \models \sigma$ oppure $T \models \neg\sigma$ per ogni enunciato atomico σ, non può essere rimossa (Esercizio 6.49).

(c) Vedremo nel Capitolo VI che una teoria ricorsivamente assiomatizzata e completa in un linguaggio con una quantità finita di simboli non logici è sempre decidibile.

Il seguente criterio è utile per verificare che una teoria ammette l'eliminazione debole dei quantificatori.

Lemma 6.8. *Sia T una teoria del prim'ordine. Le seguenti condizioni sono equivalenti:*

(a) *T ammette l'eliminazione debole dei quantificatori,*

(b) *ad ogni formula della forma $\exists x\psi$, con ψ priva di quantificatori, posiamo associare una formula θ priva di quantificatori e con le medesime variabili libere di $\exists x\psi$ e tale che $\exists x\psi$ e θ sono logicamente equivalenti modulo T,*

(c) *come* (b)*, ma con ψ della forma $\alpha_1 \wedge \cdots \wedge \alpha_n$ e α_i atomica o negazione di una formula atomica.*

Se l'assegnazione $\exists x\psi \rightsquigarrow \theta$ in (b) *e* (c) *è effettiva, allora possiamo rafforzare la condizione* (a)*:*

(a′) *T ammette l'eliminazione dei quantificatori.*

Dimostrazione. Chiaramente (a) ⇒ (b) ⇒ (c).

(c) ⇒ (b): Se ψ è priva di quantificatori, possiamo supporre sia in forma normale disgiuntiva (Sezione 3.C.1), cioè della forma $\varphi_1 \vee \cdots \vee \varphi_k$ con ogni φ_i una congiunzione di formule atomiche o negazioni di formule atomiche. Ne segue che $\exists x\psi$ è logicamente equivalente a $(\exists x\varphi_1)\vee\cdots\vee(\exists x\varphi_k)$, quindi, per (c), è logicamente equivalente modulo T ad una formula priva di quantificatori θ con le medesime variabili libere di $\exists x\psi$.

(b) ⇒ (a): È sufficiente dimostrare che per ogni φ in forma prenessa c'è una formula φ' priva di quantificatori, logicamente equivalente a φ modulo

T e con le stesse variabili libere. La dimostrazione è per induzione sulla complessità di φ.

Se φ è priva di quantificatori non c'è nulla da dimostrare. Se φ è $\exists x\psi$, allora per ipotesi induttiva c'è una formula priva di quantificatori ψ con le stesse variabili libere di ψ, e logicamente equivalente a ψ modulo T. Allora φ è logicamente equivalente a $\exists x\psi$ modulo T, e per ipotesi c'è una formula priva di quantificatori θ con le stesse variabili libere di $\exists x\psi$ e logicamente equivalente a $\exists x\psi$ modulo T. Quindi θ è la formula richiesta. Se φ è $\forall x\psi$, allora è logicamente equivalente a $\neg\exists x\neg\psi$, quindi per il caso precedente c'è una formula priva di quantificatori θ, con le stesse variabili libere di $\exists x\neg\psi$, e logicamente equivalente a $\exists x\neg\psi$ modulo T. Allora $\neg\theta$ è la formula richiesta. □

Teorema 6.9. *La teoria $\Sigma_{(\mathbb{N},S,0)}$ ammette l'eliminazione dei quantificatori.*

Osservazione 6.10. Il Teorema 6.9 non vale se si utilizza il linguaggio con soltanto il simbolo S. Per esempio la formula $\varphi_0(x)$ che definisce lo 0 non è logicamente equivalente a nessuna formula priva di quantificatori.

Ogni enunciato σ del linguaggio contenente S e 0 è equivalente modulo $\Sigma_{(\mathbb{N},S,0)}$ ad un enunciato privo di quantificatori σ', vale a dire una combinazione booleana di formule della forma $S^{(n)}(0) = S^{(m)}(0)$, ed è immediato verificare che fissato un enunciato atomico, lui o la sua negazione è conseguenza logica di $\Sigma_{(\mathbb{N},S,0)}$. Quindi:

Corollario 6.11. *Le teorie $\Sigma_{(\mathbb{N},S,0)}$ e $\Sigma_{(\mathbb{N},S)}$ sono complete.*

Il resto di questa sezione è dedicato alla dimostrazione del Teorema 6.9.

Una formula atomica è un'equazione dei seguenti tipi:

tipo 1: $S^{(n)}(x) = S^{(m)}(y)$, con x e y variabili distinte,

tipo 2: $S^{(n)}(x) = S^{(m)}(0)$,

tipo 3: $S^{(n)}(x) = S^{(m)}(x)$,

tipo 4: $S^{(n)}(0) = S^{(m)}(0)$.

L'assioma $\forall x, y\,(x \neq y \Rightarrow S(x) \neq S(y))$ implica che

- le equazioni di tipo 1 sono logicamente equivalenti modulo $\Sigma_{(\mathbb{N},S,0)}$ alla formula '$S^{(k)}(x) = y$' oppure a '$x = y$' oppure a '$x = S^{(k)}(y)$', con $k > 0$, a seconda che n sia maggiore, o uguale, o minore di m;
- le equazioni di tipo 2 sono logicamente equivalenti modulo $\Sigma_{(\mathbb{N},S,0)}$ a '$x = 0$' oppure a '$S^{(k)}(x) = 0$' oppure a '$x = S^{(k)}(0)$', con $k > 0$;
- le equazioni di tipo 3 sono logicamente equivalenti modulo $\Sigma_{(\mathbb{N},S,0)}$ a '$S^{(k)}(x) = x$' con $k \geq 0$;

- infine quelle di tipo 4 sono logicamente equivalenti modulo $\Sigma_{(\mathbb{N},S,0)}$ a '$S^{(k)}(0) = 0$' con $k \geq 0$.

Prima di proseguire con la dimostrazione del Teorema 6.9, dimostriamo il seguente risultato.

Proposizione 6.12. *Dato un enunciato privo di quantificatori, o lui o la sua negazione discendono logicamente da* $\Sigma_{(\mathbb{N},S,0)}$.

Infatti c'è un algoritmo che, dato un enunciato privo di quantificatori σ, *stabilisce se* $\Sigma_{(\mathbb{N},S,0)} \models \sigma$ *oppure se* $\Sigma_{(\mathbb{N},S,0)} \models \neg\sigma$.

Dimostrazione. Se σ è atomico, allora è una formula di tipo 4, quindi è logicamente equivalente modulo $\Sigma_{(\mathbb{N},S,0)}$ a $S^{(k)}(0) = 0$, per qualche $k \geq 0$. Se $k = 0$ allora $\Sigma_{(\mathbb{N},S,0)} \models \sigma$, e se $k > 0$ allora $\Sigma_{(\mathbb{N},S,0)} \models \neg\sigma$ per l'assioma σ_k. Un ragionamento analogo si applica agli enunciati che sono negazione di enunciati atomici. Dato che un enunciato privo di quantificatori può essere messo in forma normale disgiuntiva, il ragionamento precedente può essere modificato e fornire un metodo effettivo per stabilire se $\Sigma_{(\mathbb{N},S,0)} \models \sigma$ oppure $\Sigma_{(\mathbb{N},S,0)} \models \neg\sigma$. □

Corollario 6.13. *Le teorie* $\Sigma_{(\mathbb{N},S,0)}$ *e* $\Sigma_{(\mathbb{N},S)}$ *sono decidibili.*

Ritorniamo alla dimostrazione del Teorema 6.9. Gli assiomi $\forall x\,(S(x) \neq 0)$ e σ_k implicano che se φ è una formula atomica o la negazione di una formula atomica, allora φ è logicamente equivalente modulo $\Sigma_{(\mathbb{N},S,0)}$ ad una formula con le medesime variabili φ' della seguente lista:

(6.1)

$x = S^{(m)}(y)$	$x \neq S^{(m)}(y)$
$x = S^{(m)}(0)$	$x \neq S^{(m)}(0)$
$x = x$	$x \neq x$
$0 = 0$	$0 \neq 0$

dove $m \geq 0$. Chiameremo le formule nella prima colonna *uguaglianze*, quelle della seconda colonna *disuguaglianze*.

Lemma 6.14. *Se* θ *è una congiunzione di formule atomiche o negazione di formule atomiche*

$$\psi_1 \wedge \cdots \wedge \psi_n,$$

allora $\exists x\theta$ *è logicamente equivalente modulo* $\Sigma_{(\mathbb{N},S,0)}$ *ad una formula* θ' *priva di quantificatori con le medesime variabili libere di* $\exists x\theta$.

Dimostrazione. Supponiamo $n = 1$, vale a dire θ è una formula atomica o negazione di una formula atomica. Per quanto detto possiamo supporre che θ sia una formula della lista (6.1). Se la variabile x non occorre in θ, allora $\exists x\theta$ è logicamente equivalente a θ che è priva di quantificatori, quindi

possiamo supporre che x occorra in θ. Il risultato discende dalla seguente tabella:

Se θ è...	allora $\exists x\theta$ è equivalente a...
$x = S^{(m)}(0)$	$0 = 0$
$x \neq S^{(m)}(0)$	$0 = 0$
$x = x$	$0 = 0$
$x \neq x$	$0 \neq 0$
$S^{(m)}(x) = y$	$y \neq 0 \wedge \cdots \wedge y \neq S^{(m-1)}(0)$
$x = S^{(m)}(y)$	$y = y$
$x \neq S^{(m)}(y)$	$y = y$
$S^{(m)}(x) \neq y$	$y = y$

dove *equivalente* significa *logicamente equivalente modulo* $\Sigma_{(\mathbb{N},S,0)}$. La verifica delle equivalenze è immediata. Per esempio per ogni y ci sono infiniti x tali che $S^{(m)}(x) \neq y$ — più precisamente: fissato un $M \vDash \Sigma_{(\mathbb{N},S,0)}$ ed un elemento $b \in M$, l'insieme

$$\mathbf{T}^M_{S^{(m)}(x)\neq y} \cap M \times \{b\} \tag{6.2}$$

è cofinito e quindi non vuoto; poiché b è arbitrario segue che $\mathbf{T}^M_{\exists x(S^{(m)}(x)\neq y)} = M$.

Supponiamo ora $n > 1$ e siano $y_1, \ldots, y_k$ le variabili distinte da x che compaiono in θ. Se la variabile x non occorre in qualcuna delle ψ_i, per esempio se non occorre in ψ_1, allora $\exists x\theta$ è logicamente equivalente a $\psi_1 \wedge \exists x\,(\psi_2 \wedge \cdots \wedge \psi_n)$, e per ipotesi induttiva $\exists x\,(\psi_2 \wedge \cdots \wedge \psi_n)$ è logicamente equivalente ad una formula priva di quantificatori, da cui segue il risultato. Se qualcuna delle ψ_i fosse

$$x = x \qquad \text{oppure} \qquad S^{(k)}(x) \neq 0 \quad (k > 0) \tag{6.3}$$

allora θ sarebbe logicamente equivalente modulo $\Sigma_{(\mathbb{N},S,0)}$ alla formula ottenuta rimuovendo ψ_i dalla congiunzione, e potremmo applicare l'ipotesi induttiva. Similmente se qualcuna delle ψ_i fosse

$$x \neq x \qquad \text{oppure} \qquad S^{(k)}(x) = 0 \quad (k > 0) \tag{6.4}$$

allora $\exists x\theta$ sarebbe logicamente equivalente a $0 \neq 0 \wedge \bigwedge_{1\leq i\leq k}(y_i = y_i)$. Possiamo quindi supporre che

- la variabile x occorra in ogni ψ_i,
- nessuna ψ_i sia della forma (6.3) o (6.4),

- ogni ψ_i sia della forma

$$\begin{array}{ll} S^{(m_i)}(x) = y & S^{(m_i)}(x) \neq y \\ x = S^{(m_i)}(y) & x \neq S^{(m_i)}(y) \\ x = S^{(m_i)}(0) & x \neq S^{(m_i)}(0) \end{array}$$

dove $m_i \geq 0$ e y è una delle $y_1, \ldots, y_k$.

Caso 1: le ψ_i sono tutte disuguaglianze. Distinguiamo due casi.

- $\exists x\theta$ è un enunciato. Allora le ψ_i sono della forma $x \neq S^{(m_i)}(0)$, quindi l'enunciato $\exists x\theta$ è vero in ogni modello di $\Sigma_{(\mathbb{N},S,0)}$: basta prendere come x l'elemento $S^{(m)}(0)$ con m sufficientemente grande. In altre parole: $\exists x\theta$ è logicamente equivalente modulo $\Sigma_{(\mathbb{N},S,0)}$ a $0 = 0$.
- $\exists x\theta$ non è un enunciato. Allora le ψ_i sono della forma $S^{(m_i)}(x) \neq y_j$ o della forma $S^{(m_i)}(y_j) \neq x$ con $j = 1, \ldots, k$, e magari alcune delle ψ_i sono della forma $x \neq S^{(m)}(0)$. Ragionando come fatto per la formula (6.2), per ogni $M \vDash \Sigma_{(\mathbb{N},S,0)}$ e per ogni $b_1, \ldots, b_k \in M$

$$\mathbf{T}^M_{\theta(x,y_1,\ldots,y_k)} \cap M \times \{(b_1, \ldots, b_k)\}$$

è cofinito, in quanto intersezione di una quantità finita di insiemi cofiniti. Ne segue che $\mathbf{T}^M_{\exists x\theta} = M^k$, vale a dire: $\exists x\theta$ è logicamente equivalente modulo $\Sigma_{(\mathbb{N},S,0)}$ a $\bigwedge_{1\leq i\leq k}(y_i = y_i)$.

Il risultato vale nel Caso 1, quindi possiamo supporre che almeno una delle ψ_i sia un'uguaglianza.

Caso 2: C'è almeno una ψ_i della forma $x = t$ dove t è $S^{(m)}(0)$ oppure $S^{(m)}(y_h)$, con $1 \leq h \leq k$. Allora $\exists x\theta$ è logicamente equivalente modulo $\Sigma_{(\mathbb{N},S,0)}$ alla formula θ'

$$\bigwedge_{\substack{1\leq j\leq n \\ j\neq i}} \psi_j[\![t/x]\!]$$

ottenuta rimuovendo ψ_i dalla congiunzione θ e sostituendo il termine t nelle altre ψ_j al posto di x.

Il risultato vale nel Caso 2 e possiamo quindi supporre:

Caso 3: C'è almeno una ψ_i della forma $S^{(m_i)}(x) = y_h$, con $1 \leq h \leq k$. Sia i il primo indice siffatto e siano $j_1, \ldots, j_p$ gli altri indici j tali che ψ_j è della forma $S^{(m_j)}(x) = t_j$, che è quindi logicamente equivalente modulo $\Sigma_{(\mathbb{N},S,0)}$ a $S^{m_j}(y_h) = S^{m_i}(t_j)$. Allora $\exists x\theta$ è logicamente equivalente modulo $\Sigma_{(\mathbb{N},S,0)}$ alla formula θ' ottenuta rimuovendo la formula ψ_i dalla congiunzione θ e sostituendo $\psi_{j_1}, \ldots, \psi_{j_p}$ con le formule $S^{(m_{j_1})}(y_h) = S^{(m_i)}(t_{j_1}), \ldots, S^{(m_{j_p})}(y_h) = S^{(m_i)}(t_{j_p})$.

Poiché in entrambi i Casi 2 e 3 la formula θ' è priva di quantificatori e ha le stesse variabili libere di $\exists x\theta$, il risultato è dimostrato. □

Questo conclude la dimostrazione del Teorema 6.9.

Mediante il Teorema 6.9 possiamo analizzare la struttura dei definibili in $(\mathbb{N}, S)$ e quindi in $(\mathbb{N}, S, 0)$.

Esercizio 6.15. Dimostrare che i sottoinsiemi di $\mathbb{N}$ definibili in $(\mathbb{N}, S, 0)$ sono tutti e soli gli insiemi finiti e gli insiemi cofiniti.

Per descrivere i sottoinsiemi definibili di dimensione due conviene introdurre la seguente definizione: sia $\mathcal{D}$ la più piccola famiglia dei sottoinsiemi di $\mathbb{N}^2$ contenente

- tutti i punti di $\mathbb{N}^2$,
- le linee diagonali $\{(n, m) \in \mathbb{N}^2 \mid m = n + k\}$, per qualche $k \in \mathbb{Z}$, oppure
- le linee orizzontali e verticali $\{(n, k) \in \mathbb{N}^2 \mid n \in \mathbb{N}\}$ e $\{(k, n) \in \mathbb{N}^2 \mid n \in \mathbb{N}\}$, per qualche $k \in \mathbb{N}$,

e chiusa per intersezioni, unioni e complementi.

Esercizio 6.16. Dimostrare che:

(i) $\mathcal{D}$ è la famiglia dei sottoinsiemi di $\mathbb{N}^2$ definibili in $(\mathbb{N}, S)$,

(ii) gli insiemi in $\mathcal{D}$ sono della forma $P \triangle L$ oppure $\mathbb{N}^2 \setminus (P \triangle L)$ dove P è un insieme finito (eventualmente vuoto) di punti e L è un insieme finito (eventualmente vuoto) di linee,

(iii) $\{(n, m) \mid n < m\} \notin \mathcal{D}$.

Osservazione 6.17. L'eliminazione dei quantificatori per una teoria T fornisce importanti informazioni sui sottoinsiemi definibili di *ogni* modello di T. Per esempio il Teorema 6.9 mostra che, dato un modello non-standard $M = \mathbb{N} \cup (I \times \mathbb{Z})$ di $\Sigma_{(\mathbb{N},S,0)}$, i sottoinsiemi definibili con parametri $p_1, \ldots, p_n \in M$ di dimensione 1, sono gli insiemi finiti della forma $F \subseteq \mathbb{N} \cup \{p_1, \ldots, p_n\}$ e i loro complementi. In particolare nessun elemento di $M \setminus \mathbb{N}$ è definibile senza parametri e $\mathbb{N}$ non è definibile, neanche con parametri.

Nel Capitolo VI vedremo che una teoria completa e ricorsivamente assiomatizzata è decidibile, e dimostreremo (Sezione 32.A.1) il seguente criterio per verificare che una teoria ammette l'eliminazione.

Proposizione 6.18. *Sia T una teoria del prim'ordine nel linguaggio L con costanti. Supponiamo che per ogni coppia M, N di modelli di T e per ogni isomorfismo $F\colon M' \to N'$ dove M' è una sottostruttura di M e N' è una sottostruttura di N,*

$$M \vDash \exists y \varphi[a_1, \ldots, a_n] \Leftrightarrow N \vDash \exists y \varphi[F(a_1), \ldots, F(a_n)],$$

dove $\varphi(y, x_1, \ldots, x_n)$ è congiunzione di formule che sono atomiche o negazione di formule atomiche, e $a_1, \ldots, a_n \in M'$.

Allora T ammette l'eliminazione debole dei quantificatori.

Ci sono teorie T che non hanno costanti e che tuttavia ammettono l'eliminazione dei quantificatori per formule che non sono enunciati, cioè ad ogni formula φ non chiusa possiamo associare una formula φ' priva di quantificatori e con le medesime variabili libere, così che φ e φ' sono logicamente equivalenti modulo T. In questo caso diremo che T ammette l'eliminazione dei quantificatori per formule non chiuse e la Proposizione 6.18 qui sopra continua a valere in questo caso.

Oltre a $\Sigma_{(\mathbb{N},S)}$, ci sono altre teorie che ammettono l'eliminazione dei quantificatori:

- la teoria dei naturali con l'ordinamento (Esercizio 6.48) o con la somma (pag. 114),
- la teoria degli ordini lineari densi senza primo o ultimo elemento (Esercizio 6.67),
- la teoria dei campi algebricamente chiusi di caratteristica fissata (Teorema 6.42),
- la teoria dei campi reali chiusi (Sezione 6.D.1).

6.A.3. *L'ordinamento.* Consideriamo i numeri naturali $\mathbb{N}$ con l'ordinamento — cioè la struttura $(\mathbb{N}, <)$. La funzione successore è definibile mediante la formula

$$(\sigma(x,y)) \qquad x < y \wedge \neg\exists z\,(x < z \wedge z < y)\,,$$

quindi gli insiemi definibili in $(\mathbb{N}, <)$ sono esattamente quelli di $(\mathbb{N}, <, S, 0)$. La teoria $\Sigma_{(\mathbb{N},<,S,0)}$ è ottenuta aggiungendo a $\Sigma_{(\mathbb{N},S,0)}$ gli enunciati che asseriscono che $<$ è un ordine stretto

$$\neg\exists x\,(x < x) \tag{6.5a}$$

$$\forall x, y, z\,(x < y \wedge y < z \Rightarrow x < z) \tag{6.5b}$$

$$\forall x, y\,(x < y \vee x = y \vee y < x)\,, \tag{6.5c}$$

dove $\vee$ è la disgiunzione esclusiva (vedi pag. 6), e l'enunciato che asserisce che $S(x)$ è il successore immediato di x

$$\forall x, y\,(x < S(x) \wedge \neg\,(x < y \wedge y < S(x)))\,. \tag{6.5d}$$

Gli enunciati $\forall x(S^{(n)}(x) \neq x)$ sono conseguenza della transitività dell'ordinamento, quindi $\Sigma_{(\mathbb{N},<,S,0)}$ è finitamente assiomatizzabile. La teoria $\Sigma_{(\mathbb{N},<)}$ ammette l'eliminazione dei quantificatori (Esercizio 6.48): ne segue che $\Sigma_{(\mathbb{N},<)}$ e $\Sigma_{(\mathbb{N},<,S,0)}$ sono teorie complete e decidibili. Anche in questo caso, gli unici sottoinsiemi di $\mathbb{N}$ definibili in $(\mathbb{N}, <, S, 0)$ o, equivalentemente in $(\mathbb{N}, <)$, sono

quelli finiti e quelli cofiniti. La formula $x < y$ può essere descritta tramite S dalle espressioni

$$\exists k(y = S(S^{(k)}(x)))$$

oppure da

$$y = S(x) \vee y = S(S(x)) \vee y = S(S(S(x))) \vee \dots,$$

ma in entrambi i casi si tratta di pseudo-formule e quindi non possiamo concludere che l'ordinamento sia definibile in $(\mathbb{N}, S)$. Infatti per l'Esercizio 6.16 l'ordinamento $<$ non è definibile in $(\mathbb{N}, S)$.

Mediante un'immediata generalizzazione della dimostrazione della Proposizione 6.2 si ottiene:

Proposizione 6.19. *I modelli non-standard (M, S_M) di $\Sigma_{(\mathbb{N},<)}$ sono, a meno di isomorfismo, della forma*

$$M = \mathbb{N} \cup (I \times \mathbb{Z})$$

con $(I, \prec)$ un insieme arbitrario linearmente ordinato, e $<_M$ è l'ordinamento solito su $\mathbb{N}$, ogni $n \in \mathbb{N}$ precede ogni $(i, a) \in I \times \mathbb{Z}$, e

$$(i, a) <_M (j, b) \Leftrightarrow i \prec j \vee [i = j \wedge a < b].$$

Dato che ogni insieme I può essere linearmente ordinato,[6] ogni modello di $\Sigma_{(\mathbb{N},S)}$ può essere trasformato in un modello di $\Sigma_{(\mathbb{N},<)}$.

6.A.4. *L'addizione.* Consideriamo ora la struttura $(\mathbb{N}, +)$. L'ordinamento $x < y$ è definito dalla formula

$$x \neq y \wedge \exists z\,(x + z = y)\,,$$

quindi gli insiemi definibili nella struttura $(\mathbb{N}, +, <, S, 0)$ sono quelli nella struttura $(\mathbb{N}, +)$. Per ogni $n \geq 2$, la relazione $\equiv_n$ di congruenza modulo n è definibile in $(\mathbb{N}, +)$ mediante la formula

$(\chi_n(x, y))$ $$\exists z\,\big(x + \underbrace{z + \dots + z}_{n} = y \ \vee\ y + \underbrace{z + \dots + z}_{n} = x\big),$$

quindi gli insiemi definibili nella struttura $(\mathbb{N}, +, <, S, 0, \equiv_2, \equiv_3, \dots)$ sono quelli definibili in $(\mathbb{N}, +)$.

Definizione 6.20. L'**aritmetica di Presburger** è la teoria $\Sigma_{(\mathbb{N},+,<,S,0)}$ nel linguaggio con i simboli $+, <, S, 0$ e che ha per assiomi:

- gli assiomi per gli ordini lineari (gli enunciati (6.5) di pagina 112),
- gli assiomi per i monoidi commutativi (gli enunciati (3.9a), (3.9b), (3.9c) di pagina 38)
- $\forall x, y, z\,(x + z = y + z \Rightarrow x = y)$ (legge di cancellazione)

[6] Per lo meno se si assume qualche forma dell'Assioma di Scelta — si veda la Sezione 25.D.

- $\forall x, y\,(x + y = 0 \Rightarrow x = 0 \wedge y = 0)$ (legge di positività)
- $\forall x, y\,(x < y \Leftrightarrow x \neq y \wedge \exists z\,(x + z = y))$ (legge di compatibilità)
- gli infiniti enunciati

$$(\pi'_n) \qquad \forall x \exists! y\,(\chi_n(x, y) \wedge y < S^{(n)}(0))$$

per ogni $n \leq 2$.

Osserviamo che l'assioma π'_n può essere riscritto come $\forall x \exists! y\, \exists! z\,(x = nz + y \wedge y < S^{(n)}(0))$, e che è l'assioma π_n per gli $\mathbb{Z}$-gruppi (vedi pag. 78) riformulato per la struttura $(\mathbb{N}, +, <, S, 0, \equiv_2, \equiv_3, \dots)$.

La teoria $\Sigma_{(\mathbb{N},+,S,0)}$ non ammette l'eliminazione dei quantificatori, dato che la formula $\chi_n(x, y)$ non è equivalente ad una qualche formula aperta con variabili libere x e y. In un certo senso queste sono le uniche ostruzioni per l'eliminazione dei quantificatori. Sia $\Sigma_{(\mathbb{N},+,\equiv)}$ la teoria (che continuiamo a chiamare aritmetica di Presburger) nel linguaggio esteso mediante infiniti nuovi simboli di relazione binaria $\equiv_n$ $(n \geq 2)$ e che ha per assiomi gli assiomi di $\Sigma_{(\mathbb{N},+)}$ più gli infiniti enunciati

$$\forall x, y\ (x \equiv_n y \Leftrightarrow \chi_n(x, y))$$

per ogni $n \leq 2$. Allora $\Sigma_{(\mathbb{N},+,\equiv)}$ ammette l'eliminazione dei quantificatori e ogni enunciato atomico è decidibile [**End01**, pag. 197–201]. Quindi le teorie $\Sigma_{(\mathbb{N},+,\equiv)}$ e $\Sigma_{(\mathbb{N},+)}$ sono complete e decidibili.

Ogni sottoinsieme finito o cofinito di $\mathbb{N}$ è definibile in $(\mathbb{N}, +)$, dato che ogni insieme definibile in $(\mathbb{N}, <)$ è anche definibile in $(\mathbb{N}, +)$. Oltre ai sottoinsiemi finiti e cofiniti è anche possibile definire ogni insieme periodico, cioè ogni progressione aritmetica. Infatti $\{a \cdot n + b \mid n \in \mathbb{N}\}$ è definito da

$$x \equiv_a S^{(b)}(0).$$

Dato che la famiglia dei sottoinsiemi definibili è chiusa per differenze simmetriche, ogni sottoinsieme di $\mathbb{N}$ che sia definitivamente periodico è definibile in $(\mathbb{N}, +)$. Mediante il metodo dell'eliminazione dei quantificatori si dimostra che gli insiemi definibili in $(\mathbb{N}, +)$ di rango 1, sono esattamente i sottoinsiemi di $\mathbb{N}$ definitivamente periodici e i loro complementi. L'addizione non è definibile né in $(\mathbb{N}, <)$ né in $(\mathbb{N}, S)$: se lo fosse, allora l'insieme dei numeri pari sarebbe definibile in queste strutture, contrariamente al fatto che i sottoinsiemi di $\mathbb{N}$ definibili in $(\mathbb{N}, <)$ o in $(\mathbb{N}, S)$ sono gli insiemi finiti e i cofiniti.

Analizziamo ora i modelli nonstandard di $\Sigma_{(\mathbb{N},+)}$. Per le leggi di positività e compatibilità 0 è il minimo di $(M, <)$, per la legge di cancellazione l'elemento z di cui si asserisce l'esistenza nella legge di compatibilità è unico.

Proposizione 6.21. *$M \vDash \Sigma_{(\mathbb{N},+,\equiv)}$ se e solo se $(M, +)$ è (isomorfo a)*

$$G^+ = \{g \in G \mid 0_G = g \vee 0_G <_G g\},$$

dove G è uno $\mathbb{Z}$-gruppo.

Dimostrazione. Sia $(M, +, <, S, 0, \equiv_2, \equiv_3, \dots)$ un modello di $\Sigma_{(\mathbb{N},+,\equiv)}$, e supponiamo che $F\colon M \setminus \{0\} \to M'$ sia una biezione e che M' sia un insieme disgiunto da M. Allora mediante F si possono definire $+$ e $<$ su M' ponendo

$$\forall x, y \in M \setminus \{0\}\ [F(x) + F(y) = F(x + y) \wedge (F(x) < F(y) \Leftrightarrow y < x)]\,.$$

L'ordinamento $<$ può essere esteso ad un ordine totale su $G \stackrel{\text{def}}{=} M \cup M'$ stabilendo che gli elementi di M' vengano prima degli elementi in M. Per definire $+$ su G è sufficiente definire $x + y$ quando $x \in M'$ e $y \in M$ o quando $x \in M$ e $y \in M'$. Se imponiamo che $x + y = y + x$ possiamo ricondurci al caso in cui $x \in M'$ e $y \in M$. Se $F^{-1}(x) = y$, allora poniamo $x + y = 0$, quindi possiamo supporre che $F^{-1}(x) < y$ oppure che $y < F^{-1}(x)$. Se vale il primo caso allora $F^{-1}(x) + z = y$ per un unico $z \in M \setminus \{0\}$, e poniamo $x + y = z$; se vale il secondo caso allora $y + z = F^{-1}(x)$ per un unico $z > 0$, e poniamo $x + y = F(z)$. È facile verificare che $(G, +, <)$ è uno $\mathbb{Z}$-gruppo.

L'altra direzione, che G^+ è un modello dell'aritmetica di Presburger per ogni $\mathbb{Z}$-gruppo G, è lasciata al lettore. □

Se G è uno $\mathbb{Z}$-gruppo e $Z = \{k1_G \mid k \in \mathbb{Z}\}$, il quoziente $(G/Z, <)$ è un ordine lineare denso privo del primo e ultimo elemento, quindi l'ordinamento in un modello non standard dell'aritmetica di Presburger è della forma $\mathbb{N} \cup L \times \mathbb{Z}$, con L ordine lineare denso privo del primo e ultimo elemento. Un esempio concreto di modello non standard dell'aritmetica di Presburger è $\mathbb{N} \cup \mathbb{Q} \times \mathbb{Z}$ con l'operazione di addizione definita da $n + (q, z) = (q, z + n)$ e $(q_1, z_1) + (q_2, z_2) = (q_1 + q_2, z_1 + z_2)$ (Esercizio 6.46).

6.A.5. *Moltiplicazione, divisibilità e coprimalità.* Consideriamo le strutture $(\mathbb{N}, \perp)$, $(\mathbb{N}, |)$ e $(\mathbb{N}, \cdot)$, dove $\perp$ è il predicato binario di coprimalità, cioè

$$x \perp y \Leftrightarrow \forall z\,(z \mid x \wedge z \mid y \Rightarrow z = 1)$$

e $|$ è il predicato di divisibilità. Chiaramente la relazione $|$ è definibile in $(\mathbb{N}, \cdot)$, mentre la definibilità della relazione $\perp$ in $(\mathbb{N}, |)$ segue dalla definibilità del numero 1 nella struttura $(\mathbb{N}, |)$ (Esercizio 3.55). Il viceversa non vale, cioè $|$ non è definibile in $(\mathbb{N}, \perp)$ (Esercizio 6.45) e $\cdot$ non è definibile in $(\mathbb{N}, |)$ (Sezione 32.C.1).

Anche per la struttura $(\mathbb{N}, \cdot)$ si può trovare un sistema di assiomi completo, noto come **aritmetica di Skolem**, che ammette l'eliminazione dei quantificatori [**Smo91**].

Per l'Esercizio 3.55 l'insieme dei numeri primi è definibile in $(\mathbb{N}, |)$ e quindi in $(\mathbb{N}, \cdot)$. L'insieme dei numeri primi non è definitivamente periodico, quindi non è definibile in $(\mathbb{N}, +)$.

Corollario 6.22. *La relazione di divisibilità e la moltiplicazione non sono definibili in* $(\mathbb{N}, +)$.

Esercizio 6.23. Usare l'equivalenza

$$z = 0 \vee (x + y) = z \Leftrightarrow (xz + 1)(yz + 1) = z^2(xy + 1) + 1$$

per verificare che l'addizione è definibile mediante una formula priva di quantificatori tanto nella struttura $(\mathbb{N}, S, \cdot)$ quanto nella struttura $(\mathbb{Z}, S, \cdot)$.

Il prossimo risultato mostra che la funzione successore non può essere rimossa.

Proposizione 6.24. *L'insieme* $\{(n, m, k) \in \mathbb{N}^3 \mid n + m = k\}$ *non è definibile nella struttura* $(\mathbb{N}, \cdot)$.

Dimostrazione. Sia F una biezione sull'insieme dei numeri primi. Ogni naturale maggiore di 1 può essere espresso in un unico modo come $p_1^{n_1} \cdots p_k^{n_k}$ con $p_1 < \cdots < p_k$ primi, quindi F si estende ad una biezione di $\mathbb{N}$ ponendo $F(0) = 0$ e $F(p_1^{n_1} \cdots p_k^{n_k}) = F(p_1)^{n_1} \cdots F(p_k)^{n_k}$. È immediato verificare che $F\colon (\mathbb{N}, \cdot) \to (\mathbb{N}, \cdot)$ è un automorfismo, ma $F(n + m) \neq F(n) + F(m)$ se F non è l'identità. □

Da quanto visto le strutture $(\mathbb{N}, S)$ e $(\mathbb{N}, |)$ sono le meno espressive, tra quelle considerate, ma se le amalgamiamo in un'unica struttura $(\mathbb{N}, S, |)$ possiamo definire la somma e il prodotto, e quindi anche l'ordinamento (Esercizio 6.66). Riassumendo

Proposizione 6.25. (a) *S non è definibile in* $(\mathbb{N}, |)$ *e $|$ non è definibile in* $(\mathbb{N}, S)$.

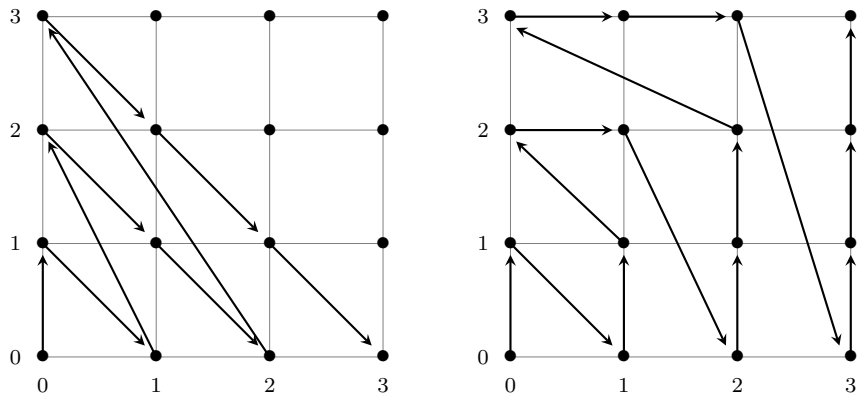
(b) *Le operazioni $+$ e $\cdot$ sono definibili in ciascuna delle seguenti strutture:*
- $(\mathbb{N}, <, |)$,
- $(\mathbb{N}, +, |)$,
- $(\mathbb{N}, <, \cdot)$.

6.B. Aritmetica. In questa sezione vedremo che, a differenza delle strutture viste in precedenza, l'**aritmetica**, cioè la struttura $(\mathbb{N}, +, \cdot)$, è in grado di trasformare le definizioni ricorsive in definizioni standard. In particolare la funzione esponenziale definita ricorsivamente da

$$x^0 = 1$$
$$x^{y+1} = x^y \cdot x$$

è definibile. Infatti, come dimostreremo nella Sezione 19.A, ogni *funzione calcolabile*[7] è definibile nell'aritmetica. Questo significa che la famiglia dei sottoinsiemi definibili di $(\mathbb{N}, +, \cdot)$ è molto ricca. D'altro canto, questa pletora

[7]La definizione rigorosa di funzione calcolabile verrà Â data nella Sezione 9.



Enumerazione triangolare Enumerazione quadrata

Figura 6. Enumerazioni di $\mathbb{N} \times \mathbb{N}$

sottoinsiemi definibili preclude la possibilità di trovare un sistema di assiomi per la teoria di $(\mathbb{N}, +, \cdot)$ che ammetta l'eliminazione dei quantificatori. Come vedremo nel Capitolo **??**, la teoria di $(\mathbb{N}, +, \cdot)$ non è ricorsivamente assiomatizzabile o decidibile. Nella Sezione 7 introdurremo l'**aritmetica di Peano**, una teoria dotata di un sistema ragionevole di assiomi, che è in grado di dimostrare buona parte delle proprietà elementari sui numeri naturali.

Cominciamo col costruire una codifica definibile delle coppie di interi, cioè un'enumerazione definibile di $\mathbb{N}^2$. Ci sono molte biezioni $\mathbb{N} \to \mathbb{N} \times \mathbb{N}$ (Esercizio 10.81), ma se ci restringiamo a quelle definibili, due sono i candidati naturali, descritti nella Figura 6:

- l'**enumerazione diagonale** o **triangolare**, ottenuta enumerando $\mathbb{N}^2$ secondo l'ordinamento

$$(x, y) \lhd (x', y') \Leftrightarrow x + y < x' + y' \vee [x + y = x' + y' \wedge x < x'],$$

- l'**enumerazione quadrata**, ottenuta enumerando $\mathbb{N}^2$ secondo l'ordinamento[8]

$$\begin{aligned}(x, y) <_{\mathrm{G}} (x', y') \Leftrightarrow \big(&\max(x, y) < \max(x', y') \\ &\vee [\max(x, y) = \max(x', y') \wedge (x < x' \vee [x = x' \wedge y < y'])]\big),\end{aligned}$$

Entrambe le biezioni $\mathbb{N} \to \mathbb{N} \times \mathbb{N}$ sono utili, ma quella diagonale ha il vantaggio di avere un'espressione analitica particolarmente semplice: la funzione $\boldsymbol{J} \colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ la cui inversa enumera diagonalmente $\mathbb{N} \times \mathbb{N}$ è data

[8] $<_{\mathrm{G}}$ si dice ordinamento di Gödel e verrà usato nella Sezione 14.D.

da

$$\boldsymbol{J}(x,y) = \frac{1}{2}(x+y)(x+y+1) + x. \tag{6.6}$$

Denoteremo con

$$(\cdot)_0, (\cdot)_1 : \mathbb{N} \to \mathbb{N} \tag{6.7}$$

le funzioni inverse, definite da $\boldsymbol{J}((n)_0, (n)_1) = n$. La funzione $\boldsymbol{J}$ è definita dalla formula

$$(\psi_{\boldsymbol{J}}(x,y,z)) \qquad \exists w(w+w = (x+y)\cdot(x+y+1) \wedge w + x = z)$$

mentre le funzioni $(\cdot)_0$ e $(\cdot)_1$ sono definite da

$$(\psi_0(z,x)) \qquad \exists y\, \psi_{\boldsymbol{J}}(x,y,z)$$
$$(\psi_1(z,y)) \qquad \exists x\, \psi_{\boldsymbol{J}}(x,y,z).$$

La biezione $\boldsymbol{J}$ induce una biezione

$$\mathscr{P}(\mathbb{N}\times\mathbb{N}) \to \mathscr{P}(\mathbb{N}), \quad X \mapsto \boldsymbol{J}[X] = \{\boldsymbol{J}(n,m) \mid (n,m) \in X\}$$

che manda insiemi definibili in insiemi definibili: se $X \subseteq \mathbb{N}\times\mathbb{N}$ è definito da $\varphi(x,y)$ allora $\boldsymbol{J}[X] \subseteq \mathbb{N}$ è definito da

$$\exists x, y\, (\psi_{\boldsymbol{J}}(x,y,z) \wedge \varphi(x,y));$$

viceversa se $Y \subseteq \mathbb{N}$ è definito da $\varphi(z)$ allora $\boldsymbol{J}^{-1}[Y] = \{(n,m) \mid \boldsymbol{J}(n,m) \in Y\}$ è definita da

$$\exists z\, (\psi_{\boldsymbol{J}}(x,y,z) \wedge \varphi(z)).$$

Per l'Osservazione 3.30 la famiglia dei sottoinsiemi definibili di dimensione 1 è sempre identificabile con una sottofamiglia della collezione dei sottoinsiemi definibili di dimensione 2, ma in questo caso si ha un'identificazione completa.

Componendo $\boldsymbol{J}$ con sé stessa possiamo definire una biezione definibile

$$\mathbb{N}\times\mathbb{N}\times\mathbb{N} \to \mathbb{N}, \quad (n,m,k) \mapsto \boldsymbol{J}(n, \boldsymbol{J}(m,k)),$$

e ripetendo questo ragionamento si ottiene per ogni $k \geq 1$ una biezione definibile $\mathbb{N}^k \to \mathbb{N}$ che manda insiemi definibili in insiemi definibili. Il nostro obbiettivo è trovare

- un sottoinsieme definibile
$$\mathrm{Seq} \subseteq \mathbb{N}$$
che codifichi tutte le successioni finite di naturali,
- una funzione definibile
$$\ell\colon \mathbb{N} \to \mathbb{N}$$
tale che $\ell(m)$ sia la lunghezza della sequenza codificata da $m \in \mathrm{Seq}$,

- una funzione definibile per la decodifica

$$\mathrm{Seq} \times \mathbb{N} \to \mathbb{N}, \quad (m, i) \mapsto (\!(m)\!)_i$$

tale che $(\!(m)\!)_i$ è l'i-esimo elemento della sequenza codificata da m, se $i < \ell(m)$.

Per comodità le sequenze finite sono indicizzate a partire da 0, e l'elemento di Seq che codifica la sequenza $(n_0, \ldots, n_k)$ è indicato con

$$\langle\!\langle n_0, \ldots, n_k \rangle\!\rangle.$$

Mostriamo ora come l'esistenza di un apparato di codifica, vale a dire l'esistenza di enti definibili Seq, ℓ e $(m, i) \mapsto (\!(m)\!)_i$ come sopra, consenta di definire molti insiemi e funzioni in $(\mathbb{N}, +, \cdot)$.

Esempio 6.26. La funzione fattoriale è definita dalla formula con variabili libere x e y che asserisce:

> c'è una successione finita $(s_0, \ldots, s_x)$ di lunghezza $x + 1$
> tale che $s_0 = 1$ e $s_x = y$ e $s_{i+1} = s_i \cdot (i + 1)$,

in simboli

$$\exists s[\varphi_{\mathrm{Seq}}(s) \wedge \ell(s) = x + 1 \wedge (\!(s)\!)_0 = 1 \wedge (\!(s)\!)_x = y \\ \wedge \forall i \leq x\, (i + 1 \leq x \Rightarrow (\!(s)\!)_{i+1} = (\!(s)\!)_i \cdot (i + 1))],$$

dove φ_{Seq} è la formula che definisce Seq.

Esempio 6.27. La funzione esponenziale $(n, m) \mapsto n^m$ è definita dalla formula con variabili libere x, y, z che asserisce:

> c'è una successione finita $(s_0, \ldots, s_y)$ tale che $s_0 = 1$ e
> $s_y = z$ e $s_{i+1} = s_i \cdot x$,

in simboli

$$\exists s[\varphi_{\mathrm{Seq}}(s) \wedge \ell(s) = y + 1 \wedge (\!(s)\!)_0 = 1 \wedge (\!(s)\!)_y = z \\ \wedge \forall i \leq x\, (i + 1 \leq x \Rightarrow (\!(s)\!)_{i+1} = (\!(s)\!)_i \cdot x)].$$

Osservazioni 6.28. (a) I due esempi mostrano che se $f\colon \mathbb{N} \to \mathbb{N}$ è definita ricorsivamente da

$$f(0) = k$$
$$f(n + 1) = g(n, f(n))$$

allora f è definibile in $(\mathbb{N}, +, \cdot)$ ogni qual volta g lo è. In particolare, se $g\colon \mathbb{N} \to \mathbb{N}$ è definibile, allora la successione delle iterate $f(n) = g^{(n)}(0)$ è definibile, quindi

$$\{g^{(n)}(0) \mid n \in \mathbb{N}\} = \{x \in \mathbb{N} \mid \exists y(f(y) = x)\}$$

è definibile nell'aritmetica.

(b) La definibilità dell'esponenziale nell'aritmetica (Esempio 6.27) permette di estendere i risultati di formalizzazione visti nelle Sezioni 2.B, 2.C e 3.B: per esempio l'ultimo Teorema di Fermat (Esercizio (vii)) e la congettura *abc* (Esempio 3.3) sono formalizzabili nel linguaggio contenente i simboli $+$ e $\cdot$. Vedremo in seguito che anche l'**Ipotesi di Riemann**, cioè l'affermazione che gli zeri non banali della funzione ζ si trovano sulla retta $\Re(s) = \frac{1}{2}$, è formalizzabile in questo linguaggio.

(c) Il fatto che le definizioni ricorsive siano riconducibili a definizioni standard è forse la conseguenza più importante dell'esistenza di un apparato di codifica definibile. Osserviamo che non tutte le strutture sono dotate di un apparato di codifica, anzi questa è l'eccezione più che la regola. Quindi la capacità di definire oggetti definiti ricorsivamente è una rarità tra le strutture. Per esempio, la funzione $g\colon \mathbb{R} \to \mathbb{R}$, $g(x) = x + 1$, è definibile in $(\mathbb{R}, +, \cdot)$, ma $\mathbb{N} = \left\{ g^{(n)}(0) \mid n \in \mathbb{N} \right\}$ non è definibile in questa struttura (vedi Capitolo **??**).

Vediamo ora come definire l'apparato di codifica. I primi due tentativi risulteranno vani, ma il terzo sarà coronato dal successo.

6.B.1. *Codifica mediante* $\boldsymbol{J}$. Dati $n_0, \dots, n_k \in \mathbb{N}$ l'intero

$$m = \boldsymbol{J}(k+1, \boldsymbol{J}(n_0, \boldsymbol{J}(n_1, \dots \boldsymbol{J}(n_{k-1}, n_k) \cdots)))$$

codifica tanto la lunghezza $\ell(m) = (m)_0 = k + 1$ della sequenza quanto le sue componenti: $((m)_1)_0 = n_0$, $(((m)_1)_1)_0 = n_1$, $\dots (\cdots ((m)_1)_1 \cdots)_1 = n_k$. Convenendo che la sequenza vuota sia codificata da 0, si ha che

$$\mathrm{Seq} = \{n \in \mathbb{N} \mid (n)_0 \neq 0\} \cup \{0\}$$

è definibile, così come lo è la funzione lunghezza. La mappa di decodifica $(m, i) \mapsto (\!(m)\!)_i$ è della forma $(\!(m)\!)_i = (f(m, i))_0$ dove f è una funzione definita ricorsivamente da $f(m, 0) = (m)_1$ e $f(m, i+1) = (f(m, i))_1$, se $i + 1 < \ell(m)$. Il problema è che le funzioni definite ricorsivamente sono definibili nell'aritmetica una volta che sia stato introdotto un sistema di codifica, che era proprio quello che cercavamo di fare.

6.B.2. *Codifica mediante esponenziale.* Sia $\mathbf{p}\colon \mathbb{N} \to \mathbb{N}$ la funzione che enumera l'insieme dei numeri primi, cioè $\mathbf{p}(0) = 2$, $\mathbf{p}(1) = 3$, $\mathbf{p}(2) = 5$, ... Dati $n_1, \dots, n_k \in \mathbb{N}$ l'intero

$$m = \mathbf{p}(0)^{n_0+1} \mathbf{p}(1)^{n_1+1} \cdots \mathbf{p}(k)^{n_k+1}$$

codifica la sequenza $(n_1, \dots, n_k)$. L'insieme Seq è formato dagli interi positivi n tali che se un primo p divide n, allora ogni primo $p' < p$ divide n. Le funzioni $\mathbf{e}\colon \mathbb{N}^2 \to \mathbb{N}$ e $\mathbf{l}\colon \mathbb{N} \to \mathbb{N}$

- $\mathbf{e}(0, i) = \mathbf{e}(1, i) = 0$ e se k è il massimo intero tale che $\mathbf{p}(i)^{k+1} \mid n$, allora $\mathbf{e}(n, i) = k$;

- $\mathbf{l}(0) = \mathbf{l}(1) = 0$ e $\mathbf{l}(n) =$ il primo i tale che $[\mathbf{p}(i) \nmid n]$.

forniscono la decodifica e la lunghezza, cioè $\mathbf{e}(n,i) = (n)_i$ e $\mathbf{l}(n) = \ell(n)$. Il problema è che questa codifica usa in modo essenziale la funzione esponenziale, di cui non abbiamo ancora provato la definibilità nell'aritmetica.

6.B.3. *Codifica mediante $\boldsymbol{\beta}$.* Indichiamo con $\mathrm{Res}(n,m)$ il resto della divisione di n per $m > 0$, cioè

$$\mathrm{Res}(n,m) = r \Leftrightarrow r < m \wedge \exists q(n = q \cdot m + r). \tag{6.8}$$

Quindi Res è una funzione definibile nell'aritmetica.

Fissiamo $1 < c_0, \dots, c_{n-1} \in \mathbb{N}$ a due a due coprimi e siano $a_0, \dots, a_{n-1} \in \mathbb{N}$ arbitrari. Quindi, posto $N = \prod_{i<n} c_i$, si ha che

$$\forall k \, [N \mid k \Leftrightarrow \forall i < n \, (c_i \mid k)]. \tag{6.9}$$

Dati $0 \leq x, y < N$, se $\forall i < n \ \mathrm{Res}(x, c_i) = \mathrm{Res}(y, c_i)$ allora $\forall i < n \ \mathrm{Res}(x - y, c_i) = 0$, cioè N divide $x - y$, da cui $x = y$. In altre parole: la successione $(\mathrm{Res}(x, c_0), \mathrm{Res}(x, c_1), \dots \mathrm{Res}(x, c_{n-1}))$ codifica in modo univoco il numero $x < N$. Abbiamo quindi dimostrato il

Teorema 6.29 (Teorema cinese del resto)**.** *Se $1 < c_0, \dots, c_{n-1} \in \mathbb{N}$ sono a due a due coprimi, allora per ogni $a_0, \dots, a_{n-1} \in \mathbb{N}$ c'è un unico $0 \leq x < \prod_{i<n} c_i$ tale che $x \equiv a_i \mod c_i$ per $i < n$.*

La strategia per la codifica sarà la seguente: dati $a_0, \dots, a_{n-1}$ scegliamo $1 < c_0, \dots, c_{n-1}$ coprimi fra loro e tali che $a_i < c_i$. Per il Teorema 6.29 possiamo trovare un x tale che $a_i = \mathrm{Res}(x, c_i)$, quindi l'intero x codifica la successione $(a_0, \dots, a_{n-1})$. Vediamo i dettagli.

Lemma 6.30. *Sia y un intero positivo tale che $\forall 1 \leq i < n \, (i \mid y)$ e siano*

$$c_i = 1 + (i+1) \cdot y.$$

Allora $c_0, \dots, c_{n-1}$ sono coprimi fra loro.

Inoltre, se $y \geq \max\{a_0, \dots, a_{n-1}\}$, dove $a_0, \dots, a_{n-1} \in \mathbb{N}$, allora $a_i < c_i$ per ogni $i < n$.

Dimostrazione. Per assurdo supponiamo che p sia un primo tale che $p \mid c_i$ e $p \mid c_j$, con $i < j < n$. Allora $p \mid (c_j - c_i) = (j - i) \cdot y$ e quindi $p \mid (j - i)$ o $p \mid y$. Poiché $j - i < n$, e per ipotesi $(j - i) \mid y$, ne segue che $p \mid y$ e quindi c_i è congruente ad 1 modulo p: assurdo. □

Definizione 6.31. $\boldsymbol{\beta} \colon \mathbb{N}^2 \to \mathbb{N}$ è la funzione

$$\boldsymbol{\beta}(m,i) = \mathrm{Res}((m)_0, 1 + (i+1) \cdot (m)_1).$$

Esercizio 6.32. Verificare in dettaglio che la funzione $\boldsymbol{\beta}$ è definibile nell'aritmetica.

Dal Lemma 6.30 segue il seguente

Lemma 6.33 (Gödel)**.** *Per ogni $n > 0$ e per ogni $(a_0, \dots, a_{n-1}) \in \mathbb{N}^n$ c'è un m tale che $\boldsymbol{\beta}(m, i) = a_i$, per $i < n$.*

Siamo ora in grado di esibire la codifica definibile delle successioni finite di naturali: dati $a_0, \dots, a_{n-1}$ poniamo

$$\langle\!\langle a_0, \dots, a_{n-1} \rangle\!\rangle = \text{il minimo } m \text{ tale che } \boldsymbol{\beta}(m, 0) = n \wedge \forall i < n\, (\boldsymbol{\beta}(m, i+1) = a_i).$$

Quindi

$$\ell(x) = \boldsymbol{\beta}(x, 0),$$
$$(\!(x)\!)_i = \boldsymbol{\beta}(x, i+1),$$

e

$$\mathrm{Seq} = \{m \in \mathbb{N} \mid \neg\exists k < m\, (\ell(m) = \ell(k) \wedge \forall i < \ell(m)\, [(\!(m)\!)_i = (\!(k)\!)_i])\}\,.$$

Lasciamo al lettore la verifica che questa codifica è definibile nella struttura $(\mathbb{N}, +, \cdot)$.

6.C. Gli interi e i razionali. I numeri 0 e 1 sono definibili in $(\mathbb{Z}, \cdot)$. L'equazione di Pell $x^2 = ny^2 + 1$ ha infinite soluzioni intere se $n > 1$ è numero naturale che non è un quadrato, quindi $\mathbb{N}$ è l'insieme di verità in $(\mathbb{Z}, S, \cdot)$ della formula $\varphi(z)$

$$\exists x \left(x^2 = z\right) \vee \exists x \exists y \left(y \neq 0 \wedge y \neq 1 \wedge x^2 = z \cdot y^2 + 1\right),$$

quindi $\varphi(z)$ definisce $\mathbb{N}$ anche in $(\mathbb{Z}, +, \cdot)$. Possiamo anche utilizzare il teorema di Lagrange [**HW79**, p. 302], che asserisce che ogni naturale è somma di quattro quadrati, quindi $\mathbb{N}$ è l'insieme di verità in $(\mathbb{Z}, +, \cdot)$ di

$$\exists y_1, y_2, y_3, y_4\, (x = y_1 \cdot y_1 + y_2 \cdot y_2 + y_3 \cdot y_3 + y_4 \cdot y_4)\,.$$

Quindi le strutture $(\mathbb{Z}, S, \cdot)$ e $(\mathbb{Z}, +, \cdot)$ hanno famiglie molto ricche di insiemi definibili.

Teorema 6.34. *La moltiplicazione è definibile nella struttura $(\mathbb{N}, S, |)$ e nella struttura $(\mathbb{Z}, S, |)$. Quindi per l'Esercizio 6.23 anche la somma è definibile in queste strutture.*

Dimostrazione. Per quanto riguarda $(\mathbb{N}, S, |)$ si veda l'Esercizio 6.66; per quanto riguarda $(\mathbb{Z}, S, |)$ si veda [**Ric85**]. □

Ne segue che le strutture $(\mathbb{N}, S, |)$ e $(\mathbb{Z}, S, |)$ hanno una famiglia molto ricca di insiemi definibili.

Per l'Esercizio 3.54, ogni $k \in \mathbb{Z}$ è definibile in $(\mathbb{Q}, +, \cdot)$.

Teorema 6.35. $\mathbb{Z}$ *è definibile in* $(\mathbb{Q}, +, \cdot)$.

La dimostrazione di questo importante risultato si basa su risultati di algebra non banali e rimandiamo il lettore interessato all'articolo originale [**Rob49**]. Per il teorema di Lagrange anche $\mathbb{N}$ è definibile in $(\mathbb{Q}, +, \cdot)$. Ne segue che anche in questo caso abbiamo una famiglia molto ricca di insiemi definibili.

Osservazione 6.36. La formula $\varphi(t)$ usata nella dimostrazione del Teorema 6.35 è:

$$\forall y, z\,(\psi(y, z, 0) \wedge \forall w\,(\psi(y, z, w) \Rightarrow \psi(y, z, w + 1)) \Rightarrow \psi(y, z, t))$$

dove $\psi(t, y, z)$ è

$$\exists a, b, c\left(t \cdot y \cdot z^2 + 2 = a^2 + t \cdot y^2 - y \cdot c^2\right).$$

Se trasformiamo $\varphi(t)$ in forma prenessa la formula risultante è una $\forall\exists\forall$-formula. Infatti può essere scritta nella forma

$$\forall x_1, x_2, \exists y_1, \ldots, y_7, \forall z_1, \ldots z_6\,[f(t, x_1, x_2, y_1, \ldots, y_7, z_1, \ldots z_6) = 0]$$

dove $f \in \mathbb{Z}[t, x_1, x_2, y_1, \ldots, y_7, z_1, \ldots z_6]$. Recentemente questo risultato è stato migliorato ottenendo una definizione di $\mathbb{Z}$ in $\mathbb{Q}$ mediante una $\forall$-formula della forma

$$\forall x_1, \ldots, x_n\,[f(t, x_1, \ldots, x_n) = 0]$$

con $f \in \mathbb{Z}[t, x_1, \ldots, x_n]$.

6.D. I reali e i complessi.

6.D.1. *Il campo reale.* Consideriamo la struttura $(\mathbb{R}, +, \cdot)$. Gli elementi 0 e 1 sono definibili mediante le formule $\forall y(y + x = y)$ e $\forall y(y \cdot x = y)$, mentre la relazione d'ordine $x < y$ è definibile mediante la formula

$$\exists z\,(z \neq 0 \wedge x + z \cdot z = y).$$

Quindi gli insiemi definibili in $(\mathbb{R}, +, \cdot)$ sono esattamente quelli definibili nel campo reale chiuso $(\mathbb{R}, +, \cdot, -, 0, 1, <)$, (Definizione 5.6 a pag. 84). Ogni $n \in \mathbb{Z}$ è definibile, dato che $\{0\}$ è definito dalla formula $x = 0$, e $\{n\}$, se $n \neq 0$, è l'insieme di verità di

$$\begin{cases} x = \underbrace{1 + \cdots + 1}_{n} & \text{se } n > 0, \\ x = -(\underbrace{1 + \cdots + 1}_{n}) & \text{se } n < 0, \end{cases}$$

Ricordiamo che un reale $r \in \mathbb{R}$ si dice algebrico se è soluzione di un qualche polinomio a coefficienti razionali o, equivalentemente, è soluzione di qualche polinomio a coefficienti interi (si vela l'Appendice A1). Ogni $f \in \mathbb{Z}[X]$ genera un termine $t(x)$ con un'unica variabile x, quindi dire che r è soluzione

di f equivale a dire che r è nell'insieme di verità della formula $t(x) = 0$. Poiché l'insieme S delle soluzioni di f è finito, possiamo individuare r in S specificandone la sua posizione rispetto all'ordine: se $S = \{r_1 < \cdots < r_k\}$ e, per esempio $r = r_3$, allora r è l'unico reale che rende vera la formula

$$t(x) = 0 \wedge \exists y_1 \exists y_2 (t(y_1) = 0 \wedge t(y_2) = 0 \\ \wedge y_1 < y_2 < x \wedge \forall z \, (t(z) = 0 \wedge z < x \Rightarrow z = y_1 \vee z = y_2))$$

Quindi ogni numero algebrico, è definibile.

Definizione 6.37. La famiglia dei sottoinsiemi **semialgebrici** di dimensione n è la più piccola famiglia di sottoinsiemi di $\mathbb{R}^n$ contenente gli insiemi della forma

$$f(x_1, \ldots, x_n) \leq g(x_1, \ldots, x_n)$$

con f, g polinomi a coefficienti in $\mathbb{R}$, e chiusa per complementi e per intersezioni e unioni finite.

È facile verificare che gli insiemi semialgebrici sono esattamente gli insiemi definibili con parametri in $(\mathbb{R}, +, \cdot, 0, 1, <)$ mediante una formula aperta. Nel Capitolo **??** dimostreremo che la teoria dei campi reali chiusi ammette l'eliminazione dei quantificatori e che si tratta di una teoria completa e decidibile. Dall'eliminazione dei quantificatori otteniamo i seguenti risultati:

Teorema 6.38 (Tarski-Seidenberg)**.** *Se $\pi \colon \mathbb{R}^{n+1} \to \mathbb{R}^n$ è la proiezione lungo la prima coordinata e $A \subseteq \mathbb{R}^{n+1}$ è semialgebrico, allora $\pi[A]$ è semialgebrico.*

Teorema 6.39. *I sottoinsiemi di $\mathbb{R}$ definibili con parametri nel campo reale sono tutte e sole le unioni finite di intervalli.*[9]

Corollario 6.40. *Nessuno degli insiemi $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ è definibile nella struttura $(\mathbb{R}, +, \cdot, 0, 1 <)$.*

Il Corollario 6.40 continua a valere se aggiungiamo al campo reale la funzione esponenziale $\exp(x) = \mathrm{e}^x$. Inoltre la teoria di $(\mathbb{R}, +, \cdot, \exp)$ è decidibile, se si assume la seguente congettura in teoria dei numeri:

Congettura di Schanuel. *Se $z_1, \ldots, z_n \in \mathbb{C}$ sono linearmente indipendenti su $\mathbb{Q}$, allora in grado di trascendenza di $\mathbb{Q}(z_1, \ldots, z_n, \mathrm{e}^{z_1}, \ldots, \mathrm{e}^{z_n})$ su $\mathbb{Q}$ è almeno n.*

Osservazioni 6.41. (a) $(\mathbb{N}, +, \cdot)$ e $(\mathbb{R}, +, \cdot)$ dimostrano che una sottostruttura di una struttura decidibile non è necessariamente decidibile.

(b) Per il Teorema 5.4, $\mathbb{Z}$ è definibile nell'anello $\mathbb{R}[X]$, anche se non è definibile in $\mathbb{R}$.

[9] Gli intervalli possono essere chiusi, aperti, semiaperti, limitati o illimitati, cioè semirette.

6.D.2. *Il campo complesso.* La teoria del campo complesso $(\mathbb{C}, +, \cdot, 0, 1)$ è assiomatizzata dagli assiomi per i campi algebricamente chiusi di caratteristica zero ACF_0 (Sezione 5.D.4).

Teorema 6.42. *Sia p un primo oppure $p = 0$. La teoria ACF_p ammette l'eliminazione debole dei quantificatori.*

Dimostrazione. Applichiamo la Proposizione 6.18. Siano M, N campi algebricamente chiusi di caratteristica p, e supponiamo che M' e N' siano una sottostruttura di M ed N, rispettivamente e che $F\colon M' \to N'$ sia un isomorfismo. Quindi M' e N' sono domini di integrità di caratteristica p e l'isomorfismo F si estende al campo dei quozienti. Senza perdita di generalità, possiamo supporre che M' e N' siano campi. Siano $\overline{M'}$ e $\overline{N'}$ la chiusura algebrica di M' calcolata in M e la chiusura algebrica di N' calcolata in N. Poiché la chiusura algebrica è unica a meno di isomorfismo, l'isomorfismo F si estende ad un isomorfismo $\overline{M'} \to \overline{N'}$.

Sia $\varphi(y, x_1, \ldots, x_n)$ una congiunzione di formule atomiche o negazioni di formule atomiche e siano $a_1, \ldots, a_n \in \overline{M'}$: vogliamo dimostrare che se $M \vDash \exists y \varphi[a_1, \ldots, a_n]$, allora $N \vDash \exists y \varphi[F(a_1), \ldots, F(a_n)]$, e viceversa. Una formula atomica è logicamente equivalente ad una formula della forma $t = 0$, con t un termine contenente soltanto variabili tra le $y, x_1, \ldots, x_n$. Dato che la congiunzione di due formule atomiche negate $(t \neq 0) \wedge (s \neq 0)$ è equivalente a $t \cdot s \neq 0$, possiamo supporre che φ sia della forma

$$s \neq 0 \wedge \bigwedge_{1 \leq i \leq k} t_i = 0.$$

Supponiamo $M \vDash \exists y \varphi[a_1, \ldots, a_n]$: questo equivale a dire che c'è un $b \in M$ che non è radice del polinomio $s[a_1, \ldots, a_n]$, e tuttavia è soluzione di ogni polinomio $t_i[a_1, \ldots, a_n]$. Osserviamo che $b \in \overline{M'}$, quindi $F(b) \in \overline{N'}$ è radice dei polinomi $t_i[F(a_1), \ldots, F(a_n)]$ e tuttavia non è radice di $s[F(a_1), \ldots, F(a_n)]$. Ne segue che $N \vDash \exists y \varphi[F(a_1), \ldots, F(a_n)]$. L'altra implicazione,

$$N \vDash \exists y \varphi[F(a_1), \ldots, F(a_n)] \Rightarrow M \vDash \exists y \varphi[a_1, \ldots, a_n],$$

è simile. □

Un enunciato atomico σ del linguaggio $L_{\text{ANELLI-1}}$ è logicamente equivalente modulo ACF_p a uno della forma '$t = 0$' con t termine chiuso, e ognuno di questi enunciati è decidibile in ACF_p, e quindi $\mathrm{ACF}_p \vDash \sigma$ oppure $\mathrm{ACF}_p \vDash \neg\sigma$.

Corollario 6.43. *Per p primo o $p = 0$, la teoria ACF_p è completa.*

Osservazione 6.44. La dimostrazione del Teorema 6.42 si basa sul fatto che la chiusura algebrica di un campo è unica a meno di isomorfismo, un risultato che dipende dall'Assioma di Scelta. Ma dato che le sottostrutture M' e N' possono essere essere prese numerabili, e dato che la dimostrazione

dell'unicità della chiusura algebrica non usa la scelta quando il campo è numerabile, l'uso di AC può essere evitato del tutto — si veda la Sezione 25.

Gli insiemi definibili con parametri mediante formule atomiche sono le varietà algebriche, cioè insiemi della forma

$$Z(f) = \{(z_1, \dots, z_n) \in \mathbb{C}^n \mid f(\vec{z}) = 0\}$$

con $f \in \mathbb{C}[x_1, \dots, x_n]$. Quindi i sottoinsiemi definibili del campo complesso sono gli insiemi ottenibili dalle varietà algebriche mediante unione, intersezione e complemento. In particolare, gli insiemi $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ non sono definibili nella struttura $(\mathbb{C}, +, \cdot, 0, 1)$.

Ogni razionale è definibile nel campo complesso, tuttavia il risultato non si estende ai numeri algebrici — come abbiamo osservato a pagina 55 l'insieme $\{\mathrm{i}, -\mathrm{i}\}$ è definibile ma nessuno dei suoi due elementi lo è.

Se lavoriamo nella struttura $(\mathbb{C}, +, \cdot, 0, 1, \exp)$, possiamo definire

$$\ker(\exp) = \{z \in \mathbb{C} \mid \exp(z) = 1\} = 2\mathrm{i}\pi\mathbb{Z}$$

e quindi $\mathbb{Z} = \{x \in \mathbb{C} \mid x \ker(\exp) \subseteq \ker(\exp)\}$ è definibile.

6.D.3. *Anelli di funzioni olomorfe.* Una funzione $f\colon U \to \mathbb{C}$, dove U è un aperto non vuoto di $\mathbb{C}$, si dice **olomorfa** se è derivabile in ogni punto del suo dominio, cioè se $\lim_{w\to z} \frac{f(w)-f(z)}{w-z}$ esiste per ogni $z \in U$. Una funzione intera è una funzione olomorfa su $\mathbb{C}$. L'insieme $\mathcal{H}(U)$ delle funzioni olomorfe su U è un anello commutativo unitario con le operazioni di somma e prodotto puntuale. Lo studio di $\mathcal{H}(U)$ è molto importante per la classificazione degli aperti U a meno di equivalenza conforme — due aperti U, U' sono conformemente equivalenti se c'è una biezione olomorfa $\phi\colon U \to U'$. Se $\phi\colon U \to U'$ è una biezione olomorfa, allora $\Phi\colon \mathcal{H}(U) \to \mathcal{H}(U')$, $f \mapsto f \circ \phi^{-1}$, è un isomorfismo di anelli tale che $\Phi(i) = i$. Viceversa, se $\Phi\colon \mathcal{H}(U) \to \mathcal{H}(U')$ è un isomorfismo di anelli tale che $\Phi(i) = i$, allora U e U' sono conformi [**LR84**, p. 130]. Quindi la struttura di anello di $\mathcal{H}(U)$ contiene in sé tutta l'informazione sulla struttura complessa di U.

Identificando un numero complesso con una funzione costante, si dimostra che $\mathbb{C}$ è un sottoinsieme definibile dell'anello $\mathcal{H}(U)$ [**Huu94**]. La dimostrazione quando $U = \mathbb{C}$ è più facile, dato che possiamo utilizzare il Piccolo Teorema di Picard [**Con78**, p. 297]:

> Una funzione intera non costante può non assumere al più un valore, cioè se f è intera e $\mathbb{C} \setminus \mathrm{ran}(f)$ ha almeno due punti, allora f è costante.

Quindi $\mathbb{C}$ è definito in $\mathcal{H}(\mathbb{C})$ dalla formula $\varphi_{\mathbb{C}}(x)$

$$x = 0 \vee x = 1 \vee (x \mid 1 \wedge (x - 1) \mid 1)\,.$$

Le costanti 0, 1 e il predicato di divisibilità $\mid$ sono definibili in $\mathcal{H}(\mathbb{C})$ a partire dalle operazioni di somma e prodotto, quindi possono essere usate liberamente.

Benché $\mathbb{N}$ non sia definibile nel campo complesso $\mathbb{C}$, è tuttavia definibile nell'anello $\mathcal{H}(\mathbb{C})$. Dimostriamo che la formula $\varphi_{\mathbb{N}}(x)$

$$x \in \mathbb{C} \wedge \forall f, g\,[f \mid g \wedge \forall y \in \mathbb{C}\ (f + y \mid g \Rightarrow f + y + 1 \mid g) \Rightarrow f + x \mid g],$$

dove $z \in \mathbb{C}$ sta per $\varphi_{\mathbb{C}}(z)$, definisce $\mathbb{N}$ in $\mathcal{H}(\mathbb{C})$.

Sia $n \in \mathbb{N}$ e siano f, g due funzioni intere tali che $f \mid g$, e tali che $f + y \mid g \Rightarrow f + y + 1 \mid g$ per ogni $y \in \mathbb{C}$. Allora $f, f + 1, \ldots, f + n$ dividono g, quindi n soddisfa $\varphi_{\mathbb{N}}(x)$.

Per dimostrare il converso dobbiamo richiamare il seguente fatto elementare sulle funzioni olomorfe:

$$\text{se } g \in \mathcal{H}(\mathbb{C}) \text{ e } g(z_0) = 0 \text{ per qualche } z_0 \in \mathbb{C}, \text{ allora } z - z_0 \text{ divide } g.$$

Sia $h \in \mathcal{H}(\mathbb{C})$ un elemento che soddisfa $\varphi_{\mathbb{N}}(x)$. Allora $h \in \mathbb{C}$. Sia $f(z) = z$ e sia g è una funzione che si annulla esattamente sull'insieme $\{-k \mid k \in \mathbb{N}\}$, per esempio $g(z) = 1/\Gamma(z)$ dove $\Gamma(z) = \int_0^\infty t^{z-1}\mathrm{e}^{-t}\,\mathrm{d}t$. Sia $y \in \mathbb{C}$: per la suddetta proprietà delle funzioni olomorfe, $f + y \mid g$ se e solo se $y \in \mathbb{N}$, quindi $f + y \mid g \Rightarrow f + y + 1 \mid g$, da cui $f + h \mid g$. Ma per quanto detto questo implica $h \in \mathbb{N}$.

Esercizi

Esercizio 6.45. Dimostrare che $\mid$ non è definibile nella struttura $(\mathbb{N}, \perp)$.

Esercizio 6.46. Dimostrare che $\langle \mathbb{N} \cup \mathbb{Q} \times \mathbb{Z}, +, <, 0\rangle$ è un modello dell'aritmetica di Presburger. Quali sono i suoi elementi definibili? L'insieme degli elementi definibili è un insieme definibile?

Esercizio 6.47. Utilizzare il Teorema 3.27 per dimostrare che le teorie $\Sigma_{(\mathbb{N},S)}$ e $\Sigma_{(\mathbb{N},<)}$ sono complete.

Esercizio 6.48. Dimostrare che $\Sigma_{(\mathbb{N},<,0)}$ ammette l'eliminazione debole dei quantificatori e che è una teoria completa.

Esercizio 6.49. Per ogni $n \in \mathbb{N}$, sia L_n il linguaggio del prim'ordine contenente soltanto i simboli di costante c_i con $0 \leq i < n$. (In particolare L_0 è il linguaggio privo di simboli non logici.) Sia Σ_n la teoria nel linguaggio L_n contenente tutti gli enunciati $\boldsymbol{\varepsilon}_{\geq k}$ per $k \geq 1$ (vedi pagina 15). Dimostrare che:

(i) Σ_n ammette l'eliminazione debole dei quantificatori se $n \geq 1$, e Σ_0 ammette l'eliminazione debole dei quantificatori per formule non chiuse,

(ii) Σ_0 e Σ_1 sono complete, mentre per $n \geq 2$ la teoria Σ_n non è completa.

Esercizio 6.50. Completare la dimostrazione della Proposizione 6.21.

Esercizio 6.51. Dimostrare che le funzioni $\mathbb{N} \to \mathbb{N}$ definite da $g(0) = G(0) = 0$, $g(1) = G(1) = 1$ e per $n \geq 2$

$$g(n) = \text{il più piccolo } k \text{ tale che } \forall x\, \exists y_1, \dots, y_k\, (x = y_1^n + \cdots + y_k^n)$$
$$G(n) = \text{il più piccolo } k \text{ tale che } \exists z\, \forall x \geq z\, \exists y_1, \dots, y_k\, (x = y_1^n + \cdots + y_k^n)$$

sono definibili in $(\mathbb{N}, +, \cdot)$. (Le funzioni g e G sono state menzionate pagina 62 in relazione al problema di Waring (3.3) a pagina 25.)

Esercizio 6.52. (i) Sia $C(x)$ il predicato unario "essere un quadrato", cioè $\exists y(y = x^2)$. Dimostrare che la funzione $q(x) = x^2$ è definibile in $(\mathbb{N}, +, C)$.

(ii) Dimostrare che il prodotto è definibile in $(\mathbb{N}, +, q)$.

(iii) Dimostrare che il prodotto è definibile in $(\mathbb{N}, +, f)$ dove $f \in \mathbb{N}[X]$ è di grado ≥ 2.

(iv) Concludere che gli unici polinomi definibili in $(\mathbb{N}, +)$ sono quelli di grado ≤ 1.

Esercizio 6.53. Dimostrare che $\mathbb{N}$ e il prodotto sono definibili in $(\mathbb{Z}, +, C)$, dove C è come nell'Esercizio 6.52.

Esercizio 6.54. Dimostrare che l'enumerazione quadrata di $\mathbb{N} \times \mathbb{N}$ della Figura 6 è definibile in $(\mathbb{N}, +, \cdot)$ dando una definizione esplicita di tale biezione $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ e per le sue inverse.

Esercizio 6.55. Verificare che la biezione $\mathbb{N} \times \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $(n, m, k) \mapsto \boldsymbol{J}(n, \boldsymbol{J}(m, k))$ è un polinomio di quarto grado. Trovare una biezione $\mathbb{N} \times \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ che sia un polinomio di terzo grado. Più in generale, per ogni inter $k > 0$ costruire una biezione $\mathbb{N}^k \to \mathbb{N}$ che sia un polinomio di grado k.

Esercizio 6.56. Sia $f(n)$ il più piccolo $x \leq n$ tale che $\sum_{k \leq x} k \leq n < \sum_{k \leq x+1} k$. Dimostrare che $(n)_0 = n - \sum_{k \leq f(n)} k$ e $(n)_1 = f(n) - \left(n - \sum_{k \leq f(n)} k\right) = f(n) - \sum_{k \leq f(n)} k$.

Esercizio 6.57. Supponiamo che $1 < c_0, \dots, c_{n-1} \in \mathbb{N}$ siano a due a due coprimi e siano $a_0, \dots, a_{n-1} \in \mathbb{N}$ arbitrari. Sia $N = \prod_{i=0}^{n-1} c_i$. Dimostrare che

(i) $x = \sum_{i=0}^{n-1} a_i (\frac{N}{c_i})^{\phi(c_i)}$ è tale che $x \equiv a_i \mod c_i$, per ogni $0 \leq i < n$, dove ϕ è la funzione di Eulero, cioè $\phi(k) =$il numero di $0 < x < k$ tali che x è coprimo con k;

(ii) se $x \in \mathbb{N}$ è tale che $x \equiv a_i \mod c_i$, per ogni $0 \leq i < n$, allora le seguenti condizioni sono equivalenti:
- $y \equiv x \mod N$
- $y \equiv a_i \mod c_i$, per ogni $0 \leq i < n$.

Esercizio 6.58. Dimostrare che $<$ è definibile senza parametri in $(\mathbb{Q}, +, \cdot)$.

Esercizio 6.59. Dimostrare che se $p, q \in \mathbb{Q}$ allora i campi $\mathbb{Q}(\sqrt{p})$ e $\mathbb{Q}(\sqrt{q})$ sono elementarmente equivalenti se e solo se coincidono.

Esercizio 6.60. Dimostrare che il campo reale $(\mathbb{R}, +, \cdot)$ è rigido.

Esercizio 6.61. Dimostrare che l'ordinamento è definibile in $(\mathbb{Z}, +, \cdot)$.

Esercizio 6.62. Dimostrare che l'operazione di somma $+$ e il campo razionale $\mathbb{Q}$ sono definibili nella struttura $(\mathbb{C}, \cdot, \exp)$.

Esercizio 6.63. Dimostrare che $\mathbb{N}$ è definibile nelle strutture $(\mathbb{R}, +, \cdot, \sin)$, $(\mathbb{R}, +, \cdot, \cos)$, $(\mathbb{C}, +, \cdot, \exp)$.

Esercizio 6.64. Consideriamo la struttura $(\mathbb{R}, +, \cdot, 0, 1, <)$. Dimostrare che:

(i) ogni intervallo chiuso, aperto, semi-aperto, limitato o no, i cui estremi sono numeri algebrici, è definibile;

(ii) le funzioni $x \mapsto |x|$, $x \mapsto x^q$ con $q \in \mathbb{Q}$ sono definibili. Se f e g sono funzioni (parziali) reali di variabile reale e sono definibili, allora anche f/g è definibile;

(iii) Scrivere la formula $\varphi(x_{11}, x_{12}, x_{21}, x_{22})$ che asserisce che la matrice

$$\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix}$$

è invertibile. Per l'eliminazione dei quantificatori nella teoria dei campi reali chiusi, c'è una formula priva di quantificatori logicamente equivalente a φ e con le medesime variabili libere: determinare questa formula.

Esercizio 6.65. Consideriamo il linguaggio degli anelli con un ulteriore simbolo di funzione 1-aria. Costruire degli enunciati σ di questo linguaggio tali che la struttura $(\mathbb{R}, +, \cdot, f)$ soddisfa σ se e solo se

(i) f è continua,

(ii) f è di classe C^n,

(iii) $f(x) = \mathrm{e}^x$,

(iv) $f(x) = \sin(x)$,

(v) $f(x) = \cos(x)$.

Esercizio 6.66. (i) Supponiamo che $a, b, x, y, p \in \mathbb{N} \setminus \{0\}$ sono tali che:

$$\begin{array}{lll} a, b > 1 & x \perp y & p \mid (\mathrm{mcm}(a, x) + 1) \\ a \perp x & a \cdot b \perp x & p \mid (\mathrm{mcm}(b, y) + 1)\,. \\ b \perp y & a \cdot b \perp y & \end{array}$$

Dimostrare che $p \mid (\mathrm{mcm}(a \cdot b, \mathrm{mcm}(x, y)) - 1)$.

(ii) Siano $a, b, c \in \mathbb{N} \setminus \{0, 1\}$ e supponiamo che valga $\varphi \Rightarrow \psi$, dove φ è

$$\Big[x \neq 0 \wedge a \perp x \wedge y \neq 0 \wedge b \perp y \wedge c \perp x \wedge c \perp y \wedge x \perp y \\ \wedge\ p \text{ è primo} \wedge p \mid (\mathrm{mcm}(a, x) + 1) \wedge p \mid (\mathrm{mcm}(b, y) + 1)\Big]$$

e ψ è $p \mid (\mathrm{mcm}(c, \mathrm{mcm}(x, y)) - 1)$. Allora $a \cdot b \equiv c \pmod{p}$.

(iii) Fissati $a, b, c \in \mathbb{N} \setminus \{0, 1\}$ sia $p > a, b, c$ un primo. Dimostrare che esistono x, y che soddisfano φ. Concludere che l'insieme di verità della formula $\sigma(a, b, c)$: $\forall x, y, p\,(\varphi \Rightarrow \psi)$, è $\Big\{(a, b, c) \in \mathbb{N}^3 \mid c = a \cdot b\Big\}$.

(iv) Usare l'Esercizio 6.23 per concludere che la somma e il prodotto sono definibili nella struttura $(\mathbb{N}, |, S)$.

Esercizio 6.67. Sia DLO la teoria degli ordini lineari densi senza primo o ultimo elemento nel linguaggio L_{ORDINI} contenente solamente il simbolo relazionale $\leq$, e sia DLO* la medesima teoria formulata nel linguaggio L^* ottenuto aggiungendo a L_{ORDINI} un simbolo di costante c. Dimostrare che DLO ammette l'eliminazione debole dei quantificatori per formule non chiuse, e che DLO* ammette l'eliminazione debole dei quantificatori (per tutte le formule).

Concludere che se $(M, \leq) \vDash$ DLO allora $\emptyset \neq X \subseteq M$ è definibile con parametri $\{p_1, \ldots, p_n\} \subseteq M$ se e solo se X è unione finita di intervalli[10] (chiusi, aperti, semi-aperti) con estremi in $\{p_1, \ldots, p_n\}$.

Concludere che DLO è completa e decidibile.

[10] Tra gli intervalli consideriamo anche le semirette e i singoletti $\{p_i\}$.

Note e osservazioni

La prima parte della Sezione 6.A segue abbastanza fedelmente il libro [**End01**]. L'assiomatizzazione di $(\mathbb{N},+)$ e l'eliminazione dei quantificatori per questa teoria è stata dimostrata nel 1929 da Presburger, a quel tempo studente di Tarski. La funzione $\boldsymbol{J}$ è stata definita da Cantor. È un polinomio quadratico e per un risultato del 1923 dovuto a Feuter e Pólya, se $f \in \mathbb{R}[x,y]$ è un polinomio quadratico che dà una biezione $\mathbb{N}\times\mathbb{N}\to\mathbb{N}$, allora $f(x,y)=\boldsymbol{J}(x,y)$ oppure $f(x,y)=\boldsymbol{J}(y,x)$ [**Smo91**]. I sottoinsiemi di $\mathbb{N}^k$ $(k>1)$ definibili nell'aritmetica di Presburger sono studiati in [**Woo**]. La definibilità degli interi nei razionali (Teorema 6.35) e la definibilità della somma e del prodotto in $(\mathbb{N},+,\cdot)$ (Esercizio 6.66) sono dovuti a J. Robinson. In quell'articolo, furono posti tre problemi:

(1) è possibile definire il prodotto nella struttura $(\mathbb{N},S,\perp)$?

(2) è possibile definire il prodotto nella struttura $(\mathbb{N},+,\perp)$?

(3) è possibile definire il prodotto nella struttura $(\mathbb{Z},S,|)$?

Il primo è ancora aperto: Woods ha dimostrato in [**Woo81**] che la definibilità del prodotto in termini di coprimalità e successore è equivalente alla congettura di Erdős-Woods della Sezione 2.C.5. Gli altri due problemi sono stati risolti in positivo: il secondo problema è stato poi risolto dalla stessa Robinson, e il terzo è il Teorema 6.34. Per una rassegna di risultati sulla definibilità nei naturali si veda [**Bès01**].

La definibilità di $\mathbb{Z}$ in $\mathbb{Q}$ nella forma descritta nell'Osservazione 6.36 è dimostrata in [**Koe**]: il polinomio $f(t,x_1,\dots,x_n)$ è di grado 28 e $n=418$. È noto che $\mathbb{Z}$ non è definibile in $\mathbb{Q}$ mediante una formula priva di quantificatori, quindi in un certo senso il risultato è ottimale. Resta aperta la possibilità che $\mathbb{Z}$ stesso sia definibile in $\mathbb{Q}$ mediante una $\exists$-formula: tuttavia è opinione diffusa che ciò non accada, in quanto questo contraddice un'importante congettura in teoria dei numeri, nota come congettura di Bombieri-Lang. I risultati nella Sezione 6.D.3 sono tratti da [**Rob51**].

L'eliminazione dei quantificatori per i campi reali chiusi (dimostrata da Tarski nel 1951) e il conseguete Teorema di Tarski-Seidenberg 6.38, sono risultati centrali per la teoria dei modelli e per le sue applicazioni alla geometria algebrica reale. Il risultato di Tarski-Seidenberg è stato utilizzato nello studio degli operatori pseudo-differenziali da Hörmander [**HÖ5**]. Il Teorema 6.39 è il primo risultato di un'importante area della teoria dei modelli, lo studio delle strutture o-minimali, cioè campi reali chiusi in cui i sottoinsiemi definibili di dimensione 1 sono unioni finite di intervalli [**vdD98**]. L'estensione del Corollario 6.40 ad $(\mathbb{R},+,\cdot,\exp)$ è dovuta a Wilkie [**Wil96**] e la dimostrazione della decidibilità di questa struttura, modulo la congettura di Schanuel, è dovuta a Wilkie e Macintyre [**MW96**]. La congettura di Schanuel porta il nome del matematico che l'ha formulata verso il 1960. È una delle congetture più importanti in teoria dei numeri, in grado di risolvere molti problemi aperti sui numeri trascendenti; per esempio implica che $\pi+\mathrm{e}$, $\pi\cdot\mathrm{e}$ sono entrambi trascendenti (si veda l'Esempio 2.1).

7. Aritmetica e induzione

7.A. Strutture di Dedekind. Useremo L_{D} per denotare il linguaggio del prim'ordine (che abbiamo già incontrato nella Sezione 6.A) contenente il simbolo di funzione unaria S e il simbolo di costante 0. Una proprietà cruciale di $(\mathbb{N},S,0)$ è il **principio di induzione al second'ordine**

$$(\mathsf{Ind}^2)\qquad \forall I\,[0\in I\wedge\forall x\,(x\in I\Rightarrow S(x)\in I)\Rightarrow\forall x\,(x\in I)]\,.$$

L'espressione *second'ordine* e il conseguente esponente 2 sono motivati dalla quantificazione $\forall I$ su sottoinsiemi arbitrari (si veda l'Osservazione 3.7(b)).

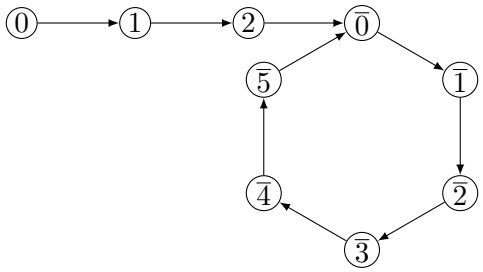


Figura 7. La struttura $\mathcal{Z}_{3,6}$.

In particolare Ind^2 non è una formula del prim'ordine. Una struttura $(M, S_M, 0_M)$ in cui valga Ind^2, cioè tale che

$$\forall I \subseteq M \; [0_M \in I \wedge \forall x \, (x \in I \Rightarrow S_M(x) \in I) \Rightarrow I = M]$$

si dice **induttiva**. Una struttura induttiva che sia un modello degli enunciati

$$\forall x \, (S(x) \neq 0) \tag{7.1}$$

$$\forall x, y \, (x \neq y \Rightarrow S(x) \neq S(y)) \tag{7.2}$$

si dice **struttura di Dedekind**, da cui la lettera D in L_{D}. Chiaramente $(\mathbb{N}, S, 0)$ è una struttura di Dedekind.

Esercizio 7.1. Dimostrare che:

(i) una struttura induttiva soddisfa l'enunciato $\forall x \, (x \neq 0 \Rightarrow \exists y (S(y) = x))$;

(ii) una struttura di Dedekind soddisfa gli enunciati $\forall x (S^{(n)}(x) \neq x)$. Quindi una struttura di Dedekind è un modello della teoria $\Sigma_{(\mathbb{N},S,0)}$ della Sezione 6.A.

Esempi 7.2. (i) $\mathcal{Z}_n = (\mathbb{Z}/n\mathbb{Z}, \sigma, \overline{0})$, dove $\sigma(\overline{k}) = \overline{k+1}$ e $\overline{k}$ è la classe di resto di k modulo n, è una struttura induttiva che non soddisfa (7.1), ma che soddisfa (7.2).

(ii) $\mathcal{Z}'_m = (\{0, \ldots, m-1\}, \tau, 0)$, dove $m > 0$, $\tau(k) = k+1$ se $0 \leq k < m-1$ e $\tau(m-1) = m-1$ è una struttura induttiva che non soddisfa (7.2); $\mathcal{Z}'_m$ soddisfa (7.1) se $m > 1$.

(iii) $\mathcal{Z}_{m,n} = (Z, S, a)$ è la struttura che ha per universo $\{0, \ldots, m-1\} \uplus \mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \ldots, \overline{n-1}\}$, dove $a = 0$ e S è definita da

$$S(x) = \begin{cases} x+1 & \text{se } x < m-1, \\ \overline{0} & \text{se } x = m-1, \\ \sigma(x) & \text{se } x \in \mathbb{Z}/n\mathbb{Z}. \end{cases}$$

La struttura $\mathcal{Z}_{m,n}$ è descritta dal grafo diretto della Figura 7. Osserviamo che $\mathcal{Z}_n = \mathcal{Z}_{0,n}$ e che $\mathcal{Z}'_m = \mathcal{Z}_{m,0}$. La struttura $\mathcal{Z}_{m,n}$ è induttiva; soddisfa (7.1) se $m > 0$, soddisfa (7.2) se $m = 0$ e $n > 0$.

(iv) $(\mathbb{N}, T, 0)$, dove $T(n) = 2n$ è una struttura non induttiva che soddisfa (7.1) e (7.2).

Un morfismo tra due L_{D}-strutture N e M è una funzione $F\colon N \to M$ tale che $F(0_N) = 0_M$ e $F(S_N(x)) = S_M(F(x))$.

Teorema 7.3. (a) *Se N è una struttura di Dedekind e M è una L_{D}-struttura, allora c'è un unico morfismo $F\colon N \to M$.*

(b) *L'immagine omomorfa di una struttura di Dedekind è una struttura induttiva. Viceversa, ogni struttura induttiva è immagine omomorfa di una qualsiasi struttura di Dedekind.*

(c) *Se N e M sono strutture di Dedekind, allora l'unico morfismo $F\colon N \to M$ di cui in* (a) *è un isomorfismo. In particolare, ogni struttura di Dedekind è isomorfa a $(\mathbb{N}, S, 0)$.*

(d) *Le strutture induttive sono, a meno di isomorfismo, $(\mathbb{N}, S, 0)$ e le $\mathcal{Z}_{m,n}$ con $m \geq 0$ e $n \geq 1$.*

Dimostrazione. (a) Cominciamo col dimostrare l'unicità del morfismo. Se $F, G\colon N \to M$ sono morfismi, sia

$$I = \{x \in N \mid F(x) = G(x)\}.$$

Poiché $0_N \in I$ e per definizione di morfismo: se $x \in I$ allora $S_N(x) \in I$, per Ind^2 sulla struttura N si ha che $I = N$, cioè $F = G$.

Per dimostrare l'esistenza di un morfismo, argomentiamo così. Sia $\mathcal{S}$ la famiglia dei sottoinsiemi W di $N \times M$ tali che $(0_N, 0_M) \in W$ e

$$(x, y) \in W \Rightarrow (S_N(x), S_M(y)) \in W. \tag{7.3}$$

È immediato verificare che $N \times M \in \mathcal{S}$ e che $F \in \mathcal{S}$ dove $F = \bigcap_{W \in \mathcal{S}} W$. Sia

$$I = \{x \in N \mid \exists! y \in M\, [(x, y) \in F]\}.$$

Verifichiamo per Ind^2 su N che $I = N$, e che quindi $F\colon N \to M$ è un morfismo. Chiaramente $(0_N, 0_M) \in F$. Se $(0_N, y) \in F$ con $y \neq 0_M$, sia $W = F \setminus \{(0_N, y)\}$. Poiché $(0_N, 0_M) \in W$, allora (7.1) implica che W soddisfa (7.3), da cui $W \in \mathcal{S}$ e quindi $F \subseteq W$: una contraddizione. Quindi $0_N \in I$. Supponiamo ora che $x \in I$ e sia $y \in M$ l'unico elemento tale che $(x, y) \in F$, così che $(S_N(x), S_M(y)) \in F$. Per assurdo, supponiamo che $(S_N(x), z) \in F$ per qualche $z \neq S_M(y)$ e sia $W' = F \setminus \{(S_N(x), z)\}$, così che $W' \notin \mathcal{S}$. Chiaramente $(0_N, 0_M) \in W'$, quindi (7.3) non vale, cioè esiste $(x', y') \in N \times M$ tale che $(x', y') \in F$ e $S_N(x') = S_N(x)$ e $S_M(y') = z$. Per (7.2) $x = x'$ e per $x \in I$ si ha che $y = y'$, da cui $z = S_M(y)$: una contraddizione.

(b) Supponiamo $F\colon N \to M$ sia un morfismo suriettivo, N una struttura di Dedekind e $I \subseteq M$ è tale che $0_M \in I$ e $\forall x \in M\,(x \in I \Rightarrow S_M(x) \in I)$. Allora Ind^2 applicata a N dimostra che $F^{-1}[I] = N$, da cui $I = M$.

Viceversa supponiamo che M sia induttiva. Sia N una struttura di Dedekind e sia $F\colon N \to M$ il morfismo garantito dalla (a). Sia

$$I = \{y \in M \mid \exists x \in N\,(F(x) = y)\}\,.$$

Allora $0_M = F(0_N) \in I$ e se $F(x) \in I$ allora $S_M(F(x)) = F(S_N(x)) \in I$. Quindi $I = M$, cioè F è suriettiva.

(c) Se N e M sono strutture di Dedekind, siano $F\colon M \twoheadrightarrow N$ e $G\colon N \twoheadrightarrow M$ dei morfismi suriettivi come da (b). Allora $F \circ G\colon N \to N$ è un morfismo suriettivo e poiché $\mathrm{id}_N\colon N \to N$ è l'unico morfismo (a), ne segue che $F \circ G = \mathrm{id}_N$, cioè $F\colon M \twoheadrightarrow N$ è un isomorfismo e G è il suo inverso.

(d) Supponiamo M sia una struttura induttiva. Per (b) fissiamo un morfismo suriettivo $F\colon \mathbb{N} \to M$. Se F è iniettivo, allora F è un isomorfismo, cioè $(M, S_M, 0_M)$ è isomorfo ad $(\mathbb{N}, S, 0)$. Se F non è iniettivo sia k il minimo naturale tale che $F(k) = F(m)$ per qualche $m < k$. Osserviamo che m è unico per la minimalità di k, cioè $\{F(0), \ldots, F(k-1)\}$ sono tutti distinti. In particolare $S_M(F(i)) = F(i+1)$ se $i + 1 < k$ e $S_M(F(k-1)) = F(m)$. Quindi M è isomorfa a $\mathcal{Z}_{m,n}$, dove $n = k - 1 - m$. □

7.B. Definizioni induttive. La dimostrazione dell'esistenza di un morfismo $F\colon N \to M$ nella parte (a) del Teorema 7.3 può sembrare esageratamente indiretta. Osserviamo che la funzione F è definita ricorsivamente da

$$\begin{cases} F(0_N) = 0_M \\ F(S_N(x)) = S_M(F(x)). \end{cases}$$

L'esistenza di una F siffatta è un fatto intuitivamente chiaro. Un'argomentazione apparentemente convincente, ma errata (e che purtroppo si trova anche in qualche manuale di logica) è la seguente: la funzione F è definita nel punto 0_N; inoltre se F è definita in $x \in N$ allora è definita in $S_N(x)$; quindi per il principio di induzione F è definita su tutto N. Questo ragionamento, anche se a prima vista ragionevole, risulta lacunoso ad una analisi attenta: parliamo del dominio di definizione di F e tuttavia non abbiamo ancora dimostrato l'esistenza di F, che è anzi proprio quello che vorremmo dimostrare! Inoltre il ragionamento precedente utilizza soltanto il principio di induzione Ind^2 nella struttura N e quindi, se corretto, dimostrerebbe che:

> se $(N, S_N, 0_N)$ è induttiva e $(M, S_M, 0_M)$ arbitraria, allora c'è un morfismo $F\colon N \to M$.

Ma questo è falso — basta considerare $N = \mathcal{Z}_n$ e $M = \mathcal{Z}'_n$ con $n \geq 2$.

Lo studio sistematico delle definizioni ricorsive è rimandato alla Sezione 13, tuttavia conviene sin da ora enunciare un risultato preliminare che permette di giustificare molte costruzioni induttive.

Teorema 7.4. *Siano A e B insiemi non vuoti, e siano $g\colon B \to A$ e $F\colon \mathbb{N} \times B \times A \to A$ delle funzioni. Allora esiste un'unica $f\colon \mathbb{N} \times B \to A$ tale che*

$$\begin{cases} f(0,b) = g(b) \\ f(n+1,b) = F(n,b,f(n,b)). \end{cases}$$

Dimostrazione. La dimostrazione è analoga alla dimostrazione del Teorema 7.3. Si considera l'insieme

$$\begin{aligned} \mathcal{S} = \{W \subseteq (\mathbb{N} \times B) \times A \mid\ & ((0,b), g(b)) \in W \\ & \wedge \forall ((n,b),a)\,[((n,b),a) \in W \Rightarrow ((n+1,b), F(n,b,a)) \in W]\} \end{aligned}$$

e sia $f = \bigcap \mathcal{S} \subseteq (\mathbb{N} \times B) \times A$. Come nella dimostrazione del Teorema 7.3, $f \in \mathcal{S}$ e $I = \mathbb{N}$ per Ind^2, dove $I = \{n \in \mathbb{N} \mid \forall b \in B\, \exists! a \in A\,[((n,b),a) \in f]\}$. Quindi f è la funzione cercata.

La dimostrazione dell'unicità è lasciata al lettore. □

Se F non dipende da $\mathbb{N}$ o da B, l'enunciato del Teorema 7.4 si semplifica notevolmente.

Corollario 7.5. *Siano A e B insiemi non vuoti e sia $g\colon B \to A$.*

(a) *Per ogni $F\colon B \times A \to A$ esiste un'unica $f\colon \mathbb{N} \times B \to A$ tale che*

$$\begin{cases} f(0,b) = g(b) \\ f(n+1,b) = F(b, f(n,b)). \end{cases}$$

(b) *Per ogni $F\colon \mathbb{N} \times A \to A$ esiste un'unica $f\colon \mathbb{N} \times B \to A$ tale che*

$$\begin{cases} f(0,b) = g(b) \\ f(n+1,b) = F(n, f(n,b)). \end{cases}$$

(c) *Per ogni $F\colon A \to A$ esiste un'unica $f\colon \mathbb{N} \times B \to A$ tale che*

$$\begin{cases} f(0,b) = g(b) \\ f(n+1,b) = F(f(n,b)). \end{cases}$$

Quando g è costante, l'enunciato del Corollario 7.5 può essere ulteriormente semplificato. Per esempio la parte (c) diventa:

Corollario 7.6. *Se $\bar{a} \in A$ e $F\colon A \to A$ allora esiste un'unica $f\colon \mathbb{N} \to A$ tale che*

$$\begin{cases} f(0) = \bar{a} \\ f(n+1) = F(f(n)). \end{cases}$$

In altre parole, f è la successione: $\bar{a}, F(\bar{a}), F(F(\bar{a})), \ldots$.

Esempio 7.7. Fissato un insieme arbitrario X e una funzione $h\colon X \to X$, se A è l'insieme delle funzioni da X in sé stesso, $\bar{a} = \mathrm{id}_X$ è la funzione identica, e $F\colon A \to A$ è la mappa $k \mapsto h \circ k$, allora per il Corollario 7.6 c'è una $f\colon \mathbb{N} \to A$ tale che

$$\forall n \in \mathbb{N}\, \forall x \in X\ \Big(f(n)(x) = h^{(n)}(x)\Big).$$

Esempio 7.8. L'addizione su $\mathbb{N}$ è definita ricorsivamente da

$$\begin{cases} f(0,m) = m \\ f(n+1,m) = S(f(n,m)). \end{cases}$$

La sua esistenza discende dal Corollario 7.5(c) con $A = B = \mathbb{N}$, $g(n) = n$ e $F\colon A \to A$, $F(n) = S(n)$.

La moltiplicazione su $\mathbb{N}$ è definita ricorsivamente da

$$\begin{cases} f(0,m) = 0 \\ f(n+1,m) = m + f(n,m). \end{cases}$$

La sua esistenza discende dal Corollario 7.5(b) con $A = B = \mathbb{N}$, $g(n) = 0$ e $F\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ la funzione somma.

Esempio 7.9. Fissiamo un insieme non vuoto A con un'operazione binaria $*$ e sia $(a_n)_n$ una successione di elementi di A. La successione

$$s\colon \mathbb{N} \to A, \quad s(n) = (\cdots (a_0 * a_1) * \cdots * a_{n-1}) * a_n$$

si ottiene dal Corollario 7.5(b) ponendo $B = \mathbb{N}$, $g(n) = a_n$ e $F\colon B \times A \to A$ tale che $F(b,a) = a * g(b+1)$. Allora c'è un'unica $f\colon \mathbb{N} \times B \to A$ tale che

$$\begin{cases} f(0,b) = g(b) \\ f(n+1,b) = f(n,b) * g(n+1) \end{cases}$$

quindi $s(n) = f(n,0)$.

Questo tipo di costruzioni è molto comune in matematica. Per esempio, se $A = \mathbb{R}$, la somma della serie $\sum_{n=0}^{\infty} a_n$ è definita come il limite (se esiste) della successione delle ridotte $s(k) = \sum_{n=0}^{k} a_n$.

Esempio 7.10. Il sottogruppo H di un gruppo G generato da un sottoinsieme X è l'intersezione di tutti i sottogruppi di G contenenti X, ma può anche essere definito prendendo prodotti e inversi a partire da X. Più precisamente, sia $f\colon \mathscr{P}(G) \to \mathscr{P}(G)$ data da $f(Y) = Y \cup \{ab^{-1} \mid a, b \in Y\}$, così che c'è una $g\colon \mathbb{N} \times \mathscr{P}(G) \to \mathscr{P}(G)$ tale che $g(0,Y) = Y$ e $g(n+1,Y) = f(g(n,Y))$. Ponndo $H_n = g(n, X \cup \{1_G\})$ allora $H = \bigcup_n H_n$.

7.C. Strutture induttive. L'Esempio 7.8 mostra che l'esistenza della somma e del prodotto discendono dal Teorema 7.4. Tuttavia la costruzione della somma e del prodotto non dipende dal Teorema 7.4 e può essere effettuata in ogni struttura induttiva.

Fissiamo una struttura induttiva N. Una traslazione di ordine $x \in N$ è un morfismo $t_x^N = t_x \colon (N, S_N, 0_N) \to (N, S_N, x)$, cioè

$$t_x(0_N) = x \quad \text{e} \quad t_x(S_N(y)) = S_N(t_x(y))$$

per ogni $y \in N$. Se $t_x, t'_x \colon N \to N$ sono traslazioni di ordine x, allora $t_x(y) = t'_x(y)$ per ogni $y \in N$, quindi la traslazione di ordine x — se esiste — è unica. La traslazione di ordine 0_N è id_N e se t_x è la traslazione di ordine x allora $S_N \circ t_x$ è la traslazione di ordine $S_N(x)$, quindi per induzione t_x esiste per ogni $x \in N$. La funzione

$$a \colon N \times N \to N, \quad a(x, y) = t_x(y)$$

è l'unica funzione che soddisfa le equazioni

$$\begin{cases} a(x, 0) = x, \\ a(x, S(y)) = S(a(x, y)). \end{cases}$$

Infatti se a' è un'altra funzione siffatta basta applicare Ind^2 all'insieme $I = \{y \in N \mid \forall x\, (a(x, y) = a'(x, y))\}$ per concludere che a e a' coincidono. La funzione a si dice addizione su N e scriveremo $x +_N y$ invece di $a(x, y)$, e le condizioni precedenti sono riscritte come

$$\forall x\, (x + 0 = x)\,, \tag{7.4}$$

$$\forall x \forall y\, (x + S(y) = S(x + y))\,. \tag{7.5}$$

Se $F \colon N \to M$ è un morfismo di strutture induttive, allora $F \circ t_x^N = t_{F(x)}^M \circ F$ per Ind^2, quindi

$$F(x +_N y) = F(t_x^N(y)) = t_{F(x)}^M(F(y)) = F(x) +_M F(y).$$

In altre parole: ogni morfismo di strutture induttive è un morfismo per le strutture espanse mediante addizione.

L'operazione di moltiplicazione su N è la funzione

$$m \colon N \times N \to N, \quad m(x, y) = u_x(y)$$

dove $u_x^N = u_x \colon N \to N$ è definita da $u_x(0_N) = 0_N$ e $u_x(S_N(y)) = u_x(y) +_N x$. Argomentando come per l'addizione, possiamo dire che la moltiplicazione su N è l'unica funzione $m \colon N \times N \to N$ tale che

$$\forall x\, (x \cdot 0 = 0)\,, \tag{7.6}$$

$$\forall x\, \forall y\, (x \cdot S(y) = (x \cdot y) + x)\,, \tag{7.7}$$

dove abbiamo scritto $x \cdot_N y$ invece di $m(x, y)$. Ogni morfismo di strutture induttive è un morfismo per le strutture espanse mediante addizione e moltiplicazione.

Abbiamo quindi dimostrato il seguente

Teorema 7.11. *Ogni struttura induttiva $(N, S_N, 0_N)$ può essere espansa in un unico modo ad una struttura della forma $(N, S_N, 0_N, +_N, \cdot_N)$ che soddisfa (7.4)–(7.7), e tale che ogni morfismo $F\colon N \to M$ tra strutture induttive è anche un morfismo tra le espansioni.*

Quindi per la parte (d) del Teorema 7.3, le operazioni di somma e prodotto sono definite[11] su $(\mathbb{N}, S, 0)$ e sulle strutture $\mathcal{Z}_{m,n}$. Come vedremo nella prossima Sezione 7.E, l'addizione e la moltiplicazione nella struttura $(\mathbb{N}, S, 0)$ sono operazioni associative e commutative, e la moltiplicazione è distributiva rispetto alla somma; in $\mathcal{Z}_{m,n}$ e in particolare in $\mathbb{Z}/n\mathbb{Z}$ valgono i medesimi risultati, dato che commutatività, associatività e distributività sono enunciati positivi (vedi pagina 50) e le $\mathcal{Z}_{m,n}$ sono immagini omomorfe di $(\mathbb{N}, S, 0)$.

La parte (a) del Teorema 7.3 può essere usato per dimostrare l'esistenza della funzione esponenziale

$$\exp\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}, \qquad \begin{cases} \exp(x, 0) = 1 \\ \exp(x, S(y)) = \exp(x, y) \cdot x. \end{cases}$$

Infatti $\exp(x, y) = F_x(y)$ dove $F_x\colon N \to M$ è l'omomorfismo tra la struttura di Dedekind $N = (\mathbb{N}, S, 0)$ e la L_{D}-struttura $M = (\mathbb{N}, u_x, 1)$, dove u_x è come sopra. Questa costruzione non si applica alle strutture induttive (Esercizio 7.22).

7.D. Il principio del minimo. Ind^2 è equivalente a due altri principi formulati nel linguaggio contenente il simbolo $<$: il **principio di induzione forte al second'ordine**

$$(\mathsf{sInd}^2) \qquad \forall I\,[\forall x\,(\forall y\,(y < x \Rightarrow y \in I) \Rightarrow x \in I) \Rightarrow \forall x\,(x \in I)]\,.$$

e il **principio del minimo al second'ordine**

$$(\mathsf{MP}^2) \qquad \forall I\,[I \neq \emptyset \Rightarrow \exists x\,(x \in I \wedge \forall y\,(y < x \Rightarrow y \notin I))]\,.$$

Proposizione 7.12. *Supponiamo che $(M, <_M, S_M, 0_M) \models \Sigma_{(\mathbb{N},<,S,0)}$. Le seguenti condizioni sono equivalenti:*

(a) *M soddisfa Ind^2,*

(b) *M soddisfa sInd^2,*

(c) *M soddisfa MP^2.*

[11] Questo non significa che $+$ o $\cdot$ siano *definibili* nella struttura $(\mathbb{N}, S, 0)$ — si veda la Sezione 6.A.

Dimostrazione. $\mathsf{Ind}^2 \Rightarrow \mathsf{sInd}^2$: Supponiamo $I \subseteq M$ sia tale che

$$\forall x \in M\,(\forall y \in M\,(y < x \Rightarrow y \in I) \Rightarrow x \in I)$$

e sia

$$J = \{x \in M \mid \forall y < x\,(y \in I)\}\,.$$

Allora $J \subseteq I$ per ipotesi, quindi $\forall y \in M\,(y < 0 \Rightarrow y \in I)$ vale banalmente, da cui $0 \in J$. Supponiamo $x \in J$ e sia $y < S(x)$: allora $y < x$ oppure $y = x$, e in ogni caso $y \in I$, da cui $S(x) \in J$. Da Ind^2 segue che $J = M$, quindi $I = M$ come richiesto.

$\mathsf{sInd}^2 \Rightarrow \mathsf{MP}^2$: Per assurdo supponiamo che $\emptyset \neq$ Â $I \subseteq M$ sia tale che

$$\forall x \in I\,\exists y \in I\,(x \neq y \wedge \neg(x < y)).$$

Applichiamo l'induzione forte a $J = M \setminus I$. Supponiamo $x \in M$ sia tale che $\forall y \in M\,(y < x \Rightarrow y \in J)$. Se $x \in I$, allora x sarebbe il minimo di I, quindi $x \in J$. Per induzione forte $J = M$, da cui $I = \emptyset$, contro la nostra ipotesi.

$\mathsf{MP}^2 \Rightarrow \mathsf{Ind}^2$: Supponiamo che M soddisfi il principio del minimo e supponiamo che $I \subseteq M$ sia chiuso per S e tale che $0 \in I$. Se $I \neq M$ allora sia x il minimo di $M \setminus I$. Poiché $x \neq 0$ allora $x = S(y)$ per qualche y per un assioma di $\Sigma_{(\mathbb{N},S,0,<)}$, quindi $y \in I$ per minimalità. Ma allora $x = S(y) \in I$: una contraddizione. □

7.E. L'aritmetica di Peano. Per studiare l'aritmetica con i metodi della logica del prim'ordine si indebolisce il principio di induzione Ind^2 richiedendo che valga soltanto per gli insiemi di verità di una formula del prim'ordine. In altre parole si richiede

$$(\mathsf{Ind}_\varphi)\qquad \begin{aligned}\forall y_1,\dots,y_n\Big[&(\varphi(0,y_1,\dots,y_n)\\ &\wedge\ \forall x(\varphi(x,y_1,\dots,y_n) \Rightarrow \varphi(S(x),y_1,\dots,y_n)))\\ &\Rightarrow \forall x\varphi(x,y_1,\dots,y_n)\Big],\end{aligned}$$

per ogni L_{D}-formula $\varphi(x,y_1,\dots,y_n)$. Indicheremo con $\mathsf{Ind}_{\mathsf{D}}$ la lista degli infiniti assiomi Ind_φ con φ una L_{D}-formula.

Questo schema di assiomi, noto come **principio di induzione del prim'ordine** non è sufficiente per dimostrare la parte (c) del Teorema 7.3. In altre parole, una struttura che soddisfi (7.1), (7.2) e $\mathsf{Ind}_{\mathsf{D}}$ non è necessariamente isomorfa a $(\mathbb{N}, S, 0)$. Per esempio la L_{D}-struttura che ha per universo $M = \mathbb{N} \cup \mathbb{Z}$ e tale che $0_M = (0,0)$ e $S_M(k,i) = (k+1,i)$, soddisfa (7.1), (7.2) e $\mathsf{Ind}_{\mathsf{D}}$ (come vedremo nella Sezione 32.C), ma chiaramente non è isomorfa a $(\mathbb{N}, S, 0)$ e quindi non soddisfa (Ind^2).

In analogia con quanto visto nella Sezione 7.D, è possibile formulare i principi sInd_φ e MP_φ quando φ è una L-formula e L è un linguaggio contenente i simboli $S, 0, <$. L'equivalenza tra Ind_φ, sInd_φ e MP_φ è conseguenza logica di $\Sigma_{(\mathbb{N},S,0,<)}$.

Definizione 7.13. Il linguaggio L_{PA} è ottenuto aggiungendo al linguaggio L_{D} due simboli di operazione binaria $+$ e $\cdot$ ed un simbolo di relazione binaria $<$.

L'**aritmetica di Peano** (PA) è la teoria nel linguaggio L_{PA} che ha per assiomi:

$$\forall x\ (S(x) \neq 0)\,, \tag{7.1}$$

$$\forall x, y\ (x \neq y \Rightarrow S(x) \neq S(y))\,, \tag{7.2}$$

$$\forall x\ (x + 0 = x)\,, \tag{7.4}$$

$$\forall x\, \forall y\ (x + S(y) = S(x + y))\,. \tag{7.5}$$

$$\forall x\ (x \cdot 0 = 0)\,, \tag{7.6}$$

$$\forall x\, \forall y\, (x \cdot S(y) = (x \cdot y) + x)\,, \tag{7.7}$$

gli enunciati per l'ordinamento

$$\forall x \neg\, (x < 0)\,, \tag{7.8}$$

$$\forall x\, \forall y\, (x < S(y) \Leftrightarrow (x < y \vee x = y))\,, \tag{7.9}$$

e il principio di induzione al prim'ordine $\mathsf{Ind}_{\mathsf{PA}}$, cioè Ind_φ per ogni L_{PA}-formula $\varphi(x, y_1, \ldots, y_n)$.

Chiaramente

$$(\mathbb{N}, S, 0, +, \cdot, <) \vDash \mathsf{PA},$$

ma, come vedremo nella Sezione 32.C, ci sono altre L_{PA}-strutture non isomorfe ad $\mathbb{N}$ che sono modelli di PA.

Il principio di induzione al prim'ordine $\mathsf{Ind}_{\mathsf{PA}}$, benché più debole di Ind, è sufficientemente forte per dimostrare molti fatti sui numeri naturali.

Proposizione 7.14. *Le seguenti affermazioni discendono dagli assiomi di* PA*:*

(a) $\forall x\, (0 + x = x)$,
(b) $\forall x \forall y\, (x + y = y + x)$,
(c) $\forall x \forall y \forall z\, (x + (y + z) = (x + y) + z)$,
(d) $\forall x\, (0 \cdot x = 0)$,
(e) $\forall x\, (x \cdot S(0) = S(0) \cdot x = x)$,
(f) $\forall x \forall y \forall z\, ((x + y) \cdot z = (x \cdot z) + (y \cdot z))$,
(g) $\forall x \forall y\, (x \cdot y = y \cdot x)$,

(h) $\forall x \forall y \forall z\, (x \cdot (y \cdot z) = (x \cdot y) \cdot z)$.

Dimostrazione. (a) Sia $\varphi(x)$ la formula $0 + x = x$: per (7.4) $0 + \hat{\mathrm{A}}\ 0 = 0$ e se vale $\varphi(x)$ allora

$$\begin{aligned} 0 + S(x) &= S(0 + x) && \text{per (7.5)} \\ &= S(x) && \text{per } \varphi(x) \end{aligned}$$

e quindi $\varphi(x) \Rightarrow \varphi(S(x))$.

(b) Sia $\varphi(x)$ la formula $\forall y\, (x + y = y + x)$: è sufficiente verificare che $\varphi(0)$ e che $\varphi(x) \Rightarrow \varphi(S(x))$ per ogni x.

- Per (7.4) e per la parte (a) si ha $\forall y\, (0 + y = y + 0)$, cioè $\varphi(0)$.
- Assumiamo $\varphi(x)$, vale a dire $\forall y\, (x + y = y + x)$ e dimostriamo per induzione su y che vale $\varphi(S(x))$, cioè $\forall y\, (S(x) + y = y + S(x))$. Da $\varphi(0)$ e (7.4) si ottiene $S(x) + 0 = 0 + S(x)$; assumendo

(*) $$S(x) + y = y + S(x)$$

e utilizzando ripetutamente (7.5) si ha

$$\begin{aligned} S(x) + S(y) &= S(S(x) + y) \\ &= S(y + S(x)) && \text{per (*)} \\ &= S(S(y + x)) \\ &= S(S(x + y)) && \text{per } \varphi(x) \\ &= S(x + S(y)) \\ &= S(S(y) + x) && \text{per } \varphi(x) \\ &= S(y) + S(x). \end{aligned}$$

Questo completa la dimostrazione di (b).

La dimostrazione delle rimanenti formule (c)–(h) è lasciata al lettore. □

In particolare, se $M \vDash \mathsf{PA}$, allora $(M, +, 0)$ è un monoide.

Vediamo qualche risultato sull'ordinamento.

Teorema 7.15. *Le seguenti affermazioni sono conseguenze degli assiomi di* PA*:*

(a) $x < y \Leftrightarrow \exists z\, (x + S(z) = y)$,
(b) $\forall x \forall y \forall z\, (x < y \wedge y < z \Rightarrow x < z)$ *(transitività),*
(c) $\forall x \forall y\, (x < y \Leftrightarrow S(x) < S(y))$,
(d) $\forall x \neg\, (x < x)$ *(irriflessività),*
(e) $\forall x\, (0 \neq x \Rightarrow 0 < x)$,
(f) $\forall x, y\, (x < y \vee x = y \vee y < x)$ *(tricotomia),*

(g) $\forall x, y, z\,(x < y \Rightarrow x + z < y + z)$ *(monotonia dell'addizione),*

(h) $\forall x, y, z\,(z \neq 0 \wedge x < y \Rightarrow x \cdot z < y \cdot z)$ *(monotonia della moltiplicazione).*

Dimostrazione. (a) Dimostriamo per induzione su y che $\forall y \varphi(y)$, dove $\varphi(y)$ è la formula

$$\forall x\,(x < y \Leftrightarrow \exists z\,(x + S(z) = y))\,.$$

Per dimostrare $\varphi(0)$ fissiamo un x: poiché $x < 0$ è impossibile per (7.8), il risultato segue immediatamente. Supponiamo valga $\varphi(y)$ e fissiamo un x arbitrario. Allora

$$\begin{aligned} x < S(y) &\Leftrightarrow x < y \vee x = y && \text{(per (7.9))} \\ &\Leftrightarrow \exists z\,(x + S(z) = y) \vee x + S(0) = S(y) && \text{(per ipotesi induttiva)} \\ &\Leftrightarrow \exists z\,(x + S(z) = S(y)) \end{aligned}$$

cioè vale $\varphi(S(y))$.

(b) Supponiamo $x < y$ e $y < z$. Per (a) fissiamo u e v tali che $x + S(u) = y$ e $y + S(v) = z$. Allora

$$z = y + S(v) = (x + S(u)) + S(v) = x + (S(u) + S(v)) = x + S(S(u) + v),$$

cioè $x < z$ per (a).

(c) Sfruttando la parte (b),

$$\begin{aligned} S(x) < S(y) &\Leftrightarrow \exists z\,(S(x) + S(z) = S(y)) \\ &\Leftrightarrow \exists z\,(S(y) = S(S(x) + z)) && (7.5) \\ &\Leftrightarrow \exists z\,(y = S(x) + z) \\ &\Leftrightarrow \exists z\,(y = x + S(z)) && \text{Proposizione 7.14(b)} \\ &\Leftrightarrow x < y. \end{aligned}$$

(d) La formula $\neg\,(0 < 0)$ segue da (7.1) e se $\neg\,(x < x)$ allora $\neg\,(S(x) < S(x))$ per (c). Quindi il risultato segue per induzione.

(e) Dimostriamo per induzione su x che vale $\forall x \varphi(x)$ dove $\varphi(x)$ è

$$0 = x \vee 0 < x.$$

$\varphi(0)$ è immediata, per $\varphi(x) \Rightarrow \varphi(S(x))$ osserviamo che da (7.9) segue che $\varphi(x) \Leftrightarrow 0 < x \vee 0 = x \Leftrightarrow 0 < S(x) \Rightarrow \varphi(S(x))$.

(f) Dimostriamo per induzione su x che vale $\forall x \varphi(x)$, dove $\varphi(x)$ è

$$\forall y\,(x < y \vee x = y \vee y < x)\,.$$

Per $x = 0$ il risultato discende da (e), quindi supponiamo $\varphi(x)$ per un certo x e fissiamo un y arbitrario: dobbiamo verificare che $S(x) < y \vee S(x) = y \vee y < S(x)$. Per ipotesi induttiva $x < y \vee x = y \vee y < x$ e consideriamo i

vari casi. Se $x < y$ allora $S(x) < S(y)$ da cui per (c) $S(x) < y \vee S(x) = y$. Se $x = y$ oppure $y < x$ allora $y < S(y) = S(x)$ oppure $y < S(y) < S(x)$ per (7.9), quindi $y < S(x)$.

(g) Per induzione dimostriamo che $\forall z\, \varphi(z)$, dove $\varphi(z)$ è la formula

$$\forall x, y\, (x < y \Rightarrow x + z < y + z)\,.$$

Se $z = 0$ il risultato è immediato, e se assumiamo $\varphi(z)$ allora

$$\begin{aligned} x + S(z) &= S(x + z) \\ &< S(y + z) && \text{per } \varphi(z) \text{ e la parte (c)} \\ &= y + S(z) \end{aligned}$$

quindi $\varphi(S(z))$.

(h) Per induzione dimostriamo che $\forall z\, \varphi(z)$, dove $\varphi(z)$ è la formula

$$\forall x, y\, (z \neq 0 \wedge x < y \Rightarrow x \cdot z < y \cdot z)\,.$$

Se $z = 0$ non c'è nulla da dimostrare, quindi possiamo supporre $\varphi(z)$ con l'obbiettivo di dimostrare $\varphi(S(z))$. Poiché $\forall w\, (w \cdot S(0) = w)$, possiamo supporre che $z > 0$. Allora

$$\begin{aligned} x \cdot S(z) &= x \cdot z + x \\ &< y \cdot z + x && \text{per } \varphi(z) \text{ e per la commutatività} \\ &< y \cdot z + y && \text{per (g)} \end{aligned}$$

quindi $\varphi(S(z))$ vale. □

Quindi un modello di PA è un semianello commutativo ordinato (Definizione 5.5).

Proposizione 7.16. *Il seguente enunciato (divisione col resto) è conseguenza logica di* PA

$$\forall x\, \forall y > 0\, \exists! q\, \exists! r\, \left[x = y \cdot q + r \wedge q \leq x \wedge r < y\right]$$

In particolare, per ogni $n \in \mathbb{N} \setminus \{0\}$, l'enunciato

$$\forall x \exists! y\, (\chi_n(x, y) \wedge y < S^{(n)}(0))$$

è una conseguenza degli assiomi di PA*, dove $\chi_n(x, y)$ è la formula*

$$\exists z\, \big(x + \underbrace{z + \cdots + z}_{n} = y \;\vee\; y + \underbrace{z + \cdots + z}_{n} = x\big)$$

di pagina 113.

Dimostrazione. Fissiamo x e y con $y > 0$. Per la monotonicità della moltiplicazione $x = 1 \cdot x < y \cdot S(x)$, quindi per il principio del minimo c'è un primo z tale che $x < y \cdot z$. Poiché z non può essere 0, allora $z = S(q)$ per qualche q. Per tricotomia $y \cdot q = x$ oppure $y \cdot q < x$. Nel primo caso poniamo $r = 0$. Nel secondo caso $y \cdot q = y \cdot q + 0 < x < y \cdot S(q) = y \cdot q + y$ quindi per il principio del minimo c'è un primo w tale che $y \cdot q + w > x$. Osserviamo che $w \leq y$, e dato che $w = 0$ è impossibile, allora $w = S(r)$ per qualche r, e quindi $y \cdot q + r$. Nuovamente per tricotomia $y \cdot q + r < x$ oppure $y \cdot q + r = x$: il primo caso implica che $x \geq S(y \cdot q + r) = y \cdot q + S(r) = y \cdot q + w > x$, una contraddizione. Ne consegue che abbiamo dimostrato che

$$\forall x\, \forall y > 0\, \exists q, r\, \big[x = y \cdot q + r \wedge q \leq x \wedge r < y\big].$$

Dobbiamo dimostrare che q e r sono unici. Supponiamo che $x = y \cdot q_1 + r_1 = y \cdot q_2 + r_2$ con $r_1, r_2 < y$. Se $q_1 < q_2$ allora $y \cdot q_1 < y \cdot q_2 + r_2 = x$, e poiché $S(q_1) \leq q_2$ allora $x = y \cdot q_1 + r_1 < y \cdot q_1 + y = y \cdot S(q_1) \leq y \cdot q_2 + r_2 = x$, una contraddizione. Analogamente l'ipotesi $q_2 < q_1$ porta ad una contraddizione. Quindi $q_1 = q_2 = q$. Se $r_1 \neq r_2$, diciamo $r_1 < r_2$, allora $x = y \cdot q + r_1 < y \cdot q + r_2 = x$, una contraddizione. Quindi $r_1 = r_2$ come richiesto e

$$\forall x\, \forall y > 0\, \exists! q\, \exists! r\, \big[x = y \cdot q + r \wedge q \leq x \wedge r < y\big].$$

Se nell'equazione qui sopra poniamo $y = S^{(n)}(0)$, poiché

$$x \cdot S^{(n)}(0) = \underbrace{x + \cdots + x}_{n \text{ volte}}$$

si ha che

$$\forall x \exists! r\, \big(\chi_n(x, r) \wedge r < S^{(n)}(0)\big).$$

è conseguenza logica di PA. □

Quindi ogni modello di PA è un modello dell'aritmetica di Presburger. Come per le teorie $\Sigma_{(\mathbb{N},S)}$, $\Sigma_{(\mathbb{N},<)}$ e $\Sigma_{(\mathbb{N},+)}$, ci sono modelli dell'aritmetica di Peano non isomorfi ad $\mathbb{N}$, ma la costruzione di tali modelli non standard non è elementare, ed è rimandata alla Sezione 32.C.

Per sviluppare adeguatamente la combinatorica e la teoria dei numeri in PA, è necessario poter descrivere nel linguaggio L_{PA} gli insiemi e le funzioni che comunemente si studiano in queste discipline. Innanzitutto introduciamo dei termini chiusi di L_{PA} per denotare i singoli numeri naturali: per $n \in \mathbb{N}$ poniamo

$$\overline{n+1} = S(\overline{n}),$$

dove abbiamo usato $\overline{0}$ per il simbolo di costante di L_{PA} onde evitare confusioni con il numero naturale $0 \in \mathbb{N}$. Il termine $\overline{n}$ si dice **numerale** di n. Diremo

che una funzione $f\colon \mathbb{N}^k \to \mathbb{N}$ è **rappresentabile in** PA se c'è una formula $\varphi(x_1, \dots, x_k, y)$ tale che per ogni $n_1, \dots, n_k \in \mathbb{N}$

$$\forall y \left(\varphi[\![\overline{n_1}/x_1, \dots, \overline{n_k}/x_k]\!] \Leftrightarrow y = \overline{f(n_1, \dots, n_k)} \right)$$

è un teorema di PA. L'espressione $\varphi[\![\overline{n_1}/x_1, \dots, \overline{n_k}/x_k]\!]$ denota l'enunciato ottenuto da φ sostituendo alle variabili $x_1, \dots, x_k$ i numerali $\overline{n_1}, \dots, \overline{n_k}$ e poiché questi sono termini chiusi, la sostituzione può essere sempre effettuata (vedi pagina 32).

Osserviamo che la nozione di rappresentabilità è un rafforzamento del concetto di definibilità : se $f\colon \mathbb{N}^k \to \mathbb{N}$ è rappresentabile in PA, allora il suo grafo

$$\mathrm{Gr}(f) = \{(n_1, \dots, n_k, m) \in \mathbb{N}^{k+1} \mid f(n_1, \dots, n_k) = m\}$$

è definibile in $(\mathbb{N}, +, \cdot)$. Nella Sezione 9 studieremo le funzioni ricorsive (che costituiscono una formalizzazione della nozione intuitiva di funzione effettivamente calcolabile) e nella Sezione 19.A dimostreremo che *ogni funzione ricorsiva è rappresentabile in* PA, un teorema che estende di molto i risultati di definibilità in $(\mathbb{N}, +, \cdot)$ visti nella Sezione 6.B.

Esercizi

Esercizio 7.17. Dimostrare che $T \models \mathsf{Ind}_T$, dove T è una delle teorie

$$\Sigma_{(\mathbb{N},S,0)}, \quad \Sigma_{(\mathbb{N},<,S,0)}, \quad \Sigma_{(\mathbb{N},+,<,S,0)}$$

della Sezione 6.A e Ind_T è lo schema di assiomi Ind_φ dove φ è una formula del linguaggio di T.

Esercizio 7.18. Completare i dettagli della dimostrazione dell'esistenza del morfismo $F\colon N \to M$ nella parte (a) del Teorema 7.3.

Esercizio 7.19. Se $F\colon N \to M$ è un morfismo di L_{D}-strutture, la relazione di equivalenza su N indotta da F è $x \equiv y \Leftrightarrow F(x) = F(y)$. Dimostrare che la relazione di equivalenza indotta da un morfismo è una congruenza di Dedekind, cioè una relazione di equivalenza $\sim$ su N tale che

$$x \sim y \Rightarrow S_N(x) \sim S_N(y),$$

e ogni congruenza di Dedekind su una L_{D}-struttura è indotta da qualche morfismo suriettivo.

Esercizio 7.20. Supponiamo $(N, S_N, 0_N)$ sia una L_{D}-struttura tale che per ogni una L_{D}-struttura $(M, S_M, 0_M)$ c'è un unico morfismo $F\colon N \to M$. Dimostrare che N è una struttura di Dedekind, e quindi è isomorfa ad $\mathbb{N}$.

Esercizio 7.21. Completare la dimostrazione della Proposizione 7.14 verificando le parti (c)–(h).

Esercizio 7.22. Dimostrare che non c'è nessuna funzione $E\colon (\mathbb{Z}/3\mathbb{Z})^2 \to \mathbb{Z}/3\mathbb{Z}$ che soddisfi le equazioni ricorsive per l'esponenziale.

Esercizio 7.23. Se $f\colon \mathbb{N}^{k+1} \to \mathbb{N}$ definiamo $\sum f\colon \mathbb{N}^{k+1} \to \mathbb{N}$ e $\prod f\colon \mathbb{N}^{k+1} \to \mathbb{N}$ mediante

$$\begin{cases} \sum f(x_1, \dots x_k, 0) = 0 \\ \sum f(x_1, \dots x_k, n+1) = f(x_1, \dots x_k, n+1) + \sum f(x_1, \dots x_k, n) \end{cases}$$

e

$$\begin{cases} \prod f(x_1, \dots x_k, 0) = 1 \\ \prod f(x_1, \dots x_k, n+1) = f(x_1, \dots x_k, n+1) \cdot \prod f(x_1, \dots x_k, n). \end{cases}$$

Verificare che l'esistenza di $\sum f$ e $\prod f$ discende dal Teorema 7.4.

Esercizio 7.24. L'ordinamento di un modello non-standard $\mathcal{M}$ di PA è $M = \mathbb{N} \cup L \times \mathbb{Z}$ dove L è un ordine lineare denso senza primo o ultimo elemento. Dimostrare che L non è completo; in particolare non è isomorfo a $\mathbb{R}$.

Note e osservazioni

Questa sezione è basata sull'articolo [**Hen60**] di Henkin, dove la dimostrazione della parte (a) del Teorema 7.3 è attribuita a Lorenzen e, indipendentemente a Hilbert e Bernays. (Si veda anche [**Jac85**, p. 16].) La prima assiomatizzazione dell'aritmetica basata sull'operazione di successore è dovuta a Dedekind, mentre quella basata sulle operazioni di somma e prodotto è dovuta a Peano.

Capitolo III

Algebre di Boole, calcolabilità, insiemi

8. Ordini, reticoli e algebre di Boole

8.A. Ordini. Ricordiamo che una relazione binaria su un insieme non vuoto X è un sottoinsieme di $X \times X$. Se L_{ORDINI} è il linguaggio che contiene il simbolo di relazione binaria $\leq$ diremo che $(M, \leq_M)$ è una struttura di ordine (o semplicemente: un ordine) se $\leq_M \subseteq M \times M$ soddisfa la proprietà riflessiva, antisimmetrica e transitiva, cioè se $(M, \leq_M)$ soddisfa gli L_{ORDINI}-enunciati

$$\forall x\,(x \leq x)$$
$$\forall x, y\,(x \leq y \wedge y \leq x \Rightarrow x = y)$$
$$\forall x, y, z\,(x \leq y \wedge y \leq z \Rightarrow x \leq z)\,.$$

Se $\leq_M$ è **connessa su** M, cioè $(M, \leq_M)$ soddisfa l'enunciato

$$\forall x, y\,(x \leq y \vee y \leq x \vee x = y)\,,$$

allora si ha un **ordine totale** o **lineare**.

Definizione 8.1. (i) Un **pre-ordine** o **quasi-ordine** è una struttura $(M, \preceq)$ tale che $\preceq$ è una relazione riflessiva e transitiva.

(ii) Un **ordine stretto** è una struttura $(M, \prec)$ tale che la relazione $\prec$ è irriflessiva e se la espandiamo aggiungendoci la diagonale si ottiene un

ordine. In altre parole $(M, \prec)$ soddisfa

$$\forall x \neg(x \prec x)$$
$$\forall x, y, z\,(x \prec y \wedge y \prec z \Rightarrow x \prec z)$$
$$\forall x, y\,((x \prec y \vee x = y) \wedge (y \prec y \vee x = y) \Rightarrow x = y)\,.$$

Il nome *ordine stretto* è poco felice perché si tratta di una relazione che non è un ordine, ma è oramai diventato consuetudine. Per analogia con quanto avviene nella pratica matematica, abbiamo usato il simbolo $\prec$ per indicare un ordine stretto, anche se si tratta pur sempre di una struttura del linguaggio L_{ORDINI}. Se $(M, \prec)$ è un pre-ordine il quoziente mediante la relazione di equivalenza

$$x \sim y \Leftrightarrow x \preceq y \wedge y \preceq x$$

è un ordine con la relazione $[x] \leq [y] \Leftrightarrow x \preceq y$.

Un sottoinsieme di un insieme ordinato/pre-ordinato/strettamente ordinato è un insieme ordinato/pre-ordinato/strettamente ordinato, visto che gli assiomi usati per definire questi concetti sono $\forall$-enunciati.

Supponiamo $(M, \preceq)$ sia un ordine: un sottoinsieme X si dice

- **catena** se è linearmente ordinato da $\preceq$,
- **intervallo** se $\forall x, y \in X\, \forall z \in M\,(x \preceq z \preceq y \Rightarrow z \in X)$.

Se $x \prec y$ diremo che x è un **predecessore** di y, ovvero che y è un **successore** di x; se inoltre non c'è nessuno z tale che $x \prec z \prec y$ allora diremo che x è un **predecessore immediato** di y e che y è un **successore immediato di** di x. (Se $\preceq$ è lineare, il predecessore immediato e il successore immediato di un elemento, se esistono, sono unici.)

Se $(M, \preceq)$ è un ordine e $A \subseteq M$,

$$\text{pred}(x, A; \preceq) = \{y \in A \mid y \prec x\}$$

è l'insieme di tutti i predecessori di x che giacciono in A — in particolare

$$\text{pred}(x) = \text{pred}(x, M; \preceq)$$

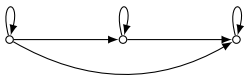
è l'insieme dei predecessori di x.

Se $x \preceq y$ gli insiemi

$$(x; y) = \{z \in X \mid x \prec z \prec y\}$$
$$[x; y] = \{z \in X \mid x \preceq z \preceq y\}$$
$$(x; y] = \{z \in X \mid x \prec z \preceq y\}$$
$$[x; y) = \{z \in X \mid x \preceq z < y\}$$

sono intervalli e si dicono, rispettivamente: intervallo aperto, chiuso, semiaperto inferiormente, semiaperto superiormente di estremi x e y. Notiamo che secondo la nostra definizione, non tutti gli intervalli hanno estremi.

Per quanto detto nella Sezione 5.H.6, una struttura finita (M, R_M), dove R_M è una relazione binaria, è descritta dal suo grafo diretto. Per esempio un ordine lineare con tre elementi è rappresentato da



L'informazione contenuta in questo grafo diretto è ridondante — dato che un ordine è una relazione è riflessiva e transitiva, è sufficiente considerare il grafo diretto della relazione di successore immediato. Inoltre è possibile utilizzare un grafo non diretto se si stipula che i vertici in basso precedono quelli in alto. Quindi l'ordine lineare con tre elementi è descritto dal grafo diretto

o anche dal grafo

Rappresentazioni di questo tipo si dicono **diagrammi di Hasse**.

Data una relazione binaria $R \subseteq M \times M$, la **conversa** di R è la relazione

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

e la sua **parte stretta** è la relazione

$$R \setminus R^{-1}.$$

In particolare, se $\preceq$ è un preordine su M, la sua parte stretta $\prec$ è definita come

$$a \prec b \Leftrightarrow a \preceq b \wedge b \not\preceq a,$$

mentre se $\preceq$ è un ordine, la sua parte stretta è l'ordine stretto

$$a \prec b \Leftrightarrow a \preceq b \wedge a \neq b.$$

Specializzando la definizione data a pagina 48, un morfismo tra pre-ordini $f\colon (P, \preceq) \to (Q, \trianglelefteq)$ è una **funzione crescente** cioè tale che

$$\forall x, y \in P\ (x \preceq y \Rightarrow f(x) \trianglelefteq f(y)).$$

Se vale anche

$$\forall x, y \in P\ (x \prec y \Rightarrow f(x) \triangleleft f(y)),$$

dove $\prec$ e $\lhd$ sono le parti strette di $\preceq$ e $\trianglelefteq$, diremo che f è **strettamente crescente**.

Esercizio 8.2. Siano $(P, \preceq)$ e $(Q, \trianglelefteq)$ degli ordini e sia $f\colon P \to Q$. Dimostrare che:

(i) $f\colon (P, \preceq) \to (Q, \trianglelefteq)$ è un'immersione (nel senso delle strutture) se e solo se

$$\forall x, y \in P\ (x \preceq y \Leftrightarrow f(x) \trianglelefteq f(y))\,,$$

(ii) se f è un'immersione allora è strettamente crescente,

(iii) l'implicazione in (ii) non può essere rovesciata.

Il **duale** di una L_{ORDINI}-struttura $\mathcal{M} = (M, \preceq)$ è la L_{ORDINI}-struttura

$$\mathcal{M}^\Delta = (M, \preceq^{-1})$$

dove $\preceq^{-1}$ è il converso di $\preceq$. Chiaramente $\mathcal{M}^{\Delta\Delta} = \mathcal{M}$. La **duale di una formula** φ del linguaggio L_{ORDINI} è la formula φ^Δ ottenuta sostituendo in φ ogni sotto-formula atomica del tipo '$x \leq y$' con '$y \leq x$' — formalmente la formula duale è definita per induzione sulla complessità, stabilendo che

- $(x = y)^\Delta$ è $x = y$,
- $(x \leq y)^\Delta$ è $y \leq x$,
- $(\neg\varphi)^\Delta$ è $\neg(\varphi^\Delta)$,
- $(\varphi \,\square\, \psi)^\Delta$ è $\varphi^\Delta \,\square\, \psi^\Delta$ dove $\square$ è un connettivo binario,
- $(\exists x\varphi)^\Delta$ è $\exists x\varphi^\Delta$ e $(\forall x\varphi)^\Delta$ è $\forall x\varphi^\Delta$.

Esercizio 8.3. Dimostrare che $\mathbf{T}^{\mathcal{M}}_{\varphi(x_1,\dots,x_n)} = \mathbf{T}^{\mathcal{M}^\Delta}_{\varphi^\Delta(x_1,\dots,x_n)}$, per ogni L_{ORDINI}-formula $\varphi(x_1, \dots, x_n)$.

In particolare

$$\mathcal{M} \vDash \sigma \quad \text{se e solo se} \quad \mathcal{M}^\Delta \vDash \sigma^\Delta$$

per ogni enunciato σ. Una formula è **autoduale** se è (logicamente equivalente al)la duale di sé stessa. Gli enunciati che assiomatizzano la classe degli ordini (le proprietà riflessiva, antisimmetrica e transitiva) sono autoduali, quindi $\mathcal{M}$ è un ordine se e solo se $\mathcal{M}^\Delta$ è un ordine. Riassumendo:

Principio di dualità per gli ordini. *Se $\mathcal{P}$ è un ordine e σ è un enunciato di L_{ORDINI} allora*

$$\mathcal{P} \vDash \sigma \quad \textit{se e solo se} \quad \mathcal{P}^\Delta \vDash \sigma^\Delta.$$

In particolare: σ è conseguenza logica degli assiomi degli ordini se e solo se σ^Δ lo è.

Dato un ordine $\mathcal{P} = (P, \preceq)$ e un $\emptyset \neq X \subseteq P$, diremo che un elemento $m \in X$ è **massimo** in X se $a \preceq m$ per ogni $a \in X$; se indeboliamo la condizione a "non esiste $a \in X$ con $m < a$" otteniamo la nozione di elemento **massimale** in X. Quando $X = P$ parleremo semplicemente di massimo e elemento massimale. Per la proprietà antisimmetrica un massimo di X (se esiste) è unico ed è indicato con $\max X$, ed è l'unico elemento che soddisfa la formula $\forall y\,(y \leq x)$ nella struttura $(X, \preceq)$. Un elemento è **minimo** o **minimale** se è massimo o massimale nell'ordine duale.

Osservazioni 8.4. Come vedremo, il principio di dualità per gli ordini è molto utile per dimezzare il numero di verifiche necessarie, ma bisogna far attenzione a non fraintenderne l'enunciato.

(a) Il principio di dualità *non* dice che se un ordine soddisfa σ allora soddisfa anche σ^Δ — per esempio ci sono ordini che hanno il minimo, ma non il massimo (o viceversa) e che quindi soddisfano $\exists x \forall y\,(x \leq y)$ ma non $\exists x \forall y\,(y \leq x)$.

(b) Similmente, *non* dice che un ordine soddisfa ogni enunciato autoduale. Per esempio, un ordine privo di massimo e minimo non soddisfa l'enunciato autoduale $\exists x \forall y\,(x \leq y) \wedge \exists x \forall y\,(y \leq x)$ che asserisce l'esistenza di massimo e minimo.

Proposizione 8.5. *Un insieme ordinato finito e non vuoto ha sempre elementi minimali e massimali.*

Dimostrazione. Fissiamo un insieme ordinato finito non vuoto $(A, \preceq)$, diciamo $A = \{a_0, \ldots, a_{n-1}\}$. Per assurdo, supponiamo che $(A, \preceq)$ non abbia elementi massimali. Applichiamo il Corollario 7.6 con $a = a_0$ e $F\colon A \to A$ definita

$$F(a_i) = a_j \text{ dove } j < n \text{ è minimo tale che } a_i \prec a_j.$$

C'è una funzione $f\colon \mathbb{N} \to A$ tale che $f(0) = a_0$ e $f(k) \prec f(k+1)$ per ogni $k \in \mathbb{N}$. Per la proprietà transitiva e per MP^2 la funzione f è iniettiva, quindi posto $g(k) = i \Leftrightarrow f(k) = a_i$ si ha che $g\colon \mathbb{N} \rightarrowtail \{0, \ldots, n-1\}$, una contraddizione dato che non c'è nessuna funzione iniettiva da $\mathbb{N}$ in un insieme finito.

La dimostrazione che $(A, \preceq)$ ha elementi minimali è ottenuta considerando l'ordine duale. □

Osservazione 8.6. La dimostrazione precedente si basa sul fatto che $\mathbb{N}$ non si inietta in un insieme finito, cosa che sarà dimostrata in dettaglio nel Teorema 10.19.

Proposizione 8.7. *Ogni ordinamento $\preceq$ su un insieme finito A può essere esteso ad un ordinamento totale $\leq$ su A, cioè*

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

Dimostrazione. Procediamo per induzione sul numero n di elementi di A. Se $n \leq 1$, il risultato è banale, quindi possiamo supporre che $n \geq 2$. Per la Proposizione 8.5 sia $\bar{a} \in A$ minimale: per ipotesi induttiva c'è un ordine totale $\leq^*$ su $A \setminus \{\bar{a}\}$ che estende $\preceq$ su $A \setminus \{\bar{a}\}$. Allora

$$x \leq y \Leftrightarrow \begin{cases} x \leq^* y \text{ and } x, y \in A \setminus \{\bar{a}\} \\ x = \bar{a} \end{cases}$$

è un ordine totale su A che estende $\preceq$. □

Nel Capitolo V vedremo che la Proposizione 8.7 vale anche per gli insiemi infiniti (Teorema 23.45.)

Proposizione 8.8. *Due ordini lineari finiti della stessa taglia sono isomorfi, e l'isomorfismo è unico.*

Dimostrazione. Dimostriamo per induzione su n che due ordini lineari finiti $(P, \leq_P)$ e $(Q, <_Q)$ di taglia n sono isomorfi, e che l'isomorfismo è unico. Se $n = 0$ allora $P = Q = \emptyset$ e non c'è nulla da dimostrare. Supponiamo che P e Q siano di cardinalità $n + 1$. Per la Proposizione 8.5 ci sono massimi $\bar{p} \in P$ e $\bar{q} \in Q$, per ipotesi induttiva c'è un unico isomorfismo $\bar{f} \colon (P \setminus \{\bar{p}\}, \leq_P) \to (Q \setminus \{\bar{q}\}, \leq_Q)$, quindi la funzione $f \colon P \to Q$ definita da

$$f(p) = \begin{cases} \bar{f}(p) & \text{se } p \neq \bar{p}, \\ \bar{q} & \text{se } p = \bar{p}, \end{cases}$$

è un isomorfismo. L'unicità di f discende dall'osservazione che ogni isomorfismo manda $\bar{p}$ in $\bar{q}$. □

Un insieme $Q \subseteq P$ è un **segmento iniziale** o **insieme inferiore** di P se

$$x \in Q \wedge y \preceq x \Rightarrow y \in Q$$

Per esempio,

$$\downarrow Q = \{y \in P \mid \exists x \in Q (y \preceq x)\}$$

è un insieme inferiore, per ogni $Q \subseteq P$; infatti Q è un insieme inferiore se e solo se $\downarrow Q = Q$. Quando Q è un singoletto $\{x\}$ scriveremo $\downarrow x$ invece di $\downarrow \{x\}$. Notiamo che

$$\downarrow x = \mathrm{pred}(x) \cup \{x\}\,.$$

La famiglia dei sottoinsiemi inferiori dell'ordine parziale $\mathcal{P}$ si denota con

$$\mathrm{Down}(\mathcal{P})$$

o semplicemente con $\mathrm{Down}(P)$ ed è anch'esso un ordine parziale sotto inclusione, con massimo P e minimo $\emptyset$. La mappa $x \mapsto \downarrow x$ è un'immersione di P in $\mathrm{Down}(P)$, quindi ogni ordine parziale $(P, \preceq)$ è isomorfo ad una

famiglia $(\mathcal{A}, \subseteq)$, con $\mathcal{A} \subseteq \mathscr{P}(P)$. Diremo che $Q \subseteq P$ è un **segmento finale** o **insieme superiore** se è un insieme inferiore dell'ordine duale $\mathcal{P}^\Delta$, e

$$\uparrow Q = \{y \in P \mid \exists x \in Q(x \preceq y)\}$$

è l'insieme $\downarrow Q$ calcolato in $\mathcal{P}^\Delta$. L'insieme dei sottoinsiemi superiori di P si denota con $\mathrm{Up}(\mathcal{P})$ o semplicemente con $\mathrm{Up}(P)$,[1] ed è ordinato per inclusione. Per il principio di dualità per gli ordini,

$$\begin{aligned} \mathrm{Down}(\mathcal{P})^\Delta &\to \mathrm{Up}(\mathcal{P}), & Q &\mapsto P \setminus Q \\ \mathrm{Up}(\mathcal{P}) &\to \mathrm{Down}(\mathcal{P}^\Delta), & Q &\mapsto Q \end{aligned}$$

sono isomorfismi, quindi

$$\mathrm{Down}(\mathcal{P})^\Delta \cong \mathrm{Down}(\mathcal{P}^\Delta) \quad \text{e} \quad \mathrm{Up}(\mathcal{P})^\Delta \cong \mathrm{Up}(\mathcal{P}^\Delta).$$

Se $(M, \preceq)$ è un ordine, diremo che $D \subseteq M$ è **denso in** M se

$$\forall a, b \in M\, [a \prec b \Rightarrow (a; b) \cap D \neq \emptyset].$$

Quindi un ordine linear M è denso nel senso della definizione a pagina 77 se e solo se è denso in sé stesso.

Un ordine è **diretto superiormente** se soddisfa l'enunciato

$$\forall x, y\, \exists z\, (x \preceq z \wedge y \preceq z).$$

Un ordine è **diretto inferiormente** se il suo duale è diretto superiormente. (Queste nozioni si generalizzano in modo ovvio al caso dei pre-ordini.)

Un **maggiorante** di un sottoinsieme X di P è un elemento $a \in P$ tale che $\forall x \in X\, (x \preceq a)$ e X^{U} è l'insieme di tutti i maggioranti di X. Un sottoinsieme X che ammette un maggiorante, cioè tale $X^{\mathrm{U}} \neq \emptyset$ si dice **limitato superiormente**. Se $a = \min X^{\mathrm{U}}$ diremo che a è **estremo superiore** di X. Le definizioni di X^{L}, **minorante**, **sottoinsieme inferiormente limitato**, **estremo inferiore** sono ottenute "dualizzando" le definizioni di X^{U}, maggiorante, sottoinsieme superiormente limitato ed estremo superiore. Per la proprietà antisimmetrica, l'estremo superiore di X (se esiste) è unico e verrà indicato con $\sup X$ o con

$$\bigvee X.$$

Quando $X = \{a, b\}$ scriveremo $\sup(a, b)$ oppure

$$a \curlyvee b.$$

[1] Nei testi anglosassoni gli insiemi inferiori e superiori sono detti *down-sets* e *up-sets* rispettivamente, da cui la notazione.

Formalizzando l'affermazione precedente (quando X è formato da due elementi) si ottiene che $\mathcal{P} \vDash \sigma$, *per ogni* ordine parziale $\mathcal{P}$, dove σ è l'enunciato

$$\forall x, y, z, w \, ([x \leq z \wedge y \leq z \wedge \forall z'(x \leq z' \wedge y \leq z' \Rightarrow z \leq z')] \\ \wedge [x \leq w \wedge y \leq w \wedge \forall w'(x \leq w' \wedge y \leq w' \Rightarrow w \leq w')] \Rightarrow z = w)$$

Fissato $\mathcal{P}$, si ha che $\mathcal{P}^\Delta \vDash \sigma$, quindi per il principio di dualità, $\mathcal{P}^{\Delta\Delta} \vDash \sigma^\Delta$, cioè $\mathcal{P} \vDash \sigma^\Delta$. In altre parole, ogni ordine parziale soddisfa l'enunciato che asserisce: l'estremo inferiore di due elementi (se esiste) è unico. L'estremo inferiore di $X \subseteq P$ verrà indicato con $\inf X$, o

$$\bigwedge X,$$

e quando $X = \{a, b\}$ scriveremo $\inf(a, b)$ o

$$a \wedge b.$$

Esercizio 8.9. In un insieme ordinato $(P, \preceq)$ sono equivalenti

(1) $\bigvee X$ esiste per ogni $X \subseteq P$,

(2) $\bigwedge X$ esiste per ogni $X \subseteq P$;

così come sono equivalenti:

(3) $\bigvee X$ esiste per ogni $\emptyset \neq X \subseteq P$ superiormente limitato,

(4) $\bigwedge X$ esiste per ogni $\emptyset \neq X \subseteq P$ inferiormente limitato;

Un insieme ordinato che soddisfi (1) e/o (2) dell'Esercizio 8.9 si dice **completo**; se soddisfa (3) e/o (4) si dice **Dedekind-completo**. La definizione di ordine (Dedekind-)completo non è al prim'ordine, dato che si quantifica su sottoinsiemi arbitrari.

Vedremo ora un metodo per immergere un ordine lineare denso in uno completo, mentre nella Sezione 23.D vedremo come questo metodo può essere generalizzato a tutti gli ordini.

Definizione 8.10. Una **sezione di Dedekind** di un ordine lineare $(L, \leq)$ è un $X \in \mathrm{Down}(L)$ che non ha massimo, cioè $\forall x \in X \, \exists y \in X \, (x < y)$, e tale che

- se $(L, \leq)$ non ha minimo, allora $\emptyset \neq X$, e
- se $(L, \leq)$ non ha massimo, allora $X \neq L$.

L'insieme delle sezioni di Dedekind di L è indicata con $\mathbf{D}(L)$, e

$$\hat{\imath} \colon L \to \mathbf{D}(L), \quad p \mapsto \{q \in L \mid q < p\}$$

è l'immersione canonica di L in $\mathbf{D}(L)$. Possiamo quindi considerare L come sottoinsieme di $\mathbf{D}(L)$.

Ogni ordine lineare $(L, \leq)$ può essere visto come spazio topologico mediante la **topologia dell'ordine**, generata dalle semirette aperte

$$(-\infty; a) \stackrel{\text{def}}{=} \{x \in L \mid x < a\},$$
$$(a; +\infty) \stackrel{\text{def}}{=} \{x \in L \mid a < x\},$$

che sono particolari tipi di insiemi iniziali e finali. Questa topologia è Hausdorff e una sua base è data dagli intervalli aperti $(a; b)$ e dagli intervalli semi-aperti $[m; b) = (-\infty; b)$ e $(a; M] = (a; +\infty)$ dove m e M sono il mimino e il massimo di L, se esistono. Quindi un insieme $D \subseteq L$ è denso nel senso dell'ordine se e solo se è denso nel senso topologico. Un isomorfismo tra ordini lineari è un omeomorfismo per la topologia dell'ordine, ma non viceversa (Esercizio 8.49).

La dimostrazione del prossimo risultato è lasciata al lettore.

Teorema 8.11. *Sia $(L, \leq)$ un ordine lineare denso dotato di massimo e minimo.*

(a) *L è denso in $\mathbf{D}(L)$,*

(b) *$\mathbf{D}(L)$ è completo,*

(c) *se E è completo e $j\colon L \to E$ è un'immersione tale che $\mathrm{ran}(j)$ è denso in E, allora E è isomorfo a $\mathbf{D}(L)$.*

Il Teorema 8.11 si estende al caso in cui L non ha massimo, o minimo, o entrambi, ma il requisito di completezza è indebolito a quello di Dedekind-completezza. Per via dell'unicità enunciata nella parte (c), $\mathbf{D}(L)$ si dice **completamento di Dedekind** di L.

Concludiamo questa Sezione con un risultato di punto fisso tanto semplice quanto utile.

Teorema 8.12. *Sia $(P, \preceq)$ un ordine completo, e sia $f\colon P \to P$ una funzione crescente. Allora c'è un punto fisso per f, vale a dire*

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

Dimostrazione. Sia $A = \{x \in P \mid x \preceq f(x)\}$ e sia $a = \bigvee A$. Se $x \in A$, allora $x \preceq a$ e $x \preceq f(x)$ da cui

$$x \preceq f(x) \preceq f(a).$$

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

Figura 1. I reticoli $\mathcal{N}_5$ e $\mathcal{M}_3$.

8.B. Reticoli. Un **semi-reticolo superiore** è un ordine $(M, \preceq)$ in cui due elementi hanno sempre un estremo superiore, cioè $(M, \preceq)$ soddisfa

$$\forall x, y \exists z \left(x \leq z \wedge y \leq z \wedge \forall w \left(x \leq w \wedge y \leq w \Rightarrow z \leq w\right)\right).$$

Il duale di un semi-reticolo superiore si dice **semi-reticolo inferiore**. Un **reticolo**[2] è un ordine che è simultaneamente semi-reticolo superiore e semi-reticolo inferiore. In un reticolo il massimo e il minimo (se esistono) si denotano con **1** e **0** o anche con $\top$ e $\bot$, e in questo caso parleremo di **reticolo limitato**. Ogni ordine lineare è un reticolo, ma la nozione di reticolo è molto più generale — nella Figura 1 sono riportati due esempi di reticoli finiti che non sono ordini lineari.

Se $(M, \preceq)$ è un reticolo, un **sotto-reticolo** è un sottoinsieme non vuoto $M' \subseteq M$ tale che

$$\sup(a, b), \inf(a, b) \in M'$$

per ogni $a, b \in M'$, dove gli estremi superiore ed inferiore sono calcolati in M. È facile verificare che M' è un reticolo e che i valori di $\sup(a, b)$ e $\inf(a, b)$, calcolati in M o M', coincidono. Un reticolo M è **generato** da $a_1, \ldots, a_n \in M$ se ogni sotto-reticolo di M che contiene $a_1, \ldots, a_n$ coincide con M.

Notazione. Finora abbiamo usato $\preceq$ per la relazione d'ordine nell'ordine parziale e $\leq$ per il simbolo del linguaggio L_{ORDINI}, ma d'ora in poi, salvo questo non comporti ambiguità, useremo $\leq$ per entrambi i concetti.

Esercizio 8.13. (i) Dimostrare che in un semi-reticolo superiore un elemento massimale (se esiste) è unico ed è il massimo. Analogamente in un semi-reticolo inferiore un elemento minimale (se esiste) è unico ed è il minimo.

(ii) Verificare che in un reticolo valgono la proprietà associativa per $\curlywedge$ e $\curlyvee$

$$\forall x, y, z \left(x \curlyvee (y \curlyvee z) = (x \curlyvee y) \curlyvee z\right) \tag{8.1a}$$

$$\forall x, y, z \left(x \curlywedge (y \curlywedge z) = (x \curlywedge y) \curlywedge z\right), \tag{8.1b}$$

[2] In inglese reticolo e semi-reticolo si dicono, rispettivamente, *lattice* e *semilattice*.

la proprietà commutativa per $\curlywedge$ e $\curlyvee$

$$\forall x, y\,(x \curlyvee y = y \curlyvee x) \tag{8.2a}$$

$$\forall x, y\,(x \curlywedge y = y \curlywedge x), \tag{8.2b}$$

e le **leggi di assorbimento**, cioè

$$\forall x, y\,((x \curlyvee y) \curlywedge y = y) \tag{8.3a}$$

$$\forall x, y\,((x \curlywedge y) \curlyvee y = y). \tag{8.3b}$$

Le equazioni (8.1)–(8.3) sono formulate nel linguaggio L_{RETICOLI} contenente due simboli di operazione binaria, $\curlywedge$ e $\curlyvee$. Una struttura per questo linguaggio che soddisfi queste equazioni si dice **algebra reticolare**. Quindi la classe delle algebre reticolari è finitamente assiomatizzabile nel linguaggio L_{RETICOLI}.

Esercizio 8.14. Sia $\mathcal{M} = (M, \curlyvee, \curlywedge)$ un'algebra reticolare. Verificare che:

(i) $\mathcal{M}$ soddisfa le proprietà di idempotenza, cioè

$$\forall x(x = x \curlyvee x) \tag{8.4a}$$

$$\forall x(x = x \curlywedge x) \tag{8.4b}$$

(ii) $\mathcal{M} \vDash \forall x, y\,(x \curlyvee y = y \Leftrightarrow x \curlywedge y = x)$,

(iii) la relazione $\preceq$ definita su M da

$$\begin{aligned} a \preceq b &\Leftrightarrow a \curlyvee b = b \\ &\Leftrightarrow a \curlywedge b = a \qquad \text{(per (ii))} \end{aligned}$$

è un ordinamento su M e l'insieme ordinato $\mathcal{M}^\circ = (M, \preceq)$ è un reticolo tale che $\sup(a, b) = a \curlyvee b$ e $\inf(a, b) = a \curlywedge b$.

Vista la loro sostanziale equivalenza, non distingueremo tra la nozione ordinale (reticolo) e la nozione algebrica (algebra reticolare) e parleremo semplicemente di reticoli. Questa equivalenza mostra come la stessa classe di oggetti può essere assiomatizzata mediante linguaggi distinti. L'assiomatizzazione dei reticoli nel linguaggio L_{RETICOLI} è un esempio di teoria equazionale, quindi per la Proposizione 3.25 la famiglia dei reticoli è chiusa per sottostrutture, immagini omomorfe, e prodotti. Invece nel linguaggio L_{ORDINI} non c'è assiomatizzazione equazionale e neppure universale per reticoli, dato che un sottoinsieme di un reticolo è un insieme ordinato, ma non è necessariamente un reticolo. La parte (iii) dell'Esercizio 8.14 mostra come le due operazioni $\curlywedge$ e $\curlyvee$ siano interdipendenti: se $(M, \curlyvee, \curlywedge_1)$ e $(M, \curlyvee, \curlywedge_2)$ sono algebre reticolari, allora $\curlywedge_1$ coincide con $\curlywedge_2$. Analogamente, se $(M, \curlyvee_1, \curlywedge)$ e $(M, \curlyvee_2, \curlywedge)$ sono algebre reticolari, allora $\curlyvee_1$ coincide con $\curlyvee_2$.

Il **duale di un termine** t di L_{RETICOLI} è il termine t^Δ ottenuto scambiando tra loro i simboli $\curlyvee$ e $\curlywedge$. La **duale di una formula** φ è la formula φ^Δ

ottenuta rimpiazzando ogni termine con il suo duale. La **struttura duale** di $\mathcal{M} = (M, \curlyvee, \curlywedge)$ è la L_{RETICOLI}-struttura $\mathcal{M}^\Delta = (M, \sqcup, \sqcap)$ dove $\sqcup = \curlywedge$ e $\sqcap = \curlyvee$. Il duale del duale è la struttura di partenza, cioè $\mathcal{M}^{\Delta\Delta} = \mathcal{M}$. Se $\mathcal{M}$ è una L_{RETICOLI}-struttura e σ è un enunciato, allora

$$\mathcal{M} \vDash \sigma \quad \text{se e solo se} \quad \mathcal{M}^\Delta \vDash \sigma^\Delta.$$

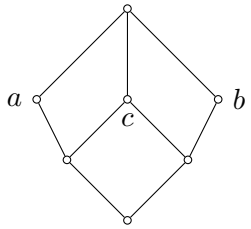
Poiché gli assiomi per le algebre reticolari sono autoduali, il duale di un reticolo è un reticolo. Il seguente risultato è l'analogo del principio di dualità per gli ordini.

Principio di dualità per i reticoli. *Se $\mathcal{M}$ è reticolo e σ è un enunciato, allora*

$$\mathcal{M} \vDash \sigma \quad \textit{se e solo se} \quad \mathcal{M}^\Delta \vDash \sigma^\Delta.$$

In particolare: σ è conseguenza logica degli assiomi dei reticoli se e solo se σ^Δ lo è.

Osservazione 8.15. Come per gli ordini, anche il principio di dualità per i reticoli non deve essere frainteso. Per l'Esercizio 8.19 qui sotto, gli *enunciati* $\forall x, y, z\, [(x \curlyvee y) \curlywedge z = (x \curlywedge z) \curlyvee (y \curlywedge z)]$ e $\forall x, y, z\, [(x \curlywedge y) \curlyvee z = (x \curlyvee z) \curlywedge (y \curlyvee z)]$ sono logicamente equivalenti modulo gli assiomi per i reticoli, ma questo non vale per le *formule* $(x \curlyvee y) \curlywedge z = (x \curlywedge z) \curlyvee (y \curlywedge z)$ e $(x \curlywedge y) \curlyvee z = (x \curlyvee z) \curlywedge (y \curlyvee z)$ (vedi Osservazione 3.18). Per esempio, nel reticolo



$(a \curlyvee b) \curlywedge c = (a \curlywedge c) \curlyvee (b \curlywedge c)$ ma $(a \curlywedge b) \curlyvee c \neq (a \curlyvee c) \curlywedge (b \curlyvee c)$.

Un reticolo si dice **completo** se $\bigvee X$ e $\bigwedge X$ esistono per ogni sottoinsieme X. Un reticolo completo è limitato, e non è nient'altro che un ordine completo.

Se $X = \{a_1, \ldots, a_n\}$, allora $\sup X = a_1 \curlyvee \ldots \curlyvee a_n$ e $\inf X = a_1 \curlywedge \ldots \curlywedge a_n$ esistono e sono ben definiti per l'Esercizio 5.10, quindi ogni reticolo finito è completo. Il seguente risultato è conseguenza immediata dell'Esercizio 8.9.

Lemma 8.16. *In un reticolo M le seguenti affermazioni sono equivalenti:*

(a) *M è completo,*

(b) *$\bigvee X$ esiste, per ogni $X \subseteq M$,*

(c) *$\bigwedge X$ esiste, per ogni $X \subseteq M$.*

Esempi 8.17. (a) Una famiglia $\mathcal{S} \subseteq \mathscr{P}(X)$ chiusa per intersezioni e unioni finite si dice **reticolo di insiemi**; l'ordinamento è $\subseteq$ e le operazioni sono $A \curlywedge B = A \cap B$ e $A \curlyvee B = A \cup B$. Se $\mathcal{S}$ contiene $\emptyset$ e X ed è chiusa per unioni e intersezioni generalizzate,

$$\bigvee \{A_i \mid i \in I\} = \bigcup_{i \in I} A_i \quad \text{e} \quad \bigwedge \{A_i \mid i \in I\} = \bigcap_{i \in I} A_i$$

con $\{A_i \mid i \in I\} \subseteq \mathscr{P}(X)$, allora $\mathcal{S}$ è un **reticolo completo di insiemi**. In particolare,

- $(\mathscr{P}(X), \subseteq)$,
- $(\mathrm{Down}(P), \subseteq)$, con $(P, \preceq)$ un ordine parziale,

sono reticoli completi di insiemi.

(b) Sia $\mathcal{S} \subseteq \mathscr{P}(X)$ chiusa per intersezioni arbitrarie, cioè se $\{A_i \mid i \in I\} \subseteq \mathcal{S}$ allora $\bigcap_{i \in I} A_i \in \mathcal{S}$, e tale che $X \in \mathcal{S}$. Allora $\mathcal{S}$ è un reticolo limitato con le operazioni $A \curlywedge B = A \cap B$ e $A \curlyvee B = \bigcap_{C \supseteq A \cup B} C$. Inoltre, se $\{A_i \mid i \in I\} \subseteq \mathcal{S}$ allora $\bigwedge_{i \in I} A_i = \bigcap_{i \in I} A_i$ quindi si tratta di un reticolo completo per il Lemma 8.16, ma in generale $\mathcal{S}$ non è un reticolo di insiemi.

Analogamente, se $\mathcal{S} \subseteq \mathscr{P}(X)$ è chiusa per unioni arbitrarie e $\emptyset \in \mathcal{S}$, allora $\mathcal{S}$ è un reticolo completo, ma non necessariamente un reticolo di insiemi.

Esempi di reticoli di questo tipo sono:

- la famiglia delle sottostrutture di una L-struttura M, dove L è un linguaggio del prim'ordine,
- il reticolo delle topologie su un insieme Y (si consideri $X = \mathscr{P}(Y)$ e $\mathcal{S} \subseteq \mathscr{P}(X)$),
- il reticolo delle partizioni.

(c) Se $\mathcal{S} \subseteq \mathscr{P}(X)$ è un reticolo di insiemi chiuso per intersezioni (oppure per unioni) arbitrarie, allora $\mathcal{S}$ è un reticolo completo, ma non è necessariamente un reticolo completo di insiemi.

Esempi di reticoli di questo tipo sono la famiglia degli aperti e la famiglia dei chiusi di uno spazio topologico.

Una generalizzazione immediata del Teorema 8.12 è il

Teorema 8.18. *Sia $(M, \leq)$ un reticolo completo, $f \colon M \to M$ una funzione crescente e sia $F = \{x \in M \mid f(x) = x\}$ l'insieme dei punti fissi. Allora F è non vuoto, $(F, \leq)$ è un reticolo completo e*

$$\bigvee \{x \in M \mid x \leq f(x)\} \quad e \quad \bigwedge \{x \in M \mid f(x) \leq x\}$$

sono, rispettivamente, il massimo e il minimo di F.

8.C. Reticoli distributivi. Dati tre elementi a, b, c in un reticolo M, allora $a \curlywedge b \leq a$ e $a \curlywedge b \leq b \leq b \curlyvee c$ quindi $a \curlywedge b \leq a \curlywedge (b \curlyvee c)$ per definizione di estremo inferiore; inoltre $a \curlywedge c \leq a$ e $a \curlywedge c \leq c \leq b \curlyvee c$, da cui $a \curlywedge c \leq a \curlywedge (b \curlyvee c)$. Per la definizione di estremo superiore $(a \curlywedge b) \curlyvee (a \curlywedge c) \leq a \curlywedge (b \curlyvee c)$. Quindi il seguente enunciato vale in ogni reticolo:

$$\forall x, y, z \left((x \curlywedge y) \curlyvee (x \curlywedge z) \leq x \curlywedge (y \curlyvee z)\right). \tag{8.5a}$$

Per il principio di dualità, tenendo presente che la formula duale di $x \leq y$, cioè di $x \curlywedge y = x$, è la formula $y \leq x$, otteniamo che

$$\forall x, y, z \left(x \curlyvee (y \curlywedge z) \leq (x \curlyvee y) \curlywedge (x \curlyvee z)\right) \tag{8.5b}$$

vale in ogni reticolo.

Esercizio 8.19. Dimostrare che in ogni reticolo valgono i seguenti enunciati:

$$\begin{aligned} &\forall x, y, z \left((x \curlyvee y) \curlywedge z = (x \curlywedge z) \curlyvee (y \curlywedge z)\right) \\ &\qquad \Leftrightarrow \forall x, y, z \left((x \curlywedge y) \curlyvee z = (x \curlyvee z) \curlywedge (y \curlyvee z)\right) \end{aligned} \tag{8.5c}$$

$$\forall x, y, z \left(z \leq x \Rightarrow (x \curlywedge y) \curlyvee z \leq x \curlywedge (y \curlyvee z)\right) \tag{8.5d}$$

$$\begin{aligned} &\forall x, y, z \left((x \curlywedge y) \curlyvee (x \curlywedge z) = x \curlywedge (y \curlyvee (x \curlywedge z))\right) \\ &\qquad \Leftrightarrow \forall x, y, z \left(z \leq x \Rightarrow x \curlywedge (y \curlyvee z) = (x \curlywedge y) \curlyvee z\right) \\ &\qquad \Leftrightarrow \forall x, y, z \left((x \curlyvee y) \curlywedge (x \curlyvee z) = x \curlyvee (y \curlywedge (x \curlyvee z))\right). \end{aligned} \tag{8.5e}$$

Definizione 8.20. Un reticolo si dice:

modulare: se soddisfa i seguenti assiomi detti **legge modulare**

$$\forall x, y, z \left((x \curlywedge y) \curlyvee (x \curlywedge z) = x \curlywedge (y \curlyvee (x \curlywedge z))\right) \tag{8.6a}$$

$$\forall x, y, z \left((x \curlyvee y) \curlywedge (x \curlyvee z) = x \curlyvee (y \curlywedge (x \curlyvee z))\right) \tag{8.6b}$$

distributivo: se soddisfa gli enunciati

$$\forall x, y, z \left((x \curlyvee y) \curlywedge z = (x \curlywedge z) \curlyvee (y \curlywedge z)\right) \tag{8.7a}$$

$$\forall x, y, z \left((x \curlywedge y) \curlyvee z = (x \curlyvee z) \curlywedge (y \curlyvee z)\right) \tag{8.7b}$$

Osservazioni 8.21. (a) Gli assiomi per i reticoli modulari o distributivi sono autoduali, quindi il duale di un reticolo modulare/distributivo è ancora dello stesso tipo, e il principio di dualità si generalizza al caso dei reticoli modulari e dei reticoli distributivi in modo ovvio: se σ è un enunciato di L_{RETICOLI} che vale in ogni reticolo modulare/distributivo, allora anche il suo duale σ^{Δ} vale in ogni reticolo modulare/distributivo.

(b) Per (8.5c) un reticolo è modulare se verifica almeno una delle due condizioni (8.6); analogamente, per verificare che un reticolo è distributivo è sufficiente verificare una delle due condizioni (8.7). Possiamo indebolire le condizioni ulteriormente: per le (8.5a) e (8.5b), un reticolo è

distributivo se soddisfa *almeno uno* degli enunciati

$$\forall x, y, z((x \curlyvee y) \curlywedge (x \curlyvee z) \leq x \curlyvee (y \curlywedge z))$$
$$\forall x, y, z(x \curlywedge (y \curlyvee z) \leq (x \curlywedge y) \curlyvee (x \curlywedge z)).$$

Analogamente per $x \curlywedge z \leq z$ si ha $x \curlywedge (y \curlyvee (x \curlywedge z)) \leq x \curlywedge (y \curlyvee z)$ quindi per la (8.5e) la definizione di modularità può essere indebolita a

$$\forall x, y, z\,((x \curlywedge y) \curlyvee (x \curlywedge z) \leq x \curlywedge (y \curlyvee (x \curlywedge z)))$$

oppure a

$$\forall x, y, z\,(z \leq x \Rightarrow x \curlywedge (y \curlyvee z) \leq (x \curlywedge y) \curlyvee z)\,.$$

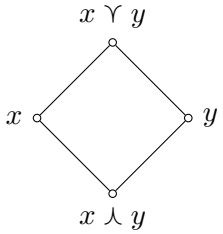
(c) Gli assiomi per i reticoli, la legge modulare, le proprietà distributive sono enunciati universali e positivi, quindi si preservano per sottostrutture e immagini omomorfe — si vedano le osservazioni a pagina 50 e la Proposizione 3.24 a pagina 51.

Esercizio 8.22. Dimostrare che:

(i) Ogni reticolo distributivo è modulare.

(ii) Il reticolo $\mathcal{N}_5$ della Figura 1 a pagina 156 non è modulare, mentre il reticolo $\mathcal{M}_3$ è modulare, ma non distributivo.

In analogia con quanto fatto nella Sezione 5.G, possiamo considerare l'algebra $\mathrm{Term}_{\text{RETICOLI}}(x_1, \ldots, x_n)/\!\sim$ dei termini del linguaggio L_{RETICOLI} con la congruenza $\sim$ data dagli assiomi (8.2) e (8.3): l'oggetto risultante si dice **reticolo libero su** n **generatori**, $\mathrm{Free}(n)$. È il reticolo più generale con n generatori, nel senso che ogni reticolo M generato da n elementi $a_1, \ldots, a_n$ è immagine omomorfa di $\mathrm{Free}(n)$: la funzione $[x_i] \mapsto a_i$ si estende ad un omomorfismo $F\colon \mathrm{Free}(n) \twoheadrightarrow M$. Se $n = 1$ si ottiene il reticolo con un unico elemento; se $n = 2$ si ottiene il reticolo



che è distributivo, mentre $\mathrm{Free}(3)$ (e quindi $\mathrm{Free}(n)$ per $n > 3$) è infinito.

Se rafforziamo la congruenza imponendo la legge distributiva o la modularità si ottiene, rispettivamente, il **reticolo distributivo libero** su n generatori $\mathrm{Free}_{\mathbf{D}}(n)$, e il **reticolo modulare libero** su n generatori $\mathrm{Free}_{\mathbf{M}}(n)$. Anche in questo caso si tratta dei reticoli con n generatori più

generali nelle classi dei reticoli distributivi e modulari, cioè ogni reticolo distributivo (modulare) M con n generatori è immagine omomorfa di $\mathrm{Free}_{\mathbf{D}}(n)$, (rispettivamente: $\mathrm{Free}_{\mathbf{M}}(n)$).

Il reticolo $\mathrm{Free}_{\mathbf{D}}(n)$ è finito. Per verificare ciò abbiamo bisogno di qualche risultato preliminare.

Un termine si dice congiunzione di variabili $\{x_1, \ldots, x_n\}$ se è della forma

$$x_{i_1} \curlywedge \ldots \curlywedge x_{i_k}$$

con $\{i_1, \ldots, i_k\} \subseteq \{1, \ldots, n\}$, mentre se è della forma

$$x_{j_1} \curlyvee \ldots \curlyvee x_{j_h}$$

con $\{j_1, \ldots, j_h\} \subseteq \{1, \ldots, n\}$, si dice disgiunzione di variabili $\{x_1, \ldots, x_n\}$. Una facile induzione sulla complessità del termine s dimostra il seguente risultato, che è la controparte algebrica del fatto che ogni formula è tautologicamente equivalente ad una formula in forma normale disgiuntiva e ad una in forma normale congiuntiva (vedi Sezione 3.C.1 ed Esercizio 3.40.)

Lemma 8.23. *Per ogni termine $s \in \mathrm{Term}_{\text{RETICOLI}}(x_1, \ldots, x_n)$ esistono termini $u, v \in \mathrm{Term}_{\text{RETICOLI}}(x_1, \ldots, x_n)$ tali che*

- *u è in **forma disgiuntiva**, vale a dire è una disgiunzione di congiunzioni delle variabili $\{x_1, \ldots, x_n\}$,*
- *v è in **forma congiuntiva**, vale a dire è una congiunzione di disgiunzioni delle variabili $\{x_1, \ldots, x_n\}$,*
- *la formula $s = u = v$ è conseguenza degli assiomi dei reticoli distributivi.*

Se $\sim$ è la congruenza che garantisce gli assiomi per i reticoli distributivi, allora per induzione sulla complessità di $t \in \mathrm{Term}(x_1, \ldots, x_n)$ si verifica che $x_1 \curlywedge \ldots \curlywedge x_n \leq t \leq x_1 \curlyvee \ldots \curlyvee x_n$. Inoltre poiché ogni termine può essere messo in forma disgiuntiva, cioè una disgiunzione di congiunzioni, gli elementi di $\mathrm{Free}_{\mathbf{D}}(n)$ sono al più quanti sono le forme disgiuntive su n variabili. Quindi $\mathrm{Free}_{\mathbf{D}}(n)$ è finito. Per esempio, gli elementi di $\mathrm{Free}_{\mathbf{D}}(3)$ sono disgiunzioni di k congiunzioni su x, y, z, cioè

$(k = 1)$ $\quad x,\ y,\ z,\ x \curlywedge y,\ x \curlywedge z,\ y \curlywedge z,\ x \curlywedge y \curlywedge z,$

$(k = 2)$ $\quad x \curlyvee y,\ x \curlyvee z,\ y \curlyvee z,\ x \curlyvee (y \curlywedge z),\ y \curlyvee (x \curlywedge z),\ z \curlyvee (x \curlywedge y),$
$(x \curlywedge y) \curlyvee (y \curlywedge z),\ (x \curlywedge y) \curlyvee (x \curlywedge z),\ (y \curlywedge z) \curlyvee (x \curlywedge z),$

$(k = 3)$ $\quad x \curlyvee y \curlyvee z,\ (x \curlywedge y) \curlyvee (y \curlywedge z) \curlyvee (x \curlywedge z).$

Il diagramma di Hasse di $\mathrm{Free}_{\mathbf{D}}(3)$ è riportato nella Figura 2. Sorge spontanea la domanda: siamo sicuri che gli elementi descritti qui sopra siano tutti distinti? È possibile che ci sia qualche ulteriore identificazione? L'Esercizio 8.57 mostra che ciò non avviene, quindi $\mathrm{Free}_{\mathbf{D}}(3)$ ha proprio 18 elementi.

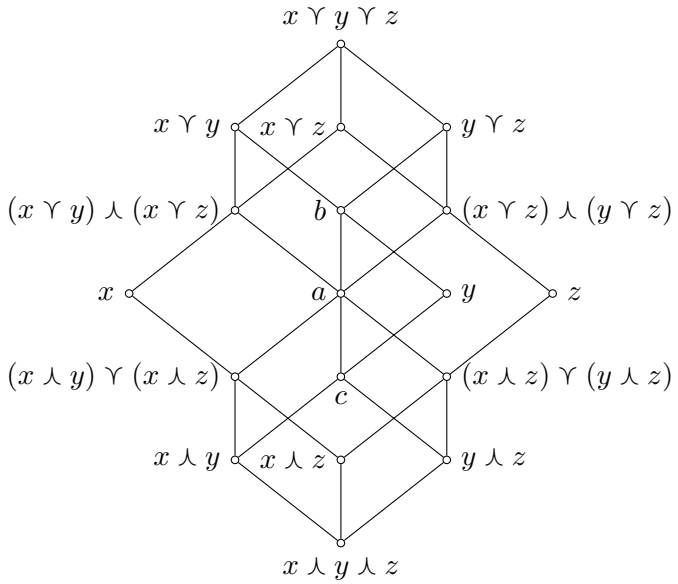


Figura 2. Il reticolo $\mathrm{Free}_{\mathbf{D}}(3)$ sui generatori x, y e z, dove $a = (x \curlyvee y) \curlywedge (x \curlyvee z) \curlywedge (y \curlyvee z) = (x \curlywedge y) \curlyvee (x \curlywedge z) \curlyvee (y \curlywedge z)$, $b = (x \curlyvee y) \curlywedge (y \curlyvee z)$, $c = (x \curlywedge y) \curlyvee (y \curlywedge z)$.

L'Esercizio 8.76 mostra che ogni reticolo distributivo *finito* è un reticolo di insiemi, cioè un sotto-reticolo di $\mathscr{P}(X)$ per qualche X finito, e questo risultato si estende al caso infinito (Esercizio 32.29, Sezione 32).

Il reticolo $\mathrm{Free}_{\mathbf{M}}(3)$ ha 28 elementi, mentre $\mathrm{Free}_{\mathbf{M}}(4)$ (e quindi $\mathrm{Free}_{\mathbf{M}}(n)$ per $n > 4$) è infinito (Esercizio 8.58).

Il seguente risultato è il converso della parte (ii) dell'Esercizio 8.22. La dimostrazione utilizza più volte la legge modulare nella seguente forma:

$$z \leq x \Rightarrow x \curlywedge (y \curlyvee z) = (x \curlywedge y) \curlyvee z.$$

Per facilitare la lettura, quando applicheremo questa regola per manipolare un termine in una formula, i termini sostituiti al posto di x e z saranno evidenziati e la trasformazione sarà indicata con

$$\begin{array}{l} x \curlywedge (y \curlyvee z) \\ (x \curlywedge y) \curlyvee z \end{array}$$

o con

$$\begin{array}{l} (x \curlywedge y) \curlyvee z \\ x \curlywedge (y \curlyvee z). \end{array}$$

Teorema 8.24. (a) *Un reticolo è modulare se e solo se non contiene un sotto-reticolo isomorfo a* $\mathcal{N}_5$.

(b) *Un reticolo è distributivo se e solo se non contiene un sotto-reticolo isomorfo a* $\mathcal{N}_5$ *o a* $\mathcal{M}_3$.

Dimostrazione. La parte (a) è lasciata al lettore (Esercizio 8.59).

(b) Per la parte (a) è sufficiente dimostrare che se M è un reticolo modulare ma non distributivo, allora contiene un sotto-reticolo isomorfo a $\mathcal{M}_3$. Per ipotesi esistono $a, b, c \in M$ tali che $(a \curlywedge b) \curlyvee (a \curlywedge c) < a \curlywedge (b \curlyvee c)$ e siano

$$\begin{aligned} e &= (a \curlywedge b) \curlyvee (b \curlywedge c) \curlyvee (c \curlywedge a) \\ f &= (a \curlyvee b) \curlywedge (b \curlyvee c) \curlywedge (c \curlyvee a) \\ d_1 &= e \curlyvee (a \curlywedge f) \\ d_2 &= e \curlyvee (b \curlywedge f) \\ d_3 &= e \curlyvee (c \curlywedge f). \end{aligned}$$

È immediato verificare che $e \leq f$, che per modularità

$$\begin{aligned} d_1 &= (e \curlyvee a) \curlywedge f \\ d_2 &= (e \curlyvee b) \curlywedge f \\ d_3 &= (e \curlyvee c) \curlywedge f. \end{aligned}$$

e quindi $e \leq d_i \leq f$ per $i = 1, 2, 3$, e che

$$a \curlywedge f = a \curlywedge (b \curlyvee c) \tag{8.8a}$$

$$b \curlyvee e = b \curlyvee (a \curlywedge c). \tag{8.8b}$$

Inoltre

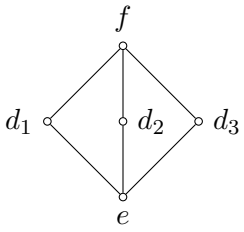
$$\begin{aligned} a \curlywedge e &= a \curlywedge ((b \curlywedge c) \curlyvee (a \curlywedge b) \curlyvee (a \curlywedge c)) \\ &= (a \curlywedge (b \curlywedge c)) \curlyvee ((a \curlywedge b) \curlyvee (a \curlywedge c)) \\ &= (a \curlywedge b) \curlyvee (a \curlywedge c). \end{aligned}$$

$x=a, z=(a \curlywedge b) \curlyvee (a \curlywedge c)$

Poiché $a \curlywedge e < a \curlywedge f$ allora

$$e < f.$$

Dimostriamo che l'insieme $\{e, f, d_1, d_2, d_3\}$ è un sotto-reticolo di M ed è isomorfo a $\mathcal{M}_3$



Per questo è sufficiente verificare che $d_i \curlywedge d_j = e$ e $d_i \curlyvee d_j = f$ per $i \neq j$. Verifichiamo innanzitutto che $d_1 \curlywedge d_2 = e$:

$$
\begin{aligned}
d_1 \curlywedge d_2 &= [\,e \curlyvee (a \curlywedge f)] \curlywedge [\,(b \curlywedge f) \curlyvee e\,] && \xleftarrow{x=e,z=(b\curlywedge f)\curlyvee e}\\
&= e \curlyvee [(a \curlywedge f) \curlywedge ((b \curlywedge f) \curlyvee e)] && \xleftarrow{x=e,z=f}\\
&= e \curlyvee [(a \curlywedge f) \curlywedge ((e \curlyvee b) \curlywedge f)] &&\\
&= e \curlyvee [(a \curlywedge f) \curlywedge (b \curlyvee e)] &&\\
&= e \curlyvee [(a \curlywedge (b \curlyvee c)) \curlywedge (b \curlyvee (a \curlywedge c))] && \text{per (8.8)}\\
&= e \curlyvee [a \curlywedge ((b \curlyvee c) \curlywedge ((a \curlywedge c) \curlyvee b))] && \xleftarrow{x=b\curlyvee c,z=b}\\
&= e \curlyvee [a \curlywedge ([(b \curlyvee c) \curlywedge (a \curlywedge c)] \curlyvee b)] &&\\
&= e \curlyvee [a \curlywedge (b \curlyvee [a \curlywedge c])] && (\text{per } a \curlywedge c \leq b \curlyvee c)\\
&= e \curlyvee [(a \curlywedge b) \curlyvee (a \curlywedge c)] &&\\
&= e. &&
\end{aligned}
$$

Lasciamo al lettore l'onere di completare la dimostrazione: la verifica di $d_1 \curlyvee d_2 = f$ è ottenuta "dualizzando" quella di $d_1 \curlywedge d_2 = e$ qui sopra, utilizzando le identità $a \curlyvee e = a \curlyvee (b \curlywedge c)$ e $b \curlywedge f = b \curlywedge (a \curlyvee c)$. Una volta stabilito ciò, i rimanenti casi $d_1 \curlywedge d_3 = d_2 \curlywedge d_3 = e$ e $d_1 \curlyvee d_3 = d_2 \curlyvee d_3 = f$ seguono facilmente permutando opportunamente le lettere a, b e c. □

Esempi 8.25. (a) Il reticolo $\mathscr{P}(X)$ con le operazioni di intersezione e unione è distributivo, quindi anche ogni suo sotto-reticolo lo è. Per esempio $\mathrm{Fin} = \{A \subseteq \mathbb{N} \mid A \text{ è finito}\}$ è un reticolo distributivo che ha minimo, ma non ha massimo, il cui duale è (isomorfo a)

$$\{A \subseteq \mathbb{N} \mid \mathbb{N} \setminus A \text{ è finito}\}.$$

(b) Sia $\mathcal{F}$ l'insieme delle funzioni da un insieme I a valori in un ordine $(M, \leq)$ con l'ordinamento

$$f \preceq g \Leftrightarrow \forall i \in I\, (f(i) \leq g(i)).$$

Se $m \in M$ è massimo/minimo allora la funzione costante m è massimo/minimo di $\mathcal{F}$. Se $(M, \leq)$ è un semi-reticolo superiore, allora la funzione $I \ni i \mapsto \sup(f(i), g(i))$ è l'estremo superiore di f e g nell'ordinamento $\preceq$, quindi $(\mathcal{F}, \preceq)$ è un semi-reticolo superiore. Analogamente, se $(M, \leq)$ è un semi-reticolo inferiore, allora anche $(\mathcal{F}, \preceq)$ è un semi-reticolo inferiore, quindi se $(M, \leq)$ è un reticolo, allora anche $(\mathcal{F}, \preceq)$ è un reticolo. Inoltre se $(M, \leq)$ è un reticolo modulare/distributivo, allora anche $(\mathcal{F}, \preceq)$ lo è.

(c) L'insieme $\mathrm{Sgr}(G)$ dei sottogruppi di un gruppo G è un reticolo con l'ordinamento per inclusione. Le operazioni sono

$$\begin{aligned} H \curlywedge K &= H \cap K \\ H \curlyvee K &= \text{il sottogruppo generato da } H \cup K \\ &= \bigcap \{J \in \mathrm{Sgr}(G) \mid H \cup K \subseteq J\}. \end{aligned}$$

Il reticolo $\mathrm{Sgr}(G)$ non caratterizza il gruppo G a meno di isomorfismo, per esempio $\mathrm{Sgr}(\mathbb{Z}/4\mathbb{Z}) \cong \mathrm{Sgr}(\mathbb{Z}/9\mathbb{Z})$.

Il reticolo $\mathrm{Sgr}(G)$ non è necessariamente distributivo o neppure modulare — per un esempio considerare il gruppo diedrale D_4 delle simmetrie del quadrato — ma se G è abeliano $\mathrm{Sgr}(G)$ è modulare. Più in generale, l'insieme $\mathrm{NSgr}(G)$ dei sottogruppi normali di un gruppo G è un sotto-reticolo di $\mathrm{Sgr}(G)$ ed è un reticolo modulare — questo discende dal fatto che per sottogruppi normali $H \curlyvee K = HK = \{hk \mid h \in H, k \in K\}$.

(d) Analogamente, l'insieme dei sottomoduli di un modulo sinistro M su un anello unitario R è un reticolo modulare, dato che $(N_1 \cap N_2) + (N_1 \cap N_3) \subseteq N_1 \cap (N_2 + (N_1 \cap N_3))$. In generale, il reticolo dei sottomoduli non è distributivo (Esercizio 8.55).

(e) Se $H, K \in \mathrm{Sgr}(G)$ sono finitamente generati, allora $H \curlyvee K$ è finitamente generato, ma $H \curlywedge K = H \cap K$ può non essere finitamente generato, se G non è abeliano (Esempio 14.21 a pagina 313). Quindi la famiglia dei sottogruppi finitamente generati di G non è un reticolo, ma soltanto un semireticolo superiore.

(f) L'insieme $\mathrm{Prt}(X)$ delle relazioni di equivalenza su un insieme non vuoto X ordinate da

$$E_1 \leq E_2 \Leftrightarrow \forall x, y \in X \, (x \; E_1 \; y \Rightarrow x \; E_2 \; y)$$

è un reticolo. Equivalentemente, $\mathrm{Prt}(X)$ può essere visto come l'insieme delle partizioni su X, con l'ordinamento

$$\mathcal{P}_1 \leq \mathcal{P}_2 \Leftrightarrow \forall A \in \mathcal{P}_1 \, \exists B \in \mathcal{P}_2 \, (A \subseteq B).$$

Il minimo di $\mathrm{Prt}(X)$ è la diagonale $\{(x, x) \mid x \in X\}$ e il massimo è la relazione banale $X \times X$, e le operazioni di inf e sup sono date da

$E \curlywedge F = E \cap F$ e $E \curlyvee F = \bigcap \{D \in \mathrm{Prt}(X) \mid E \cup F \subseteq D\}$. Il reticolo $\mathrm{Prt}(X)$ non è (quasi mai) modulare (Esercizio 8.60).

(g) Una famiglia $\mathcal{S} \subseteq \mathscr{P}(X)$ chiusa per intersezioni arbitrarie e contenente X è un reticolo completo con le operazioni $A \curlywedge B = A \cap B$ e $A \curlyvee B = \bigcap \{C \in \mathcal{S} \mid A \cup B \subseteq C\}$, ma in generale non è un reticolo di insiemi. Gli esempi (c), (d) e (f) qui sopra e la famiglia dei chiusi di uno spazio topologico (Esempio 8.17(c)) sono di questo tipo; un altro esempio importante è il reticolo delle topologie su un insieme fissato. Nella Sezione 11.K vedremo una formulazione equivalente di questo tipo di reticoli.

8.D. Algebre di Boole. Un reticolo limitato è **complementato** se per ogni x c'è un y, detto **complemento** di x, tale che

$$x \curlywedge y = \mathbf{0} \quad \text{e} \quad x \curlyvee y = \mathbf{1}.$$

Se il complemento di x è unico, esso verrà denotato con x^*. Quindi

$$\mathbf{0}^* = \mathbf{1} \quad \text{e} \quad \mathbf{1}^* = \mathbf{0}.$$

Se ogni x ha un unico complemento, diremo che il reticolo è **univocamente complementato**. Chiaramente in un reticolo siffatto $x^{**} = x$ per ogni x. Il prossimo risultato mostra che un reticolo distributivo complementato è univocamente complementato.

Lemma 8.26. *In un reticolo distributivo e limitato, il complemento di un elemento, se esiste è unico.*

Dimostrazione. Supponiamo y e z siano complementi di un x:

$$y = \mathbf{1} \curlywedge y = (x \curlyvee z) \curlywedge y = (x \curlywedge y) \curlyvee (z \curlywedge y) = \mathbf{0} \curlyvee (y \curlywedge z) = y \curlywedge z,$$

da cui $y \leq z$. Scambiando y con z si ottiene $z \leq y$. □

Osservazione 8.27. $\mathcal{M}_3$ della Figura 1 e l'insieme dei sottospazi di uno spazio vettoriale, sono esempi di reticoli modulari, complementati, ma non univocamente complementati. Se R è un anello regolare di von Neumann (Sezione 5.D.2) l'insieme $\mathrm{Lr}(R) = \{xR \mid x \in R\}$ è un reticolo complementato modulare. Un importante teorema di von Neumann asserisce essenzialmente il converso: ogni reticolo complementato modulare che soddisfi un'ulteriore condizione tecnica è isomorfo a $\mathrm{Lr}(R)$, con R anello regolare di von Neumann e per di più R è unico a meno di isomorfismo [**Grä11**, pp. 394–397].

Definizione 8.28. Sia L_{BOOLE} il linguaggio che estende L_{RETICOLI} mediante un simbolo di operazione unaria * e che contiene due simboli di costante $\mathbf{1}$ e $\mathbf{0}$. Un'**algebra di Boole** è una struttura in questo linguaggio che soddisfa

le proprietà associativa 8.1, commutativa (8.2) e distributiva (8.7) per $\curlywedge$ e per $\curlyvee$, l'esistenza del complemento

(8.9a) $\forall x\,(x \curlyvee x^* = \mathbf{1})$

(8.9b) $\forall x\,(x \curlywedge x^* = \mathbf{0})$,

e

(8.10a) $\forall x\,(x \curlyvee \mathbf{0} = x)$

(8.10b) $\forall x\,(x \curlywedge \mathbf{1} = x)$,

e tale che $\mathbf{0} \neq \mathbf{1}$. In altre parole: una L_{BOOLE}-struttura è un'algebra di Boole se soddisfa Σ_{BOOLE}, il sistema di assiomi costituito dagli enunciati (8.2a), (8.2b), (8.7a), (8.7b), (8.9a), (8.9b), (8.10a), (8.10b) e $\mathbf{0} \neq \mathbf{1}$.

Il duale di un termine di L_{BOOLE} è il termine ottenuto scambiando $\curlywedge$ con $\curlyvee$ e $\mathbf{1}$ con $\mathbf{0}$; la duale di una formula φ è la formula φ^Δ ottenuta sostituendo ogni termine col suo duale. La duale dell'algebra di Boole $\mathcal{B} = (B, \curlywedge, \curlyvee, ^*, \mathbf{0}, \mathbf{1})$ è $\mathcal{B}^\Delta = (B, \sqcap, \sqcup, ^*, \bot, \top)$ dove $\sqcap = \curlyvee$, $\sqcup = \curlywedge$, $\bot = \mathbf{1}$ e $\top = \mathbf{0}$. Poiché l'enunciato $(n\text{a})$ è il duale di $(n\text{b})$ (per $n = 8.2, 8.7, 8.9, 8.10$), e poiché $\bot \neq \top$ è autoduale, la duale di un'algebra di Boole è un'algebra di Boole. Inoltre la mappa $\mathcal{B} \to \mathcal{B}^\Delta$, $x \mapsto x^*$, è un isomorfismo.

Principio di dualità per le algebre di Boole. *Se $\mathcal{B}$ è un'algebra di Boole e σ è un enunciato, allora*

$$\mathcal{B} \vDash \sigma \quad \textit{se e solo se} \quad \mathcal{B} \vDash \sigma^\Delta.$$

In particolare: σ è conseguenza logica degli assiomi delle algebre di Boole se e solo se σ^Δ lo è.

Ogni reticolo complementato e distributivo $(B, \leq)$ con almeno due elementi definisce un'algebra di Boole $(B, \curlywedge, \curlyvee, ^*, \mathbf{0}, \mathbf{1})$. Viceversa,

Proposizione 8.29. *Ogni algebra di Boole è un reticolo complementato e distributivo con almeno due elementi.*

Dimostrazione. Sia $(B, \curlywedge, \curlyvee, ^*, \mathbf{0}, \mathbf{1})$ un'algebra di Boole. Vogliamo dimostrare che $(B, \curlywedge, \curlyvee)$ è un'algebra reticolare che ha $\mathbf{0}$ come minimo e $\mathbf{1}$ come massimo. Applicando gli assiomi otteniamo

$$x \curlywedge \mathbf{0} = (x \curlywedge \mathbf{0}) \curlyvee \mathbf{0} = (x \curlywedge \mathbf{0}) \curlyvee (x \curlywedge x^*) = x \curlywedge (\mathbf{0} \curlyvee x^*) = x \curlywedge x^* = \mathbf{0}$$

cioè $\mathbf{0}$ è il minimo, e

$$x \curlywedge (x \curlyvee y) = (x \curlyvee \mathbf{0}) \curlywedge (x \curlyvee y) = x \curlyvee (\mathbf{0} \curlywedge y) = x \curlyvee \mathbf{0} = x$$

cioè vale la (8.3a). Per il Principio di dualità $\mathbf{1}$ è il massimo, e vale la proprietà di assorbimento (8.3b) per $\curlyvee$. □

Chiaramente, la corrispondenza

$$(B, \curlyvee, \curlywedge, ^*, \mathbf{0}, \mathbf{1}) \mapsto (B, \leq)$$

che trasforma le algebre di Boole in reticoli distributivi complementati è l'inversa della corrispondenza $(B, \leq) \mapsto (B, \curlyvee, \curlywedge, ^*, \mathbf{0}, \mathbf{1})$.

Un'algebra di Boole, in quanto reticolo distributivo complementato, soddisfa le proprietà viste sinora: le operazioni $\curlywedge$ e $\curlyvee$ sono commutative (8.2), associative (8.1) e idempotenti (8.4), valgono la legge modulare e l'unicità del complemento (Lemma 8.26). Vediamo ora qualche proprietà specifica delle algebre di Boole.

Esercizio 8.30. Dimostrare che in un'algebra di Boole valgono le seguenti proprietà :

(i) $x \curlywedge y = \mathbf{0} \Leftrightarrow x \leq y^*$;

(ii) $(x \curlywedge y)^* = x^* \curlyvee y^*$ e $(x \curlyvee y)^* = x^* \curlywedge y^*$ (Leggi di De Morgan);

(iii) $x \leq y \Leftrightarrow y^* \leq x^*$;

(iv) $x \curlywedge y \leq z \Leftrightarrow x \leq z \curlyvee y^*$.

Gli enunciati (8.10a) e (8.10b) sono deducibili l'uno dall'altro a partire dagli altri assiomi in Σ_{BOOLE}. La ragione per questa ridondanza è che sono enunciati duali e questo ci permette di enunciare facilmente il Principio di dualità per le algebre di Boole. Se rimuoviamo uno (ed uno solo) tra i due assiomi (8.10a) e (8.10b) si ottiene un sistema indipendente di assiomi per le algebre di Boole (Esercizio 8.73).

Un'**algebra di Boole completa** è un'algebra di Boole B che è completa come reticolo, cioè tale che $\bigvee X$ e $\bigwedge X$ esistono per ogni $X \subseteq B$. Ogni algebra finita è completa, ma questo non vale per le algebre infinite (Sezione 23). Il prossimo risultato generalizza le ben note identità insiemistiche $B \cap \bigcup_{i \in I} A_i = \bigcup_{i \in I} B \cap A_i$ e $B \cup \bigcap_{i \in I} A_i = \bigcap_{i \in I} B \cup A_i$.

Lemma 8.31. *Sia B un'algebra di Boole e $X \subseteq B$ un insieme tale che $\bigvee X$ esiste. Allora $\bigvee\{b \curlywedge x \mid x \in X\}$ esiste per ogni $b \in B$, e*

$$b \curlywedge \bigvee X = \bigvee\{b \curlywedge x \mid x \in X\}.$$

Analogamente, se $\bigwedge X$ esiste, allora anche $\bigwedge\{b \curlyvee x \mid x \in X\}$ esiste ed è $b \curlyvee \bigwedge X$.

Dimostrazione. $b \curlywedge x \leq b \curlywedge \bigvee X$ per ogni $x \in X$, allora $b \curlywedge \bigvee X$ è un maggiorante di $\{b \curlywedge x \mid x \in X\}$. Se c è un altro maggiorante di questo insieme, allora per ogni $x \in X$,

$$b \curlywedge x \leq c \Rightarrow x \leq b^* \curlyvee c$$

per la parte (iv) dell'Esercizio 8.30 e quindi $\bigvee X \leq b^* \curlyvee c$, da cui $b \curlywedge \bigvee X \leq c$. □

8.E. Algebre finitamente generate. Data un'algebra di Boole B e un suo sottoinsieme X, l'algebra generata da X è la più piccola subalgebra B' di B contenente X; diremo che X è un insieme di generatori di B'. Un'algebra di Boole si dice **finitamente generata** se ha un insieme finito di generatori. Se B ha un insieme di n generatori, allora B è un sotto-reticolo di $\mathrm{Free}_{\mathbf{D}}(n)$, quindi B è finita. Vogliamo descrivere più in dettaglio la struttura delle algebre finitamente generate.

Il Lemma 8.31 implica che

$$x \curlywedge \bigvee_{i\in I} y_i = \bigvee_{i\in I}(x \curlywedge y_i) \quad \text{e} \quad x \curlyvee \bigwedge_{i\in I} y_i = \bigwedge_{i\in I}(x \curlyvee y_i),$$

dove I è un insieme arbitrario. È possibile generalizzare questa formula a patto di considerare insiemi finiti di indici. Per formulare efficacemente il prossimo risultato, ricordiamo che se I è un insieme finito e gli J_i sono insiemi non vuoti per $i \in I$, allora gli elementi del prodotto cartesiano

$$\bigtimes_{i\in I} J_i$$

si possono identificare con le funzioni f di dominio I tali che $f(i) \in J_i$ per ogni $i \in I$.

Lemma 8.32. *Sia B un'algebra di Boole, sia I un insieme finito e non vuoto e siano J_i ($i \in I$) degli insiemi finiti e non vuoti. Allora, per ogni $x_{i,j} \in B$ ($i \in I$ e $j \in J_i$)*

$$\text{(8.11)} \quad \bigwedge_{i\in I}\bigvee_{j\in J_i} x_{i,j} = \bigvee_{f\in\bigtimes_{i\in I} J_i}\bigwedge_{i\in I} x_{i,f(i)} \quad e \quad \bigvee_{i\in I}\bigwedge_{j\in J_i} x_{i,j} = \bigwedge_{f\in\bigtimes_{i\in I} J_i}\bigvee_{i\in I} x_{i,f(i)}.$$

Dimostrazione. Per dualità è sufficiente dimostrare la prima delle due formule. La dimostrazione procede per induzione su $|I| \geq 1$. Se $|I| = 1$ il risultato è banale, quindi possiamo assumere che il risultato valga per ogni insieme I di cardinalità $n \geq 1$ e dimostrarlo per insiemi di cardinalità $n+1$. Supponiamo $|I| = n+1$ e chiaramente possiamo supporre che $I = \{0, \ldots, n\}$.

Allora:

$$\begin{aligned}
\bigwedge_{i\le n}\bigvee_{j\in J_i} x_{i,j} &= \Big(\bigvee_{j\in J_0} x_{0,j}\Big) \curlywedge \Big(\bigwedge_{1\le i\le n}\bigvee_{j\in J_i} x_{i,j}\Big)\\
&= \Big(\bigvee_{j\in J_0} x_{0,j}\Big) \curlywedge \Big(\bigvee_{f\in J_1\times\cdots\times J_n}\bigwedge_{1\le i\le n} x_{i,f(i)}\Big)\\
&= \bigvee_{j\in J_0}\Big(x_{0,j} \curlywedge \Big(\bigvee_{f\in J_1\times\cdots\times J_n}\bigwedge_{1\le i\le n} x_{i,f(i)}\Big)\Big)\\
&= \bigvee_{j\in J_0}\bigvee_{f\in J_1\times\cdots\times J_n}\Big(x_{0,j} \curlywedge \Big(\bigwedge_{1\le i\le n} x_{i,f(i)}\Big)\Big)\\
&= \bigvee_{f\in \bigtimes_{i\le n} J_i}\bigwedge_{i\le n} x_{i,f(i)},
\end{aligned}$$

dove nella seconda riga abbiamo usato l'ipotesi induttiva e nella terza riga abbiamo usato il Lemma 8.31. □

Definiamo, per $X \subseteq B$,

$$\begin{aligned}
X^{\curlywedge} &= \{x_1 \curlywedge \ldots \curlywedge x_n \mid x_1,\ldots,x_n \in X \text{ e } n \ge 1\}\\
X^{\curlyvee} &= \{x_1 \curlyvee \ldots \curlyvee x_n \mid x_1,\ldots,x_n \in X \text{ e } n \ge 1\}.
\end{aligned}$$

Teorema 8.33. *Se B è un'algebra di Boole e $X \subseteq B$, l'algebra generata da X è*

$$C \stackrel{\text{def}}{=} \Big((X \cup \{x^* \mid x \in X\} \cup \{\mathbf{0},\mathbf{1}\})^{\curlywedge}\Big)^{\curlyvee}.$$

Dimostrazione. C è non vuoto, chiuso per $\curlyvee$, ed è contenuto nell'algebra generata da X. Quindi è sufficiente dimostrare che è chiuso per complementi: un generico elemento di C è della forma

$$\bigvee_{i\in I}\bigwedge_{j\in J_i} y_{i,j}$$

dove $y_{i,j} \in X \cup \{x^* \mid x \in X\} \cup \{\mathbf{0},\mathbf{1}\}$ e I e J_i sono insiemi finiti, quindi il suo complemento è

$$\bigwedge_{i\in I}\bigvee_{j\in J_i} y^*_{i,j} = \bigvee_{f\in \bigtimes_{i\in I} J_i}\bigwedge_{i\in I} y^*_{i,f(i)} \in C.$$ □

Osservazione 8.34. Il motivo della presenza di $\mathbf{0}$ e $\mathbf{1}$ nella formula che definisce C è per il caso in cui $X = \emptyset$. Se $X \neq \emptyset$, allora $\mathbf{0} \in (X \cup \{x^* \mid x \in X\})^{\curlywedge}$ e $\mathbf{1} \in \Big((X \cup \{x^* \mid x \in X\})^{\curlywedge}\Big)^{\curlyvee}$, quindi l'algebra generata da X è

$$C \stackrel{\text{def}}{=} \Big((X \cup \{x^* \mid x \in X\})^{\curlywedge}\Big)^{\curlyvee}.$$

Corollario 8.35. *Sia A un'algebra di Boole, $B \subseteq A$ e $x \in A \setminus B$. La sub-algebra di A generata da $B \cup \{x\}$ è*

$$\{(b_1 \curlywedge x) \curlyvee (b_2 \curlywedge x^*) \mid b_1, b_2 \in B\}.$$

8.F. Morfismi e prodotti. A pagina 48 abbiamo detto che un morfismo è una mappa tra strutture che preserva tutti i predicati, le funzioni e le costanti. Quindi un morfismo di ordini parziali è semplicemente una funzione che preserva l'ordine, mentre un morfismo di reticoli è una mappa crescente che preserva le operazioni di inf e di sup, cioè è un morfismo di L_{RETICOLI}-strutture. Se i due reticoli sono complementati e se f è un morfismo di reticoli che preserva massimo e minimo, cioè se è un morfismo delle strutture $f\colon (M, \curlywedge_M, \curlyvee_M, \mathbf{0}_M, \mathbf{1}_M) \to (N, \curlywedge_N, \curlyvee_N, \mathbf{0}_N, \mathbf{1}_N)$ allora per il Lemma 8.26 il morfismo f preserva i complementari, cioè

$$\forall x \in M\, (f(x^*) = f(x)^\star)$$

dove * è il complemento in N. Un **omomorfismo di algebre di Boole** è una mappa tra algebre di Boole che è un morfismo di L_{BOOLE}-strutture. Per quanto detto è sufficiente che preservi $\curlywedge$, $\curlyvee$, $\mathbf{0}$ e $\mathbf{1}$; equivalentemente, per le leggi di De Morgan (Esercizio 8.30(ii)) è sufficiente che preservi $\curlywedge$ e * o che preservi $\curlyvee$ e *.

Gli assiomi delle algebre di Boole sono enunciati universali, quindi per la Proposizione 3.24 ogni L_{BOOLE}-sottostruttura C di un'algebra di Boole B è a sua volta un'algebra di Boole e diremo che C è una **sub-algebra** di B. L'**algebra minimale** è l'unica algebra di Boole (a meno di isomorfismo) con esattamente due elementi $\mathbf{1}$ e $\mathbf{0}$, ed è (isomorfa ad) una sub-algebra di ogni algebra di Boole.

Gli assiomi (8.2), (8.7), (8.9) e (8.10) sono formule positive, quindi per la Proposizione 3.23 si preservano per immagini omomorfe. Tuttavia tra gli assiomi delle algebre di Boole c'è anche $\mathbf{1} \neq \mathbf{0}$, che non è positivo. Riassumendo abbiamo che: se $f\colon B \to C$ è un morfismo suriettivo di L_{BOOLE}-strutture e se B è un'algebra di Boole e se $\mathbf{1}_C \neq \mathbf{0}_C$, allora anche C è un'algebra di Boole.

Infine per la Proposizione 3.25 il prodotto di algebre di Boole è ancora un'algebra di Boole — gli assiomi (8.2), (8.7), (8.9) e (8.10) sono delle equazioni e quindi si preservano per prodotti e così pure $\mathbf{1} \neq \mathbf{0}$, anche se non è un'equazione.

8.G. Algebre libere. Sia t un termine di L_{BOOLE} nelle variabili $x_1, \dots, x_n$: rimpiazzando le occorrenze di $\mathbf{0}$ e $\mathbf{1}$ con $x_1 \curlywedge x_1^*$ e $x_1 \curlyvee x_1^*$ rispettivamente, e applicando ripetutamente le leggi di De Morgan (Esercizio 8.30(ii)), è possibile trasformare t in un termine t' nelle medesime variabili $x_1, \dots, x_n$ in cui il simbolo di complementazione * compaia solo applicato alle variabili. In altre

parole $t' = s[x_1^*/y_1, \dots, x_n^*/y_n]$ dove $s \in \mathrm{Term}_{\text{RETICOLI}}(x_1, \dots, x_n, y_1, \dots, y_n)$. Per il Lemma 8.23, s è equivalente tanto ad un termine in forma disgiuntiva u quanto ad un termine in forma congiuntiva v. Per la (8.10a) possiamo supporre che in ciascuna disgiunzione di u non compaia mai una variabile e il suo complemento e un discorso analogo vale per v. Abbiamo quindi dimostrato il:

Lemma 8.36. *Per ogni termine $t \in \mathrm{Term}_{\text{BOOLE}}(x_1, \dots, x_n)$ esistono termini $u, v \in \mathrm{Term}_{\text{RETICOLI}}(x_1, \dots, x_n, y_1, \dots, y_n)$ tali che, posto*

$$u' \stackrel{\text{def}}{=} u[x_1^*/y_1, \dots, x_n^*/y_n], \quad v' \stackrel{\text{def}}{=} v[x_1^*/y_1, \dots, x_n^*/y_n]$$

allora $u', v' \in \mathrm{Term}_{\text{BOOLE}}(x_1, \dots, x_n)$ e

- *u' è in **forma disgiuntiva**, vale a dire è una disgiunzione di congiunzioni di $\{x_1, \dots, x_n, x_1^*, \dots, x_n^*\}$ in cui in nessuna congiunzione compaiono tanto x_i quanto x_i^*, $(1 \leq i \leq n)$,*
- *v' è in **forma congiuntiva**, vale a dire è una congiunzione di disgiunzioni delle variabili $\{x_1, \dots, x_n, x_1^*, \dots, x_n^*\}$ in cui in nessuna disgiunzione compaiono tanto x_i quanto x_i^*, $(1 \leq i \leq n)$,*
- *la formula $t = u' = v'$ è conseguenza degli assiomi delle algebre di Boole.*

Se $\sim$ è la congruenza che asserisce la validità di (8.2), (8.7), (8.9) e (8.10), la struttura $\mathrm{Term}_{\text{BOOLE}}(x_1, \dots, x_n)/\!\sim$ è un'algebra di Boole che ha per atomi (le classi di equivalenza de) i termini della forma

$$x_1^{\varepsilon_1} \curlywedge \cdots \curlywedge x_n^{\varepsilon_n}$$

dove $\varepsilon_i \in \{1, -1\}$, $x_i^1 = x_i$ e $x_i^{-1} = x_i^*$. Questo è l'esempio più generale di algebra di Boole generata da n oggetti $[x_1], \dots, [x_n]$ e si dice **algebra di Boole libera su n-generatori**.

8.H. Anelli booleani. La **somma in un'algebra di Boole** è l'operazione binaria $+$ definita da

$$x + y \stackrel{\text{def}}{=} (x \curlywedge y^*) \curlyvee (y \curlywedge x^*).$$

Osserviamo che l'operazione di somma è commutativa e che se $f\colon B \to C$ è un omomorfismo di algebre di Boole, allora $f(x + y) = f(x) + f(y)$.

Esercizio 8.37. (i) $x = y \Leftrightarrow x + y = \mathbf{0}$;
(ii) $x + y = (x \curlyvee y) \curlywedge (x \curlywedge y)^*$;
(iii) $(x + y)^* = (x \curlywedge y) \curlyvee (x^* \curlywedge y^*)$;
(iv) $x \curlywedge y = \mathbf{0} \Rightarrow x + y = x \curlyvee y$;
(v) $x \curlyvee y = (x + y) + (x \curlywedge y)$;
(vi) $x + (y + z) = (x + y) + z$;

(vii) $x \curlywedge (y + z) = (x \curlywedge y) + (x \curlywedge z)$.

Quindi ad ogni algebra di Boole possiamo associare un anello commutativo unitario,

$$(B, \curlyvee, \curlywedge, ^*, \mathbf{0}, \mathbf{1}) \mapsto (B, +, \cdot, 0, 1) \tag{8.12}$$

ponendo $x + y$ come sopra, $0 = \mathbf{0}$, $1 = \mathbf{1}$ e

$$x \cdot y \stackrel{\text{def}}{=} x \curlywedge y.$$

Questo è un esempio di **anello booleano** cioè un anello unitario che soddisfa $\forall x(x^2 = x)$. Ogni anello booleano è commutativo ed è l'anello costruito a partire da una qualche algebra di Boole (Esercizio 8.68); ogni omomorfismo $f\colon B \to C$ di algebre di Boole è un omomorfismo di anelli con unità . Abbiamo quindi un'altra assiomatizzazione della nozione di algebra di Boole, come una $L_{\text{ANELLI-1}}$-struttura che soddisfa gli assiomi di anello booleano.

Il **nucleo** di un morfismo di algebre di Boole $f\colon B \to C$ è

$$\ker(f) \stackrel{\text{def}}{=} \{b \in B \mid f(b) = \mathbf{0}_C\}.$$

Quindi f è iniettivo se e solo se il suo nucleo è $\{\mathbf{0}_B\}$.

Definizione 8.38. Un **ideale di un'algebra di Boole** B è un sottoinsieme non vuoto I tale che

- se $x, y \in I$ allora $x \curlyvee y \in I$ e
- se $x \in I$ e $y \leq x$ allora $y \in I$.

I è **proprio** se $I \neq B$; è **banale** se $I = \{\mathbf{0}\}$.

Questa terminologia è giustificata dal seguente:

Esercizio 8.39. Sia B un'algebra di Boole. Dimostrare che I è un ideale nel senso della Definizione 8.38 se e solo se è un ideale nel senso degli anelli.

Se R è un anello commutativo unitario e I un suo ideale proprio possiamo costruire il quoziente R/I che sarà ancora un anello commutativo unitario; inoltre se R è booleano anche il quoziente è un anello booleano — questo può essere verificato direttamente oppure osservando che $\forall x(x^2 = x)$ è una formula positiva e applicando la Proposizione 3.22 a pagina 50. Un ideale proprio I si dice

- **primo** se $x \cdot y \in I \Rightarrow x \in I \vee y \in I$, o equivalentemente se R/I è un dominio di integrità;
- **massimale** se non esiste alcun ideale proprio che contiene I, o equivalentemente se R/I è un campo.

Quindi un ideale massimale è primo. A partire da queste osservazioni si ottiene facilmente il seguente risultato la cui dimostrazione è lasciata al lettore (Esercizio 8.71).

Proposizione 8.40. *Sia* $(B, \curlywedge, \curlyvee, ^*, \bot, \top)$ *un'algebra di Boole e* I *un ideale proprio.*

(a) *Sia* $\sim_I$ *la relazione d'equivalenza su* B *data da*

$$x \sim_I y \Leftrightarrow x + y \in I.$$

L'insieme quoziente che si denota usualmente con B/I *è un'algebra di Boole ponendo*

$$\begin{aligned} \mathbf{0} &= [\bot] \\ \mathbf{1} &= [\top] \\ [x] \sqcap [y] &= [x \curlywedge y] \\ [x] \sqcup [y] &= [x \curlyvee y] \\ [x]' &= [x^*]. \end{aligned}$$

L'ordinamento su B/I *è dato da*

$$[x] \sqsubseteq [y] \Leftrightarrow x^* \curlywedge y \in I.$$

(b) I *è primo se e solo se* I *è massimale se e solo se* $\forall x(x \notin I \Leftrightarrow x^* \in I)$.

Osservazione 8.41. L'equivalenza "primo se e solo se massimale" in (b) vale non solo per le algebre di Boole, ma più in generale per gli anelli regolari di von Neumann (Sezione 5.D.2).

Un ideale I di un'algebra di Boole B è **principale** se è della forma $\downarrow x = \{y \in B \mid y \leq x\}$ per qualche $x \in B$; l'elemento x si dice **generatore di** I e diremo che I è generato da x.

Un **atomo** di un'algebra di Boole B è un elemento minimale di $B \setminus \{\mathbf{0}\}$ cioè un $a \in B \setminus \{\mathbf{0}\}$ per cui non esistono $\mathbf{0} < b < a$. Indicheremo l'insieme degli atomi di B con $\mathrm{At}(B)$. Un'algebra si dice **atomica** se per ogni $b \in B \setminus \{\mathbf{0}\}$ c'è un atomo $a \leq b$. Per la Proposizione 8.5 si ha

Proposizione 8.42. *Ogni algebra di Boole finita è atomica.*

8.I. Esempi di algebre di Boole e di ideali.

8.I.1. *L'algebra dei sottoinsiemi di* X. Sia X un insieme non vuoto. La struttura algebrica

$$(\mathscr{P}(X), \cap, \cup, \complement, \emptyset, X),$$

dove $\complement Y = X \setminus Y$ è il complementare di Y in X è un'algebra completa (Esempio 8.17(a)) e atomica (gli atomi sono i singoletti). Per la Definizione 3.29 un'**algebra di insiemi** è una subalgebra di $\mathscr{P}(X)$ per qualche X, cioè è

una famiglia $\mathcal{S} \subseteq \mathscr{P}(X)$ contenente $\emptyset$ e X e chiusa per unioni, intersezioni e complementi. In particolare, la famiglia dei sottoinsiemi definibili di dimensione n di una L-struttura M (vedi la Sezione 3.F.5) è un esempio di algebra di Boole.

8.I.2. *Ideali di $\mathscr{P}(X)$.* L'operazione di somma nell'algebra $\mathscr{P}(X)$ è l'operazione di differenza simmetrica $Y + Z = Y \triangle Z$. Un ideale di una subalgebra $\mathcal{S} \subseteq \mathscr{P}(X)$ è una famiglia $I \subseteq \mathcal{S}$ chiusa per unioni finite e per sottoinsiemi. L'ideale generato da un $A \in \mathcal{S}$ è $\{B \in \mathcal{S} \mid B \subseteq A\}$. Non tutti gli ideali di $\mathscr{P}(X)$ sono principali — per esempio

$$\mathrm{Fin} = \{A \subseteq \mathbb{N} \mid A \text{ è finito}\}$$

il reticolo dell'Esempio (a), è un ideale non principale di $\mathscr{P}(\mathbb{N})$. Se I è un ideale di una subalgebra $\mathcal{S} \subseteq \mathscr{P}(X)$ l'ordinamento dell'algebra quoziente $\mathcal{S}/I$ è dato da

$$[Y] \leq [Z] \Leftrightarrow Y \setminus Z \in I.$$

L'algebra quoziente $\mathscr{P}(\mathbb{N})/\operatorname{Fin}$ è priva di atomi: infatti se A è infinito (cioè $[A] \neq \mathbf{0} = \mathrm{Fin}$) allora A può essere scritto come unione di due insiemi B e C infiniti e disgiunti, $A = B \cup C$ e $B \cap C = \emptyset$, quindi $\mathbf{0} < [B] < [A]$.

8.I.3. *Ideale di convergenza.* Fissiamo una successione strettamente decrescente di reali positivi a_n tale che $\lim_{n\to\infty} a_n = 0$ e $\sum_{n=0}^{\infty} a_n = +\infty$. Allora

$$I = \{S \subseteq \mathbb{N} \mid \textstyle\sum_{n\in S} a_n < \infty\}$$

è un ideale non principale. Poiché la convergenza/divergenza di una serie non dipende da un numero finito di termini, $\mathrm{Fin} \subseteq I$ cioè se $S \triangle S' \in \mathrm{Fin}$ allora $S \in I \Leftrightarrow S' \in I$. La proiezione di I sul quoziente $\mathscr{P}(\mathbb{N})/\operatorname{Fin}$ è l'ideale

$$I' = \{[S] \mid \textstyle\sum_{n\in S} a_n < \infty\}\,.$$

8.I.4. *Ideale di densità nulla.* Un sottoinsieme X di $\mathbb{N}$ ha densità 0 se

$$\lim_{n\to\infty} \frac{|X \cap n|}{n} = 0.$$

I sottoinsiemi di densità nulla formano un ideale proprio non principale di $\mathscr{P}(\mathbb{N})$.

8.I.5. *Insiemi chiusi-aperti.* Se X è uno spazio topologico, un insieme U si dice **chiuso-aperto**[3] se è simultaneamente chiuso ed aperto.

$$\mathbf{CLOP}(X) = \{U \subseteq X \mid U \text{ è chiuso-aperto in } X\}$$

è una sub-algebra di $\mathscr{P}(X)$ che si chiama **algebra dei chiusi-aperti**. Se X è connesso $\mathbf{CLOP}(X)$ è l'algebra minimale. In generale $\mathbf{CLOP}(X)$ non è completa.

[3] In inglese *clopen*.

Viceversa, dato un insieme $X \neq \emptyset$ ogni subalgebra $B \subseteq \mathscr{P}(X)$ genera una topologia in cui $B = \mathbf{CLOP}(X)$.

8.I.6. *Aperti regolari.* Un aperto U di uno spazio topologico X si dice **regolare** se

$$r(U) \stackrel{\text{def}}{=} \mathrm{Int}(\mathrm{Cl}(U)) = U.$$

Esercizio 8.43. Dato uno spazio topologico X, dimostrare che se U è aperto e A, B sono sottoinsiemi arbitrari:

(i) $U \subseteq r(U)$;

(ii) $A \subseteq B \Rightarrow r(A) \subseteq r(B)$;

(iii) $r(r(A)) = r(A)$;

(iv) $r(U)$ è il più piccolo aperto regolare contenente U;

(v) $\mathrm{Int}(X \setminus U)$ è regolare.

Se U, V sono aperti regolari, allora $r(U \cap V) \subseteq r(U) = U$ e $r(U \cap V) \subseteq r(V) = V$, da cui $r(U \cap V) \subseteq U \cap V$. Quindi l'intersezione di due aperti regolari è un aperto regolare.

Se U è aperto (non necessariamente regolare) e Y arbitrario, allora $U \cap \mathrm{Cl}(Y) \subseteq \mathrm{Cl}(U \cap Y)$, quindi, tenendo presente che l'interno di un'intersezione è l'intersezione degli interni,

$$\begin{aligned} U \cap \mathrm{Int}(\mathrm{Cl}(Y)) &= \mathrm{Int}(U) \cap \mathrm{Int}(\mathrm{Cl}(Y)) \\ &= \mathrm{Int}(U \cap \mathrm{Cl}(Y)) \\ &\subseteq \mathrm{Int}(\mathrm{Cl}(U \cap Y)). \end{aligned} \tag{8.13}$$

L'insieme

$$\mathbf{RO}(X) = \{U \subseteq X \mid U \text{ è regolare}\}$$

ordinato per inclusione è un reticolo limitato: le operazioni $\curlywedge$ e $\curlyvee$ sono definite da

$$U \curlywedge V = U \cap U \quad \text{e} \quad U \curlyvee V = r(U \cup V)$$

e $\mathbf{0} = \emptyset$ e $\mathbf{1} = X$. È un reticolo distributivo: per l'Osservazione 8.21(b) è sufficiente verificare che $U \curlywedge (V \curlyvee W) \subseteq (U \curlywedge V) \curlyvee (U \curlywedge W)$ per ogni $U, V, W \in \mathbf{RO}(X)$,

$$\begin{aligned} U \curlywedge (V \curlyvee W) &= U \cap r(V \cup W) \\ &\subseteq r(U \cap (V \cup W)) \qquad \text{(per (8.13) con } Y = V \cup W) \\ &= r((U \cap V) \cup (U \cap W)) \\ &= (U \curlywedge V) \curlyvee (U \curlywedge W). \end{aligned}$$

Posto $U^* = \mathrm{Int}(\mathrm{Cl}(X \setminus U))$ si ha che $U \curlywedge U^* = \emptyset$ e che $U \cup U^*$ è denso in X, quindi $U \curlyvee U^* = X$. Ne segue che $\mathbf{RO}(X)$ è un'algebra di Boole,

detta l'**algebra degli aperti regolari** di X. Se $\mathcal{A}$ è una famiglia di aperti regolari, $\bigvee \mathcal{A} = r(\bigcup \mathcal{A})$; quindi $\mathbf{RO}(X)$ è un'algebra completa.

$\mathbf{CLOP}(X)$ è una sub-algebra di $\mathbf{RO}(X)$ e di $\mathscr{P}(X)$, ma, in generale, $\mathbf{RO}(X)$ non è una sub-algebra di $\mathscr{P}(X)$, dato che l'operazione di $\curlyvee$ può non coincidere con l'unione.

8.I.7. *L'algebra degli intervalli.* Sia $(L, \leq)$ linearmente ordinato e sia $\mathcal{I}$ l'insieme di tutti gli intervalli della forma $(a; b]$ e delle semirette della forma

$$\{x \in L \mid x \leq b\} \quad \text{e} \quad \{x \in L \mid a < x\}.$$

B, l'insieme delle unioni finite di elementi di $\mathcal{I}$, è una sub-algebra di $\mathscr{P}(L)$ e si dice l'**algebra degli intervalli** di $(L, \leq)$.

8.J. Teorema di rappresentazione per le algebre atomiche.

Proposizione 8.44. *Se B è un'algebra di Boole e $a \in B$, le seguenti condizioni sono equivalenti:*

(a) *a è un atomo;*

(b) *$a \neq \mathbf{0}$ e per ogni $b, c \in B$, $a \leq b \curlyvee c$ se e solo se $a \leq b$ oppure $a \leq c$;*

(c) *per ogni $b \in B$, $a \leq b$ oppure $a \leq b^*$, ma non entrambi;*

(d) *l'ideale generato da a^* è primo.*

Dimostrazione. (a) $\Rightarrow$ (b). Se $a \leq b$ oppure $a \leq c$ allora, chiaramente, $a \leq b \curlyvee c$. Viceversa, se $a \not\leq b$ e $a \not\leq c$, allora $a \curlywedge b^* \neq \mathbf{0}$ e $a \curlywedge c^* \neq \mathbf{0}$ per la parte (i) dell'Esercizio 8.30. Poiché a è un atomo, $a \curlywedge b^* = a$ e $a \curlywedge c^* = a$, cioè $a \leq b^*$ e $a \leq c^*$, da cui $a \leq b^* \curlywedge c^* = (b \curlyvee c)^*$. Se $a \leq b \curlyvee c$ allora $a \leq (b \curlyvee c)^* \curlywedge (b \curlyvee c) = \mathbf{0}$: una contraddizione. Quindi $a \not\leq b \curlyvee c$.

(b) $\Rightarrow$ (c). Fissato $b \in B$, si ha che $a \leq \mathbf{1} = b \curlyvee b^*$ e quindi $a \leq b$ oppure $a \leq b^*$. Tuttavia, non è possibile che $a \leq b$ e $a \leq b^*$ valgano entrambe poiché ciò implicherebbe $a \leq \mathbf{0} = b \curlywedge b^*$.

(c) $\Rightarrow$ (a). Osserviamo che (c) implica banalmente che $a \neq \mathbf{0}$. Se esistesse $\mathbf{0} < b < a$, allora $a \not\leq b$ implica che $a \leq b^*$, da cui $\mathbf{0} = a \curlywedge b^{**} = a \curlywedge b = b$, contraddizione.

(b) $\Leftrightarrow$ (d) segue dal principio di dualità. □

Teorema 8.45. (a) *Per ogni algebra di Boole B tale che $\mathrm{At}(B) \neq \emptyset$, la funzione $f \colon B \to \mathscr{P}(\mathrm{At}(B))$*

$$f(b) = \{a \in \mathrm{At}(B) \mid a \leq b\}$$

è un omomorfismo.

(b) *B è atomica se e solo se f è iniettivo.*

(c) *Se B è completa, o anche solo: se $\bigvee X$ esiste per ogni $X \subseteq \mathrm{At}(B)$, allora f è suriettivo.*

Dimostrazione. (a) Sia $a \in \mathrm{At}(B)$. Allora $a \leq b \curlywedge c$ se e solo se $a \leq b$ e $a \leq c$ e per la Proposizione 8.44, $a \leq b \curlyvee c$ se e solo se $a \leq b$ oppure $a \leq c$. Quindi $f(b \curlywedge c) = f(b) \cap f(c)$ e $f(b \curlyvee c) = f(b) \cup f(c)$, cioè f è un omomorfismo.

(b) È immediato verificare che B è atomica se e solo se $\ker(f) = \{\mathbf{0}\}$.

(c) Sia $X \subseteq \mathrm{At}(B)$: vogliamo dimostrare che $X = f(b)$ per qualche b. Sia $b = \bigvee X$. Chiaramente $X \subseteq f(b)$ e se per assurdo esistesse $a \in f(b) \setminus X$, allora, trattandosi di atomi, $\forall x \in X\, (a \curlywedge x = \mathbf{0})$, quindi per il Lemma 8.31

$$a = a \curlywedge b = a \curlywedge \bigvee X = \bigvee \{a \curlywedge x \mid x \in X\} = \mathbf{0},$$

contraddizione. Quindi $f(b) = X$. □

Corollario 8.46. *Ogni algebra di Boole atomica è isomorfa ad un'algebra di insiemi. Ogni algebra di Boole atomica e completa (o anche solo: tale che $\bigvee X$ esiste per ogni $X \subseteq \mathrm{At}(B)$) è isomorfa all'algebra dell'insieme delle parti di un insieme.*

Il Corollario 8.46 si generalizza ai reticoli distributivi finiti (Esercizio 8.76). Nel Capitolo V dimostreremo che ogni algebra di Boole è isomorfa ad un'algebra di insiemi e nel Capitolo VI questo risultato verrà esteso ai reticoli distributivi.

8.K. Altre assiomatizzazioni*. Abbiamo visto come la nozione di algebra di Boole possa essere formalizzata in più modi: come reticolo complementato distributivo, come anello booleano, e come struttura $(B, \curlywedge, \curlyvee, {}^*, \mathbf{0}, \mathbf{1})$ che soddisfa Σ_{BOOLE}. Le costanti $\mathbf{1}$ e $\mathbf{0}$ sono definibili a partire da $\curlywedge$, $\curlyvee$ e *, e per le leggi di De Morgan le operazioni $\curlywedge$ e $\curlyvee$ sono definibili l'una a partire dall'altra mediante l'operazione di complemento. Quindi per assiomatizzare le algebre di Boole è sufficiente utilizzare l'operazione di complemento * ed una sola tra $\curlywedge$ e $\curlyvee$. Per trovare un sistema di assiomi che utilizzi solo, per esempio, $\curlyvee$ e * potremmo riformulare gli enunciati in Σ_{BOOLE} eliminando $\curlywedge$, $\mathbf{0}$ e $\mathbf{1}$, ma è anche possibile trovare assiomatizzazioni più semplici. Per esempio le algebre di Boole sono esattamente le strutture $(B, \curlyvee, {}^*)$ che soddisfano le proprietà associativa e commutativa per $\curlyvee$ e

$$\forall x, y \big[(x^* \curlyvee y^*)^* \curlyvee (x^* \curlyvee y)^* = x\big]. \tag{8.14}$$

(Un esempio di assiomatizzazione di algebre di Boole mediante $\curlywedge$, * e $\mathbf{0}$ è dato dall'Esercizio 8.72.)

In analogia con quanto visto nella Sezione 5.A.1 possiamo chiederci se le algebre di Boole possano essere assiomatizzate mediante un'unica formula

della forma $t = s$, dove t e s sono termini di un linguaggio del prim'ordine quale L_{BOOLE} o un suo sottolinguaggio. La risposta è affermativa — per esempio

$$(((x \curlyvee y)^* \curlyvee z)^* \curlyvee (x \curlyvee (z^* \curlyvee (z \curlyvee u)^*)^*)^*)^* = z$$

è un assioma siffatto. Se vogliamo risparmiare ulteriormente sul numero di simboli del linguaggio, possiamo rimpiazzare $\curlywedge$, $\curlyvee$ e * con una delle seguenti operazioni binarie $\mid$ o $\uparrow$

$$x \mid y = (x \curlywedge y)^*$$
$$x \uparrow y = (x \curlyvee y)^*.$$

Poiché $x \mid x = x \uparrow x = x^*$, le operazioni $\curlywedge$, $\curlyvee$ e * sono definibili nelle strutture $(B, \mid)$ e $(B, \uparrow)$ e quindi è possibile assiomatizzare le algebre di Boole mediante un linguaggio contenente un unico simbolo di operazione binaria. Infatti è possibile trovare un'assiomatizzazione mediante un'unica identità di termini costruiti a partire dalle variabili e da $\mid$:

$$(x \mid ((y \mid x) \mid x)) \mid (y \mid (z \mid x)) = y.$$

Esercizi

Esercizio 8.47. Siano $\mathcal{P} = (P, \preceq)$ e $\mathcal{Q} = (Q, \trianglelefteq)$ degli ordini e sia $f\colon \mathcal{P} \to \mathcal{Q}$ un isomorfismo. Dimostrare che:

(i) la mappa $\mathscr{P}(P) \to \mathscr{P}(Q)$, $X \mapsto f[X]$ manda segmenti iniziali/finali in segmenti iniziali/finali e

$$(\text{Down}(\mathcal{P}), \subseteq) \to (\text{Down}(\mathcal{Q}), \subseteq) \quad \text{e} \quad (\text{Up}(\mathcal{P}), \subseteq) \to (\text{Up}(\mathcal{Q}), \subseteq),$$

sono degli isomorfismi.

(ii) Se $a \in P$, allora

$$f \restriction \operatorname{pred} a\colon (\operatorname{pred} a, \preceq) \to (\operatorname{pred} f(a), \trianglelefteq)$$

è un isomorfismo.

Esercizio 8.48. (i) Dimostrare che l'insieme degli elementi massimali e l'insieme degli elementi minimali sono definibili nel linguaggio L_{ORDINI}.

(ii) Dare un esempio di ordine in cui ci sono più elementi massimali.

(iii) Dare un esempio di ordine in cui c'è un unico elemento massimale, ma non è il massimo.

Esercizio 8.49. Sia $(L, \leq)$ un ordine lineare e sia $x \in L$. Dimostrare che:

(i) la topologia dell'ordine su L è di Hausdorff;

(ii) x è un punto isolato nella topologia dell'ordine se e solo se
- x ha un predecessore immediato e un successore immediato, oppure
- $x = \min L$ ha un successore immediato, oppure
- $x = \max L$ ha un predecessore immediato, oppure
- $L = \{x\}$;

(iii) $\{1 - 2^{-n} \mid n \in \mathbb{N}\} \cup \{1\}$ e $\{1 - 2^{-n} \mid n \in \mathbb{N}\} \cup \{1, 2\}$ sono insiemi linearmente ordinati omeomorfi, ma non isomorfi.

Esercizio 8.50. Dimostrare il Teorema 8.11.

Esercizio 8.51. Un'**algebra semi-reticolare** è un semigruppo commutativo $(S, \cdot)$ che soddisfa la proprietà di idempotenza, cioè $\forall x\,(x \cdot x = x)$.

(i) Dimostrare che se $(M, \leq)$ è un semi-reticolo superiore, allora $(M, \curlyvee)$ è un'algebra semi-reticolare. Analogamente, se $(M, \leq)$ è un semi-reticolo inferiore, allora $(M, \curlywedge)$ è un'algebra semi-reticolare.

(ii) In un'algebra semi-reticolare $(S, \cdot)$ definiamo le relazioni $\leq_{\curlyvee}$ e $\leq_{\curlywedge}$ su M ponendo

$$a \leq_{\curlyvee} b \Leftrightarrow a \cdot b = b$$
$$a \leq_{\curlywedge} b \Leftrightarrow a \cdot b = a.$$

Dimostrare che $(M, \leq_{\curlyvee})$ è un semi-reticolo superiore e $(M, \leq_{\curlywedge})$ è un semi-reticolo inferiore, e che $(M, \leq_{\curlyvee})$ e $(M, \leq_{\curlywedge})$ sono duali. Inoltre

$$\sup_{\leq_{\curlyvee}}(a, b) = a \cdot b = \inf_{\leq_{\curlywedge}}(a, b).$$

Esercizio 8.52. Sia $f\colon M \to N$ dove M e N sono reticoli.

(i) Sono equivalenti
  (a) f è un morfismo di ordini, cioè f è crescente (pagina 149),
  (b) $\forall a, b \in M\,(f(a \curlyvee b) \geq f(a) \curlyvee f(b))$
  (c) $\forall a, b \in M\,(f(a \curlywedge b) \leq f(a) \curlywedge f(b))$

  Quindi un morfismo di algebre reticolari è una funzione crescente.

(ii) f è un isomorfismo di algebre reticolari se e solo se è un isomorfismo di ordini.

(iii) Dare un esempio di reticoli M, N e di funzione crescente $f\colon M \to N$ che non è un morfismo di reticoli.

Esercizio 8.53. Sia $(P, \leq)$ un ordine in cui ogni $X \subseteq P$ ha un estremo superiore o, equivalentemente per l'Esercizio 8.9, ogni $X \subseteq P$ ha un estremo inferiore. Allora $(P, \leq)$ è un reticolo completo.

Esercizio 8.54. Dimostrare il Teorema 8.12: se M è un reticolo completo e $f\colon M \to M$ è un morfismo di reticoli, allora l'insieme dei punti fissi di f è un sottoreticolo di M ed è un reticolo completo.[4]

Esercizio 8.55. Dimostrare che se V è uno spazio vettoriale di dimensione n su un campo $\Bbbk$, l'insieme

$$M = \{W \subseteq V \mid W \text{ sottospazio vettoriale di } V\},$$

ordinato per inclusione è un reticolo modulare, complementato, ma non distributivo se $n > 1$.

Esercizio 8.56. Dimostrare che l'insieme $\mathscr{C}[0;1]$ delle funzioni continue su $[0;1]$ a valori reali è un reticolo distributivo con l'ordinamento

$$f \preccurlyeq g \Leftrightarrow \forall x \in [0;1]\,(f(x) \leq g(x))\,.$$

Il suo sottoinsieme $\mathrm{Co}[0;1]$ delle funzioni convesse è un semi-reticolo superiore, ma non inferiore.

Esercizio 8.57. Sia T un triangolo del piano e indichiamo con x, y e z i suoi lati. Verificare che il reticolo di insiemi generato dagli insiemi x, y, z è isomorfo a $\mathrm{Free}_{\mathbf{D}}(3)$.

Esercizio 8.58. Nel reticolo dei sottospazi vettoriali di $\mathbb{R}^3$ consideriamo le rette a, b, c e d generate dai vettori $(1,0,1)$, $(0,1,1)$, $(0,0,1)$ e $(1,1,1)$. Dimostrare che il sotto-reticolo generato da a, b, c, d è infinito. Concludere che $\mathrm{Free}_{\mathbf{M}}(4)$ è infinito.

Il prossimo esercizio mostra che un reticolo non modulare contiene una copia isomorfa del reticolo $\mathcal{N}_5$ di pagina 156.

Esercizio 8.59. Supponiamo $a, b, c \in M$ testimoniano che il reticolo M non è modulare, cioè $a \leq b$ e $a_1 \stackrel{\text{def}}{=} a \curlyvee (b \curlywedge c) < b_1 \stackrel{\text{def}}{=} b \curlywedge (a \curlyvee c)$. Dimostrare che:

(i) $c \curlywedge b_1 = c \curlywedge b$ e $c \curlyvee a_1 = c \curlyvee a$,

[4] Ma non è necessariamente un sottoreticolo completo di M.

(ii) $c \curlywedge b \leq a_1 \leq b_1$ e quindi $c \curlywedge b_1 = c \curlywedge a_1$.

(iii) $c \curlyvee a_1 \geq b_1$ da cui $c \curlyvee a_1 = c \curlyvee b_1$.

(iv) Concludere che il reticolo formato da $a_1, b_1, c, c \curlywedge b_1, c \curlyvee a_1$ è isomorfo a $\mathcal{N}_5$.

Esercizio 8.60. Sia $\mathrm{Prt}(X)$ il reticolo delle partizioni su un insieme non vuoto X (Esempio 8.25(f)). Verificare che

(i) se X ha al più due elementi, allora $\mathrm{Prt}(X)$ è distributivo;

(ii) se X ha tre elementi, allora $\mathrm{Prt}(X)$ è isomorfo a $\mathcal{M}_3$;

(iii) se X ha almeno quattro elementi, allora $\mathrm{Prt}(X)$ contiene una copia di $\mathcal{N}_5$.

Esercizio 8.61. Dimostrare che in ogni reticolo distributivo vale

$$(x \curlywedge y) \curlyvee (y \curlywedge z) \curlyvee (x \curlywedge z) = (x \curlyvee y) \curlywedge (y \curlyvee z) \curlywedge (x \curlyvee z).$$

Esercizio 8.62. Dimostrare il Lemma 8.23.

Esercizio 8.63. Verificare che le algebre di Boole sono finitamente assiomatizzabili nel linguaggio L_{ORDINI}.

Esercizio 8.64. Sia $\preccurlyeq$ la relazione di divisibilità [5] sui naturali, cioè $m \preccurlyeq n \Leftrightarrow \exists k\,(km = n)$. Sia

$$\mathrm{Div}(n) = \{m \in \mathbb{N} \mid m \preccurlyeq n\}$$

l'insieme dei divisori di n.

Dimostrare che:

(i) $\mathrm{Div}(0) = \mathbb{N}$ e $(\mathrm{Div}(n), \preccurlyeq)$ è un reticolo distributivo con minimo 1 e massimo n.

(ii) $a \preccurlyeq b \Leftrightarrow \mathrm{Div}(a) \subseteq \mathrm{Div}(b)$, nel qual caso $\mathrm{Div}(a)$ è un sotto-reticolo di $\mathrm{Div}(b)$.

(iii) Se $a = p_1^{k_1} \cdots p_n^{k_n}$ e $b = q_1^{h_1} \cdots q_m^{h_m}$ con $p_1, \ldots, p_n$ e $q_1, \ldots, q_m$ primi distinti, $1 \leq k_1 \leq \cdots \leq k_n$ e $1 \leq h_1 \leq \cdots \leq h_m$, allora $\mathrm{Div}(a) \cong \mathrm{Div}(b)$ se e solo se $n = m$ e $k_i = h_i$.

(iv) $\mathrm{Div}(n) \cong \mathrm{Sgr}(\mathbb{Z}/n\mathbb{Z})^{\Delta}$, dove $\mathrm{Sgr}(\mathbb{Z}/n\mathbb{Z})$ è il reticolo dei sottogruppi di $\mathbb{Z}/n\mathbb{Z}$.

(v) Se a non è divisibile per un quadrato allora $\mathrm{Div}(a)$ è un'algebra di Boole.

Esercizio 8.65. Dimostrare che:

(i) se M è un reticolo (distributivo) e $a \in M$, allora $\downarrow a$ è un reticolo (distributivo), e analogamente per $\uparrow a$;

(ii) se B è un'algebra di Boole e $a \neq \mathbf{0}$, allora $\downarrow a$ è un'algebra di Boole ed è isomorfa a $\uparrow a^*$. In particolare se $a \in B \setminus \{\mathbf{0}, \mathbf{1}\}$ allora B è isomorfa al prodotto $(\downarrow a) \times (\downarrow a^*)$.

(iii) Se $f\colon B \to C$ è un morfismo di algebre di Boole, allora $f \restriction \downarrow b\colon \downarrow b \to \downarrow f(b)$ è un morfismo di algebre di Boole.

(iv) Se $f\colon B \to C$ è un morfismo di algebre di Boole tale che $\ker(f)$ è principale, cioè $\ker(f) = \downarrow b$ per qualche $b \in B$, allora b^* è il massimo elemento $a \in B$ tale che $f \restriction \downarrow a$ è iniettivo.

Esercizio 8.66. Dimostrare che $\mathscr{P}(A)$ e $\mathscr{P}(B)$ sono algebre di Boole isomorfe se e solo se A e B sono equipotenti.

Esercizio 8.67. Siano $B \subseteq \mathscr{P}(X)$ e $C \subseteq \mathscr{P}(Y)$ algebre di insiemi e supponiamo che $X \cap Y = \emptyset$. Dimostrare che $B \times C$ è isomorfa a $\{b \cup c \mid b \in B \wedge c \in C\} \subseteq \mathscr{P}(X \cup Y)$.

Esercizio 8.68. Sia $(B, +, \cdot, 0, 1)$ un anello booleano, cioè un anello con unità in cui $x^2 = x$ per ogni x. Definiamo

$$x \curlywedge y = x \cdot y \qquad x \curlyvee y = x + y + x \cdot y \qquad x^* = 1 + x$$
$$\mathbf{0} = 0 \qquad \mathbf{1} = 1.$$

Dimostrare che

[5] Usiamo il simbolo $\preccurlyeq$ invece di $|$ già utilizzato nella Sezione 2.C per sottolineare che stiamo lavorando con on ordine parziale.

(i) $x + x = 0$, cioè ogni elemento del gruppo additivo $(B, +)$ ha ordine 2;

(ii) B è un anello commutativo;

(iii) B con le operazioni $\curlywedge$, $\curlyvee$ e * è un'algebra di Boole.

Verificare che la corrispondenza

$$(B, +, \cdot, \mathbf{0}, \mathbf{1}) \mapsto (B, \curlyvee, \curlywedge, ^*, \mathbf{0}, \mathbf{1})$$

tra anelli booleani e algebre di Boole è l'inversa della corrispondenza (8.12).

Esercizio 8.69. Sia $(R, +, \cdot, 0, 1)$ un anello unitario (non necessariamente commutativo) e sia

$$\bar{R} = \{x \in R \mid x^2 = x \text{ e } \forall y \in R\,(x \cdot y = y \cdot x)\}.$$

(Un elemento di un anello R per cui vale $x^2 = x$ si dice idempotente.) Definiamo

$$x \oplus y = x + y - 2x \cdot y.$$

Dimostrare che $(\bar{R}, \oplus, \cdot, 0, 1)$ è un anello booleano.

Esercizio 8.70. Completare la dimostrazione del Teorema 8.24.

Esercizio 8.71. Dimostrare la Proposizione 8.40.

Esercizio 8.72. Sia $(B, \curlywedge, ^*, \mathbf{0})$ una struttura tale che $\curlywedge$ soddisfa le proprietà commutativa (8.2b), associativa (8.1b) e di idempotenza (8.4b), e tale che $\mathbf{0} \neq \mathbf{0}^*$ e

$$x \curlywedge y^* = \mathbf{0} \Leftrightarrow x \curlywedge y = x. \tag{8.15}$$

Definiamo $\mathbf{1}$, $\leq$ e $\curlyvee$ nel modo ovvio, cioè $\mathbf{1} = \mathbf{0}^*$ e

$$x \leq y \Leftrightarrow x \curlywedge y = x \quad \text{e} \quad x \curlyvee y = (x^* \curlywedge y^*)^*.$$

Osserviamo che la commutatività di $\curlywedge$ implica quella di $\curlyvee$.

Dimostrare che:

(i) $x \curlywedge x^* = \mathbf{0}$;

(ii) $\leq$ è una relazione di ordine su B, $x \curlywedge y \leq x$ e $x \curlywedge y \leq y$ per ogni x, y. Inoltre $\mathbf{0}$ è il minimo e $x \leq y \Leftrightarrow x \curlywedge y^* = \mathbf{0}$ per ogni x, y;

(iii) $x^{**} = x$, quindi la funzione $x \mapsto x^*$ è una biezione di B. Inoltre $\curlyvee$ è idempotente, cioè $x \curlyvee x = x$, e $x \curlyvee x^* = \mathbf{1}$;

(iv) $x \curlywedge y = (x^* \curlyvee y^*)^*$ e $\curlyvee$ è associativa, $x \curlyvee (y \curlyvee z) = (x \curlyvee y) \curlyvee z$;

(v) $x \leq y \Leftrightarrow y^* \leq x^* \Leftrightarrow x \curlyvee y = y$;

(vi) se $x \leq y$ allora $x \curlywedge z \leq y \curlywedge z$ e $x \curlyvee z \leq y \curlyvee z$. In particolare: se $x \leq y, z$ allora $x \leq y \curlywedge z$ e se $x, y \leq z$ allora $x \curlyvee y \leq z$;

(vii) $x \curlywedge (x^* \curlyvee y) = x \curlywedge y$ e $x \curlyvee (x^* \curlywedge y) = x \curlyvee y$;

(viii) valgono le leggi di assorbimento (8.3) $(x \curlyvee y) \curlywedge y = y$ e $(x \curlywedge y) \curlyvee y = y$;

(ix) valgono le leggi distributive (8.7) $(x \curlyvee y) \curlywedge z = (x \curlywedge z) \curlyvee (y \curlywedge z)$ e $(x \curlywedge y) \curlyvee z = (x \curlyvee z) \curlywedge (y \curlyvee z)$.

Concludere che B è un'algebra di Boole.

Esercizio 8.73. Sia Σ_a l'insieme degli enunciati ottenuti rimuovendo (8.10b) da Σ_{BOOLE} e sia Σ_b l'insieme degli enunciati ottenuti rimuovendo (8.10a) da Σ_{BOOLE}. Dimostrare che:

(i) gli assiomi (8.9a) e (8.9b) sono logicamente equivalenti modulo gli altri assiomi di Σ_{BOOLE}, vale a dire

$$B \vDash \Sigma_a \;\Leftrightarrow\; B \vDash \Sigma_b \;\Leftrightarrow\; B \vDash \Sigma_{\text{BOOLE}}$$

per ogni L_{BOOLE}-struttura B.

(ii) Σ_a e Σ_b sono sistemi di assiomi indipendenti.

Esercizio 8.74. Se M è un reticolo definiamo

$$\mathcal{J}(M) = \{x \in M \setminus \{\mathbf{0}\} \mid \forall y, z\, (x = y \curlyvee z \Rightarrow x = y \vee x = z)\}.$$

Dimostrare che

(i) se M è finito e $a \not\leq b$ allora $\exists x \in \mathcal{J}(M)\, (x \leq a \wedge x \not\leq b)$;

(ii) se M è finito, allora $a = \bigvee \{x \in \mathcal{J}(M) \mid x \leq a\}$, per ogni $a \in M$;

(iii) se M è distributivo $x \in \mathcal{J}(M)$ se e solo se per ogni scelta di $a_1, \ldots, a_n \in M$ se $x \leq a_1 \curlyvee \ldots \curlyvee a_n$ allora $x \leq a_i$ per qualche $1 \leq i \leq n$.

Esercizio 8.75. Sia $(P, \leq)$ un ordine parziale finito, sia $\mathrm{Down}(P)$ il reticolo dei suoi segmenti iniziali (Esempio 8.17(a)). Dimostrare che $\downarrow x \in \mathcal{J}(\mathrm{Down}(P))$ e che la funzione

$$P \to \mathcal{J}(\mathrm{Down}(P)), \quad x \mapsto \downarrow x,$$

è un isomorfismo di ordini.

Esercizio 8.76. Dimostrare che se M è un reticolo distributivo finito, allora la funzione

$$M \to \mathrm{Down}(\mathcal{J}(M)), \quad x \mapsto \{y \in \mathcal{J}(M) \mid y \leq x\}$$

è un isomorfismo. In altre parole: i reticoli finiti distributivi sono, a meno di isomorfismo, reticoli di insiemi.

Esercizio 8.77. Dimostrare che se A è una sub-algebra finita di $\mathscr{P}(X)$ e A è atomica, allora $\mathrm{At}(A)$ è una partizione di X.

Dimostrare con un controesempio che il risultato non vale se A è infinita.

Esercizio 8.78. Dimostrare che se B e C sono algebre di Boole, con B atomica e C priva di atomi, allora $B \times C$ è un'algebra di Boole che ha atomi, ma non è atomica.

Esercizio 8.79. Dimostrare con un esempio che l'unione di aperti regolari non è necessariamente regolare.

Esercizio 8.80. Dimostrare che se $(L, \leq)$ è un ordine lineare e denso, allora l'algebra degli intervalli è priva di atomi.

Esercizio 8.81. Dimostrare che due insiemi A e B sono in biezione se e solo se le algebre di Boole $\mathscr{P}(A)$ e $\mathscr{P}(B)$ sono isomorfe. (Nota bene: è coerente con gli assiomi della teoria degli insiemi che esistano insiemi infiniti A e B che non siano in biezione e tuttavia $\mathscr{P}(A)$ e $\mathscr{P}(B)$ sono in biezione.)

Note e osservazioni

[**DP02**] è un'ottima introduzione ai reticoli, per trattazione completa sui reticoli si veda [**Grä11**]. Il Teorema di punto fisso 8.12 è generalmente attribuito a Knaster e Tarski. Il Teorema 8.18 è tratto da [**Tar55**], mentre in [**Dav55**] si dimostra il converso, cioè se ogni funzione crescente in un reticolo M ammette punti fissi, allora il reticolo M è completo. I reticoli sono stati introdotti alla fine dell'Ottocento da Dedekind nello studio dell'ordinamento per inclusione degli ideali di un anello; la nozione di reticolo modulare emerge da queste ricerche (Esempio 8.25(d)). La descrizione dettagliata di $\mathrm{Free}_{\mathbf{M}}(3)$ è anche dovuta a Dedekind nel 1900. La cardinalità D_n di $\mathrm{Free}_{\mathbf{D}}(n)$ si dice numero di Dedekind di ordine n e interviene in molte questioni combinatoriali. I valori di D_n sono stati determinati esplicitamente solo fino a $n = 8$, e sono:

$$1,\ 4,\ 18,\ 166,\ 7579,\ 7828352,\ 2414682040996,\ 56130437228687557907786.$$

La parte (a) del Teorema 8.24 è dovuta a Dedekind, mentre la parte (b) è dovuta a Birkhoff. Come i gruppi e le algebre di Boole, così anche i reticoli possono essere assiomatizzati mediante un'unica identità — per esempio [**MPV03**]

$$(((y \curlyvee x) \curlywedge x) \curlyvee (((z \curlywedge (x \curlywedge x)) \curlyvee (u \curlywedge x)) \curlywedge v)) \curlywedge (w \curlyvee ((s \curlyvee x) \curlywedge (x \curlyvee t))) = x.$$

Huntington nel 1904 si chiese se il Lemma 8.26 ammettesse un converso: è vero che ogni reticolo univocamente complementato è distributivo? Benché la congettura valga per specifiche classi di reticoli (modulari, completi e atomici, ecc.), nel 1945 Dilworth refutò la congettura dimostrando che ogni reticolo è immergibile in un reticolo univocamente complementato.

Le algebre di Boole sono state introdotte nel 1847 da Boole, ma la loro trattazione assiomatica come strutture algebriche che soddisfano certi postulati è stata introdotta nel 1904 da Huntington. Sempre Huntington nel 1933 dimostrò che la proprietà associativa e commutativa di $\curlyvee$ assieme all'enunciato (8.14) costituiscono un sistema di assiomi per le algebre di Boole. Poco dopo Robbins si chiese se la (8.14) potesse essere rimpiazzata da

$$\forall x, y \Big[((x \curlyvee y)^* \curlyvee (x^* \curlyvee y^*)^*)^* = x\Big].$$

Il problema rimase aperto per sessant'anni finché nel 1997 McCune dimostrò questa congettura utilizzando il programma Otter per il calcolo simbolico. L'Esercizio 8.72 è tratto da [**Byr46**] — si veda anche [**Men70**]. Le operazioni binarie $|$ e $\uparrow$ descritte nella Sezione 8.K sono le controparti algebriche dei connettivi di Sheffer e Peirce dell'Esercizio 3.41. Per una trattazione enciclopedica sulle algebre di Boole si vedano i tre volumi dell'Handbook of Boolean Algebras [**Kop89, MB89a, MB89b**]. In particolare, l'articolo di S. Koppelberg nel primo volume è un'ottima introduzione all'argomento.

I risultati presentati nella Sezione 8.K sono tratti da [**MVF$^+$02**], articolo a cui rimandiamo il lettore per le dimostrazioni, per l'inquadramento storico dei problemi, nonché per le referenze bibliografiche. Il risultato dell'Esercizio 8.76 è noto come teorema di rappresentazione dei reticoli distributivi finiti ed è dovuto a Birkhoff.

9. Calcolabilità

Certe costruzioni in matematica possono essere eseguite in modo meccanico seguendo un protocollo prestabilito, mentre certe altre richiedono idee nuove e creatività . Per esempio: *dimostrare* un nuovo risultato (non banale) richiedere ingegno, mentre *controllare* che una certa argomentazione è proprio una dimostrazione del risultato in questione è soltanto una questione solo di pazienza ed attenzione.[6] Una procedura effettiva è un protocollo che può essere eseguito in modo meccanico da un utente: accetteremo come *input* degli oggetti finiti (numeri interi, grafi finiti, ...) e seguendo questo protocollo, anch'esso finito, produrremo in un numero finito di passi un oggetto finito come *output*. In altre parole: una procedura è effettiva se può essere implementata al calcolatore. Per esempio, dato un linguaggio del prim'ordine con un numero finito di simboli non logici, c'è una procedura effettiva per controllare se una stringa finita di simboli è un termine of una formula. Analogamente, c'è una procedura effettiva per determinare se un $L_{\text{ANELLI-1}}$-enunciato è un assioma della teoria ACF_0 dei campi algebricamente chiusi di caratteristica zero.

Visto che gli oggetti finiti possono essere codificati nell'aritmetica, cominciamo con lo studiare le procedure effettive o *calcolabili* sui numeri naturali. Negli anni venti del secolo scorso sono state introdotte numerose definizioni matematicamente precise di "funzione calcolabile", ed è risultato che tutte

[6] Questo nell'assunzione piuttosto ottimistica che la dimostrazione sia stata scritta con chiarezza e che tutti i passaggi siano stati esplicitati.

queste definizioni individuano la stessa classe di funzioni. In questa sezione *funzione* significa *funzione k-aria sui numeri naturali*, cioè una mappa della forma $f\colon \mathbb{N}^k \to \mathbb{N}$, con la convenzione che una funzione 0-aria è semplicemente un numero naturale.

Molte delle usuali funzioni aritmetiche sono calcolabili e di solito è sufficiente esaminare la definizione di una funzione per convincersi se essa è calcolabile. Questo approccio ingenuo è prono ad errori (si veda le Osservazioni 9.1 qui sotto) e mostra i suoi limiti quando dobbiamo dimostrare che una certa funzione *non è* calcolabile. In questo caso la richiesta di una definizione rigorosa diventa ineludibile. Negli anni venti del secolo scorso è stata introdotta la definizione di **funzione ricorsiva** come controparte rigorosa alla nozione intuitiva di funzione calcolabile. Nelle prossime sezioni vedremo due sottoclassi importanti delle funzioni ricorsive: le **funzioni elementari ricorsive** e le **funzioni primitive ricorsive**.

Osservazioni 9.1. (a) Alcune funzioni sono calcolabili, anche se a prima vista sembrerebbe di no. Per esempio, le funzioni costanti sono calcolabili, secondo ogni possibile accezione del termine *calcolabile*, quindi è calcolabile la funzione unaria

$$f(n) = \begin{cases} 1 & \text{se vale P,} \\ 0 & \text{altrimenti,} \end{cases}$$

dove P è un qualche problema aperto della matematica, per esempio uno delle congetture in teoria dei numeri viste nell'Esercizio 2.8 del Capitolo I. Sappiamo cioè che l'algoritmo che calcola f è uno tra due algoritmi, ma non siamo a tutt'oggi in grado di determinare quale dei due sia quello giusto. La situazione è, per certi versi, simile a quanto visto nell'Esempio 2.5 del Capitolo I. Anche la funzione di Ramsey $R\colon \mathbb{N} \to \mathbb{N}$ introdotta a pagina 102, che ad n assegna il più piccolo m per cui ogni 2-colorazione del grafo completo K_m ha un sottografo monocromatico isomorfo a K_n (Teorema 5.19) è calcolabile, ma il valore esatto di $R(n)$ per $n \geq 5$ non è noto.

(b) Per verificare che $f\colon \mathbb{N}^2 \to \mathbb{N}$ è calcolabile sembrerebbe sufficiente verificare che per ogni k la funzione $f_k\colon \mathbb{N} \to \mathbb{N}$, $n \mapsto f(k,n)$, è calcolabile e poi argomentare così: dati (k,n) fissiamo un algoritmo per f_k ed usiamolo per calcolare $f_k(n)$. Tuttavia il ragionamento non è corretto in quanto è necessario assicurarci che sia calcolabile la procedura che ad ogni k associa l'algoritmo per f_k. Per esempio, se $g\colon \mathbb{N} \to \mathbb{N}$ non è calcolabile e $f(k,n) = g(k)$, allora f_k è costante e quindi calcolabile, ma la funzione f non lo è.

(c) Nella maggior parte dei casi, è routine verificare che un certo insieme è calcolabile, ma ci sono eccezioni. Woods congetturò in [**Woo81**] che per

ogni k e ogni a c'è un $i \leq k$ tale che $a+i$ è relativamente primo con a e con $a+k$, ma poco dopo trovò in controesempio: $k = 16$ e $a = 2184$. (Infatti questo è il minimo controesempio siffatto.) Diremo che k è un **intero di Erdős-Woods** se è un controesempio alla congettura di Woods, cioè se c'è un numero naturale a tale che ognuno dei $a, a+1, \ldots, a+k$ ha un fattore primo in comune con a o $a+k$. L'insieme degli interi di Erdős-Woods è infinito [**Dow89**], ed è calcolabile [**CHR03**], ma la dimostrazione di questi fatti non è banale.

9.A. Funzioni elementari ricorsive. Molte delle funzioni aritmetiche sono calcolabili: per esempio la somma $+$, il prodotto $\cdot$, la distanza tra numeri $|x-y|$, e la (parte intera della) divisione

$$\lfloor x/y \rfloor = \begin{cases} \text{il più grande } k \text{ tale che } y \cdot k \leq x & \text{se } y \neq 0 \\ 0 & \text{altrimenti.} \end{cases}$$

Ci sono poi alcune costruzioni che ci permettono di costruire nuove funzioni calcolabili.

Definizione 9.2. (i) Supponiamo che f sia k-aria e che $g_0, \ldots, g_{k-1}$ siano n-arie. La **composizione** di f con $g_0, \ldots, g_{k-1}$ è la funzione $h\colon \mathbb{N}^n \to \mathbb{N}$

$$h(x_0, \ldots, x_{n-1}) = f(g_0(x_0, \ldots, x_{n-1}), \ldots, g_{k-1}(x_0, \ldots, x_{n-1})).$$

(ii) Se f è $k+1$-aria, la **somma generalizzata su** f e il **prodotto generalizzato su** f sono le funzioni $k+1$-arie

$$\textstyle\sum f(x_0, \ldots, x_{k-1}, x_k) = \sum_{y<x_k} f(x_0, \ldots, x_{k-1}, y),$$
$$\textstyle\prod f(x_0, \ldots, x_{k-1}, x_k) = \prod_{y<x_k} f(x_0, \ldots, x_{k-1}, y),$$

dove quando $x_k = 0$ poniamo

$$\textstyle\sum f(x_0, \ldots, x_{k-1}, 0) = 0$$
$$\textstyle\prod f(x_0, \ldots, x_{k-1}, 0) = 1.$$

La definizione di composizione può apparire troppo restrittiva in quanto spesso capita di dover comporre delle g_i di arietà differente o che l'ordine delle variabili nelle g_i non sia lo stesso. Per esempio consideriamo la funzione 3-aria

$$h(x_0, x_1, x_2) = f(g_0(x_1, x_2), g_1(x_0), g_2(x_1, x_0, x_0)).$$

Per ricondurci alla definizione ufficiale di 'composizione di funzioni' dobbiamo utilizzare le **funzioni di proiezione** I^n_k, con $k < n$

$$I^n_k\colon \mathbb{N}^n \to \mathbb{N}, \quad (x_0, \ldots, x_{n-1}) \mapsto x_k.$$

Allora la funzione h qui sopra è la composizione della funzione f con $\tilde{g}_0$, $\tilde{g}_1$ e $\tilde{g}_2$, dove $\tilde{g}_i$ è ottenuta da g_i mediante proiezioni:

$$\begin{aligned}\tilde{g}_0(\vec{x}) &= g_0(I^3_1(\vec{x}), I^3_2(\vec{x}))\\ \tilde{g}_1(\vec{x}) &= g_1(I^3_0(\vec{x}))\\ \tilde{g}_2(\vec{x}) &= g_2(I^3_1(\vec{x}), I^3_0(\vec{x}), I^3_0(\vec{x})).\end{aligned}$$

Qui sopra abbiamo usato $\vec{x}$ per denotare (x_0, x_1, x_2). Più in generale scriveremo $\vec{x}$ per denotare $(x_0, \dots, x_{n-1})$, quando n risulti chiaro dal contesto. Mediante le funzioni di proiezione possiamo quindi permutare, identificare, e anche introdurre nuove variabili.

Esercizio 9.3. (i) Supponiamo $\mathcal{F}$ sia una famiglia di funzioni contenente le proiezioni e chiusa per composizione. Se $\sigma\colon \{0, \dots, n-1\} \to \{0, \dots, m-1\}$ e $f \in \mathcal{F}$ è n-aria, allora la funzione m-aria

$$(x_0, \dots, x_{m-1}) \mapsto f(x_{\sigma(0)}, \dots, x_{\sigma(n-1)})$$

è in $\mathcal{F}$.

(ii) Se $\mathcal{F}$ è una famiglia di funzioni chiusa per composizione e per somme e prodotti generalizzati e $f, g \in \mathcal{F}$ sono $k+1$-arie, allora

$$\begin{aligned}(x_0, \dots, x_k) &\mapsto \sum_{y<g(x_0,\dots,x_k)} f(x_0, \dots, x_{k-1}, y)\\ (x_0, \dots, x_k) &\mapsto \prod_{y<g(x_0,\dots,x_k)} f(x_0, \dots, x_{k-1}, y)\end{aligned}$$

sono in $\mathcal{F}$.

Definizione 9.4. La famiglia $\mathcal{E}$ delle **funzioni elementari ricorsive** è la più piccola classe di funzioni contenenti la somma, il prodotto, la distanza di due numeri, la (parte intera della) divisione e le proiezioni, cioè:

$$+ \qquad \cdot \qquad |x-y| \qquad \lfloor x/y \rfloor, \qquad I^n_k \quad (k<n)$$

e chiusa per composizione e per somma e prodotto generalizzate.

Lemma 9.5. *Le seguenti funzioni sono in $\mathcal{E}$:*

- *la funzione $c_k\colon \mathbb{N} \to \mathbb{N}$, $n \mapsto k$;*
- *la funzione* $\mathrm{sgn}\colon \mathbb{N} \to \mathbb{N}$ *che vale* 0 *in* 0*, e vale* 1 *altrimenti; la funzione* $\overline{\mathrm{sgn}}(n) = 1 - \mathrm{sgn}(n)$*;*
- *la funzione successore $S(n) = n+1$ e la funzione predecessore $x \mapsto x \dot{-} 1$, dove $0 \dot{-} 1 = 0$;*
- *l'esponenziale e il fattoriale.*

Dimostrazione. Osserviamo che

$$\begin{aligned} c_0(x) &= |x - x| & \overline{\mathrm{sgn}}(x) &= \textstyle\prod_{y<x} c_0(y) \\ \mathrm{sgn} &= \overline{\mathrm{sgn}} \circ \overline{\mathrm{sgn}} & c_1 &= \overline{\mathrm{sgn}} \circ c_0 \\ c_{m+1} &= c_m + c_1 & S(x) &= x + c_1 \\ x^y &= \prod_{z<y} x & x! &= \prod_{z<x} S(z) \\ x \dot{-} 1 &= |x - c_1(x)| \cdot \mathrm{sgn}(x). \end{aligned}$$

□

Osservazione 9.6. Se $F\colon \mathbb{N}^2 \to \mathbb{N}$ è una funzione elementare ricorsiva, allora per ogni n le funzioni

$$F_n\colon \mathbb{N} \to \mathbb{N} \quad m \mapsto F(n, m)$$

sono elementari ricorsive, dato che $F_n(m) = F(c_n(m), m) = F(c_n(m), I^1_0(m))$.

Il viceversa non è vero: se F_n è elementare ricorsiva per ogni n, non è detto che F sia elementare ricorsiva. Se $f\colon \mathbb{N} \to \mathbb{N}$ non è una funzione calcolabile, non lo è neppure la funzione $F(n, m) = f(n)$, anche se ogni $F_n = c_{f(n)}\colon \mathbb{N} \to \mathbb{N}$ è elementare ricorsiva.

Seguendo una pratica comune in logica matematica, spesso scriveremo $A(\vec{x})$ al posto di $\vec{x} \in A$ e diremo che l'insieme $A \subseteq \mathbb{N}^k$ è un predicato k-ario. Per esempio i predicati $x = y$, $x \leq y$, … denotano gli insiemi $\{(x, y) \in \mathbb{N}^2 \mid x = y\}$, $\{(x, y) \in \mathbb{N}^2 \mid x \leq y\}$, …. Diremo che $A \subseteq \mathbb{N}^k$ è un **insieme elementare ricorsivo** o, equivalentemente, è un **predicato elementare ricorsivo** k-ario se la sua funzione caratteristica $\boldsymbol{\chi}_A\colon \mathbb{N}^k \to \{0, 1\}$,

$$\boldsymbol{\chi}_A(\vec{x}) = 1 \Leftrightarrow \vec{x} \in A$$

appartiene ad $\boldsymbol{\mathcal{E}}$. Più in generale: se $\mathcal{F}$ è una famiglia di funzioni, diremo che A è in $\mathcal{F}$ o che è un $\mathcal{F}$-predicato se $\boldsymbol{\chi}_A \in \mathcal{F}$.

Lemma 9.7. *Supponiamo $\mathcal{F} \supseteq \boldsymbol{\mathcal{E}}$ sia una famiglia di funzioni, chiusa per composizione e somma e prodotto generalizzate. Il grafo $\mathrm{Gr}(f)$ di una funzione k-aria $f \in \mathcal{F}$ è un $\mathcal{F}$-predicato $k+1$-ario.*

Dimostrazione. $\boldsymbol{\chi}_{\mathrm{Gr}(f)}(n_1, \ldots, n_k, m) = \overline{\mathrm{sgn}}(|f(n_1, \ldots, n_k) - m|)$. □

Osservazione 9.8. L'implicazione inversa del Lemma 9.7 non vale per le funzioni e predicati elementari ricorsivi, cioè non è vero che se $\boldsymbol{\chi}_{\mathrm{Gr}(f)}$ è elementare ricorsivo, allora f è elementare ricorsiva. Per esempio esistono biezioni elementari ricorsive $f\colon \mathbb{N} \to \mathbb{N}$ (il cui grafo è in $\boldsymbol{\mathcal{E}}$ per il Lemma 9.7) tale che la sua inversa f^{-1} (il cui grafo $\{(y, x) \mid (x, y) \in \mathrm{Gr}(f)\}$ è in $\boldsymbol{\mathcal{E}}$) non è elementare ricorsiva (Proposizione 9.38).

Esempi 9.9. Sia $\mathcal{F} \supseteq \boldsymbol{\mathcal{E}}$ una famiglia di funzioni, chiusa per composizione e per somma e prodotto generalizzati.

(A) Se $A(x_1, \ldots, x_m)$ è un $\mathcal{F}$-predicato m-ario e $f_1, \ldots, f_m \in \mathcal{F}$ sono k-arie, allora

$$A(f_1(x_1, \ldots, x_k), \ldots, f_m(x_1, \ldots, x_k))$$

è un $\mathcal{F}$-predicato k-ario.

Infatti questo predicato è l'insieme

$$\Big\{(x_1, \ldots, x_k) \in \mathbb{N}^k \mid (f_1(x_1, \ldots, x_k), \ldots, f_m(x_1, \ldots, x_k)) \in A\Big\}$$

e la sua funzione caratteristica è $\boldsymbol{\chi}_A(f_1(x_1, \ldots, x_k), \ldots, f_m(x_1, \ldots, x_k))$.

(B) Se $A, B \subseteq \mathbb{N}^n$ sono $\mathcal{F}$-predicati, allora

$$\neg A \stackrel{\text{def}}{=} \mathbb{N}^n \setminus A$$

e $A \cap B$ sono $\mathcal{F}$-predicati, dato che $\boldsymbol{\chi}_{\neg A} = \overline{\text{sgn}} \circ \boldsymbol{\chi}_A$ e $\boldsymbol{\chi}_{A\cap B} = \boldsymbol{\chi}_A \cdot \boldsymbol{\chi}_B$. Quindi anche

$$A \cup B = \neg(\neg A \cap \neg B), \quad A \setminus B = A \cap \neg B \quad \text{e} \quad A \triangle B = (A \setminus B) \cup (B \setminus A)$$

sono $\mathcal{F}$-predicati. I predicati

$$A(x_1, \ldots, x_n) \Rightarrow B(x_1, \ldots, x_n) \text{ e } A(x_1, \ldots, x_n) \Leftrightarrow B(x_1, \ldots, x_n)$$

non sono nient'altro che gli insiemi $\neg A \cup B$ e $(\neg A \cup B) \cap (\neg B \cup A)$ rispettivamente, quindi sono anch'essi $\mathcal{F}$-predicati. Quindi la famiglia dei sottoinsiemi di $\mathbb{N}^k$ la cui funzione caratteristica è in $\mathcal{F}$ è un'algebra di Boole.

(C) Il predicato $x < y$ è in $\mathcal{F}$, visto che la sua funzione caratteristica è $\overline{\text{sgn}}\lfloor S(x)/S(y)\rfloor$. Quindi per (A) e (B) sono $\mathcal{F}$-predicati

- $x \leq y$, dato che è equivalente a $\neg(y < x)$,
- $x = y$, dato che è equivalente a $x \leq y \wedge y \leq x$,
- $x \neq y$.

(D) Se $\{A_1, \ldots, A_k\}$ è una partizione di $\mathbb{N}^n$ e gli A_i sono in $\mathcal{F}$, e se $g_1, \ldots, g_k \in \mathcal{F}$ sono n-arie, allora la funzione $f\colon \mathbb{N}^n \to \mathbb{N}$ definita da

$$f(\vec{x}) = \begin{cases} g_1(\vec{x}) & \text{se } \vec{x} \in A_1, \\ g_2(\vec{x}) & \text{se } \vec{x} \in A_2, \\ \quad\vdots & \\ g_k(\vec{x}) & \text{se } \vec{x} \in A_k, \end{cases}$$

è in $\mathcal{F}$, dato che

$$f(\vec{x}) = g_1(\vec{x}) \cdot \boldsymbol{\chi}_{A_1}(\vec{x}) + \cdots + g_k(\vec{x}) \cdot \boldsymbol{\chi}_{A_k}(\vec{x}).$$

(E) Se $A \subseteq \mathbb{N}^{n+1}$ è in $\mathcal{F}$ allora l'insieme

$$B = \{(\vec{x}, y) \in \mathbb{N}^{n+1} \mid \forall z\, (z < y \Rightarrow A(\vec{x}, z))\}$$

è in $\mathcal{F}$ dato che la sua funzione caratteristica è $\prod_{k<y} \boldsymbol{\chi}_A(\vec{x}, k)$. Quindi anche

$$\begin{aligned} C &= \{(\vec{x}, y) \in \mathbb{N}^{n+1} \mid \exists z\, (z < y \wedge A(\vec{x}, z))\} \\ &= (\mathbb{N}^{n+1} \setminus \{(\vec{x}, y) \in \mathbb{N}^{n+1} \mid \forall z\, (z < y \Rightarrow \neg A(\vec{x}, z))\}) \end{aligned}$$

sono elementari ricorsivi.

$$\forall z < y\, A(\vec{x}, z) \quad \text{e} \quad \exists z < y\, A(\vec{x}, z)$$

denotano, rispettivamente, i predicati B e C. Analogamente anche

$$\forall z \leq y\, A(\vec{x}, z) \quad \text{e} \quad \exists z \leq y\, A(\vec{x}, z)$$

sono in $\mathcal{F}$. Diremo che i predicati $\forall z < y\, A(\vec{x}, z)$, $\exists z < y\, A(\vec{x}, z)$, $\forall z \leq y\, A(\vec{x}, z)$ e $\exists z \leq y\, A(\vec{x}, z)$ sono ottenuti da A per **quantificazione limitata**.

(F) Se $A \subseteq \mathbb{N}^{n+1}$ è in $\mathcal{F}$, allora la funzione $n+1$-aria

$$f(\vec{x}, y) = \begin{cases} \min\{z \leq y \mid A(\vec{x}, z)\} & \text{se questo insieme è non vuoto,} \\ y & \text{altrimenti,} \end{cases}$$

è in $\mathcal{F}$.

Infatti la funzione

$$g(\vec{x}, w) = \overline{\operatorname{sgn}}(\textstyle\sum_{z<S(w)} \boldsymbol{\chi}_A(\vec{x}, z)) = \begin{cases} 0 & \text{se } \exists z \leq w\, A(\vec{x}, z), \\ 1 & \text{altrimenti,} \end{cases}$$

è in $\mathcal{F}$, quindi

$$f(\vec{x}, y) = \sum_{w<y} g(\vec{x}, w)$$

è in $\mathcal{F}$. Diremo che la funzione f di cui sopra è ottenuta per **minimizzazione limitata** e scriveremo

$$f(\vec{x}, y) = \boldsymbol{\mu} z \leq y\, A(\vec{x}, z). \tag{9.1}$$

Naturalmente, se $g(\vec{y})$ è in $\mathcal{F}$, allora anche la funzione

$$h(\vec{x}, \vec{y}) = f(\vec{x}, g(\vec{y})) = \boldsymbol{\mu} z \leq g(\vec{y})\, A(\vec{x}, z)$$

è in $\mathcal{F}$.

(G) Se $g \in \mathcal{F}$ è $n+1$-aria, allora per ogni $k \in \mathbb{N}$ la funzione $n+1$-aria

$$f(\vec{x}, y) = \begin{cases} \min\{z \leq y \mid g(\vec{x}, z) = k\} & \text{se questo insieme è non vuoto,} \\ y & \text{altrimenti,} \end{cases}$$

è in $\mathcal{F}$.

Infatti $f(\vec{x}, y) = \boldsymbol{\mu} z \leq y\, A(\vec{x}, z)$, dove $A \subseteq \mathbb{N}^{n+1}$ è ottenuto dal grafo di g,

$$\left\{(\vec{x}, y, w) \in \mathbb{N}^{n+2} \mid g(\vec{x}, y) = w\right\},$$

sostituendo alla variabile w il valore k, o meglio: la funzione $c_k(I_0^n(\vec{x}))$. Il risultato segue dal Lemma 9.7, e dall'Esempio (F) qui sopra.

Il seguente risultato è converso parziale del Lemma 9.7.

Proposizione 9.10. *Supponiamo $\mathcal{F} \supseteq \mathcal{E}$ sia una famiglia di funzioni, chiusa per composizione e somma e prodotto generalizzate. Siano f, g funzioni k-arie tali che*

- $\mathrm{Gr}(f) \in \mathcal{F}$,
- $g \in \mathcal{F}$,
- $\forall \vec{x} \in \mathbb{N}^k \, f(\vec{x}) \leq g(\vec{x})$.

Allora $f \in \mathcal{F}$.

Dimostrazione. $f(\vec{x}) = \boldsymbol{\mu} y \leq g(\vec{x}) \, [(\vec{x}, y) \in \mathrm{Gr}(f)]$. □

Esercizio 9.11. Dimostrare che le seguenti funzioni sono elementari ricorsive:

(i) la differenza troncata

$$x \dot{-} y = \begin{cases} x - y & \text{se } x \geq y, \\ 0 & \text{altrimenti;} \end{cases}$$

(ii) il resto $\mathrm{Res} \colon \mathbb{N}^2 \to \mathbb{N}$ definito in (6.8), dove poniamo $\mathrm{Res}(n, 0) = 0$;

(iii) le funzioni di massimo e minimo $\mathbb{N}^k \to \mathbb{N}$ definite da

$$\max_k(x_0, \ldots, x_{k-1}) = \max\{x_0, \ldots, x_{k-1}\}$$
$$\min_k(x_0, \ldots, x_{k-1}) = \min\{x_0, \ldots, x_{k-1}\};$$

(iv) $\boldsymbol{J} \colon \mathbb{N}^2 \to \mathbb{N}$ e $(\cdot)_0, (\cdot)_1 \colon \mathbb{N} \to \mathbb{N}$ definite a pagina 118;

(v) $\boldsymbol{\beta} \colon \mathbb{N}^2 \to \mathbb{N}$ della Definizione 6.31.

Quindi anche le funzioni

$$\ell(x) = \boldsymbol{\beta}(x, 0) \quad \text{e} \quad (x, i) \mapsto (\!(x)\!)_i = \boldsymbol{\beta}(x, i + 1)$$

sono elementari ricorsive. Poiché

$$n \in \mathrm{Seq} \Leftrightarrow \neg \exists m < n \, [\ell(m) = \ell(n) \wedge \forall i < \ell(n) \, (\boldsymbol{\beta}(n, i) = \boldsymbol{\beta}(m, i))]$$

si vede che Seq è elementare ricorsivo.

Ricordiamo che $\langle\!\langle n_0, \ldots, n_{k-1} \rangle\!\rangle$ è l'intero che codifica $(n_0, \ldots, n_{k-1})$, cioè il più piccolo m tale che $\boldsymbol{\beta}(m, 0) = k$ e $\boldsymbol{\beta}(m, i + 1) = n_i$ per $i < k$. La funzione $\mathrm{IS} \colon \mathbb{N}^2 \to \mathbb{N}$

$$\mathrm{IS}(x, i) = \boldsymbol{\mu} y \leq x \, (\ell(y) = i \wedge \forall j < i (\!(x)\!)_j = (\!(y)\!)_j))$$

è elementare ricorsiva. Se $x = \langle\!\langle n_0, \ldots, n_{k-1} \rangle\!\rangle$ e $i \leq k$, allora $\mathrm{IS}(x, i) = \langle\!\langle n_0, \ldots, n_{i-1} \rangle\!\rangle$; per questo motivo IS è detta *funzione segmento iniziale*. La

funzione concatenazione $\mathrm{Conc}\colon \mathbb{N}^2 \to \mathbb{N}$ è definita da

$$\mathrm{Conc}(x,y) = \begin{cases} \langle\!\langle a_0,\dots,a_{n-1},b_0,\dots,b_{m-1}\rangle\!\rangle & \text{se } x = \langle\!\langle a_0,\dots,a_{n-1}\rangle\!\rangle \\ & \text{e } y = \langle\!\langle b_0,\dots,b_{m-1}\rangle\!\rangle, \\ 0 & \text{se } x,y \notin \mathrm{Seq}. \end{cases}$$

Proposizione 9.12. (a) *C'è una funzione elementare ricorsiva* $B\colon \mathbb{N}^2 \to \mathbb{N}$ *tale che per ogni* $a_0,\dots,a_{n-1} \in \mathbb{N}$

$$\langle\!\langle a_0,\dots,a_{n-1}\rangle\!\rangle \le B(\max\{a_0,\dots,a_{n-1}\},n).$$

(b) *Per ogni* $n \ge 1$ *la funzione* $\mathbb{N}^n \to \mathbb{N}$, $(a_0,\dots,a_{n-1}) \mapsto \langle\!\langle a_0,\dots,a_{n-1}\rangle\!\rangle$, *è elementare ricorsiva.*

(c) $\mathrm{Conc}, \mathrm{IS} \in \boldsymbol{\mathcal{E}}$.

Dimostrazione. (a) La funzione

$$w(k,n) = \max\{k,n\}\cdot n!$$

è elementare quindi lo è anche

$$B(k,n) = \boldsymbol{J}\big(\textstyle\prod_{i\le n} c(i,k,n), w(k,n)\big)$$

dove $c(i,k,n) = 1 + (i+1)\cdot w(k,n)$. Fissati $a_0,\dots,a_{n-1} \in \mathbb{N}$, per il Teorema 6.29 e il Lemma 6.30 c'è un $x < \prod_{i\le n} c(i,k,n)$ tale che $n \equiv x \mod c(0,k,n)$ e $a_i \equiv x \mod c(i+1,k,n)$. Poiché $\boldsymbol{J}$ è crescente in entrambe le variabili, possiamo concludere che

$$\exists z \le B(k,n)\,\big[\ell(z) = n \wedge \forall i < n\,((\!(z)\!)_{i+1} = a_i)\big].$$

(b) Posto $k = \max\{a_0,\dots,a_{n-1},n\}$ si ha

$$\langle\!\langle a_0,\dots,a_{n-1}\rangle\!\rangle = \boldsymbol{\mu} z \le B(k,n)\,\big[\ell(z) = n \wedge \forall i < n\,((\!(z)\!)_{i+1} = a_i)\big],$$

quindi $(a_0,\dots,a_{n-1}) \mapsto \langle\!\langle a_0,\dots,a_{n-1}\rangle\!\rangle$ è elementare ricorsiva.

(c) È sufficiente trovare una funzione elementare ricorsiva $g\colon \mathbb{N}^2 \to \mathbb{N}$ tale che per ogni $x,y \in \mathrm{Seq}$

$$\begin{aligned}\mathrm{Conc}(x,y) = \boldsymbol{\mu} z \le g(x,y)\,\big[&\ell(z) = \ell(x) + \ell(y) \\ &\wedge \forall i < \ell(x)\,((\!(z)\!)_i = (\!(x)\!)_i) \wedge \forall j < \ell(y)\,((\!(z)\!)_{\ell(x)+j} = (\!(y)\!)_j)\big].\end{aligned}$$

Poiché $\boldsymbol{\beta}(x,i) \le x$ per ogni i, la funzione

$$\begin{aligned} h(x) &= \max\{(\!(x)\!)_0,\dots,(\!(x)\!)_{\ell(x)-1}\} \\ &= \boldsymbol{\mu} n \le x\,[\forall i < \ell(x)\,(\boldsymbol{\beta}(x,i+1) \le n)] \end{aligned}$$

è elementare ricorsiva, così come lo sono

$$w(x,y) = \max\{h(x), h(y), \ell(x), \ell(y)\} \cdot (\ell(x) + \ell(y))!$$
$$c_i(x,y) = 1 + (i+1)w(x,y).$$

Argomentando come nella parte (a) possiamo definire

$$g(x,y) = \boldsymbol{J}(\textstyle\prod_{i \le \ell(x)+\ell(y)} c_i(x,y), w(x,y)).$$ □

9.B. Funzioni primitive ricorsive.

Definizione 9.13. Se f è k-aria e g è $k+2$-aria, diremo che la funzione $k+1$-aria

$$h(\vec{x}, n) = \begin{cases} f(\vec{x}) & \text{se } n = 0, \\ g(\vec{x}, n-1, h(\vec{x}, n-1)) & \text{se } n > 0, \end{cases}$$

è ottenuta per **ricorsione primitiva a partire da** f **e** g. Le variabili $\vec{x}$ si dicono **parametri della ricorsione**; quando non sono presenti, cioè se g è 2-aria e $a \in \mathbb{N}$, allora diremo che la funzione $h\colon \mathbb{N} \to \mathbb{N}$ definita da

$$h(n) = \begin{cases} a & \text{se } n = 0, \\ g(n-1, h(n-1)) & \text{se } n > 0, \end{cases}$$

è ottenuta per **ricorsione senza parametri a partire da** a **e** g.

Osservazioni 9.14. (a) L'esistenza di funzioni definite per ricorsione primitiva discende dal Teorema 7.4.

(b) Gli schemi di ricorsione primitiva (con e senza parametri) possono essere riassunti in un unico schema se consideriamo le costanti come funzioni zero-arie. Se nello schema di ricorsione (con o senza parametri) la funzione g non dipende dalla $k+1$-esima variabile, cioè se g è $k+1$-aria e

$$h(\vec{x}, n) = g(\vec{x}, h(\vec{x}, n-1)), \quad (n > 0)$$

diremo che h è ottenuta per **iterazione** mediante g a partire da f o da a.

Definizione 9.15. La famiglia $\boldsymbol{\mathcal{P}}$ delle funzioni **primitive ricorsive** è la più piccola classe di funzioni chiusa per composizione e ricorsione primitiva e contenente $\boldsymbol{\mathcal{E}}$.

Diremo che $A \subseteq \mathbb{N}^k$ è un **insieme primitivo ricorsivo** o, equivalentemente, è un **predicato primitivo ricorsivo** k-ario se la sua funzione caratteristica è una funzione primitiva ricorsiva.

La famiglia $\boldsymbol{\mathcal{P}}$ è molto più grande di $\boldsymbol{\mathcal{E}}$ (Esercizio 9.60). La famiglia $\boldsymbol{\mathcal{E}}$ nella Definizione 9.15 può essere sostituita da una famiglia molto più piccola.

Proposizione 9.16. *$\boldsymbol{\mathcal{P}}$ è la più piccola classe di funzioni contenente I^n_k, c_0, S e chiusa per composizione e ricorsione primitiva.*

La dimostrazione è lasciata al lettore (Esercizio 9.55).

Per ogni $f\colon \mathbb{N}^{k+1} \to \mathbb{N}$ sia $f^{\mathrm{m}}\colon \mathbb{N}^{k+1} \to \mathbb{N}$ la funzione definita da

$$f^{\mathrm{m}}(x_1, \ldots, x_k, y) = \begin{cases} 0 & \text{se } y = 0, \\ \langle\!\langle f(x_1, \ldots, x_k, 0), \ldots, f(x_1, \ldots, x_k, y) \rangle\!\rangle & \text{altrimenti.} \end{cases}$$

In altre parole: $f^{\mathrm{m}}(\vec{x}, y)$ si ricorda di tutti i valori $f(x, y')$ con $y' < y$, e per questo motivo è detta la **funzione-memoria di** f. Chiaramente è possibile definire (un'analoga del)la funzione f^{m} mediante un differente sistema di codifica, per esempio quello basato sui numeri primi (Sezione 6.B.2).

Esercizio 9.17. Sia $\mathcal{F} \supseteq \boldsymbol{\mathcal{P}}$ una famiglia di funzioni finitarie su $\mathbb{N}$, chiusa per composizione e ricorsione primitiva. Dimostrare che

$$f \in \mathcal{F} \Leftrightarrow f^{\mathrm{m}} \in \mathcal{F}.$$

Il risultato dell'Esercizio 9.17 vale anche quando $\mathcal{F} = \boldsymbol{\mathcal{E}}$ (Esercizio 9.58).

Nella Definizione 9.13, per calcolare il valore $h(\vec{x}, n)$ è sufficiente conoscere il valore immediatamente precedente $h(\vec{x}, n-1)$, ma ci sono delle situazioni in matematica in cui il valore $h(\vec{x}, n)$ dipende anche da $h(\vec{x}, i)$, per $i < n$.

Definizione 9.18. Se f è k-aria e g è $k+2$-aria, diremo che la funzione $k+1$-aria

$$h(\vec{x}, n) = \begin{cases} f(\vec{x}) & \text{se } n = 0, \\ g(\vec{x}, n-1, h^{\mathrm{m}}(\vec{x}, n)) & \text{se } n > 0, \end{cases}$$

è ottenuta per **ricorsione primitiva generalizzata a partire da** f **e** g.

Proposizione 9.19. *Sia $\mathcal{F} \supseteq \boldsymbol{\mathcal{P}}$ una famiglia di funzioni finitarie su $\mathbb{N}$ chiuso per composizione e ricorsione primitiva. Se h è ottenuta per ricorsione primitiva generalizzata a partire da f e g, allora*

$$f, g \in \mathcal{F} \Rightarrow h \in \mathcal{F}.$$

Dimostrazione. Sia $H\colon \mathbb{N}^{k+1} \to \mathbb{N}$ la funzione definita per ricorsione primitiva

$$H(\vec{x}, n) = \begin{cases} F(\vec{x}) & \text{se } n = 0, \\ G(\vec{x}, n-1, H(\vec{x}, n-1)) & \text{se } n > 0, \end{cases}$$

dove

$$F\colon \mathbb{N}^k \to \mathbb{N} \qquad F(\vec{x}) = \langle\!\langle f(\vec{x}) \rangle\!\rangle,$$
$$G\colon \mathbb{N}^{k+2} \to \mathbb{N} \qquad G(\vec{x}, m, y) = \mathrm{Conc}(y, g(\vec{x}, m, y)).$$

Poiché F e G sono primitive ricorsive, allora anche H è primitiva ricorsiva. Quindi anche h è primitiva ricorsiva, dato che

$$h(\vec{x}, n) = (\!(H(\vec{x}, n))\!)_{\ell(H(\vec{x}, n)) \dot{-} 1}. \qquad \square$$

9.C. Funzioni ricorsive. Sia f una funzione $k+1$-aria tale che

$$\forall x_1, \dots, x_k \exists y\, f(x_1, \dots, x_k, y) = 0.$$

La funzione k-aria

$$g\colon \mathbb{N}^k \to \mathbb{N}, \qquad g(x_1, \dots, x_k) = \min\{y \in \mathbb{N} \mid (f(x_1, \dots, x_k, y) = 0)\}$$

si dice ottenuta da f per **minimizzazione** e la si indica solitamente con

$$\boldsymbol{\mu} y\, (f(x_1, \dots, x_k, y) = 0)$$

o anche solo con $\boldsymbol{\mu} y\, f$ quando le variabili sono chiare dal contesto. Se f è calcolabile, allora anche $\boldsymbol{\mu} y\, (f(x_1, \dots, x_k, y) = 0)$ lo è: basta calcolare $f(x_1, \dots, x_k, 0)$, $f(x_1, \dots, x_k, 1)$, ... fin tanto che non otteniamo un y per cui $f(x_1, \dots, x_k, y) = 0$, e questo y è il valore cercato.

Definizione 9.20. La collezione $\mathfrak{R}$ delle **funzioni ricorsive** è la più piccola famiglia $\mathcal{F}$ di funzioni contenente $\mathfrak{R}$, chiusa per composizione, ricorsione primitiva e minimizzazione, cioè se $f\colon \mathbb{N}^{k+1} \to \mathbb{N}$ è in $\mathcal{F}$ e $\forall \vec{x}\, \exists y\, f(\vec{x}, y) = 0$, allora $\boldsymbol{\mu} y\, (f(\vec{x}, y) = 0)$ è in $\mathcal{F}$.

Ogni funzione ricorsiva è calcolabile. Viceversa,

Tesi di Church. *Ogni funzione calcolabile è ricorsiva.*

La tesi di Church non è né un teorema né una congettura. È un'osservazione empirica: asserisce che la definizione rigorosa di funzione ricorsiva cattura il concetto di funzione intuitivamente calcolabile. Naturalmente, non possiamo escludere che la tesi di Church possa essere un giorno confutata: basterebbe esibire una funzione che risulti essere calcolabile nel senso comune del termine e per cui si possa dimostrare che non è ricorsiva. Esistono tuttavia delle buone ragioni per credere nella tesi di Church dato che:

(A) tutti gli esempi noti in matematica di funzione calcolabile sono in realtà funzioni ricorsive;

(B) nel secolo scorso sono state proposte numerose formalizzazioni del concetto di funzione calcolabile — la definizione di funzione ricorsiva descritta qui sopra è una di queste, tra le altre citiamo le *macchine di Turing* e i *sistemi di Post*. Queste formalizzazioni, benché all'apparenza molto diverse tra loro, *individuano tutte lo stesso insieme di funzioni*, cioè le funzioni ricorsive.

Per questi motivi la tesi di Church è comunemente accettata (come fatto empirico) dalla comunità matematica e viene spesso usata nel corso di una dimostrazione per argomentare che una qualche funzione è ricorsiva. Questo è del tutto analogo a quanto avviene nei corsi di Analisi, dove da un certo punto in poi si tende ad argomentare in modo informale che una certa funzione è continua, invece di esibire esplicitamente il δ a partire dall'ε.

In realtà, tutto ciò equivale a chiedere al lettore di effettuare una verifica che l'autore del testo è troppo pigro per scrivere. Naturalmente questo tipo di verifiche possono essere lasciate al lettore soltanto quando questi abbia sviluppato una familiarità sufficiente con i calcoli di base, quindi all'inizio la nostra trattazione sarà piuttosto dettagliata.

Osservazioni 9.21. (a) Ogni funzione primitiva ricorsiva è ricorsiva, ma non vale il viceversa: nella prossima Sezione 9.D.1 vedremo un esempio di funzione ricorsiva che non è primitiva ricorsiva. Quindi la nozione di funzione primitiva ricorsiva non cattura in modo adeguato la nozione di funzione calcolabile.

(b) Sapere che una funzione è ricorsiva non significa conoscere l'algoritmo che la calcola. Per esempio consideriamo la funzione f definita da $f(n) = 0$ se vale un problema aperto in teoria dei numeri (quali quelli descritti nell'Esercizio 2.8) e $f(n) = 1$ se questa congettura non vale; f è ricorsiva in quanto è una funzione costante e tuttavia non sappiamo quale sia il programma che la calcola.

(c) Il concetto di funzione ricorsiva individua una nozione di calcolabilità piuttosto idealizzata, svincolata dai limiti fisici dei meccanismi di computo. In altre parole, anche se conosciamo l'algoritmo che testimonia che una funzione f è ricorsiva, non è detto che riusciamo a calcolare $f(n)$ per valori di n non troppo grandi. Per esempio la funzione fattoriale $n!$ benché primitiva ricorsiva, non è *praticamente calcolabile* per valori non troppo piccoli di n. Per questo motivo dalla seconda metà dello scorso secolo si è sviluppata la teoria della complessità che studia classi di funzioni *praticamente calcolabili*.

Un $A \subseteq \mathbb{N}^k$ è un **predicato ricorsivo** se la sua funzione caratteristica lo è; in altre parole A è ricorsivo se c'è un algoritmo per decidere se un elemento gli appartiene o meno.

Osservazione 9.22. Il lettore potrebbe avere la falsa impressione che quasi tutti i sottoinsiemi di $\mathbb{N}^k$ siano ricorsivi, mentre l'opposto è vero: gli insiemi ricorsivi sono in quantità numerabile e quindi sono una sparuta minoranza in $\mathscr{P}(\mathbb{N}^k)$ (si veda la Sezione 10 per maggiori informazioni). Analogamente, le funzioni ricorsive sono in quantità numerabile e quindi sono una minuscola parte dell'insieme di tutte le funzioni k-arie sui naturali.

Il prossimo risultato, la cui dimostrazione è lasciata al lettore (Esercizio 9.65), è l'analogo della Proposizione 9.16.

Proposizione 9.23. *$\mathcal{R}$ è la più piccola famiglia $\mathcal{F}$ di funzioni contenente $I_k^n, +, \cdot, \boldsymbol{\chi}_{\leq}$ e chiusa per composizione e minimizzazione.*

Ricordiamo da pagina 53 che una funzione k-aria (eventualmente parziale) è definibile in una struttura se il suo grafo è un sottoinsieme definibile di dimensione $k+1$,e che le funzioni definibili sono chiuse per composizione (Esercizio 3.51). Sia $\mathcal{N}$ una struttura con universo $\mathbb{N}$ in cui $<$ è definibile, per esempio $\mathcal{N} = (\mathbb{N}, +, \cdot)$. Se $f(\vec{x}) = \boldsymbol{\mu} y\,[g(\vec{x}, y) = 0]$ e g è definibile in $\mathcal{N}$ mediante φ_g, allora f è definibile in $\mathcal{N}$ dato che

$$(\vec{x}, y) \in \mathrm{Gr}(f) \Leftrightarrow \varphi_g(\vec{x}, y, 0) \wedge \forall z\,[z < y \Rightarrow \neg\varphi_g(\vec{x}, z, 0)].$$

Quindi abbiamo dimostrato:

Teorema 9.24. *Ogni funzione e predicato ricorsivo è definibile in* $(\mathbb{N}, +, \cdot)$.

L'Esempio 9.9(A) si generalizza al caso ricorsivo, vale a dire:

> Se $A(x_1, \ldots, x_m)$ è ricorsivo e $f_1, \ldots, f_m$ sono funzioni ricorsive k-arie, allora
>
> $$A(f_1(x_1, \ldots, x_k), \ldots, f_m(x_1, \ldots, x_k))$$
>
> è ricorsivo.

Un discorso simile vale per gli Esempi 9.9(B)–(F). In particolare, la famiglia dei sottoinsiemi ricorsivi di $\mathbb{N}^k$ è un'algebra di Boole. Se A è un predicato ricorsivo $k+1$-ario tale che $\forall \vec{x} \in \mathbb{N}^k\, \exists y \in \mathbb{N}\, A(\vec{x}, y)$, allora la funzione $\boldsymbol{\mu} y\, A(\vec{x}, y)$ che assegna a $(n_1, \ldots, n_k)$ il più piccolo m tale che $A(n_1, \ldots, n_k, m)$, è ricorsiva, dato che

$$\boldsymbol{\mu} y\, A(\vec{x}, y) = \boldsymbol{\mu} y\,[1 \dot{-} \boldsymbol{\chi}_A(\vec{x}, y) = 0].$$

Lemma 9.25. *Una funzione k-aria $f\colon \mathbb{N}^k \to \mathbb{N}$ è ricorsiva se e solo se il suo grafo*

$$\mathrm{Gr}(f) = \{(\vec{x}, y) \in \mathbb{N}^{k+1} \mid f(\vec{x}) = y\}$$

è un predicato ricorsivo $k+1$-ario.

Dimostrazione. Una direzione segue dal Lemma 9.7. Viceversa, se $\boldsymbol{\chi}_{\mathrm{Gr}(f)}$ è calcolabile, anche f lo è: dato $\vec{x}$ si cerca il primo (ed unico) y tale che $(\vec{x}, y) \in \mathrm{Gr}(f)$, e questo y è $f(\vec{x})$. Formalmente:

$$f(\vec{x}) = \boldsymbol{\mu} y\,[1 - \boldsymbol{\chi}_{\mathrm{Gr}(f)}(\vec{x}, y) = 0]. \qquad \square$$

Si confronti il prossimo risultato con l'Osservazione 9.8.

Corollario 9.26. *Se $f\colon \mathbb{N} \to \mathbb{N}$ è ricorsiva ed è una biezione, allora anche f^{-1}, è una funzione ricorsiva.*

In particolare l'insieme delle biezioni ricorsive è un gruppo.

La **funzione enumerante** di un insieme infinito $A \subseteq \mathbb{N}$ è la funzione $f\colon \mathbb{N} \to \mathbb{N}$ che ad n associa l'n-esimo elemento di A.

Proposizione 9.27. *Supponiamo $A \subseteq \mathbb{N}$ sia infinito e sia f la sua funzione enumerante.*

$$A \text{ è ricorsivo } \Leftrightarrow f \text{ è ricorsiva.}$$

Dimostrazione. Supponiamo A ricorsivo: f è ricorsiva dato che

$$f(n) = \begin{cases} \min(A) & \text{se } n = 0 \\ g(n-1, f(n-1)) & \text{se } n > 0 \end{cases}$$

dove

$$g(i,k) = \boldsymbol{\mu} m\, [A(m) \wedge m > k].$$

L'altra direzione discende da $A(x) \Leftrightarrow \exists y \leq x\, [f(y) = x]$. □

Osservazione 9.28. La Proposizione 9.27 non si generalizza ad altre classi, quali $\boldsymbol{\mathcal{E}}$ o $\boldsymbol{\mathcal{P}}$. In altre parole: se $\mathcal{F}$ è $\boldsymbol{\mathcal{E}}$ o $\boldsymbol{\mathcal{P}}$, ci sono insiemi in $\mathcal{F}$ la cui funzione enumerante è in $\boldsymbol{\mathcal{R}} \setminus \mathcal{F}$ — Proposizione 9.38(a).

Lemma 9.29. *Siano A e B insiemi infiniti che formano una partizione di $\mathbb{N}$ e siano f_A e f_B le loro funzioni enumeranti. Se $\mathrm{Gr}(f_A) \in \mathcal{F}$, dove $\mathcal{F}$ è $\boldsymbol{\mathcal{E}}$ o $\boldsymbol{\mathcal{P}}$, allora $\mathrm{Gr}(f_B)$, A e B sono in $\mathcal{F}$.*

Dimostrazione. $(x,y) \in \mathrm{Gr}(f_B)$ se e solo se

$$x = y < f_A(0) \vee \big(\exists u, v < y\, [(u,v) \in \mathrm{Gr}(f_A) \\ \wedge \neg \exists z, w < y\, (u < z \wedge (z,w) \in \mathrm{Gr}(f_A)) \wedge y = x + u]\big)$$

quindi $\mathrm{Gr}(f_B) \in \mathcal{F}$. Inoltre $A = \{y \mid \exists x \leq y\, [(x,y) \in \mathrm{Gr}(f_A)]\} \in \mathcal{F}$ e quindi $B = \mathbb{N} \setminus A \in \mathcal{F}$. □

Esercizio 9.30. Sia $\mathcal{F} = \boldsymbol{\mathcal{E}}$ oppure $\mathcal{F} = \boldsymbol{\mathcal{P}}$. Dimostrare che:

(i) se $f\colon \mathbb{N} \to \mathbb{N}$ è crescente ed è in $\mathcal{F}$, allora $\mathrm{ran}(f)$ è in $\mathcal{F}$;

(ii) se $A \subseteq \mathbb{N}$ è in $\mathcal{F}$ e f è la sua funzione enumerante, ed esiste $h\colon \mathbb{N} \to \mathbb{N}$ tale che $h \in \mathcal{F}$ e $\forall n\, (f(n) \leq h(n))$, allora $f \in \mathcal{F}$;

(iii) la funzione enumerante di Seq è elementare ricorsiva.

A partire dalla biezione $\boldsymbol{J}\colon \mathbb{N}^2 \to \mathbb{N}$ di (6.6) si possono definire le biezioni

$$\boldsymbol{J}^n\colon \mathbb{N}^n \to \mathbb{N}, \qquad \boldsymbol{J}^n(x_0, \ldots, x_{n-1}) = \boldsymbol{J}(x_0, \boldsymbol{J}^{n-1}(x_1, \ldots, x_{n-1})) \tag{9.2}$$

dove $\boldsymbol{J}^1 = \mathrm{id}_{\mathbb{N}}$ e $\boldsymbol{J}^2 = \boldsymbol{J}$. Le funzioni inverse

$$(\cdot)^n_k\colon \mathbb{N} \to \mathbb{N} \qquad (k < n)$$

sono definite da

$$\boldsymbol{J}^n((x)^n_0, \ldots, (x)^n_{n-1}) = x. \tag{9.3}$$

Una funzione

$$f\colon \mathbb{N}^n \to \mathbb{N}^m, \qquad f(\vec{x}) = (f_0(\vec{x}), \ldots, f_{m-1}(\vec{x}))$$

si dice (elementare/primitiva) ricorsiva se le $f_i\colon \mathbb{N}^n \to \mathbb{N}$ $(i < m)$ sono (elementari/primitive) ricorsive.

Esercizio 9.31. Sia $\mathcal{F}$ una delle classi $\boldsymbol{\mathcal{E}}, \boldsymbol{\mathcal{P}}, \boldsymbol{\mathcal{R}}$. Verificare che:

(i) le funzioni $\boldsymbol{J}^m$ e $(\cdot)^m_i$ $(i < m)$ sono elementari ricorsive;

(ii) $f\colon \mathbb{N}^n \to \mathbb{N}^m$ è in $\mathcal{F}$ se e solo se
$$\tilde{f}\colon \mathbb{N}^n \to \mathbb{N}, \qquad \tilde{f}(\vec{x}) = \boldsymbol{J}^m(f_0(\vec{x}), \dots, f_{m-1}(\vec{x}))$$
è in $\mathcal{F}$.

(iii) $A \subseteq \mathbb{N}^m$ è in $\mathcal{F}$ se e solo se
$$\tilde{A} \stackrel{\text{def}}{=} \left\{ n \in \mathbb{N} \mid ((n)^m_0, \dots, (n)^m_{m-1}) \in A \right\}$$
è in $\mathcal{F}$.

(iv) $f\colon \mathbb{N}^n \to \mathbb{N}$ è in $\mathcal{F}$ se e solo se
$$\check{f}\colon \mathbb{N} \to \mathbb{N}, \qquad \check{f}(x) = f((x)^n_0, \dots, (x)^n_{n-1})$$
è in $\mathcal{F}$.

La nozione di funzione e insieme calcolabile può essere estesa ad altri domini, per esempio $\mathbb{N}^{<\mathbb{N}}$: una funzione
$$F\colon \mathbb{N}^{<\mathbb{N}} \to \mathbb{N}^{<\mathbb{N}}$$
è (elementare/primitiva) ricorsiva se e solo se c'è una funzione (elementare/primitiva) ricorsiva $f\colon \mathbb{N} \to \mathbb{N}$ tale che
$$F(x_0, \dots, x_n) = (y_0, \dots, y_m) \Leftrightarrow f(\langle\!\langle x_0, \dots, x_n \rangle\!\rangle) = \langle\!\langle y_0, \dots, y_m \rangle\!\rangle$$
e un insieme
$$A \subseteq \mathbb{N}^{<\mathbb{N}}$$
è (elementare/primitivo) ricorsivo se e solo se l'insieme
$$\{\langle\!\langle x_0, \dots, x_n \rangle\!\rangle \mid (x_0, \dots, x_n) \in A\}$$
è (elementare/primitivo) ricorsivo.

9.D. Funzioni calcolabili, ma non primitive ricorsive.

9.D.1. *La funzione di Ackermann.* Vediamo un esempio concreto di funzione calcolabile che non è primitiva ricorsiva.

La **funzione di Ackermann** $\mathrm{Ack}\colon \mathbb{N}^2 \to \mathbb{N}$ è definita da
$$\mathrm{Ack}(m,n) = \begin{cases} n+1 & \text{se } m = 0, \\ \mathrm{Ack}(m-1, 1) & \text{se } m > 0 \text{ e } n = 0, \\ \mathrm{Ack}(m-1, \mathrm{Ack}(m, n-1)) & \text{se } m > 0 \text{ e } n > 0. \end{cases}$$
Sia
$$\mathrm{Ack}_m\colon \mathbb{N} \to \mathbb{N}, \qquad n \mapsto \mathrm{Ack}(m,n).$$

Notiamo che Ack_0 è calcolabile, dato che $\mathrm{Ack}_0(n) = n + 1$.

Esercizio 9.32. Dimostrare che

(i) se $m > 0$ allora $\mathrm{Ack}_m(n) = \mathrm{Ack}_{m-1}^{(n+1)}(1)$,

(ii) Ack_m è strettamente crescente, per ogni m.

Quindi il computo dei valori della funzione Ack_{m-1} può essere successivamente ricondotto al computo dei valori delle funzioni $\mathrm{Ack}_{m-2}, \mathrm{Ack}_{m-3}, \ldots, \mathrm{Ack}_0$. Ne segue che la funzione di Ackermann è calcolabile, quindi per la tesi di Church è ricorsiva. Per verificare formalmente che Ack è ricorsiva ragioniamo come segue.

Per l'Esercizio 9.32, per calcolare $\mathrm{Ack}(m, n)$ è sufficiente conoscere la funzione di Ackermann ristretta a un $D \subseteq \mathbb{N} \times \mathbb{N}$ finito. Sia $\mathcal{F}$ l'insieme delle coppie (f, D) tali che:

(A) $D \subseteq \mathbb{N} \times \mathbb{N}$ è finito e $f \colon D \to \mathbb{N}$,

(B) $\forall m, n \, [(m, n+1) \in D \Rightarrow (m, n) \in D]$,

(C) $\forall n \, [(0, n) \in D \Rightarrow f(0, n) = n + 1]$,

(D) $\forall m \, [(m+1, 0) \in D \Rightarrow f(m+1, 0) = f(m, 1)]$,

(E) $\forall m, n \, [(m+1, n+1) \in D \Rightarrow (m+1, n) \in D \wedge (m, f(m+1, n)) \in D \wedge f(m+1, n+1) = f(m, f(m+1, n))]$.

Esercizio 9.33. Dimostrare che per ogni (m, n), se definiamo $k_0 = n$ e per $0 < i \leq m$

$$k_{i+1} = \mathrm{Ack}_{m-i}^{(k_i+1)}(1),$$

allora $(f, D) \in \mathcal{F}$, dove $D = \{(i, j) \in \mathbb{N} \times \mathbb{N} \mid i \leq m \wedge j \leq k_{m-1}\}$ e $f = \mathrm{Ack} \restriction D$.

Quindi

$$\mathrm{Ack}(m, n) = k \Leftrightarrow \exists (f, D) \in \mathcal{F} \, [(m, n) \in D \wedge f(m, n) = k].$$

Ogni $(f, D) \in \mathcal{F}$ è essenzialmente una sequenza finita di numeri naturali, quindi è codificabile come un elemento di Seq e sia $S \subseteq \mathrm{Seq}$ l'insieme dei numeri che codificano un elemento di $\mathcal{F}$. Quindi un elemento di S è una sequenza di naturali, ciascuno dei quali codifica una tripla $\boldsymbol{J}(\boldsymbol{J}(n, m), f(n, m))$.

Le (A)–(E) si traducono in condizioni sui naturali che mostrano che S è elementare ricorsivo. Per esempio, la condizione (A) la si traduce in

$$\forall i, i' < \ell(s) \, \forall m, n, k, k' < s \, [(\!(s)\!)_i = \boldsymbol{J}(\boldsymbol{J}(n, m), k) \wedge (\!(s)\!)_{i'} = \boldsymbol{J}(\boldsymbol{J}(n, m), k') \Rightarrow k = k']$$

mentre le (B) e (C) diventano rispettivamente

$$\forall i, i' < \ell(s)\, \forall m, n, k, k' < s\, [(\!(s)\!)_i = \boldsymbol{J}(\boldsymbol{J}(n,m),k) \\ \wedge\ (\!(s)\!)_{i'} = \boldsymbol{J}(\boldsymbol{J}(n,m),k') \Rightarrow k = k']$$

e

$$\forall m, n < s\, [\exists i < \ell(s)\, \exists k < s\, \boldsymbol{J}(\boldsymbol{J}(m,n+1),k) = (\!(s)\!)_i \\ \Rightarrow\ \exists i' < \ell(s)\, \exists k < s\, \boldsymbol{J}(\boldsymbol{J}(m,n),k') = (\!(s)\!)_{i'}].$$

Esercizio 9.34. Trasformare (D) e (E) in condizioni sui naturali e verificare che S è elementare ricorsivo.

Quindi

$$\mathrm{Ack}(m,n) = k \Leftrightarrow \exists s \in S\, \exists i < \ell(s)\, [(\!(s)\!)_i = \boldsymbol{J}(\boldsymbol{J}(m,n),k)]$$

e allora

$$\mathrm{Ack}(m,n) = (\boldsymbol{\mu} y\, A(m,n,y))_1 \tag{9.4}$$

dove

$$A(m,n,\boldsymbol{J}(s,k)) \Leftrightarrow s \in S \wedge \exists i < \ell(s)\, [(\!(s)\!)_i = \boldsymbol{J}(\boldsymbol{J}(m,n),k)].$$

Poiché $A \subseteq \mathbb{N}^3$ elementare ricorsivo, ne segue che $\mathrm{Ack} \in \mathfrak{R}$.

Teorema 9.35. *Se $f\colon \mathbb{N}^n \to \mathbb{N}$ è primitiva ricorsiva, allora c'è un c tale che*

$$\forall x_1, \ldots, x_n\ (f(x_1, \ldots, x_n) < \mathrm{Ack}(c, x_1 + \cdots + x_n))\,.$$

Per la dimostrazione si veda l'Esercizio 9.64.

Corollario 9.36. *La funzione di Ackermann non è primitiva ricorsiva.*

Dimostrazione. Se per assurdo Ack fosse primitiva ricorsiva, allora anche $f(n) = \sum_{i=0}^{n} \mathrm{Ack}(i,n)$ lo sarebbe, quindi $\forall n\, (f(n) < \mathrm{Ack}(c,n))$ per un opportuno c. In particolare, se $n \geq c$ allora

$$\mathrm{Ack}(c,n) \leq \sum_{i=0}^{n} \mathrm{Ack}(i,n) = f(n) < \mathrm{Ack}(c,n)$$

contraddizione! □

9.D.2. *Forma normale.* La (9.4) è il caso particolare di un risultato più generale noto come **Teorema di forma normale di Kleene** che dimostreremo nella Sezione 19 del Capitolo V:

Teorema 9.37. *Per ogni $n \geq 1$ c'è un predicato elementare ricorsivo $\mathrm{K}_n \subseteq \mathbb{N}^{n+2}$ tale che: per ogni $f\colon \mathbb{N}^n \to \mathbb{N}$ ricorsiva c'è un $e \in \mathbb{N}$ tale che*

$$f(\vec{x}) = (\boldsymbol{\mu} y\, \mathrm{K}_n(e, \vec{x}, y))_1$$

In particolare ogni funzione ricorsiva è ottenibile mediante un'unica applicazione dell'operatore di minimizzazione. Per la parte (iv) dell'Esercizio 9.31, nel Teorema 9.37 ci si potrebbe limitare al caso $n = 1$.

Il Teorema di forma normale può essere descritto in termini informatici così. C'è un computer K tale che per ogni funzione calcolabile $f\colon \mathbb{N} \to \mathbb{N}$, il valore $f(x)$ è ottenuto facendo girare il programma e sul computer con input x: il risultato è una coppia (c, y) dove y è il risultato $f(x)$ e c è il numero che codifica la stringa finita di computi che ci consentono di arrivare a y.

Per il Corollario 9.26, l'inversa di una biezione ricorsiva è ricorsiva.

Proposizione 9.38. (a) *C'è un sottoinsieme elementare di* $\mathbb{N}$ *la cui funzione enumerante è in* $\boldsymbol{\mathcal{R}} \setminus \boldsymbol{\mathcal{P}}$.

(b) *C'è una funzione in* $\boldsymbol{\mathcal{R}} \setminus \boldsymbol{\mathcal{P}}$ *il cui grafo è in* $\boldsymbol{\mathcal{E}}$.

(c) *C'è una biezione elementare di* $\mathbb{N}$ *la cui inversa è in* $\boldsymbol{\mathcal{R}} \setminus \boldsymbol{\mathcal{P}}$.

Dimostrazione. Sia A il predicato elementare della (9.4). La funzione

$$f_0\colon \mathbb{N} \to \mathbb{N}, \qquad x \mapsto \boldsymbol{\mu} y\, A(x, x, y)$$

è strettamente crescente e domina ogni funzione unaria primitiva ricorsiva, dato che $n \mapsto \mathrm{Ack}(n, n)$ ha queste proprietà e $(k)_1 \leq k$ per ogni k. In particolare $f_0 \in \boldsymbol{\mathcal{R}} \setminus \boldsymbol{\mathcal{P}}$, e $\mathrm{ran}(f_0)$ e $\mathbb{N} \setminus \mathrm{ran}(f_0)$ sono infiniti. Sia f_1 la funzione enumerante di $\mathbb{N} \setminus \mathrm{ran}(f_0)$. Poiché

$$\mathrm{Gr}(f_0) = \{(x, y) \mid A(x, x, y) \wedge \forall y' < y\, [\neg A(x, x, y')]\}$$

è in $\boldsymbol{\mathcal{E}}$, anche $\mathrm{Gr}(f_1)$ e $\mathrm{ran}(f_0)$ sono in $\boldsymbol{\mathcal{E}}$ per il Lemma 9.29. Questo prova (a) e (b).

Sia $g\colon \mathbb{N} \to \mathbb{N}$ la biezione ottenuta copiando f_0 sui pari e f_1 sui dispari:

$$g(x) = \begin{cases} f_0(n) & \text{se } x = 2n, \\ f_1(n) & \text{se } x = 2n + 1. \end{cases}$$

La g è una biezione, il suo grafo

$$\{(2x, y) \mid (x, y) \in \mathrm{Gr}(f_0)\} \cup \{(2x + 1, y) \mid (x, y) \in \mathrm{Gr}(f_1)\}$$

è elementare, e $g^{-1}(y) \leq 2y + 1$, quindi $g^{-1} \in \boldsymbol{\mathcal{E}}$ per la Proposizione 9.10. Poiché $f_0(n) = g(2n)$ ne segue che $g \in \boldsymbol{\mathcal{R}} \setminus \boldsymbol{\mathcal{P}}$. □

9.E. Programmi. Per dimostrare che $f\colon \mathbb{N}^k \to \mathbb{N}$ è in $\mathcal{F}$ dove $\mathcal{F}$ è $\boldsymbol{\mathcal{E}}$, $\boldsymbol{\mathcal{P}}$, oppure $\boldsymbol{\mathcal{R}}$, bisogna dimostrare che f è ottenibile a partire da funzioni di base mediante specifiche costruzioni, quali la composizione, somma e prodotto limitati, ricorsione primitiva e minimizzazione.

9.E.1. *Programmi per le funzioni elementari ricorsive.* Il linguaggio del prim'ordine $L_{\mathcal{E}}$ per le funzioni elementari ricorsive ha

$$\texttt{Add}, \quad \texttt{Mult}, \quad \texttt{Div}, \quad \texttt{Quot}, \quad \texttt{Proj}^n_k \quad (0 \leq k < n)$$

come simboli di costante,

$$\texttt{Com}_k$$

dei simboli $k+1$-ari di funzione, e dei simboli unari di funzione

$$\texttt{Sum} \quad \text{e} \quad \texttt{Prod}.$$

Dimostreremo ora che ogni funzione elementare ricorsiva può essere calcolata a partire da un termine chiuso di $L_{\mathcal{E}}$, e per questo motivo questi sono detti **programmi** per funzioni elementari ricorsive. I programmi `Add`, `Mult`, `Div`, e `Quot` calcolano le funzioni binarie $x+y$, $x \cdot y$, $|x-y|$, e $\lfloor x/y \rfloor$, rispettivamente, e il programma $\texttt{Proj}^n_k$ calcola la funzione proiezione I^n_k. Se $\texttt{P}$ è il programma che calcola una funzione k-aria f e $\texttt{Q}_0, \dots \texttt{Q}_{k-1}$ sono i programmi che computano le funzioni n-arie $g_0, \dots, g_{k-1}$ allora

- $\texttt{Com}_k(\texttt{P}, \texttt{Q}_0, \dots, \texttt{Q}_{k-1})$ è un programma che calcola la funzione n-aria $f(g_0(\vec{x}), \dots, g_{k-1}(\vec{x}))$;
- $\texttt{Sum}(\texttt{P})$ e $\texttt{Prod}(\texttt{P})$ sono i programmi che calcolano le funzioni k-arie $\sum f$ e $\prod f$.

Quindi ogni funzione elementare ricorsiva è calcolata da un programma, ma non ogni programma calcola una funzione elementare, dato che $\texttt{Com}_k(\texttt{P}, \texttt{Q}_0, \dots, \texttt{Q}_{k-1})$ ha significato solo quando le arietà delle funzioni descritte si corrispondono correttamente. Quando questo capita diremo che il programma è ben-formato e Elm è la famiglia dei programmi ben-formati. Un programma che non sia ben formati si dice mal-formato.[7] Sia $\mathrm{C}_{\mathcal{E}}$ l'insieme dei termini chiusi di $L_{\mathcal{E}}$, e sia $\mathrm{ar}\colon \mathrm{C} \to \mathbb{N}$ la funzione così definita per induzione sulla complessità dei termini:

$$\mathrm{ar}(\texttt{Add}) = \mathrm{ar}(\texttt{Mult}) = \mathrm{ar}(\texttt{Div}) = \mathrm{ar}(\texttt{Quot}) = 2$$
$$\mathrm{ar}(\texttt{Sum}(\texttt{P})) = \mathrm{ar}(\texttt{Prod}(\texttt{P})) = \mathrm{ar}(\texttt{P})$$
$$\mathrm{ar}\left(\texttt{Com}_k(\texttt{P}, \texttt{Q}_0, \dots, \texttt{Q}_{k-1})\right) = \begin{cases} n & \text{se } \mathrm{ar}(\texttt{Q}_0) = \dots = \mathrm{ar}(\texttt{Q}_{k-1}) = n \text{ e } \mathrm{ar}(\texttt{P}) = k \\ 0 & \text{altrimenti.} \end{cases}$$

Allora $\textsc{Elm} = \{\texttt{P} \in \mathrm{C}_{\mathcal{E}} \mid \mathrm{ar}(\texttt{P}) \neq 0\}$, e quando $\texttt{P} \in \textsc{Elm}$ e $f\colon \mathbb{N}^k \to \mathbb{N}$ è la funzione definita da P, allora $k = \mathrm{ar}(\texttt{P})$.

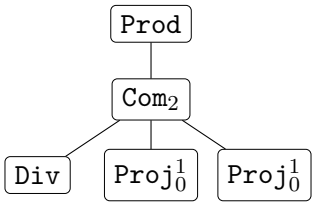
Se $\texttt{P}$ calcola $f\colon \mathbb{N}^k \to \mathbb{N}$, e $\texttt{Q}$ ed $\texttt{R}$ calcolano $x \mapsto x+1$ e $x \mapsto x \dot{-} 1$, rispettivamente, allora anche $\texttt{Com}_1(\texttt{R}, \texttt{Com}_1(\texttt{Q}, \texttt{P}))$ calcola f. Ripetendo la

[7] In informatica diremmo che il compilatore risponde con un messaggio `syntax-error` quando lavoriamo con un programma mal-formato.

semplice procedura di aggiungere e poi sottrarre 1 possiamo costruire infiniti programmi che computano la medesima funzione, cioè

$$\forall f \in \boldsymbol{\mathcal{E}}\,[\{\mathtt{P} \in \textsc{Elm} \mid \mathtt{P} \text{ calcola } f\} \text{ è infinito}]. \tag{9.5}$$

Come osservato nella Sezione 3.A, ogni termine di un linguaggio del prim'ordine lo si può descrivere in modo efficace mediante il suo albero sintattico. Per esempio, il programma ben-formato $\mathtt{Prod}(\mathtt{Com}_2(\mathtt{Div}, \mathtt{Proj}^1_0, \mathtt{Proj}^1_0))$ che calcola $\overline{\mathrm{sgn}}(x)$ può essere scritto come



9.E.2. *Programmi per funzioni primitive ricorsive.* Il linguaggio $L_{\boldsymbol{\mathcal{P}}}$ per le funzioni primitive ricorsive ha come simboli di costante `Zero`, `Succ` e $\mathtt{Proj}^n_k$ con $0 \leq k < n$, un simbolo di funzione binaria `Rec`, ed i simboli di funzione $k+1$-ari $\mathtt{Com}_k$ come prima. Un programma per una funzione primitiva ricorsiva è un termine chiuso di $L_{\boldsymbol{\mathcal{P}}}$, e sia $\mathrm{C}_{\boldsymbol{\mathcal{P}}}$ l'insieme di questi programmi. Ogni funzione in $\boldsymbol{\mathcal{P}}$ è calcolata da un qualche programma:

- `Zero` e `Succ` calcolano le funzioni $n \mapsto c_0(n) = 0$ e $n \mapsto n+1$ rispettivamente,
- $\mathtt{Proj}^n_k$ e $\mathtt{Com}_k$ si comportano come nel caso delle funzioni elementari,
- se `P` calcola la funzione k-aria f e `Q` calcola la funzione $k+2$-aria g, allora $\mathtt{Rec}(\mathtt{P}, \mathtt{Q})$ è il programma che calcola la funzione $k+1$-aria $h(\vec{x}, 0) = f(\vec{x})$ e $h(\vec{x}, y+1) = g(\vec{x}, y, h(\vec{x}, y))$.

Per la Proposizione 9.16 ogni funzione primitiva ricorsiva è calcolata da un programma in $\mathrm{C}_{\boldsymbol{\mathcal{P}}}$ e, come nel caso delle funzioni elementari ricorsive, non tutti i programmi calcolano una funzione. L'insieme del programmi ben-formati lo si indica con PRec.

Esercizio 9.39. Definiamo una funzione $\mathrm{ar}\colon \mathrm{C}_{\boldsymbol{\mathcal{P}}} \to \mathbb{N}$ tale che

$$\textsc{PRec} = \{\mathtt{P} \in \mathrm{C}_{\boldsymbol{\mathcal{P}}} \mid \mathrm{ar}(\mathtt{P}) \neq 0\}$$

e l'arietà della funzione calcolata da $\mathtt{P} \in \mathrm{C}_{\boldsymbol{\mathcal{P}}}$ è $\mathrm{ar}(\mathtt{P})$.

L'enunciato seguente è l'analogo di (9.5)

$$\forall f \in \boldsymbol{\mathcal{P}}\,[\{\mathtt{P} \in \textsc{PRec} \mid \mathtt{P} \text{ calcola } f\} \text{ è infinito}].$$

9.E.3. *Programmi per le funzioni ricorsive.* Il linguaggio $L_{\mathfrak{R}}$ per le funzioni ricorsive ha per simboli di costante $\mathtt{Add}$, $\mathtt{Mult}$, $\mathtt{Less}$ e $\mathtt{Proj}^n_k$ con $0 \leq k < n$, un simbolo di funzione unaria $\mathtt{Min}$, e i simboli di funzione $k+1$-aria $\mathtt{Com}_k$ come prima. L'insieme dei termini chiusi lo si denota con $\mathrm{C}_{\mathfrak{R}}$, e i suoi elementi sono detti programmi per funzioni ricorsive. Qui $\mathtt{Less}$ è il programma che calcola la funzione binaria $\boldsymbol{\chi}_{\leq}(x, y)$, e se $\mathtt{P}$ è un programma che calcola una funzione $k+1$-aria $f(\vec{x}, y)$ tale che $\forall \vec{x}\, \exists y\, [f(\vec{x}, y) = 0]$, allora $\mathtt{Min}(\mathtt{P})$ è un programma che calcola la funzione$k$-aria $\vec{x} \mapsto \boldsymbol{\mu} y\, [f(\vec{x}, y) = 0]$.

Ogni funzione ricorsiva è calcolata da qualche programma — infatti per un ragionamento come in (9.5) è calcolata da infiniti programmi. Come nel caso di $\boldsymbol{\mathcal{E}}$ e $\boldsymbol{\mathcal{P}}$, non ogni elemento di $\mathrm{C}_{\mathfrak{R}}$ calcola una funzione in $\boldsymbol{\mathcal{R}}$, e indicheremo con Rec l'insieme dei programmi ben-formati che calcolano funzioni ricorsive, vale a dire si definisce un'appropriata funzione $\mathrm{ar}\colon \mathrm{C}_{\mathfrak{R}} \to \mathbb{N}$ di arietà e poniamo $\mathtt{P} \in \textsc{Rec}$ se e solo se

(A) $\mathrm{ar}(\mathtt{P}) \neq 0$, e

(B) se $\mathtt{P}$ is $\mathtt{Min}(\mathtt{Q})$ e $\mathtt{Q}$ calcola qualche $f\colon \mathbb{N}^{k+1} \to \mathbb{N}$, allora per ogni $\vec{x}$ c'è un y tale che $f(\vec{x}, y) = 0$.

Notiamo che verificare (A) è routine, ma garantire (B) è molto più difficile.

Possiamo dare un'idea della dimostrazione del Teorema di forma normale di Kleene 9.37. Dato un programma $\mathtt{P}$ per una funzione ricorsiva $f\colon \mathbb{N}^k \to \mathbb{N}$, la **computazione completa** di $\mathtt{P}$ sull'*input* $\vec{x} = (x_0, \ldots, x_{k-1})$ è la sequenza che riporta tutti i calcoli che portano a $f(\vec{x})$. La definizione formale è un po' complessa, dato che dobbiamo codificare ogni cosa (programmi, sequenze di computi, ...) nei numeri naturali. Una volta che ciò è stato fatto, si definiscono i predicati $\mathrm{K}_k \subseteq \mathbb{N}^{k+2}$ con $k > 0$ in modo che $\mathrm{K}_k(e, \vec{x}, y)$ valga se e solo se

- e è un programma per funzioni ricorsive che soddisfa (A),
- $y = \boldsymbol{J}(n, s)$ dove $s \in \mathrm{Seq}$ codifica i calcoli che testimoniano che n è il risultato voluto.

La definizione di K_k è per induzione sulla complessità del termine chiuso e. Data una funzione ricorsiva $f\colon \mathbb{N}^k \to \mathbb{N}$ scegliamo un programma $\mathtt{P}$ che la calcoli. Allora, per ogni $x_0, \ldots, x_{k-1}$ c'è una sequenza finita di calcoli che danno $f(\vec{x})$, e sia s il numero che codifica tale sequenza; allora $\mathrm{K}_k(\mathtt{P}, \vec{x}, \boldsymbol{J}(f(\vec{x}), s))$ vale e quindi $f(\vec{x}) = \big(\boldsymbol{\mu} y\, \mathrm{K}_k(\mathtt{P}, \vec{x}, y)\big)_0$.

9.F. Insiemi ricorsivamente enumerabili.

Definizione 9.40. Un insieme $A \subseteq \mathbb{N}^m$ si dice **ricorsivamente enumerabile** se è vuoto oppure è della forma $\mathrm{ran}(f)$ per qualche $f\colon \mathbb{N}^n \to \mathbb{N}^m$ ricorsiva.

In altre parole: un insieme ricorsivamente enumerabile non vuoto è ottenibile come *output* di un programma. Un esempio concreto di insieme ricorsivamente enumerabile è dato da un **insieme diofanteo**, cioè insieme della forma

$$\mathbb{N} \cap \{f(n_1, \dots, n_k) \mid n_1, \dots, n_k \in \mathbb{Z}\},$$

dove $f \in \mathbb{Z}[x_1, \dots, x_n]$. Nel Capitolo **??** dimostreremo il converso, cioè: ogni insieme ricorsivamente enumerabile è diofanteo.

Proposizione 9.41. *Ogni insieme ricorsivo è ricorsivamente enumerabile.*

Dimostrazione. Per l'Esercizio 9.31(iii) possiamo limitarci ai sottoinsiemi di $\mathbb{N}^k$ con $k = 1$: dato un $A \subseteq \mathbb{N}$ ricorsivo e non vuoto, dobbiamo trovare una $f\colon \mathbb{N} \to \mathbb{N}$ ricorsiva tale che $A = \operatorname{ran}(f)$. Se A è finito, $A = \{n_0, \dots, n_k\}$, allora

$$f(i) = \begin{cases} n_0 & \text{se } i = 0, \\ n_1 & \text{se } i = 1, \\ \vdots & \\ n_k & \text{se } i \geq k, \end{cases}$$

è ricorsiva per l'Esempio 9.9(D). Se A è infinito applichiamo la Proposizione 9.27. □

Il converso non vale: ci sono insiemi ricorsivamente enumerabili non ricorsivi. Per dimostrare ciò ricordiamo che il Teorema di forma normale di Kleene 9.37 asserisce che c'è un insieme elementarmente ricorsivo $\mathrm{K}_1 \subseteq \mathbb{N}^3$ tale che, posto

$$W_e = \{x \in \mathbb{N} \mid \exists y\, \mathrm{K}_1(e, x, y)\} \quad \text{e} \quad \varphi_e(x) = (\boldsymbol{\mu} y\, \mathrm{K}_1(e, x, y))_0,$$

ogni funzione ricorsiva unaria è di questa forma, vale a dire per ogni $f\colon \mathbb{N} \to \mathbb{N}$ ricorsiva c'è un $e \in \mathbb{N}$ tale che $W_e = \mathbb{N}$ e $f(x) = \varphi_e(x)$ per tutti gli $x \in \mathbb{N}$. Per verificare se φ_e è definita per un certo x, cioè se $x \in W_e$, è sufficiente dimostrare che c'è un y tale che $\mathrm{K}_1(e, x, y)$, e in questo caso diremo che il programma e termina se applicato all'*input* x. Sia

$$H = \{e \in \mathbb{N} \mid \exists y\, \mathrm{K}_1(e, e, y)\}$$

l'insieme dei programmi e che terminano se applicati a se stessi. È un insieme ricorsivamente enumerabile, dato che è la proiezione di un sottoinsieme ricorsivo (anzi: elementare ricorsivo) di $\mathbb{N}^2$. Se H fosse ricorsivo, allora $f(x) = (\boldsymbol{\mu} y\, [\boldsymbol{\chi}_{\mathrm{K}_1}(x, x, y) \cdot \overline{\operatorname{sgn}} \circ \boldsymbol{\chi}_H(x)])_0$ sarebbe una funzione ricorsiva unaria, quindi $f = \varphi_e$ per qualche $e \in \mathbb{N}$. Poiché $W_e = \mathbb{N}$ ne segue che $e \in H$ e dato che

$$f(x) = \begin{cases} \varphi_x(x) + 1 & \text{se } x \in H \\ 0 & \text{altrimenti} \end{cases}$$

allora $\varphi_e(e) = f(e) = \varphi_e(e) + 1$, una contraddizione.

Quindi abbiamo dimostrato il

Teorema 9.42. *H è ricorsivamente enumerabile, ma non ricorsvo.*

Corollario 9.43. *L'insieme $H_2 = \{(e, x) \in \mathbb{N}^2 \mid x \in W_e\}$ è ricorsivamente enumerabile, ma non ricorsvo.*

Dimostrazione. H_2 è chiaramente ricorsivamente enumerabile. Se fosse ricorsivo, allora anche $H = \{e \mid (e, e) \in H_2\}$ sarebbe ricorsivo. □

Esercizio 9.44. Dimostrare che un insieme ricorsivamente enumerabile è definibile in $(\mathbb{N}, +, \cdot)$.

Proposizione 9.45. *Se A è ricorsivamente enumerabile e infinito, allora $A = \mathrm{ran}(f)$ per una qualche funzione iniettiva e ricorsiva.*

Dimostrazione. Supponiamo $A = \mathrm{ran}(g)$ con g ricorsiva. Definiamo una funzione iniettiva $f\colon \mathbb{N} \to \mathbb{N}$ tale che $\mathrm{ran}(f) = \mathrm{ran}(g)$:

- $f(0) = g(0)$;
- $f(1) = g(i_1)$, dove i_1 è il primo $i > 0$ tale che $g(i) \neq g(0)$;
- $f(2) = g(i_2)$, dove i_2 è il primo $i > i_1$ tale che $g(i) \neq g(0), g(i_1)$;
- e così via.

La funzione f è chiaramente calcolabile e il risultato è dimostrato.

Se non vogliamo appellarci alla tesi di Church, argomentiamo così: definiamo $i\colon \mathbb{N} \to \mathbb{N}$ mediante ricorsione primitiva generalizzata

$$i(n) = \begin{cases} 0 & \text{se } n = 0, \\ h(n-1, \langle\!\langle i(0), \ldots, i(n-1) \rangle\!\rangle) & \text{se } n > 0, \end{cases}$$

dove

$$h(m, k) = \boldsymbol{\mu} j\, [\forall i < m\, g(j) \neq (\!(k)\!)_i].$$

Allora $g \circ i$ è la funzione cercata. □

Teorema 9.46. *Se un predicato 1-ario A e il suo complemento $\neg A$ sono ricorsivamente enumerabili, allora A e $\neg A$ sono ricorsivi.*

Dimostrazione. Supponiamo che $A = \mathrm{ran}(f)$ e $\neg A = \mathrm{ran}(g)$, con f e g ricorsive. Poiché gli insiemi ricorsivi sono chiusi per complementazione, è sufficiente verificare che A è ricorsivo. Si decide se $n \in A$ ragionando come segue: si calcolano i valori $f(0), g(0), f(1), g(1), \ldots$ fino a che non si raggiunge un k tale che $n = f(k)$ oppure $n = g(k)$; nel primo caso otteniamo che $n \in A$, nel secondo che $n \in \neg A$, cioè $n \notin A$. La procedura così descritta è effettiva e

quindi, per la tesi di Church, l'insieme A è ricorsivo. La verifica formale di questo fatto è data da

$$\boldsymbol{\chi}_A(x) = (\boldsymbol{\mu} n \left[((n)_0 = 1 \wedge f((n)_1) = x) \vee ((n)_0 = 0 \wedge g((n)_1) = x)\right])_0. \quad \square$$

La famiglia degli insiemi ricorsivamente enumerabili non è chiusa per complementi e quindi non può essere un'algebra di Boole. Tuttavia è un reticolo distributivo.

Teorema 9.47. *Se A e B sono ricorsivamente enumerabili, allora anche $A \cup B$ e $A \cap B$ lo sono.*

Dimostrazione. Il risultato è immediato se uno tra A e B è vuoto, quindi possiamo supporre che $A = \operatorname{ran}(f)$ e $B = \operatorname{ran}(g)$.

La funzione

$$h(n) = \begin{cases} f(m) & \text{se } n = 2m, \\ g(m) & \text{se } n = 2m+1, \end{cases}$$

è ricorsiva e $\operatorname{ran}(h) = A \cup B$.

Per dimostrare che $A \cap B$ è ricorsivamente enumerabile distinguiamo due casi. Se $A \cap B$ è finito, allora è ricorsivo e quindi è ricorsivamente enumerabile. Se $A \cap B$ è infinito definiremo una funzione ricorsiva k tale che

$$\{k(0), \dots, k(n+1)\} = \{a\} \cup C_n,$$

dove $a = \min(A \cap B)$ e

$$C_n = \{f(0), \dots, f(n)\} \cap \{g(0), \dots, g(n)\}.$$

Questa condizione assicura che $\operatorname{ran}(k) = A \cap B$.

La funzione k è definita da $k(0) = a$ e

$$k(n+1) = \begin{cases} \min[C_n \setminus \{k(0), \dots, k(n)\}] & \text{se } C_n \setminus \{k(0), \dots, k(n)\} \neq \emptyset, \\ a & \text{altrimenti.} \end{cases}$$

Chiaramente k è calcolabile, quindi è ricorsiva per la tesi di Church. $\square$

Esercizio 9.48. Senza usare la tesi di Church, verificare che la funzione k nella dimostrazione del Teorema 9.47 è ricorsiva.

9.G. Presentazioni alternative della funzioni ricorsive. Una funzione $f\colon \mathbb{N}^k \to \mathbb{N}$ è ricorsiva se e solo se $\check{f}\colon \mathbb{N} \to \mathbb{N}$ è ricorsiva, dove

$$f(x_1, \dots, x_k) = \check{f}(\Phi^k(x_1, \dots, x_k))$$

e $\Phi^k\colon \mathbb{N}^k \to \mathbb{N}$ è una biezione ricorsiva. (Questa è la parte (iv) dell'Esercizio 9.31 quando $\Phi^k = \boldsymbol{J}^k$ è ottenuta da $\boldsymbol{J}$ per composizione mediante le funzioni di proiezione.) Dato che $\boldsymbol{\mathcal{R}}$ è completamente determinato da $\boldsymbol{\mathcal{R}} \cap \mathbb{N}^{\mathbb{N}}$ e da una qualsiasi biezione ricorsiva delle sequenze finite, è naturale cercare una definizione di $\boldsymbol{\mathcal{R}} \cap \mathbb{N}^{\mathbb{N}}$ che utilizzi esclusivamente funzioni ricorsive 1-arie.

Nel corso dei calcoli che ci porteranno a questa definizione, otterremo anche una nuova caratterizzazione di $\mathcal{R}$ (Teorema 9.51). Il nostro primo obbiettivo è definire delle opportune varianti di $\boldsymbol{J}$ e $\boldsymbol{\beta}$.

La funzione $\lfloor\sqrt{n}\rfloor$ è elementarmente ricorsiva, così come lo sono

$$\mathrm{Exc}(n) = n \dot{-} (\lfloor\sqrt{n}\rfloor)^2$$
$$\overline{\boldsymbol{J}}(n,m) = ((n+m)^2+m)^2+n.$$

Osserviamo che $(\mathbb{N}, +, \mathrm{Exc})$ definisce l'insieme dei quadrati, quindi definisce la moltiplicazione (Esercizio 6.52).

Esercizio 9.49. Dimostrare che:

(i) se $\mathrm{Exc}(n+1) \neq 0$, allora $\mathrm{Exc}(n+1) = \mathrm{Exc}(n)+1$, and $\mathrm{Exc}\lfloor\sqrt{n+1}\rfloor = \mathrm{Exc}\lfloor\sqrt{n}\rfloor$,

(ii) $\mathrm{Exc}(\overline{\boldsymbol{J}}(n,m)) = n$ and $\mathrm{Exc}\lfloor\sqrt{\overline{\boldsymbol{J}}(n,m)}\rfloor = m$.

Quindi $\overline{(n)_0} = \mathrm{Exc}(n)$ e $\overline{(n)_0} = \mathrm{Exc}\lfloor\sqrt{n}\rfloor$ da cui

$$\forall n,m\ \Big(\overline{(\overline{\boldsymbol{J}}(n,m))_0} = n \wedge \overline{(\overline{\boldsymbol{J}}(n,m))_1} = m\Big)$$

La funzione

$$\overline{\boldsymbol{\beta}}(n,i) = \mathrm{Res}(\overline{(x)_0}, 1+(i+1)\overline{(x)_1})$$

è l'analogo della funzione $\boldsymbol{\beta}$ di Gödel.

L'**inversione** di una suriezione $f\colon \mathbb{N} \twoheadrightarrow \mathbb{N}$ è la mappa $f^{-1}\colon \mathbb{N} \rightarrowtail \mathbb{N}$ definita da $f^{-1}(m) = \boldsymbol{\mu} n\, f(n) = m$. Una famiglia $\mathcal{F}$ di funzioni finitarie è **chiusa per inversione** se $f^{-1} \in \mathcal{F}$ per ogni suriezione $f \in \mathcal{F} \cap \mathbb{N}^{\mathbb{N}}$.

Esercizio 9.50. Dimostrare che:

(i) $\mathrm{ran}\,\mathrm{Exc} = \mathbb{N}$, e $\mathrm{Exc}^{-1}(2x) = x^2+2x$ and $\mathrm{Exc}^{-1}(2x+1) = x^2+4x+2$;

(ii) $\mathrm{Exc} \circ S \circ \mathrm{Exc}^{-1}(2x) = 0 = c_0(x)$;

(iii) $\mathrm{Exc}(\mathrm{Exc}^{-1}(2x+2y)+3x+y+4) = x \ominus y$, dove

$$x \ominus y = \begin{cases} x-y & \text{se } y \leq x, \\ 3x+y+3 & \text{altrimenti;} \end{cases}$$

(iv) $\mathrm{ran}(\mathrm{Exc} \circ S) = \mathbb{N}$ e $\mathrm{Exc} \circ (\mathrm{Exc} \circ S)^{-1} = x \dot{-} 1$;

(v) $\boldsymbol{\chi}_{\geq}(x,y) = \mathrm{sgn}\,((x \ominus y) \ominus (3x+y+3))$;

(vi) $\boldsymbol{\chi}_{\mathrm{PARI}}(x) = \mathrm{Exc} \circ S \circ S \circ \mathrm{Exc}^{-1}(x)$;

(vii) la funzione $F(x) \stackrel{\mathrm{def}}{=} 2\,\mathrm{Exc}(x) + \overline{\mathrm{sgn}} \circ \boldsymbol{\chi}_{\mathrm{PARI}}(x)$ è suriettiva, $F^{-1}(2y) = y^2+y$ e $F^{-1}(2y+1) = (y+1)^2+y$, e $\lfloor x/2 \rfloor = \mathrm{Exc}(F^{-1}(x))$.

Teorema 9.51. *$\mathcal{R}$ è la più piccola classe di funzioni finitarie contenenti $I^n_k, +, S, \mathrm{Exc}$, chiusa per composizione ed inversione.*

Dimostrazione. Sia $\mathcal{F}$ la più piccola classe di funzioni finitarie contenenti I^n_k, $+$, S, Exc e chiusa per composizione ed inversione. Per la Proposizione 9.23 è sufficiente dimostrare che

(9.6) la moltiplicazione e la funzione caratteristica di $\leq$ sono in $\mathcal{F}$

e che

(9.7) $\mathcal{F}$ è chiusa per minimizzazione.

Poiché $\mathrm{Exc}^{-1}(2x) \ominus 2x = x^2$, $\mathrm{sgn}(x) = \mathrm{Exc}(S(x^2))$, e poiché $2x = I^1_0(x) + I^1_0(x)$ è in $\mathcal{F}$, dall'Esercizio 9.50 segue che le seguenti funzioni sono in $\mathcal{F}$:

$$c_n \quad (n \in \mathbb{N}), \qquad \ominus, \qquad x \mapsto x^2, \qquad \boldsymbol{\chi}_{\mathrm{PARI}}, \qquad \boldsymbol{\chi}_{\geq}, \qquad x \mapsto \lfloor x/2 \rfloor.$$

Poiché

$$\boldsymbol{\chi}_{\leq}(x,y) = \boldsymbol{\chi}_{\geq}(I^2_1(x,y), I^2_0(x,y)) \text{ e } x \cdot y = \lfloor ((x+y)^2 - (x^2+y^2))/2 \rfloor,$$

la (9.6) vale.

Per dimostrare la (9.7) dobbiamo innanzitutto verificare che $\lfloor \sqrt{x} \rfloor$ è in $\mathcal{F}$. Questo segue da $\lfloor \sqrt{x} \rfloor = G(x \ominus \mathrm{Exc}\, x) = G(x - \mathrm{Exc}\, x)$ dove $G(x) = \lfloor (\mathrm{Exc}(x \dot{-} 1)/2) \rfloor$, e dal fatto che $G(x^2) = x$. Quindi la funzione $\overline{\boldsymbol{J}}$ e le sue inverse $\overline{(\cdot)_0}$ e $\overline{(\cdot)_1}$ sono in $\mathcal{F}$.

Supponiamo $f \in \mathcal{F}$ sia $k+1$-aria e tale che $\forall \vec{x}\, \exists y\, [f(\vec{x}, y) = 0]$: dobbiamo dimostrare che $g(\vec{x}) = \boldsymbol{\mu} y\, [f(\vec{x}, y) = 0]$ è in $\mathcal{F}$.

Consideriamo dapprima il caso in cui $k = 1$, cioè $g(x) = \boldsymbol{\mu} y\, [f(x, y) = 0]$.

Fatto 9.51.1. $g(x) = \overline{(\boldsymbol{\mu} z\, [f(\overline{(z)_0}, \overline{(z)_1}) = 0 \wedge \overline{(z)_0} = x])_1}$.

Dimostrazione del Fatto. Sia $z = \overline{\boldsymbol{J}}(x, g(x))$. Allora

$$f(\overline{(z)_0}, \overline{(z)_1}) = 0 \wedge \overline{(z)_0} = x$$

e se w è tale che

$$f(\overline{(w)_0}, \overline{(w)_1}) = 0 \wedge \overline{(w)_0} = x$$

allora $g(x) \leq \overline{(w)_1}$ e quindi $\overline{\boldsymbol{J}(x, g(x))} \leq w$. □

La funzione $h\colon \mathbb{N} \to \mathbb{N}$

$$h(z) = \overline{\mathrm{sgn}}(f(\overline{(z)_0}, \overline{(z)_1})) \cdot \overline{(z)_0}$$

è in $\mathcal{F}$. Per ipotesi, per ogni x c'è un y tale che $f(x, y) = 0$, quindi ponendo $z = \overline{\boldsymbol{J}}(x, y)$ si ha che $h(z) = x$. Essendo x arbitrario, ne segue che $\mathrm{ran}\, h = \mathbb{N}$, e poiché

$$h^{-1}(x) = \boldsymbol{\mu} z\, [f(\overline{(z)_0}, \overline{(z)_1}) = 0 \wedge \overline{(z)_0} = x],$$

$(h^{-1}(x))_1$ è un y tale che $f(x, y) = 0$. Dobbiamo verificare che è il minimo y siffatto: ma questo è chiaro dato che $\overline{\boldsymbol{J}}$ è crescente in entrambe le coordinate. Quindi $g = h^{-1}$ è in $\mathcal{F}$ come richiesto.

Consideriamo il caso generale in cui f è $k+1$-aria, e procediamo per induzione su $k \geq 1$. Il caso $k = 1$ è stato appena dimostrato, quindi possiamo supporre che $k = n+1$ con $n \geq 1$. La funzione

$$f'(x_1, x_2, \ldots, x_n, y) = f(\overline{(x_1)_0}, \overline{(x_1)_1}, x_2, \ldots, x_n, y)$$

è $n+1$-aria e per ipotesi induttiva $g'(x_1, \ldots, x_n) = \boldsymbol{\mu} y\,[f'(x_1, \ldots, x_n, y) = 0]$ è in $\mathcal{F}$. Ne segue che

$$g(x_0, x_1, \ldots, x_n) = \boldsymbol{\mu} y\,[f(x_0, x_1, \ldots, x_n, y) = 0] = g'(\overline{\boldsymbol{J}}(x_0, x_1), \ldots, x_n)$$

è in $\mathcal{F}$. □

Una famiglia di funzioni unarie $\mathcal{F}$ è chiusa per somme se $f, g \in \mathcal{F} \Rightarrow f+g \in \mathcal{F}$, dove $(f+g)(n) = f(n) + g(n)$.

Teorema 9.52. *$\boldsymbol{\mathcal{R}} \cap \mathbb{N}^{\mathbb{N}}$ è la più piccola classe di funzioni unarie contenente S e* Exc*, chiusa per composizione, addizione e inversione.*

Dimostrazione. Sia $\mathcal{F} \subseteq \mathbb{N}^{\mathbb{N}}$ la più piccola famiglia di funzioni contenente S e Exc,e chiusa per composizione, somme, inversione. Poiché $\mathcal{F} \subseteq \boldsymbol{\mathcal{R}} \cap \mathbb{N}^{\mathbb{N}}$, è sufficiente verificare l'inclusione inversa. Innanzi tutto osserviamo che $I^1_0 = \mathrm{Exc} \circ \mathrm{Exc}^{-1} \in \mathcal{F}$. È sufficiente dimostrare che

$$\forall m \geq 1\, \forall f_1, \ldots f_m \in \mathcal{F}\, \forall g \in \boldsymbol{\mathcal{R}} \cap \mathbb{N}^{\mathbb{N}^m}\, (g(f_1, \ldots, f_m) \in \mathcal{F})$$

dove $g(f_1, \ldots, f_m)$ è la funzione unaria $x \mapsto g(f_1(x), \ldots, f_m(x))$. Infatti, da $m = 1$ e $f_1 = I^1_0$ si ottiene $g \in \mathcal{F}$ per ogni $g \in \boldsymbol{\mathcal{R}} \cap \mathbb{N}^{\mathbb{N}}$, che è quanto dobbiamo dimostrare. Sia

$$\mathcal{G} = \{g \mid \mathrm{dom}(g) = \mathbb{N}^m \Rightarrow \forall f_1, \ldots f_m \in \mathcal{F}\, (g(f_1, \ldots, f_m) \in \mathcal{F})\}.$$

Osserviamo che $\mathcal{G} \cap \mathbb{N}^{\mathbb{N}} = \mathcal{F}$, quindi è sufficiente dimostrare che $\mathcal{G} = \boldsymbol{\mathcal{R}}$. Dalla definizione di $\mathcal{G}$ segue che $+, S, \mathrm{Exc}, I^n_k \in \mathcal{G}$ per tutti i $k < n$, e che $\mathcal{G}$ è chiusa per inversioni, quindi per il Teorema 9.51 è sufficiente dimostrare che $\mathcal{G}$ è chiusa per composizione. Supponiamo che $g \in \mathcal{G}$ sia m-aria e $h_1, \ldots, h_m \in \mathcal{G}$ sono n-arie, e che

$$k(x_1, \ldots, x_n) = g(h_1(x_1, \ldots, x_n), \ldots, h_m(x_1, \ldots, x_n)).$$

Se $f_1, \ldots f_n \in \mathcal{F}$ allora

$$\begin{aligned} k(f_1, \ldots, f_n)(x) &= k(f_1(x), \ldots, f_n(x)) \\ &= g(h_1(f_1(x), \ldots, f_n(x)), \ldots, h_m(f_1(x), \ldots, f_n(x))) \\ &= g\Big(h_1(f_1, \ldots, f_n)(x), \ldots, h_m(f_1, \ldots, f_n)(x)\Big) \\ &= g(h_1(f_1, \ldots, f_n), \ldots, h_m(f_1, \ldots, f_n))(x) \end{aligned}$$

e poiché $h_1(f_1, \ldots, f_n), \ldots, h_m(f_1, \ldots, f_n) \in \mathcal{F}$ e $g \in \mathcal{G}$, allora $k(f_1, \ldots, f_n) \in \mathcal{F}$. Quindi $\mathcal{G}$ è chiusa per composizione, che è quanto dovevamo dimostrare. □

Ricordiamo (Osservazione 9.14) che una famiglia di funzioni $\mathcal{F}$ è chiusa per iterazioni senza parametri se $g(n) = f^{(n)}(0)$ è in $\mathcal{F}$, per ogni $f \in \mathcal{F} \cap \mathbb{N}^{\mathbb{N}}$.

Enunciamo e non dimostriamo i prossimi due risultati.

Teorema 9.53. *$\boldsymbol{\mathcal{P}}$ è la più piccola classe di funzioni contenente S,* Exc*, $+$, I^n_k, e chiusa per composizione e iterazioni senza parametri.*

Teorema 9.54. *$\boldsymbol{\mathcal{P}} \cap \mathbb{N}^{\mathbb{N}}$ è la più piccola classe di funzioni contenente S e* Exc*, e chiusa per composizione, somme e iterazioni senza parametri.*

Esercizi

Esercizio 9.55. Sia $\mathcal{F}$ la più piccola famiglia di funzioni chiusa per composizione e ricorsione primitiva e contenente c_0, S e le proiezioni I^n_k. Dimostrare che le seguenti funzioni e predicati sono in $\mathcal{F}$:

- le operazioni $x + y$, $x \cdot y$, x^y, $x \dot{-} 1$;
- $\overline{\mathrm{sgn}}(x)0^x$, $\mathrm{sgn}(x) = 0^{0^x}$, $x \dot{-} y$, $|x - y|$;
- $x < y$, $x \leq y$, $x = y$, $\lfloor x/y \rfloor$;
- se $f \in \mathcal{F}$ è $k+1$-aria, allora $\sum f, \prod f \in \mathcal{F}$.

Concludere che $\boldsymbol{\mathcal{P}} \subseteq \mathcal{F}$.

Esercizio 9.56. Sia $\mathcal{F} \supseteq \boldsymbol{\mathcal{E}}$ una famiglia di funzioni chiusa per composizione e per somma e prodotto generalizzato. Dimostrare che se la funzione g e il predicato A sono in $\mathcal{F}$, allora le seguenti funzioni sono in $\mathcal{F}$:

$$f_1(\vec{x}, y) = \begin{cases} \min\{z \leq y \mid A(\vec{x}, z)\} & \text{se questo insieme è non vuoto,} \\ 0 & \text{altrimenti;} \end{cases}$$

$$f_2(\vec{x}, y) = \begin{cases} \max\{z \leq y \mid A(\vec{x}, z)\} & \text{se questo insieme è non vuoto,} \\ y & \text{altrimenti;} \end{cases}$$

$$f_3(\vec{x}, y) = \begin{cases} \max\{z \leq y \mid A(\vec{x}, z)\} & \text{se questo insieme è non vuoto,} \\ 0 & \text{altrimenti;} \end{cases}$$

$$f_4(\vec{x}, y) = \min\{g(\vec{x}, z) \mid z \leq y\};$$

$$f_5(\vec{x}, y) = \max\{g(\vec{x}, z) \mid z \leq y\}.$$

Esercizio 9.57. Dimostrare che le seguenti funzioni e predicati sono in $\boldsymbol{\mathcal{E}}$:

(i) la relazione di divisibilità $x \mid y$, l'insieme Pr dei numeri primi e il predicato $P(k, x)$: "x è il k-esimo primo";

(ii) la funzione $\mathbf{p}\colon \mathbb{N} \to \mathbb{N}$ che enumera Pr [suggerimento: $\mathbf{p}(k) \leq 2^{2^k}$];

(iii) la codifica delle sequenze mediante esponenziale vista nella Sezione 6.B.2, cioè le funzioni $\mathbf{e}\colon \mathbb{N}^2 \to \mathbb{N}$ e $\mathbf{l}\colon \mathbb{N} \to \mathbb{N}$ definite a pagina 120 e l'insieme $\mathrm{Seq}^* = \left\{\mathbf{p}(0)^{n_0+1} \cdots \mathbf{p}(k)^{n_k+1} \mid n_0, \ldots, n_k \in \mathbb{N}\right\}$;

(iv) le funzioni mcm e mcd;

(v) la funzione che ad n associa il numero di primi $\leq n$;

(vi) la funzione φ di Eulero, dove $\varphi(n)$ è il numero dei $k < n$ che sono coprimi con n, e per definizione $\varphi(0) = 0$;

(vii) le funzioni ω e Ω definite da $\omega(0) = \omega(1) = \Omega(0) = \Omega(1) = 0$ e se $m = p_1^{k_1} \cdots p_n^{k_n}$ con $p_1 < \cdots < p_n$ primi, allora $\omega(m) = n$ e $\Omega(m) = k_1 + \cdots + k_n$;

(viii) la funzione $\sigma_k\colon \mathbb{N} \to \mathbb{N}$ che manda 0 in 0 e che ad $n > 0$ associa $\sum_{d|n} d^k$ la somma dei divisori di n elevati alla potenza k. In particolare $\sigma_0(n)$ conta il numero dei divisori di n e $\sigma_1(n)$ è la somma dei divisori di n. Quindi l'insieme dei **numeri perfetti**, cioè dei numeri n che sono somma dei loro divisori $d < n$, ovvero tali che $\sigma_1(n) = 2n$, è elementare;

(ix) la funzione $f\colon \mathbb{N}^2 \to \mathbb{N}$ definita da

$$f(n,m) = \begin{cases} \binom{n}{m} & \text{se } m \leq n, \\ 0 & \text{altrimenti;} \end{cases}$$

(x) la funzione $L_b\colon \mathbb{N} \to \{0, \dots, b-1\}$, con $b > 1$, che associa ad n l'ultima cifra nell'espansione in base b di n.

Esercizio 9.58. (i) Data $f\colon \mathbb{N}^{k+1} \to \mathbb{N}$ sia $f^*\colon \mathbb{N}^{k+1} \to \mathbb{N}$ definita da

$$f^*(\vec{x}, y) = 2^{f(\vec{x},0)+1} \cdot 3^{f(\vec{x},1)+1} \cdots \mathbf{p}(y)^{f(\vec{x},y)+1}$$

dove $\mathbf{p}(i)$ è l'i-esimo numero primo (Esercizio 9.57). In altre parole: f^* è l'analogo della funzione-memoria f^{m} per la codifica vista nella Sezione 6.B.2. Dimostrare che

$$f \in \mathcal{E} \Leftrightarrow f^* \in \mathcal{E}.$$

(ii) Supponiamo che $h\colon \mathbb{N}^{n+1} \to \mathbb{N}$ sia ottenuta per ricorsione primitiva a partire da $g\colon \mathbb{N}^{n+2} \to \mathbb{N}$ e $f\colon \mathbb{N}^n \to \mathbb{N}$. (Se $n = 0$, cioè la ricorsione è senza parametri, si intende che f è un numero naturale.) Supponiamo inoltre che

$$\forall \vec{x} \in \mathbb{N}^{n+1}\, [h(\vec{x}) \leq k(\vec{x})].$$

Dimostrare che se $f, g, k \in \mathcal{E}$ allora $h \in \mathcal{E}$. Questo fatto si esprime dicendo che $\mathcal{E}$ è chiusa per **ricorsione primitiva limitata**.

(iii) Dimostrare che

$$f \in \mathcal{E} \Leftrightarrow f^{\mathrm{m}} \in \mathcal{E}.$$

(iv) Ripetere la parte (ii) nel caso in cui h sia ottenuta da g e f mediante ricorsione primitiva generalizzata (Definizione 9.18).

(v) Dimostrare che $\mathcal{E}$ è la più piccola famiglia di funzioni finitarie su $\mathbb{N}$ contenente c_0, S, I^n_k e chiusa per composizione e ricorsione limitata.

Esercizio 9.59. Dimostrare che la **successione di Fibonacci** definita da $F(0) = F(1) = 1$ e $F(n) = F(n-1) + F(n-2)$, per $n \geq 2$, è elementare ricorsiva.

Esercizio 9.60. Sia $E\colon \mathbb{N}^2 \to \mathbb{N}$ la funzione primitiva ricorsiva definita da

$$\begin{cases} E(x,0) = x \\ E(x,y+1) = x^{E(x,y)}. \end{cases}$$

Dimostrare che:

(i) $x \leq E(x,y)$;

(ii) $E(x,y) < E(x,y+1)$, se $x > 1$;

(iii) $E(x,y) < E(x+1,y)$, se $x > 1$;

(iv) $E(x,y) + E(x,z) < E(x, \max(y,z)+1)$, se $x > 1$;

(v) $E(x,y) \cdot E(x,z) < E(x, \max(y,z)+1)$, se $x > 1$;

(vi) $E(x,y)^{E(x,z)} < E(x, \max(y+1, z+2))$, se $x > 1$;

(vii) $E(E(x,y),z) \leq E(x, y+2z)$, se $x > 1$;

(viii) se $f \in \mathcal{E}$ è k-aria, allora c'è un $c \in \mathbb{N}$ tale che

$$\max(\vec{x}) > 1 \Rightarrow f(\vec{x}) < E(\max(\vec{x}), c);$$

(ix) $E \notin \mathcal{E}$.

Esercizio 9.61. Dimostrare che se $f\colon \mathbb{N} \to \mathbb{N}$ è in $\boldsymbol{\mathcal{P}}$, allora la funzione $(x, n) \mapsto f^{(n)}(x)$ che codifica la successione delle iterate $f^{(n)}$ è in $\boldsymbol{\mathcal{P}}$.

È vero l'analogo enunciato per $\boldsymbol{\mathcal{E}}$?

Esercizio 9.62. Sia $\mathcal{F} = \boldsymbol{\mathcal{P}}$ oppure $\mathcal{F} = \boldsymbol{\mathcal{R}}$. Siano h_0, h_1 definite mediante la ricorsione simultanea

$$\begin{cases} h_0(\vec{x}, 0) = f_0(\vec{x}) \\ h_0(\vec{x}, y+1) = g_0(\vec{x}, y, h_0(\vec{x}, y), h_1(\vec{x}, y)) \end{cases}$$
$$\begin{cases} h_1(\vec{x}, 0) = f_1(\vec{x}) \\ h_1(\vec{x}, y+1) = g_1(\vec{x}, y, h_0(\vec{x}, y), h_1(\vec{x}, y)). \end{cases}$$

Dimostrare che se $f_0, f_1, g_0, g_1 \in \mathcal{F}$, allora $h_0, h_1 \in \mathcal{F}$.

Esercizio 9.63. Verificare che per ogni $m \in \mathbb{N}$ la funzione

$$\mathrm{Ack}_m\colon \mathbb{N} \to \mathbb{N}, \quad n \mapsto \mathrm{Ack}(m, n)$$

è primitiva ricorsiva, dove Ack è la funzione di Ackermann.

Esercizio 9.64. Dimostrare il Teorema 9.35 verificando le seguenti affermazioni:

(i) $y < \mathrm{Ack}(x, y)$;

(ii) $\mathrm{Ack}(x, y) < \mathrm{Ack}(x, y+1)$;

(iii) $\mathrm{Ack}(x, y+1) \leq \mathrm{Ack}(x+1, y)$;

(iv) $\mathrm{Ack}(x, y) \leq \mathrm{Ack}(x+1, y)$;

(v) $\mathrm{Ack}(1, y) = y + 2$;

(vi) $\mathrm{Ack}(2, y) = 2y + 3$;

(vii) per ogni $c_1, \ldots, c_n$ c'è un d tale che

$$\forall x \left(\textstyle\sum_{1 \leq i \leq n} \mathrm{Ack}(c_i, x) \leq \mathrm{Ack}(d, x) \right);$$

(viii) per ogni funzione n-aria $f \in \boldsymbol{\mathcal{P}}$ c'è un c tale che

$$\forall x_1, \ldots, x_n \, (f(x_1, \ldots, x_n) < \mathrm{Ack}(c, x_1 + \cdots + x_n)).$$

Esercizio 9.65. Sia $\mathcal{F}$ una famiglia di funzioni come nell'enunciato della Proposizione 9.23. Dimostrare che le seguenti funzioni e predicati sono in $\mathcal{F}$:

(i) $\overline{\mathrm{sgn}}(n) = \boldsymbol{\chi}_{\leq}(n+n, n)$ e $\mathrm{sgn} = \overline{\mathrm{sgn}} \circ \overline{\mathrm{sgn}}$.

(ii) I predicati in $\mathcal{F}$ sono chiusi per operazioni booleane (negazione, conginuzione, disgiunzione). Quindi $=$, $\neq$, e $\leq$ sono in $\mathcal{F}$.

(iii) $c_k\colon \mathbb{N} \to \mathbb{N}$, $n \mapsto k$, sono in $\mathcal{F}$, dato che $c_0(n) = \boldsymbol{\mu} x \, [n = n + x]$, $c_1(n) = \boldsymbol{\mu} x \, [n \neq n + x]$, e $c_{k+1}(n) = c_k(n) + c_1(n)$.

(iv) Se $P \in \mathcal{F}$ è $n+1$-ario, allora $Q(\vec{x}, y) \Leftrightarrow \exists z < y \, P(\vec{x}, z)$ è in $\mathcal{F}$.

(v) $\boldsymbol{J}, (\cdot)_0, (\cdot)_1, \boldsymbol{\beta} \in \mathcal{F}$.

(vi) $f \in \mathcal{F} \Leftrightarrow f^{\mathrm{m}} \in \mathcal{F}$, dove f^{m} è la funzione-memoria di f.

Sia h ottenuta per ricorsione primitiva da $f, g \in \mathcal{F}$ come nella Definizione 9.13, e sia

$$G(\vec{x}, n, m) = \begin{cases} f(\vec{x}, n) & \text{se } m = 0, \\ g(\vec{x}, n, m) & \text{altrimenti} \end{cases}$$

Allora $G \in \mathcal{F}$ e $h(\vec{x}, n) = G(\vec{x}, n, h^{\mathrm{m}}(\vec{x}, n))$. Dato che

$$h^{\mathrm{m}}(\vec{x}, n) = \boldsymbol{\mu} y \Big[\mathrm{Seq}(y) \wedge \boldsymbol{\beta}(y, 0) = n \wedge \forall i < n \, \exists z \leq y \, (\forall j < i \, ((\!(y)\!)_j = (\!(z)\!)_i) \wedge (\!(y)\!)_i = G(z, i, n)) \Big]$$

è in $\mathcal{F}$, ne segue che $h \in \mathcal{F}$.

Concludere che $\mathcal{F} = \boldsymbol{\mathcal{R}}$.

Esercizio 9.66. Se $\mathcal{F}$ è chiusa per ricorsione primitiva, composizione, e contiene I^2_1, allora $\mathcal{F}$ è chiusa per iterazioni. In particolare, $\mathcal{P}$ è chiusa per iterazioni.

Note e osservazioni

La rostra trattazione delle funzioni ricorsive segue abbastanza fedelmente [**Mon75**, Capitolo 1]. Le funzioni elementari ricorsive $\mathcal{E}$, introdotte da Kalmár nel 1943, sono le funzioni rilevanti per l'informatica. È possibile evitare la somma e il prodotto generalizzati nella definizione di funzione elementare ricorsiva; infatti $\mathcal{E}$ è la più piccola classe chiusa per composizione e contenente le proiezioni ed un insieme fissato di funzioni di base, quali per esempio $\{S, x \dot{-} y, \lfloor x/y \rfloor, x^y\}$, o $\{x+y, x \dot{-} y, \lfloor x/y \rfloor, 2^y\}$, oppure $\left\{x+y, x^2, x \mod y, 2^y\right\}$ [**Maz02**]. Le famiglie $\mathcal{P}$ e $\mathcal{R}$ erano state definite in precedenza, per catturare la nozione intuitiva di funzione calcolabile, da numerosi mathematic, tra cui Gödel, Turing, e Post. Negli anni venti del XX secolo Ackermann e Sudan, a quel tempo studenti di Hilbert, diedero i primi esempi di funzioni calcolabili ma non primitive ricorsive. La funzione Ack è una variante, dovuta a Péter e R. Robinson, della definizione originale di Ackermann e Sudan.

10. Ordinali e cardinali

10.A. Buoni ordini e ordinali. Fissiamo due insiemi ordinati $(P, \leq_P)$ e $(Q, \leq_Q)$. Se P e Q sono disgiunti possiamo definire un ordine $\preceq$ detto ordinamento somma su $P \cup Q$ ponendo gli elementi di P prima di quelli di Q cioè $x \preceq y$ se e solo se

$$(x \in P \wedge y \in Q) \vee (x, y \in P \wedge x \leq_P y) \vee (x, y \in Q \wedge x \leq_Q y).$$

È immediato verificare che se $(P', \leq_{P'}) \cong (P, \leq_P)$, $(Q', \leq_{Q'}) \cong (Q, \leq_Q)$ e $P' \cap Q' = \emptyset$, allora l'ordinamento somma su $P' \cup Q'$ è isomorfo all'ordinamento somma su $P \cup Q$. Quindi possiamo definire la **somma** di due ordini parziali

$$(P, \leq_P) + (Q, \leq_Q),$$

non necessariamente disgiunti, come l'ordinamento somma sull'unione disgiunta di P e Q, cioè l'ordinamento somma su $P' \cup Q'$ dove $(P', \leq_{P'})$ e $(Q', \leq_{Q'})$ sono isomorfi a $(P, \leq_P)$ e $(Q, \leq_Q)$ rispettivamente. In altre parole: la somma è definita a meno di isomorfismi. (Quando è necessario essere più precisi possiamo prendere, per esempio $P' = \{0\} \times P$ e $Q' = \{1\} \times Q$.) Dalla definizione di ordinamento somma discende subito che

$$(P + Q) + R \cong P + (Q + R), \tag{10.1}$$

cioè la somma di ordini parziali è associativa.

Il **prodotto** di $(P, \leq_P)$ e $(Q, \leq_Q)$, in simboli $(P, \leq_P) \times (Q, \leq_Q)$ o più semplicemente $P \times Q$, è l'**ordinamento lessicografico inverso** $\leq$ sul prodotto cartesiano $P \times Q$ definito da

$$(p_1, q_1) \leq (p_2, q_2) \Leftrightarrow q_1 \leq_Q q_2 \vee (q_1 = q_2 \wedge p_1 \leq_P p_2).$$

Se invece consideriamo il prodotto delle strutture $(P, \leq_P)$ e $(Q, \leq_Q)$ si ottiene l'**ordinamento prodotto** su $P \times Q$ definito da

$$(p_1, q_1) \trianglelefteq (p_2, q_2) \Leftrightarrow (p_1 \leq_P p_2 \wedge q_1 \leq_Q q_2).$$

Anche nel caso del prodotto abbiamo un'operazione associativa, nel senso che

$$(P \times Q) \times R \cong P \times (Q \times R). \tag{10.2}$$

Esercizio 10.1. Dimostrare che:

(i) se $(P, \leq_P)$ e $(Q, \leq_Q)$ sono ordini lineari, allora $P + Q$ e $P \times Q$ sono ordini lineari.

Dimostrare con un controesempio che questo non vale se al posto dell'ordinamento lessicografico si considera l'ordinamento prodotto;

(ii) se Q' è segmento iniziale di Q, allora $P + Q'$ e $P \times Q'$ sono segmenti iniziali di $P + Q$ e $P \times Q$, rispettivamente.

Dimostrare con un controesempio che se P' è segmento iniziale di P, allora non segue che $P' + Q$ e $P' \times Q$ sono segmenti iniziali di $P + Q$ e $P \times Q$.

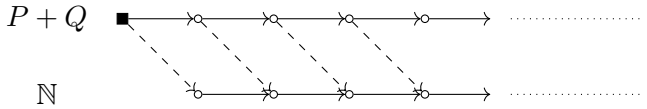
Cominciamo a studiare la somma di ordini lineari.

Se P e Q sono ordini lineari finiti di taglia n e m, allora $P + Q$ e $Q + P$ sono ordini lineari di taglia $n + m$ e quindi sono isomorfi,

$$P + Q \cong Q + P.$$

L'assunzione che P e Q siano finiti è essenziale. Se P è l'ordinamento con un solo elemento $\blacksquare$ e $Q = \mathbb{N}$ è descritto dal diagramma

allora $P + Q$ è isomorfo a Q, cioè ad $\mathbb{N}$



Se identifichiamo P con $\{-1\}$ e Q con la successione di reali $\{\frac{n}{n+1} \mid n \in \mathbb{N}\}$, allora $P + Q$ è identificabile con $\{-1\} \cup \{\frac{n}{n+1} \mid n \in \mathbb{N}\}$. Invece $Q + P$ ha un elemento massimo

e quindi non è isomorfo a $\mathbb{N}$, cioè a $P+Q$. Osserviamo che questo ordinamento è isomorfo all'insieme di reali

$$\{\tfrac{n}{n+1} \mid n \in \mathbb{N}\} \cup \{1\}.$$

L'ordine lineare $\mathbb{Z}_- = \{k \in \mathbb{Z} \mid k < 0\}$ ha come diagramma

quindi $\mathbb{Z}_- + \mathbb{N} \cong \mathbb{Z}$. Invece $\mathbb{N} + \mathbb{Z}_-$ è l'ordine lineare che ha minimo e massimo isomorfo all'insieme di reali

$$\{-1 + \tfrac{n}{n+1} \mid n \in \mathbb{N}\} \cup \{1 - \tfrac{n}{n+1} \mid n \in \mathbb{N}\}$$

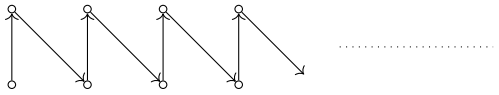
e ha per diagramma

L'ordine $\mathbb{N} + \mathbb{N}$ ha per diagramma

quindi non è isomorfo a $P + \mathbb{N}$ o a $\mathbb{N} + P$, ma è isomorfo tanto all'insieme di reali

$$\{\tfrac{n}{n+1} \mid n \in \mathbb{N}\} \cup \{\tfrac{2n+1}{n+1} \mid n \in \mathbb{N}\}$$

quanto a $\mathbb{N} \times 2$ dove 2 è l'ordine lineare con due elementi $\circ \longrightarrow \circ$. Più in generale $P + P \cong P \times 2$ per ogni insieme ordinato P. Invece $2 \times \mathbb{N}$ è isomorfo a $\mathbb{N}$



Quindi $P \times Q \ncong Q \times P$. Naturalmente, se P e Q sono ordini lineari finiti di taglia n e m rispettivamente, allora $P \times Q$ e $Q \times P$ sono ordini lineari con nm elementi e quindi sono isomorfi.

Un ordine lineare $(P, \leq)$ è un **buon ordine** se ogni $\emptyset \neq X \subseteq P$ ha un minimo. Ogni ordine lineare finito è un buon ordine, $\mathbb{N}$ è un buon ordine, ogni sottoinsieme di un buon ordine è un buon ordine con l'ordinamento indotto. Invece $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$ non sono buoni ordini.

Osservazione 10.2. Le nozioni di buon ordine non è formalizzabile prim'ordine, dato che si quantifica su sottoinsiemi arbitrari. Nella Sezione 32 dimostreremo che non c'è nessun enunciato σ di un linguaggio L del prim'ordine contenente un simbolo di relazione binaria $\leq$ tale che i modelli di σ sono tutti e soli gli insiemi bene ordinati.

Proposizione 10.3. *Se $(P, \leq)$ è un buon ordine e $Q \subseteq P$ è un segmento iniziale, allora $Q = P$ oppure $Q = \{x \in P \mid x < a\}$ per qualche $a \in P$.*

Dimostrazione. Supponiamo che $Q \neq P$ sia un segmento iniziale del buon ordine P e sia $a = \min(P \setminus Q)$: allora $Q = \{x \in P \mid x < a\}$. □

I buoni ordini sono oggetti molto più rigidi degli ordini lineari.

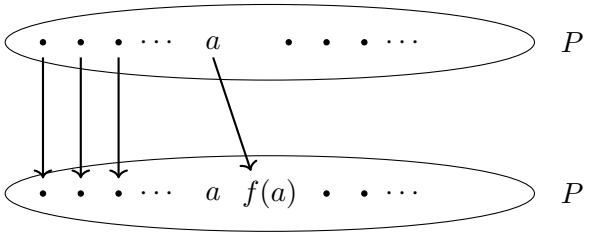
Proposizione 10.4. *Se $(P, \leq)$ è un insieme bene ordinato e $f\colon P \to P$ è strettamente crescente, allora*

$$\forall x \in P\,(x \leq f(x))\,.$$

Dimostrazione. Per assurdo, supponiamo che $\{x \in P \mid f(x) < x\} \neq \emptyset$ e sia a il suo minimo. Poiché f è crescente $f(f(a)) < f(a)$, ma $f(a) < a$ e la minimalità di a implicano che $f(f(a)) \geq f(a)$: contraddizione. □

Proposizione 10.5. *Se $(P, \leq)$ è un insieme bene ordinato e $f\colon P \to P$ è una biezione strettamente crescente, allora $f(x) = x$ per ogni $x \in P$.*

Dimostrazione. Per assurdo supponiamo $a \in P$ sia minimo tale che $f(a) \neq a$. La Proposizione 10.4 implica che $a < f(a)$:



Quindi la funzione f non può essere suriettiva, visto che $a \notin \operatorname{ran}(f)$. □

Corollario 10.6. *Se $(P, \leq)$ e $(Q, \trianglelefteq)$ sono buoni ordini isomorfi, allora l'isomorfismo $f\colon P \to Q$ è unico.*

Corollario 10.7. *Se $(P, \leq)$ è un buon ordine e $Q \subset P$ è un suo segmento iniziale, allora P e Q non sono isomorfi.*

Dimostrazione. Per la Proposizione 10.3 $Q = \{x \in P \mid x < a\}$ per qualche $a \in P$. Se $f\colon P \to Q$ è un isomorfismo, allora $f\colon P \to P$ è crescente e $f(a) < a$, contraddicendo la Proposizione 10.4. □

L'unione crescente di insiemi bene ordinati è un ordine lineare, ma non è necessariamente un buon ordine — per esempio $P_n = \{k \in \mathbb{Z} \mid -n \leq k\}$ è un buon ordine isomorfo a $\mathbb{N}$, ma $\bigcup_{n\in\mathbb{N}} P_n = \mathbb{Z}$ non è un buon ordine. Per ottenere un buon ordine dobbiamo richiedere che ogni buon ordine sia segmento iniziale dei buoni ordini successivi. Più precisamente: se P e Q sono buoni ordini poniamo

$$Q \sqsubseteq P \Leftrightarrow Q \cong P \vee \exists a \in P\,(Q \cong \operatorname{pred} a)$$

vale a dire: $Q \sqsubseteq P$ se e solo se Q è isomorfo ad un segmento iniziale di P. Per il Corollario 10.7 le due condizioni sono mutualmente esclusive, quindi

$$P \sqsubseteq Q \wedge Q \sqsubseteq P \Rightarrow P \cong Q. \tag{10.3}$$

Quando $Q \sqsubseteq P$ e $Q \ncong P$ scriveremo $Q \sqsubset P$.

Teorema 10.8. *Se $(P, <_P)$ e $(Q, <_Q)$ sono insiemi bene ordinati, allora una ed una sola delle seguenti condizioni vale:*

(1) $P \sqsubset Q$,
(2) $Q \sqsubset P$,
(3) $P \cong Q$.

Dimostrazione. Per il Corollario 10.7 le tre condizioni sono mutualmente esclusive, quindi è sufficiente dimostrare che almeno una di esse deve valere. Sia

$$f = \{(p, q) \in P \times Q \mid \operatorname{pred} p \cong \operatorname{pred} q\}.$$

Se $(p, q_1), (p, q_2) \in f$, allora

$$(\operatorname{pred} q_1, <_Q) \cong (\operatorname{pred} p, <_P) \cong (\operatorname{pred} q_2, <_Q)$$

e quindi $q_1 = q_2$. Analogamente se $(p_1, q), (p_2, q) \in f$, allora $p_1 = p_2$. Segue che f è una funzione iniettiva. Se $p \in \operatorname{dom}(f)$ e g è l'isomorfismo che testimonia $(\operatorname{pred} p, <_P) \cong (\operatorname{pred} f(p), <_Q)$ e se $p' < p$, allora $p' \in \operatorname{dom}(g)$ e quindi $(\operatorname{pred} p', <_P) \cong (\operatorname{pred} g(p'), <_Q)$ (Esercizio 8.47). In altre parole: $\operatorname{dom}(f)$ è un segmento iniziale di P nell'ordinamento $<_P$. In modo analogo si verifica che $\operatorname{ran}(f)$ è un segmento iniziale di Q nell'ordinamento $<_Q$. Se $p_1, p_2 \in \operatorname{dom} f$ con $p_2 < p_1$ e g è l'isomorfismo tra $(\operatorname{pred} p_1, <_P)$ e $(\operatorname{pred} f(p_1), <_Q)$, allora, per l'Esercizio 8.47, $g \restriction \operatorname{pred} p_2$ è un isomorfismo tra $(\operatorname{pred} p_2, <_P)$ e $(\operatorname{pred} g(p_2), <_Q)$ e quindi $f(p_2) = g(p_2) <_Q f(p_1)$. Da questo segue che f è un isomorfismo di un segmento iniziale di $(P, <_P)$ su un segmento iniziale di $(Q, <_Q)$. Il teorema è completamente dimostrato se verifichiamo che

$$\operatorname{dom}(f) = P \vee \operatorname{ran}(f) = Q.$$

Supponiamo per assurdo che questo non valga e siano $\bar{p} = \min(P \setminus \operatorname{dom} f)$ e $\bar{q} = \min(Q \setminus \operatorname{ran} f)$. Per quanto detto $f \colon (\operatorname{pred} \bar{p}, <_P) \to (\operatorname{pred} \bar{q}, <_Q)$, quindi $(\bar{p}, \bar{q}) \in f$, per definizione di f, una contraddizione. □

Osserviamo che questo teorema di "confrontabilità " tra buoni ordini non si generalizza agli ordini lineari. Per esempio se $\leq$ è l'usuale ordinamento sui numeri naturali e $\preceq$ è la relazione conversa, cioè

$$n \preceq m \Leftrightarrow m \leq n,$$

allora i due ordini lineari $(\mathbb{N}, \leq)$ e $(\mathbb{N}, \preceq)$ non sono isomorfi, né l'uno è isomorfo ad un segmento iniziale dell'altro — infatti nessuno dei due ordini si immerge nell'altro.

Se P_n è un segmento iniziale di P_{n+1} per tutti gli n, allora $\bigcup_{n \in \mathbb{N}} P_n$ è bene ordinato dalla relazione $x \preceq y \Leftrightarrow \exists n \in \mathbb{N}\, (x, y \in P_n \wedge x \leq_n y)$. In realtà questo fatto continua a valere anche quando P_n è isomorfo ad un segmento iniziale di P_{n+1} e l'insieme degli indici $\mathbb{N}$ è rimpiazzato da un

generico buon ordine. Supponiamo $(P_i, \leq_i)$ sia un buon ordine per ogni $i \in I$ e che $\trianglelefteq$ sia un buon ordine su I tale che

$$i \trianglelefteq j \Rightarrow P_i \sqsubseteq P_j.$$

Siano $f_{i,j} \colon P_i \to P_j$ le funzioni crescenti che testimoniano $P_i \sqsubseteq P_j$, cioè $f_{i,j}$ è un isomorfismo di P_i su un segmento iniziale di P_j — per i Corollari 10.6 e 10.7 le $f_{i,j}$ sono univocamente determinate. Sia

$$\bigsqcup_{i \in I} P_i = (\cup_{i \in I} P_i)/\!\sim$$

il quoziente dell'unione disgiunta dei P_i mediante la relazione di equivalenza

$$(i, x) \sim (j, y) \Leftrightarrow (i \trianglelefteq j \wedge f_{i,j}(x) = y) \vee (j \trianglelefteq i \wedge f_{j,i}(y) = x)\,.$$

Definiamo l'ordinamento $\preceq$ su $\bigsqcup_{i \in I} P_i$ così: se $x \in P_i$ e $y \in P_j$ allora

$$x \preceq y \Leftrightarrow f_{i,h}(x) \leq_h f_{j,h}(y)$$

dove $h = \max(i, j)$.

Esercizio 10.9. Dimostrare che

(i) $\preceq$ è un buon ordine su $\bigsqcup_{i \in I} P_i$

(ii) $(P_j, \leq_j) \sqsubseteq (\bigsqcup_{i \in I} P_i, \preceq)$ per ogni $j \in I$,

(iii) se $(Q, \leq_Q) \sqsubseteq (\bigsqcup_{i \in I} P_i, \preceq)$ allora $(Q, \leq_Q) \sqsubseteq (P_i, \leq_i)$ per qualche $i \in I$.

Un **ordinale** è un buon ordine a meno di isomorfismo; per esempio i numeri naturali 1, 2, 3, ... sono identificabili con i diagrammi

mentre 0 è identificato con il diagramma vuoto. L'ordinale associato all'ordinamento di un buon ordine P si dice **tipo d'ordine** di P. Il tipo d'ordine di $\mathbb{N}$ (o di un suo sottoinsieme infinito) è denotato con ω. Gli ordinali sono indicati con lettere greche α, β, γ, ... Certi ordinali (per esempio ω) non hanno massimo e si dicono **ordinali limite**.

Le operazioni di somma e prodotto sugli ordinali sono definite mediante le operazioni $+$ e $\times$ sugli ordini, cioè se A e B sono buoni ordini di tipo d'ordine α e β, allora definiamo

$$\begin{aligned} \alpha + \beta &= \text{il tipo d'ordine di } A + B \\ \alpha \cdot \beta &= \text{il tipo d'ordine di } A \times B \\ \alpha \leq \beta &\Leftrightarrow A \sqsubseteq B. \end{aligned}$$

Proposizione 10.10. *La relazione $\leq$ sugli ordinali è un buon ordine.*

Dimostrazione. Le proprietà riflessiva e transitiva sono immediate, la proprietà antisimmetrica discende da (10.3), e per il Teorema 10.8 $\leq$ è un ordine lineare. Verifichiamo che è un buon ordine: dato X un insieme non vuoto di ordinali, sia $(P, \leq_P)$ un buon ordine il cui tipo d'ordine α è in X e sia Q l'intersezione di tutti i segmenti iniziali di P che hanno tipo d'ordine in X; chiaramente Q è un segmento iniziale di P e se il suo tipo d'ordine β appartiene a X, allora β è il minimo di X. Quindi è sufficiente verificare che $\beta \in X$. Se $Q = P$ allora $\alpha = \beta$ e il risultato segue subito, quindi possiamo supporre che $Q \neq P$ e quindi, per la Proposizione 10.3, $Q = \{x \in P \mid x <_P a\}$ per qualche $a \in P$. Poiché $a \notin Q$ e per definizione di Q, deve esistere un segmento iniziale $Q' = \{x \in P \mid x <_P a'\}$ di P il cui tipo d'ordine β' è in X e tale che $a \notin Q'$. Ma questo significa che $a \not<_P a'$, cioè $a' \leq_P a$. Per la minimalità di Q si ha $a' = a$, cioè $Q' = Q$, da cui $\beta = \beta'$ e quindi $\beta \in X$ come richiesto. □

Quindi, un insieme di ordinali è della forma $X = \{\alpha_i \mid i \in I\}$ dove $(I, \trianglelefteq)$ è un buon ordine, per cui se P_i è un buon ordine di tipo α_i, per l'Esercizio 10.9 il tipo d'ordine di $\bigsqcup_{i\in I} P_i$ è

$$\sup X = \sup_{i\in I} \alpha_i$$

l'estremo superiore degli ordinali in X.

Da (10.1) e (10.2) segue che le operazioni di somma e prodotto su ordinali sono associative:

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

Nella Sezione 15 dimostreremo altre proprietà della somma, prodotto, e ordinamento degli ordinali: la proprietà distributiva *a destra* della somma rispetto al prodotto, cioè

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

mentre l'analoga proprietà a sinistra non vale (Esercizio 10.64). Inoltre la somma e il prodotto sono funzioni strettamente crescenti nella seconda coordinata,

$$\beta < \beta' \Rightarrow \alpha + \beta < \alpha + \beta'$$
$$0 < \alpha \wedge \beta < \beta' \Rightarrow \alpha \cdot \beta < \alpha \cdot \beta'$$

e debolmente crescenti nella prima,

$$\alpha < \alpha' \Rightarrow \alpha + \beta \leq \alpha' + \beta$$
$$\alpha < \alpha' \Rightarrow \alpha \cdot \beta \leq \alpha' \cdot \beta.$$

Vale la formula della divisione con resto

$$0 < \alpha < \beta \Rightarrow \exists!\gamma < \beta\, \exists!\delta < \alpha\, (\alpha \cdot \gamma + \delta = \beta).$$

Applicando gli Esercizi 10.1(ii) e 10.9 quando β è limite, si ottiene la definizione ricorsiva di somma e prodotto:

$$\alpha + \beta = \begin{cases} \alpha & \text{se } \beta = 0, \\ (\alpha + \gamma) + 1 & \text{se } \beta = \gamma + 1, \\ \sup_{\gamma<\beta}(\alpha + \gamma) & \text{se } \beta \text{ è limite,} \end{cases}$$

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

Questo suggerisce la seguente definizione di esponenziazione di ordinali:

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

Anche in questo caso, si dimostrano per gli ordinali alcune delle proprietà che valgono per i numeri naturali:

$$1 < \alpha \wedge \beta < \beta' \Rightarrow \alpha^\beta < \alpha^{\beta'}$$
$$\alpha < \alpha' \Rightarrow \alpha^\beta \leq (\alpha')^\beta$$
$$1 < \alpha < \beta \Rightarrow \exists!\gamma \leq \beta\, \exists!\delta\, (1 \leq \delta < \alpha) \exists!\epsilon < \alpha^\gamma\, (\alpha^\gamma \cdot \delta + \epsilon = \beta).$$

Quindi possiamo costruire buoni ordini di tipo

$$\omega, \quad \omega^\omega, \quad \omega^{\omega^\omega}, \quad \ldots$$

e per l'Esercizio 10.78 possiamo trovare sottoinsiemi chiusi di $\mathbb{R}$ con questi tipi d'ordine. Il seguente esempio mostra un sottoinsieme chiuso di $\mathbb{R}$ che ha tipo d'ordine ω^ω — questo esempio richiede conoscenze avanzate di geometria e non sarà usato nel seguito, quindi il lettore può ignorarlo.

Esempio 10.11. Una **varietà iperbolica n-dimensionale** è una varietà connessa n-dimensionale dotata di una metrica completa Riemanniana in cui ogni punto ha un intorno isometrico ad un aperto di $\mathbb{H}^n$, dove

$$\mathbb{H}^n = \{\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{R}^n \mid x_n \geq 0\}$$

è il piano iperbolico dotato di metrica Riemanniana completa $\mathrm{d}s = \frac{\mathrm{d}\mathbf{x}}{x_n}$ di curvatura sezionale -1. Ad ogni varietà M siffatta possiamo associare un numero reale positivo $\mathrm{vol}(M)$ detto il suo volume, e

$$\{\mathrm{vol}(M) \mid M \text{ è una varietà iperbolica 3-dimensionale}\}$$

è un sottoinsieme chiuso, bene ordinato di $\mathbb{R}$ di tipo d'ordine ω^ω.

Anche l'esponenziale può essere definito mediante operazione sui buoni ordini, così com'era stato fatto per la somma e il prodotto. Cominciamo con un esempio: il semianello $\mathbb{N}[X]$ è bene ordinato da

$$f \prec g \Leftrightarrow \exists n \forall m \geq n \; (f(m) < g(m)) \, .$$

Inoltre $\prec$ ristretto ai polinomi di grado $\leq k$ ha tipo d'ordine ω^{k+1} e $(\mathbb{N}[X], \prec)$ ha tipo d'ordine ω^ω (Esercizio 10.66). Poiché un polinomio di $\mathbb{N}[X]$ è semplicemente una funzione $f \colon \mathbb{N} \to \mathbb{N}$ che è quasi ovunque 0, questo esempio ci suggerisce la seguente

Definizione 10.12. Siano $(A, <_A)$ e $(B, <_B)$ insiemi bene ordinati, e indichiamo con 0 il minimo di B, se $B \neq \emptyset$. Sia

$$E(A,B) = \Big\{ f \in B^A \mid \{a \in A \mid f(a) \neq 0\} \text{ è finito} \Big\} \, .$$

Se $f, g \in E(A,B)$ sono distinti, c'è un $<_A$-massimo $\bar{a} \in A$ tale che $f(\bar{a}) \neq g(\bar{a})$ e poniamo

$$f \prec g \Leftrightarrow f(\bar{a}) <_B g(\bar{a}).$$

La relazione $\prec$ è un buon ordine su $E(A,B)$ (Esercizio **??**) e se α e β sono gli ordinali di $(A, <_A)$ e $(B, <_B)$, rispettivamente, allora α^β è il tipo d'ordine di $(E(A,B), \prec)$.

10.B. Induzione, ricorsione e buoni ordini.

10.B.1. *Induzione e buoni ordini.* Ricordiamo dalla Sezione 7.D che il principio di induzione al second'ordine Ind^2 è equivalente al principio del minimo

$$(\mathsf{MP}^2) \qquad \forall I \, [I \neq \emptyset \Rightarrow \exists x \, (x \in I \wedge \forall y \, (y < x \Rightarrow y \notin I))] \, .$$

Il principio del minimo vale per ogni buon ordine e non solo per $<$ su $\mathbb{N}$, e le dimostrazioni della Sezione 7.E possono essere riformulate utilizzando il principio del minimo applicato ad un buon ordine appropriato. Per esempio la dimostrazione della Proposizione 7.14(b) a pagina 139 può essere vista come una dimostrazione che utilizza il principio del minimo per il buon ordine $<_{\text{lex}}$ su $\mathbb{N}^2$, che ha lunghezza $\omega \cdot \omega$. Supponiamo, per assurdo, che

$$I = \Big\{ (n,m) \in \mathbb{N}^2 \mid n + m \neq m + n \Big\}$$

sia non vuoto, così che per il principio del minimo ha un elemento $<_{\text{lex}}$-minimo (n^*, m^*). Chiaramente $(n^*, m^*) \neq (0,0)$. Se $n^* = 0$ allora $m^* = \bar{m} + 1$ quindi

$$\begin{aligned} n^* + m^* &= (0 + \bar{m}) + 1 \\ &= (\bar{m} + 0) + 1 \qquad \text{per la minimalità di } (n^*, m^*) \\ &= \bar{m} + 1 \\ &= (\bar{m} + 1) + 0 \\ &= m^* + n^*, \end{aligned}$$

contraddizione! Ne segue che $n^* = \bar{n} + 1$ per qualche $\bar{n}$ e $\forall x\,(0 + x = x + 0)$. Quindi ponendo $x = n^*$, si ottiene che $m^* \neq 0$. Possiamo quindi supporre che $m^* = \bar{m} + 1$ e ripetendo il ragionamento a pagina 140 otteniamo una contraddizione.

10.B.2. *Ricorsione e buoni ordini.* Se f è definita per ricorsione da

$$\begin{cases} f(0) = a \\ f(n+1) = F(n, f(n)) \end{cases}$$

allora il computo di uno specifico valore $f(\bar{n})$ dipende dai $\bar{n}$ valori precedentemente calcolati: $f(0), f(1), \ldots, f(\bar{n} - 1)$. In altre parole

$$f(n) = \tilde{F}(f \restriction \operatorname{pred} n) \tag{10.4}$$

dove $\tilde{F}$ è un'opportuna funzione definita sulle funzioni parziali da $\mathbb{N}$ in $\mathbb{N}$. Se sostituiamo l'ordinamento $<$ su $\mathbb{N}$ con un buon ordine $\lhd$ su un insieme X, la (10.4) mostra come generalizzare la nozione di definizione induttiva di funzioni. Per esempio per calcolare un valore della funzione di Ackermann $\mathrm{Ack}(m, n)$ vista nella Sezione 9.D.1, è sufficiente conoscere i valori di $\mathrm{Ack}(m', n')$ quando $(m', n') <_{\mathrm{lex}} (m, n)$ quindi Ack può essere definita mediante

$$\mathrm{Ack}(m, n) = \tilde{F}\,(\mathrm{Ack} \restriction \operatorname{pred}((m, n), <_{\mathrm{lex}}))$$

dove $\tilde{F}$ è definita così: se f è una funzione definita su $\operatorname{pred}((m, n), <_{\mathrm{lex}})$,

$$\tilde{F}\,(f) = \begin{cases} n + 1 & \text{se } m = 0, \\ f(m - 1, 1) & \text{se } m > 0 \text{ e } n = 0, \\ f(m - 1, f(m, n - 1)) & \text{se } m > 0 \text{ e } n > 0. \end{cases}$$

Lo schema (10.4) può essere esteso ad ordini parziali in cui ogni sottoinsieme non vuoto ha un elemento minimo.[8]

Esempio 10.13. Consideriamo la funzione $M\colon \mathbb{N} \to \mathbb{N}$ definita da

$$M(n) = \begin{cases} n - 10 & \text{se } n > 100, \\ M(M(n + 11)) & \text{se } n \leq 100. \end{cases}$$

A prima vista non è neppure chiaro che la funzione sia ben definita per $n \leq 100$. Per prima cosa osserviamo che $M(101) = 91$. Se $91 \leq n \leq 100$, allora $M(n) = M(M(n + 11)) = M(n + 1)$ e quindi

$$M(91) = M(92) = \cdots = M(100) = M(101) = 91.$$

[8] Ordini siffatti si dicono ben-fondati e verranno studiati nel Capitolo IV.

Se $80 \leq n \leq 90$, allora $91 \leq n+11 \leq 101$ e quindi $M(n) = M(M(n+11)) = M(91) = 91$. Ripetendo il ragionamento qui sopra è facile verificare che

$$M(n) = \begin{cases} n-10 & \text{se } n > 100, \\ 91 & \text{se } n \leq 100. \end{cases}$$

Inoltre, se $n \leq 100$

$$M(n) = \tilde{F}(M \restriction \mathrm{pred}(n, \prec))$$

dove $\prec$ è l'ordine parziale su $\{0, \ldots, 101\}$ definito da

$$n \prec m \Leftrightarrow [m < n \wedge n \equiv m \mod 11] \vee [91 \leq n, m \leq 101 \wedge m < n].$$

10.C. Cardinalità. Due insiemi X e Y sono **equipotenti**, in simboli

$$X \approx Y,$$

se c'è una funzione $f\colon X \to Y$ biettiva. La relazione $\approx$ è una relazione di equivalenza; spesso diremo che due insiemi equipotenti X e Y hanno la medesima **cardinalità** e scriveremo

$$|X| = |Y|$$

o anche

$$\mathrm{card}(X) = \mathrm{card}(Y).$$

Un insieme X **si inietta in** Y, in simboli

$$X \precsim Y$$

se c'è una funzione iniettiva $f\colon X \to Y$; in questo caso scriveremo che

$$|X| \leq |Y|.$$

Il simbolo $\leq$ suggerisce che si tratti di una relazione di ordine sulle cardinalità : la proprietà riflessiva e transitiva sono immediate, mentre la proprietà antisimmetrica è garantita dal seguente risultato.

Teorema 10.14 (Cantor-Schröder-Bernstein)**.** *Se $X \precsim Y$ e $Y \precsim X$ allora $X \approx Y$.*

Dimostrazione. Fissiamo due funzioni iniettive $f\colon X \to Y$ e $g\colon Y \to X$. L'ordine parziale $(\mathscr{P}(X), \subseteq)$ e la funzione $\Phi\colon \mathscr{P}(X) \to \mathscr{P}(X)$

$$\Phi(Z) = X \setminus g[Y \setminus f[Z]]$$

soddisfano le ipotesi del Teorema 8.12, quindi esiste un $Z \subseteq X$ tale che $\Phi(Z) = Z$, ovvero $X \setminus Z = g[Y \setminus f[Z]]$. Poiché g^{-1} è una biezione tra $X \setminus Z$ e $Y \setminus f[Z]$, la funzione $h\colon X \to Y$

$$h(x) = \begin{cases} f(x) & \text{se } x \in Z \\ g^{-1}(x) & \text{se } x \in X \setminus Z \end{cases}$$

è una biezione. □

Un insieme è equipotente ad un suo sottoinsieme proprio se e solo se contiene una copia dell'insieme dei naturali.

Proposizione 10.15. $\mathbb{N} \precsim X \Leftrightarrow \exists Y \subset X\, (Y \approx X)$.

Dimostrazione. Supponiamo $f\colon \mathbb{N} \rightarrowtail X$ e sia $Y = X \setminus \operatorname{ran} f$. Allora $g\colon X \to Y$

$$g(x) = \begin{cases} x & \text{se } x \in X \setminus \{f(0)\} \\ f(n+1) & \text{se } \exists n \in \mathbb{N}\, (f(n) = x). \end{cases}$$

è una biezione.

Viceversa, fissiamo $g\colon X \to Y \subset X$ una biezione e supponiamo $x_0 \in X \setminus \operatorname{ran}(f)$; allora definiamo induttivamente $x_{n+1} = g(x_n)$. Una facile induzione mostra che gli x_n sono distinti, quindi $\mathbb{N} \precsim X$. □

Se $X \neq \emptyset$ e $X \precsim Y$ allora c'è una suriezione da Y in X: se $f\colon X \to Y$ è iniettiva e $x_0 \in X$, allora la funzione $g\colon Y \to X$

$$g(y) = \begin{cases} x & \text{se } f(x) = y, \\ x_0 & \text{se } y \neq f(x) \text{ per ogni } x \in X \end{cases}$$

è suriettiva e $g \circ f = \mathrm{id}_X$.

Per dimostrare il viceversa bisogna fare un'ipotesi ulteriore su Y.

Proposizione 10.16. *Se $g\colon Y \to X$ è suriettiva e $\trianglelefteq$ è un buon ordine su Y, allora c'è un'iniezione $f\colon X \to Y$ tale che $g \circ f = \mathrm{id}_X$.*

In particolare, se $\mathbb{N}$ si surietta su un insieme X allora $X \precsim \mathbb{N}$.

Dimostrazione. Sia $f(x)$ il $\trianglelefteq$-minimo $y \in Y$ tale che $g(y) = x$. □

Il simbolo 2 verrà usato per indicare la cardinalità di un insieme con due elementi, per esempio[9] l'insieme $\{0, 1\}$. Quindi scrivere che $2 \leq |X|$ equivale a dire che X ha almeno due elementi. Indicheremo la cardinalità di $\mathbb{N}$ con il simbolo $\aleph_0$.

Esercizio 10.17. Siano X, Y, Z e W degli insiemi tali che $X \precsim Z$ e $Y \precsim W$. Dimostrare che:

(i) se $X \cap Y = Z \cap W = \emptyset$, allora $X \cup Y \precsim Z \cup W$;
(ii) $X \times Y \precsim Z \times W$.

Possiamo quindi definire la **somma** e **prodotto di cardinalità** come

$$|X| + |Y| = |X \cup Y|$$
$$|X| \cdot |Y| = |X \times Y|.$$

[9]Come vedremo nel Capitolo IV, nella teoria assiomatica degli insiemi il numero naturale 0 è identificato con l'insieme vuoto $\emptyset$ e il numero naturale $n+1$ è identificato con l'insieme $\{0, 1, \ldots, n\}$.

Se X e Y sono insiemi disgiunti, ciascuno dei quali contiene almeno due elementi, $x_0, x_1 \in X$ e $y_0, y_1 \in Y$, allora la funzione

$$f\colon X \cup Y \to X \times Y$$

data da $f(x) = (x, y_0)$ se $x \in X$ e per $y \in Y$

$$f(y) = \begin{cases} (x_0, y) & \text{se } y \neq y_0, \\ (x_1, y_1) & \text{se } y = y_0, \end{cases}$$

è iniettiva. Quindi

$$2 \leq |X|, |Y| \Rightarrow |X| + |Y| \leq |X \times Y|. \tag{10.5}$$

Poiché la funzione $\boldsymbol{J}\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ definita in (6.6) è una biezione, ne segue subito che:

Teorema 10.18. $\mathbb{N} \times \mathbb{N} \approx \mathbb{N}$ *e quindi* $\aleph_0 + \aleph_0 = \aleph_0 \cdot \aleph_0 = \aleph_0$.

10.C.1. *Insiemi finiti.* Per definizione, un insieme è finito se e solo se è in biezione con $\{0, \dots, n-1\}$, per qualche $n \in \mathbb{N}$, dove poniamo $\{0, \dots, n-1\} = \emptyset$ quando $n = 0$. Se X è finito scriveremo

$$|X| = n.$$

Questa notazione è giustificata dal fatto che un insieme finito è in biezione con un unico $n \in \mathbb{N}$. Ciò 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 10.19. (a) *Se* $n, m \in \mathbb{N}$ *e* $\{0, \dots, n-1\} \precsim \{0, \dots, m-1\}$, *allora* $n \leq m$. *In particolare: se* $\{0, \dots, n-1\} \approx \{0, \dots, m-1\}$, *allora* $n = m$.

(b) $\mathbb{N}$ *è infinito e quindi* $\mathbb{N} \not\precsim \{0, \dots, n-1\}$ *per ogni* $n \in \mathbb{N}$.

Dimostrazione. (a) Per induzione su $n \in \mathbb{N}$. Se $n = 0$ il risultato è banale, quindi possiamo supporre che $n = n' + 1$ e che $f\colon \{0, \dots, n'\} \rightarrowtail \{0, \dots, m'\}$. Chiaramente $m > 0$, cioè $m = m' + 1$. Sia $g\colon \{0, \dots, m'\} \to \{0, \dots, m'\}$ la biezione che scambia $f(n')$ con m' e lascia invariato il resto. Allora

$$(g \circ f) \restriction \{0, \dots, n'\} : \{0, \dots, n'\} \rightarrowtail \{0, \dots, m'\}$$

e quindi, per ipotesi induttiva, $n' \leq m'$, da cui $n = n' + 1 \leq m' + 1 = m$.

(b) Se $\mathbb{N} \approx \{0, \dots, n-1\}$ per qualche $n \in \mathbb{N}$, allora da $\{0, \dots, n\} \precsim \mathbb{N}$ e $\mathbb{N} \precsim \{0, \dots, n-1\}$, otterremmo $\{0, \dots, n\} \precsim \{0, \dots, n-1\}$ contraddicendo la parte (a). □

Osservazione 10.20. Se $f\colon \{0,\dots,n-1\} \to X$ è una biezione e $n > 0$, allora possiamo elencare gli elementi di X mediante f

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

dove $x_i = f(i)$. Quando in matematica si dice:

$$\text{Consideriamo un insieme finito } X = \{x_0,\dots,x_{n-1}\}\ \dots,$$

in realtà si sta usando una biezione tra $\{0,\dots,n-1\}$ e l'insieme X.

Proposizione 10.21. *Se X è un insieme finito e $Y \subseteq X$, allora Y è finito e $|Y| \leq |X|$.*

Dimostrazione. È sufficiente dimostrare che se $Y \subseteq \{0,\dots,n-1\}$ allora Y è in biezione con $\{0,\dots,m-1\}$ per qualche $m \leq n$. Se $Y = \emptyset$ il risultato è immediato, quindi possiamo supporre che $Y \neq \emptyset$. Sia $b \notin Y$, e sia $F\colon \mathbb{N} \to Y \cup \{b\}$ la funzione definita da

$$F(k) = \begin{cases} \min(Y \setminus \{0,\dots,k\}) & \text{se } Y \setminus \{0,\dots,k\} \neq \emptyset \\ b & \text{altrimenti.} \end{cases}$$

Per il Corollario 7.5(c) c'è una $f\colon \mathbb{N} \to Y \cup \{b\}$ tale che $f(0) = \min Y$ e

$$f(n+1) = \begin{cases} \min(Y \setminus \{0,\dots,f(n)-1\}) & \text{se } Y \setminus \{0,\dots,f(n)-1\} \neq \emptyset \\ b & \text{altrimenti.} \end{cases}$$

La f enumera progressivamente gli elementi di Y e una volta esauriti questi, è costantemente uguale a b. Più precisamente: si verifica per induzione che $\forall n\ (f(n) \in Y \Rightarrow \forall k < n\ (f(k) \neq f(n)))$, quindi per il Teorema 10.19 $\{k \in \mathbb{N} \mid f(k) = b\}$ è non vuoto, e sia m il minimo di tale insieme. Allora $f\colon \{0,\dots,m-1\} \to Y$ è una biezione. □

Proposizione 10.22. *Se X e Y sono insiemi finiti, allora $X \times Y$ e $X \cup Y$ sono finiti.*

Dimostrazione. Siano $n = |X|$ e $m = |Y|$. Poiché

$$\{0,\dots,n-1\} \times \{0,\dots,m-1\} \subseteq \{0,\dots,k-1\} \times \{0,\dots,k-1\}$$

dove $k = \max(n,m)$, e poiché $\forall i,j < k\ (\boldsymbol{J}(i,j) < k \cdot (2k+1))$, ne segue che $X \times Y \precsim \{0,\dots,k\cdot(2k+1)\}$ è finito.

Dimostriamo ora che $X \cup Y$ è finito. Poiché $X \cup Y = X \cup (Y \setminus X)$ possiamo supporre che X e Y siano disgiunti. Dato che il risultato è immediato se uno tra i due insiemi è vuoto o è un singoletto, possiamo supporre che $|X|, |Y| \geq 2$. Allora $X \cup Y \precsim X \times Y$ per quanto visto a pagina 228, quindi $X \cup Y$ è finito, in quanto in biezione con un sottoinsieme di $X \times Y$. □

10.C.2. *Insiemi e sequenze finite.* Se X è non vuoto, indichiamo con

$$X^{<\mathbb{N}} = \{(x_0, \dots, x_{k-1}) \mid k \in \mathbb{N} \wedge \forall i < k\, (x_i \in X)\},$$

l'insieme delle sequenze finite di elementi di X, con la convenzione che se $k = 0$ si prende la sequenza vuota $\emptyset$, e con

$$[X]^{<\mathbb{N}} = \{A \subseteq \mathbb{N} \mid \exists k \in \mathbb{N}\, |A| = k\}$$

l'insieme dei sottoinsiemi finiti di X. La funzione $f\colon X^{<\mathbb{N}} \to [X]^{<\mathbb{N}}$, $s \mapsto \mathrm{ran}(s)$ è suriettiva, e se $<$ è un ordine lineare su X la funzione $g\colon [X]^{<\mathbb{N}} \to X^{<\mathbb{N}}$, $\{x_0 < \cdots < x_n\} \mapsto (x_0 < \cdots < x_n)$ è iniettiva e $f \circ g$ è l'identità su $[X]^{<\mathbb{N}}$. Nella Sezione 6.B abbiamo costruito un insieme $\mathrm{Seq} \subseteq \mathbb{N}$ ed una biezione

$$\mathbb{N}^{<\mathbb{N}} \to \mathrm{Seq}, \quad (n_0, \dots, n_k) \mapsto \langle\!\langle n_0, \dots, n_k \rangle\!\rangle$$

che mostra che $\mathbb{N}^{<\mathbb{N}}$ e $[\mathbb{N}]^{<\mathbb{N}}$ sono numerabili. Ogni biezione $X \to \mathbb{N}$ induce delle biezioni $X^{<\mathbb{N}} \to \mathbb{N}^{<\mathbb{N}}$ e $[X]^{<\mathbb{N}} \to [\mathbb{N}]^{<\mathbb{N}}$, quindi

$$|X| = \aleph_0 \Rightarrow |X^{<\mathbb{N}}| = |[X]^{<\mathbb{N}}| = \aleph_0. \tag{10.6}$$

Usando il fatto che $[\mathbb{N}]^{<\mathbb{N}}$ è numerabile, si può costruire direttamente un grafo numerabile che soddisfa la proprietà Â ρ del grafo aleatorio R_ω. Come annunciato nella Sezione 5.H.5 dimostreremo tra poco che ogni grafo numerabili con la proprietà Â ρ è isomorfo a R_ω (Teorema 10.35) e quindi si dirà grafo aleatorio numerabile. L'insieme

$$\mathcal{F} = \{(A, B) \mid A, B \in [\mathbb{N}]^{<\mathbb{N}} \wedge\ A \cap B = \emptyset\}$$

è numerabile, quindi c'è una biezione $\mathbb{N} \to \mathcal{F}$, $n \mapsto (A_n, B_n)$. Fissiamo una successione strettamente crescente di numeri naturali $(x_n)_n$ tale che $\max(A_n \cup B_n) < x_n$. Il grafo su $\mathbb{N}$ dato da

$$\forall m < k\ (m\ E\ k \Leftrightarrow \exists n\ (k = x_n \wedge m \in A_n))$$

soddisfa ρ.

Questa ricetta può essere utilizzata per costruire altri oggetti aleatori. Un **ordine aleatorio** è un ordine $(P, \leq)$ che soddisfa la seguente proprietà : presi $A, B, C \subseteq P$ finiti, disgiunti e tali che

$$\forall a \in A\, \forall b \in B\, \forall c \in C\ (b \not\leq a \wedge c \not\leq a \wedge b \not\leq c),$$

esiste $p \in P \setminus (A \cup B \cup C)$ tale che

$$\forall a \in A\, \forall b \in B\, \forall c \in C\ (a \leq p \leq b \wedge p \not\leq c \wedge c \not\leq p).$$

Due ordini aleatori numerabili sono isomorfi (Esercizio 10.61) e ogni ordine numerabile si immerge in ognuno di questi.

Per costruire un ordine aleatorio numerabile $(\mathbb{N}, \preceq)$ fissiamo un'enumerazione $(A_n, B_n, C_n)_n$ di tutte le triple di sottoinsiemi finiti di $\mathbb{N}$ a due a due

disgiunti, fissiamo una successione $(x_n)_n$ strettamente crescente di numeri naturali tali che $\max(A_n \cup B_n \cup C_n) < x_n$, e poniamo

$$m \prec k \Leftrightarrow \exists n\ (k = x_n \wedge m \in A_n) \vee \exists n\ (m = x_n \wedge k \in B_n)\,.$$

Posto $n \preceq m \Leftrightarrow n \prec m \vee n = m$ si ha che $(\mathbb{N}, \preceq)$ è un ordine aleatorio.

10.D. Insieme potenza.

Teorema 10.23 (Cantor)**.** *Non esiste alcuna suriezione da X su $\mathscr{P}(X)$ e quindi $\mathscr{P}(X) \not\precsim X$.*

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 $\bar{x} \in Y \Leftrightarrow \bar{x} \notin \pi(\bar{x}) = Y$: contraddizione. □

L'insieme potenza $\mathscr{P}(X)$ non è in biezione con X — in particolare esistono insiemi non numerabili, per esempio $\mathscr{P}(\mathbb{N})$. Nel Capitolo IV dimostreremo che esistono anche buoni ordini più che numerabili. Il più piccolo ordinale non numerabile è indicato con

$$\omega_1.$$

L'insieme $\mathscr{P}(X)$ è in biezione con $\{0,1\}^X$, l'insieme delle funzioni da X in $\{0,1\}$: ad ogni $Y \subseteq X$ associamo la sua funzione caratteristica $\boldsymbol{\chi}_Y^X = \boldsymbol{\chi}_Y\colon X \to \{0,1\}$.

Esercizio 10.24. Dimostrare che:

(i) $X \precsim Y \Rightarrow \mathscr{P}(X) \precsim \mathscr{P}(Y)$;
(ii) $X \precsim Y \wedge Z \precsim W \Rightarrow X^Z \precsim Y^W$;
(iii) $X^{(Y \cup Z)} \approx X^Y \times X^Z$;
(iv) $(X \times Y)^Z \approx X^Z \times Y^Z$;
(v) $(X^Y)^Z \approx X^{Y \times Z}$.

L'**esponenziale** di due cardinalità è definito come

$$|X|^{|Y|} = |X^Y|$$

e per l'Esercizio 10.24 valgono le usuali proprietà algebriche

$$|X|^{(|Y|+|Z|)} = |X|^{|Y|} \cdot |X|^{|Z|} \quad \text{e} \quad \left(|X|^{|Y|}\right)^{|Z|} = |X|^{|Y| \cdot |Z|}.$$

Se identifichiamo una funzione $f \in \mathbb{N}^{\mathbb{N}}$ con il suo grafo $\mathrm{Gr}(f) \in \mathscr{P}(\mathbb{N} \times \mathbb{N})$ allora $\{0,1\}^{\mathbb{N}} \subseteq \mathbb{N}^{\mathbb{N}} \precsim \mathscr{P}(\mathbb{N} \times \mathbb{N})$, e per il Teorema 10.18 $\mathscr{P}(\mathbb{N} \times \mathbb{N}) \approx \mathscr{P}(\mathbb{N}) \approx \{0,1\}^{\mathbb{N}}$, da cui

$$\{0,1\}^{\mathbb{N}} \approx \mathbb{N}^{\mathbb{N}}. \tag{10.7}$$

10.E. Gli insiemi numerici. Nella Sezione 7.A abbiamo visto come $\mathbb{N}$ possa essere caratterizzato a meno di isomorfismo a partire dagli assiomi di Dedekind (Teorema 7.3(c)) e come definire le operazioni di somma e prodotto su $\mathbb{N}$. Vediamo ora come costruire gli altri insiemi numerici a partire da $(\mathbb{N}, +, \cdot)$.

10.E.1. *Gli interi.* L'insieme $\mathbb{Z}$ degli interi relativi è definito come $(\mathbb{N}\times\mathbb{N})/E_{\mathbb{Z}}$ dove $E_{\mathbb{Z}}$ è la relazione di equivalenza definita da

$$(n, m)\ E_{\mathbb{Z}}\ (h, k) \Leftrightarrow n + k = h + m.$$

L'ordinamento $<^{\mathbb{Z}}$ e le operazioni di somma $+^{\mathbb{Z}}$ e prodotto $\cdot^{\mathbb{Z}}$ su $\mathbb{Z}$ sono definite da

$$\begin{aligned}
[(n, m)]_{E_{\mathbb{Z}}} <^{\mathbb{Z}} [(n', m')]_{E_{\mathbb{Z}}} &\Leftrightarrow n + m' < n' + m.\\
[(n, m)]_{E_{\mathbb{Z}}} +^{\mathbb{Z}} [(h, k)]_{E_{\mathbb{Z}}} &= [(n + h, m + k)]_{E_{\mathbb{Z}}},\\
[(n, m)]_{E_{\mathbb{Z}}} \cdot^{\mathbb{Z}} [(h, k)]_{E_{\mathbb{Z}}} &= [(n \cdot h + m \cdot k, n \cdot k + m \cdot h)]_{E_{\mathbb{Z}}}.
\end{aligned}$$

La funzione

$$\mathbb{N} \to \mathbb{Z}, \quad n \mapsto [(n, 0)]_{E_{\mathbb{Z}}}$$

è un morfismo iniettivo rispetto all'ordinamento e alle operazioni di somma e prodotto, quindi, a tutti gli effetti, $\mathbb{N}$ può essere identificato con un sottoinsieme di $\mathbb{Z}$ ed è possibile tralasciare l'apice $^{\mathbb{Z}}$ nella definizione di ordine, somma e prodotto. Gli interi della forma $[(n, 0)]_{E_{\mathbb{Z}}}$ si denotano con n e quelli della forma $[(0, n)]_{E_{\mathbb{Z}}}$ con $-n$. Chiaramente ogni $z \in \mathbb{Z}$ è della forma n oppure $-n$, con $n \in \mathbb{N}$, quindi la funzione $f\colon \mathbb{N} \to \mathbb{Z}$

$$f(n) = \begin{cases} m & \text{se } n = 2m,\\ -m & \text{se } n = 2m - 1, \end{cases}$$

è una biezione.

10.E.2. *I razionali.* L'insieme $\mathbb{Q}$ è definito come $(\mathbb{Z} \times (\mathbb{Z} \setminus \{0\}))/E_{\mathbb{Q}}$ dove $E_{\mathbb{Q}}$ è la relazione di equivalenza

$$(x, y)\ E_{\mathbb{Q}}\ (z, w) \Leftrightarrow x \cdot w = y \cdot z.$$

L'ordinamento $<^{\mathbb{Q}}$ e le operazioni di somma $+^{\mathbb{Q}}$ e prodotto $\cdot^{\mathbb{Q}}$ su $\mathbb{Q}$ sono date da

$$\begin{aligned}
[(x, y)]_{E_{\mathbb{Q}}} <^{\mathbb{Q}} [(z, w)]_{E_{\mathbb{Q}}} &\Leftrightarrow x \cdot w < y \cdot z,\\
[(x, y)]_{E_{\mathbb{Q}}} +^{\mathbb{Q}} [(z, w)]_{E_{\mathbb{Q}}} &= [(x \cdot w + z \cdot y, y \cdot w)]_{E_{\mathbb{Q}}}\\
[(x, y)]_{E_{\mathbb{Q}}} \cdot^{\mathbb{Q}} [(z, w)]_{E_{\mathbb{Q}}} &= [(x \cdot z, y \cdot w)]_{E_{\mathbb{Q}}}
\end{aligned}$$

La funzione

$$\mathbb{Z} \to \mathbb{Q}, \qquad z \mapsto [(z, 1)]_{E_{\mathbb{Q}}}$$

è un morfismo iniettivo di anelli e preserva l'ordine e quindi $\mathbb{Z}$ viene identificato con un sottoinsieme di $\mathbb{Q}$. Come per gli interi tralasceremo l'apice $^{\mathbb{Q}}$ dai

simboli di ordinamento, somma e prodotto. I razionali della forma $[(z,w)]_{E_{\mathbb{Q}}}$ si denotano con z/w e ogni razionale può essere scritto nella forma z/w con z e w relativamente primi e $w > 0$. Quindi $\mathbb{Q}$ è in biezione con un sottoinsieme di $\mathbb{Z} \times \mathbb{Z}$ che è a sua volta in biezione con $\mathbb{N} \times \mathbb{N}$. Dal Teorema 10.18 segue che $\mathbb{Q}$ è in biezione con un sottoinsieme di $\mathbb{N}$ e poiché $\mathbb{N} \precsim \mathbb{Z} \precsim \mathbb{Q}$, per il Teorema di Cantor-Schröder-Bernstein 10.14 gli insiemi $\mathbb{N}$ e $\mathbb{Q}$ sono in biezione. Quindi

$$|\mathbb{Z}| = |\mathbb{Q}| = \aleph_0.$$

La struttura $(\mathbb{Q}, <)$ può essere caratterizzata a meno di isomorfismo come l'unico ordine lineare numerabile, denso, senza primo ultimo elemento (Teorema 10.32 più sotto). Quindi gli insiemi ordinati

- $\mathbb{Q}$,
- $\mathbb{Q} \cup \{\pi\}$ e
- l'insieme dei numeri algebrici reali

sono isomorfi e tuttavia non è facile definire esplicitamente tale isomorfismo.

Sia $\mathbf{p}\colon \mathbb{N} \to \mathbb{N}$ la funzione che enumera i numeri primi (Esempio 9.9(G)). Ogni elemento di $\mathbb{Q}_+$ diverso da 1 si scrive in un unico modo come $\mathbf{p}(i_1)^{n_1} \cdot \mathbf{p}(i_2)^{n_2} \cdots \mathbf{p}(i_k)^{n_k}$ con $0 \leq i_1 < i_2 < \cdots < i_k$ e $n_1, n_2, \ldots, n_k \in \mathbb{Z} \setminus \{0\}$ Allora la funzione $\mathbb{Q}_+ \to \mathbb{Z}[X]$ definita da

$$1 \mapsto 0 \quad \text{e} \quad \mathbf{p}(i_1)^{n_1} \cdot \mathbf{p}(i_2)^{n_2} \cdots \mathbf{p}(i_k)^{n_k} \mapsto n_1 X^{i_1} + n_2 X^{i_2} + \cdots + n_k X^{i_k} \tag{10.8}$$

è una biezione. Poiché $\mathbb{Q}_+ \approx \mathbb{N}$, se ne deduce che

$$|\mathbb{Z}[X]| = \aleph_0.$$

Ogni $(n_0, n_1, \ldots, n_{k-1}) \in \mathbb{N}^{<\mathbb{N}}$ individua un unico polinomio $n_0 + n_1 X + \cdots + n_{k-1} X^{k-1} \in \mathbb{N}[X]$ e viceversa. Poiché $\mathbb{N}[X] \approx \mathbb{Z}[X]$, otteniamo una nuova dimostrazione del fatto che $\mathbb{N} \approx \mathbb{N}^{<\mathbb{N}}$.

Osserviamo che $\oplus_n \mathbb{Z}$, la **somma diretta** di ω copie di $\mathbb{Z}$, è isomorfo a $\mathbb{Z}[X]$ e quindi ha taglia $\aleph_0$, mentre $\prod_n \mathbb{Z}$, il **prodotto diretto** di ω copie di $\mathbb{Z}$, è in biezione con $\mathbb{N}^{\mathbb{N}}$ e quindi ha taglia $2^{\aleph_0}$.

10.E.3. *I numeri algebrici.* L'insieme dei numeri algebrici è $\overline{\mathbb{Q}} \subseteq \mathbb{C}$ l'insieme delle soluzioni dei polinomi di $\mathbb{Z}[X]$. Ogni $f \in \mathbb{Z}[X]$ individua un insieme finito (eventualmente vuoto) $Z(f)$ di numeri complessi che sono soluzioni di f: l'insieme $Z(f)$ può essere esplicitamente enumerato come $\{z_0, \ldots, z_m\}$ richiedendo che se $i < j$ allora $|z_i| \leq |z_j|$ e se $z_i = r\mathrm{e}^{\mathrm{i}\theta}$ e $z_j = r\mathrm{e}^{\mathrm{i}\eta}$, allora $0 \leq \theta < \eta < 2\pi$. Possiamo quindi definire una suriezione

$$F\colon \mathbb{N} \times \mathbb{Z}[X] \to \overline{\mathbb{Q}}$$

ponendo

$$F(n,f)=\begin{cases} z_n & \text{se } Z(f)=\{z_0,\dots,z_m\} \text{ e } n\leq m,\\ z_m & \text{se } Z(f)=\{z_0,\dots,z_m\} \text{ e } m<n,\\ 0 & \text{se } Z(f)=\emptyset. \end{cases}$$

Per il Teorema 10.18 $|\mathbb{N}\times\mathbb{Z}[X]|=\aleph_0$, quindi c'è una suriezione $\tilde{F}\colon\mathbb{N}\to\overline{\mathbb{Q}}$ dai numeri naturali sui numeri algebrici. Per la Proposizione 10.16 $\overline{\mathbb{Q}}\precsim\mathbb{N}$ e poiché $\mathbb{N}\subseteq\overline{\mathbb{Q}}$ si ha che

$$|\overline{\mathbb{Q}}|=\aleph_0.$$

10.E.4. *I reali e i complessi.* L'insieme dei **numeri reali** è il completamento di Dedekind dell'insieme ordinato $\mathbb{Q}$. Poiché $(\mathbb{Q},<)$ è un ordine lineare si ha che

$$\mathbb{R}=\{x\in\mathscr{P}(\mathbb{Q})\mid x \text{ è una sezione di Dedekind}\}.$$

Quindi $x\in\mathbb{R}$ se e solo se

- $x\neq\emptyset,\mathbb{Q}$,
- $\forall q\in x\forall p\in\mathbb{Q}(p<q\Rightarrow p\in x)$,
- $\forall q\in x\exists p\in x(q<p)$.

La somma su $\mathbb{R}$ è definita da

$$x+^{\mathbb{R}}y=\{p+q\mid p\in x\wedge q\in y\}.$$

La definizione di moltiplicazione $x\cdot^{\mathbb{R}}y$ è più laboriosa ed è presentata nell'Esercizio 10.76.

Esercizio 10.25. Dimostrare che la somma di due numeri reali è ancora un numero reale e che la mappa $\mathbb{Q}\to\mathbb{R}$, $q\mapsto\{p\in\mathbb{Q}\mid p<q\}$ è un morfismo per l'ordine e la somma.

La funzione $x\mapsto\frac{1}{b-x}-\frac{1}{x-a}$ è un isomorfismo tra $(a;b)$ ed $\mathbb{R}$ e se a e b sono razionali, è un isomorfismo tra $(a;b)\cap\mathbb{Q}$ e $\mathbb{Q}$. Per il Teorema 10.32 o per l'Esercizio 10.51, $(a;b)\cap\mathbb{Q}\cong\mathbb{Q}$ anche quando a o b sono irrazionali; in particolare $(0;\sqrt{2})\cap\mathbb{Q}\cong(0;1)\cap\mathbb{Q}$ e $(\sqrt{2};2)\cap\mathbb{Q}\cong(1;2)\cap\mathbb{Q}$ e quindi

$$\begin{aligned}(0;2)\cap\mathbb{Q}&=((0;\sqrt{2})\cap\mathbb{Q})\cup((\sqrt{2};2)\cap\mathbb{Q})\\&\cong((0;1)\cap\mathbb{Q})\cup((1;2)\cap\mathbb{Q})\\&=((0;2)\setminus\{1\})\cap\mathbb{Q}.\end{aligned}$$

Al contrario l'ordine $(0;2)$ non è isomorfo a $(0;2)\setminus\{1\}$ dato che il primo spazio è connesso mentre il secondo non lo è.

Teorema 10.26 (Cantor)**.** *Ogni ordine lineare, denso, Dedekind-completo e con almeno due elementi, è più che numerabile. In particolare: $\mathbb{R}$ è più che numerabile.*

Dimostrazione. Sia $(L, \leq)$ un ordine lineare, denso, Dedekind-completo e con almeno due elementi. È immediato verificare che L è infinito, quindi per assurdo supponiamo che $\{x_n \mid n \in \mathbb{N}\}$ sia una enumerazione di L. Costruiremo una successione crescente $(a_n)_n$ ed una successione decrescente $(b_n)_n$ di elementi di L

$$a_0 < a_1 < a_2 < \ldots \cdots < b_2 < b_1 < b_0$$

tali che non esiste nessun $x \in L$ che maggiora tutti gli a_n e minora tutti i b_n. In particolare L non è Dedekind-completo, contraddicendo la nostra ipotesi. Fissiamo due elementi $a_0 < b_0$: dati $a_0 < \cdots < a_{n-1} < b_{n-1} < \cdots < b_0$, per densità possiamo trovare degli elementi tra a_{n-1} e b_{n-1}, e sia k_n il minimo k tale che $a_{n-1} < x_k < b_{n-1}$. Poniamo $a_n = x_{k_n}$. Analogamente sia $b_n = x_{h_n}$ dove h_n è il minimo h tale che $a_n < x_h < b_{n-1}$. Dalla definizione di k_i segue che

$$n < m \Rightarrow k_n < k_m \tag{10.9a}$$

e

$$a_n < x_i < b_{n-1} \Rightarrow k_n < i. \tag{10.9b}$$

Quindi se x_i fosse un elemento maggiore degli a_n e minore dei b_n, l'indice i dovrebbe essere maggiore di ogni k_n per (10.9b) e dato che $\lim_{n\to\infty} k_n = \infty$ per (10.9a), tale i non può esistere. □

Ricordiamo che ad ogni ordine lineare $(L, \leq)$ possiamo associare la **topologia degli intervalli** o **topologia dell'ordine** generata dalle semirette aperte $\{x \in L \mid x < b\}$ e $\{x \in L \mid a < x\}$, con $a, b \in L$. Un isomorfismo tra ordini lineari è un omeomorfismo tra gli spazi topologici corrispondenti. Osserviamo che $D \subseteq L$ è denso secondo la definizione di pagina 153 se e solo se è un insieme denso in questa topologia. Se L contiene un insieme denso e numerabile (cioè se è separabile in questa topologia) diremo che è **separabile**.

Teorema 10.27. $(\mathbb{R}, \leq)$ *è, a meno di isomorfismo, l'unico ordine lineare Dedekind-completo, separabile, senza primo o ultimo elemento.*

Dimostrazione. Sia $(X, \trianglelefteq)$ un ordine lineare Dedekind-completo, separabile, senza primo o ultimo elemento e sia D il suo sottoinsieme denso e numerabile. Allora $(D, \trianglelefteq)$ un ordine lineare numerabile senza primo o ultimo elemento e quindi per il Teorema 10.32 c'è una biezione strettamente crescente $F\colon \mathbb{Q} \to D$. Per ogni $r \in \mathbb{R}$ possiamo trovare un $p \in \mathbb{Q}$ tale che $r \leq p$ e quindi l'insieme $\{F(q) \mid q \in \mathbb{Q} \wedge q \leq r\}$ è limitato superiormente da $F(p)$. Possiamo quindi estendere F ad $\mathbb{R}$ ponendo

$$F(r) = \sup\{F(q) \mid q \in \mathbb{Q} \wedge q \leq r\}$$

dove il sup è calcolato secondo l'ordinamento $\trianglelefteq$. Chiaramente $r \leq s \Rightarrow F(r) \trianglelefteq F(s)$ e se $r < s$ prendiamo $q_1, q_2 \in \mathbb{Q}$, con $r < q_1 < q_2 < s$: allora $F(r) \trianglelefteq F(q_1) \triangleleft F(q_2) \trianglelefteq F(s)$. Quindi F è strettamente crescente. Dobbiamo verificare che F è suriettiva. Se $x \in X$ scelgo $d \in D$ tale che $x \triangleleft d$ e sia $p \in \mathbb{Q}$ tale che $F(p) = d$. L'insieme

$$A = \{r \in \mathbb{R} \mid F(r) \trianglelefteq x\}$$

è limitato superiormente da p e quindi possiamo calcolare $\bar{r} = \sup A$ secondo l'ordinamento $\leq$. Verifichiamo che $F(\bar{r}) = x$. Se $F(\bar{r}) \triangleleft x$ fissiamo un $d' \in D$ con $F(\bar{r}) \triangleleft d' \triangleleft x$. Sia $p' = F^{-1}(d')$: allora $p' \in A$ e quindi $p' \leq \bar{r}$, ma d'altra parte $F(\bar{r}) \triangleleft d'$ implica che $\bar{r} < p'$: contraddizione. Il caso in cui $x \triangleleft F(\bar{r})$ porta ugualmente ad una contraddizione ed è lasciato al lettore. □

10.F. La cardinalità del continuo e l'insieme di Cantor. Per ogni $x \in \{0,1\}^{\mathbb{N}}$ sia

$$\Phi(x) = \sum_{n=0}^{\infty} \frac{2x(n)}{3^{n+1}}. \tag{10.10}$$

Osservazione 10.28. $\Phi(x)$, essendo la somma di una serie, è data da una definizione induttiva (Esempio 7.9).

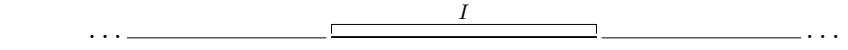
La serie in (10.10) converge ad un numero in $[0;1]$ e Φ è iniettiva (Esercizio 10.94), quindi $\mathscr{P}(\mathbb{N}) \precsim \mathbb{R}$. Poiché $\mathbb{R} \subseteq \mathscr{P}(\mathbb{Q})$ e $\mathscr{P}(\mathbb{Q})$ è in biezione con $\mathscr{P}(\mathbb{N})$, ne segue che $\mathbb{R} \precsim \mathscr{P}(\mathbb{N})$. Per il Teorema di Cantor-Schröder-Bernstein 10.14 e per la (10.7) segue che:

Proposizione 10.29. *Gli insiemi* $\mathbb{R}$, $\{0,1\}^{\mathbb{N}}$ *e* $\mathbb{N}^{\mathbb{N}}$ *sono equipotenti.*

10.F.1. *L'insieme di Cantor.* L'insieme $\operatorname{ran}(\Phi)$ della formula (10.10) è un insieme ben noto in Analisi. Per descriverlo introduciamo qualche definizione. Fissiamo un intervallo chiuso $I = [a;b]$ non degenere (cioè $a < b$) di $\mathbb{R}$ e fissiamo un $r \in (0;1)$. Rimuoviamo da I l'intervallo aperto centrato nel punto medio di I di ampiezza $r(b-a)$. Otteniamo così due intervalli chiusi non degeneri

$$\begin{aligned} I_{(0;r)} &= \left[a; a + \frac{1+2r}{2}(b-a)\right] \\ I_{(1;r)} &= \left[b - \frac{1+2r}{2}(b-a); b\right] \end{aligned} \tag{10.11}$$

Nella figura qui sotto vediamo un esempio con $r = 1/2$: dato un intervallo chiuso $I \subseteq \mathbb{R}$



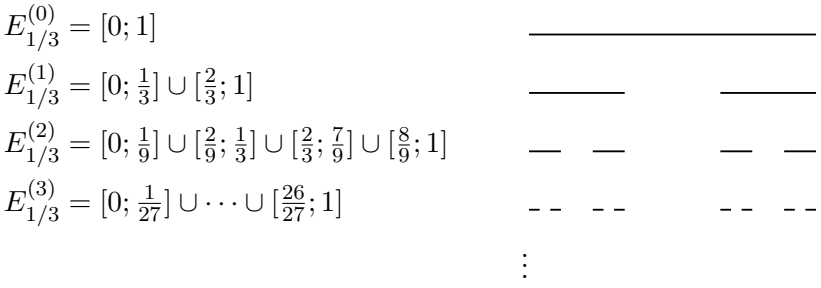
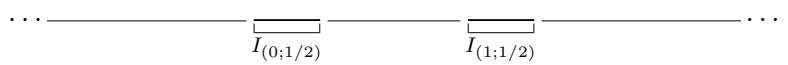


Figura 3. La costruzione dell'insieme di Cantor.

rimuoviamo la parte centrale di I di lunghezza $1/2$ della lunghezza di I e otteniamo $I_{(0;1/2)}$ e $I_{(1;1/2)}$:



L'**insieme ternario di Cantor** è definito come

$$E_{1/3} = \bigcap_n E^{(n)}_{1/3}, \tag{10.12}$$

dove $E^{(0)}_{1/3}$ è l'intervallo $[0;1]$, $E^{(n)}_{1/3} \subseteq E^{(n-1)}_{1/3}$ è unione di 2^n intervalli chiusi di lunghezza 3^{-n} ottenuti applicando la costruzione (10.11) con $r = 1/3$ a ciascuno dei 2^{n-1} intervalli di $E^{(n-1)}_{1/3}$.

Osservazione 10.30. La costruzione di $E_{1/3}$ è giustificata dal Corollario 7.5. Sia A la famiglia di tutti i sottoinsiemi di $\mathbb{R}$ della forma $I_1 \cup \cdots \cup I_m$ con $I_1, \ldots, I_m$ intervalli chiusi e disgiunti, sia $a = [0;1] \in A$, sia

$$F\colon A \to A, \qquad I_1 \cup \cdots \cup I_m \mapsto I'_1 \cup \cdots \cup I'_m$$

dove per ogni intervallo chiuso $I = [a;b]$

$$I' = [a; a + (b-a)/3] \cup [b - (b-a)/3; b],$$

allora si ha $f\colon \mathbb{N} \to A$ tale che $f(n) = E^{(n)}_{1/3}$.

Non è difficile verificare (Esercizio 10.95) che $\operatorname{ran}(\Phi) = E_{1/3}$ e quindi Φ è una biezione tra $2^{\mathbb{N}}$ e $E_{1/3}$. Ma è possibile dimostrare molto di più.

Se $\trianglelefteq$ è un ordinamento lineare su A, l'**ordinamento lessicografico** su $A^{\mathbb{N}}$ è così definito: dati $x, y \in A^{\mathbb{N}}$,

$$x \leq_{\text{lex}} y \;\Leftrightarrow\; x = y \vee \exists n \in \mathbb{N}\,[x(n) \lhd y(n) \wedge \forall i < n\,(x(i) = y(i))]$$

dove $\lhd$ è l'ordine stretto definito da $\trianglelefteq$. In particolare $\leq_{\text{lex}}$ è un ordine lineare su $2^{\mathbb{N}}$ e per l'Esercizio 10.94

$$\Phi\colon (2^{\mathbb{N}}, \leq_{\text{lex}}) \to (E_{1/3}, \leq)$$

è un isomorfismo, quindi è un omeomorfismo tra lo spazio $2^{\mathbb{N}}$ con la topologica dell'ordine indotta da $\leq_{\text{lex}}$ e $E_{1/3}$ con la topologia indotta da $[0;1]$. In particolare $2^{\mathbb{N}}$ è compatto.

10.G. Insiemi equipotenti ad $\mathbb{R}$.

10.G.1. *Prodotti di copie di* $\mathbb{R}$. Per ogni insieme X, la funzione che associa alla n-upla $(x_0, \dots, x_{n-1}) \in X^n$ la successione

$$(x_0, \dots, x_{n-1}, x_{n-1}, x_{n-1}, \dots) \in X^{\mathbb{N}}$$

è iniettiva e testimonia che $X^n \precsim X^{\mathbb{N}}$, quindi per il Teorema 10.18 e l'Esercizio 10.24, per ogni $n \geq 1$

$$(\{0,1\}^{\mathbb{N}})^n \precsim (\{0,1\}^{\mathbb{N}})^{\mathbb{N}} \approx \{0,1\}^{\mathbb{N}\times\mathbb{N}} \approx \{0,1\}^{\mathbb{N}}$$

da cui per il Teorema di Cantor-Schröder-Bernstein 10.14,

$$\mathbb{R} \approx \mathbb{R}^n \approx \mathbb{R}^{\mathbb{N}}.$$

In particolare $\mathbb{R} \approx \mathbb{C}$.

Osservazione 10.31. Non è possibile rimpiazzare l'esponente $\mathbb{N}$ con $\mathbb{R}$ nell'equazione precedente: poiché $\mathscr{P}(\mathbb{R}) \approx \{0,1\}^{\mathbb{R}} \precsim \mathbb{R}^{\mathbb{R}}$, allora per il Teorema di Cantor 10.23 $\mathbb{R}^{\mathbb{R}}$ non è equipotente ad $\mathbb{R}$.

10.G.2. *Lo spazio delle funzioni continue da* $\mathbb{R}$ *in* $\mathbb{R}$. L'insieme $\mathcal{C}(\mathbb{R},\mathbb{R})$ delle funzioni continue su $\mathbb{R}$ a valori reali è equipotente ad $\mathbb{R}$. Per vedere questo consideriamo la mappa $\mathcal{C}(\mathbb{R},\mathbb{R}) \to \mathbb{R}^{\mathbb{Q}}$, $f \mapsto f \restriction \mathbb{Q}$. Se $f, g \in \mathcal{C}(\mathbb{R},\mathbb{R})$ differiscono in $x_0 \in \mathbb{R}$, allora per continuità esiste un $\varepsilon > 0$ tale che f e g sono sempre distinte sull'intervallo $(x_0-\varepsilon; x_0+\varepsilon)$. Sia $q \in \mathbb{Q} \cap (x_0-\varepsilon; x_0+\varepsilon)$: allora $f(q) \neq g(q)$ e quindi $f \restriction \mathbb{Q} \neq g \restriction \mathbb{Q}$. Di conseguenza la mappa $f \mapsto f \restriction \mathbb{Q}$ è iniettiva e poiché $\mathbb{Q}$ è in biezione con $\mathbb{N}$, per l'esempio precedente si ha che $\mathcal{C}(\mathbb{R},\mathbb{R})$ si inietta in $\mathbb{R}$. Ovviamente $\mathbb{R}$ si inietta in $\mathcal{C}(\mathbb{R},\mathbb{R})$ e quindi i due insiemi sono equipotenti.

10.G.3. *Spazi metrici separabili.* Sia (X, d) uno spazio metrico separabile e sia $Q = \{q_n \mid n \in \mathbb{N}\}$ un sotto-insieme denso e numerabile di X. La funzione $F\colon X \to \mathbb{R}^{\mathbb{N}}$

$$F(x)\colon \mathbb{N} \to \mathbb{R} \qquad n \mapsto d(x, q_n)$$

è iniettiva, quindi $X \precsim \mathbb{R}$. In particolare questo vale quando X è una varietà topologica (metrica e separabile) o uno spazio vettoriale normato e separabile, e poiché $\mathbb{R}$ si inietta in un X siffatto, abbiamo un'altra famiglia di esempi di insiemi equipotenti ad $\mathbb{R}$. In particolare ogni **spazio di Banach** (cioè uno spazio vettoriale su $\mathbb{R}$ normato e completo) separabile è equipotente ad $\mathbb{R}$.

10.G.4. *Spazi secondo numerabili.* Sia X uno spazio secondo numerabile e sia $\mathcal{B} = \{V_n \mid n \in \mathbb{N}\}$ una base per la sua topologia $\mathcal{T}$.

La funzione

$$\mathcal{T} \to \mathscr{P}(\mathbb{N}) \qquad U \mapsto \{n \in \mathbb{N} \mid V_n \subseteq U\}$$

è iniettiva, quindi $\mathcal{T} \precsim \mathbb{R}$. Passando ai complementi si ha che $\mathcal{C}$, l'insieme dei chiusi di X, si inietta in $\mathbb{R}$.

Se X è T_2 allora la funzione

$$F\colon X \to \{0,1\}^{\mathbb{N}}, \qquad F(x)(n) = 1 \Leftrightarrow x \in V_n$$

è iniettiva, quindi $X \precsim \mathbb{R}$.

Poiché $\mathbb{R}^n$, $\mathbb{R}^{\mathbb{N}}$, uno spazio di Banach separabile, ecc., sono spazi T_1, e quindi i singoletti sono dei chiusi, si ha che le loro topologie sono equipotenti ad $\mathbb{R}$.

10.H. Costruzioni mediante *back-and-forth*.

Teorema 10.32 (Cantor)**.** *Se $(X, \trianglelefteq)$ è un ordine lineare, numerabile, denso, senza primo o ultimo elemento, allora è isomorfo a $(\mathbb{Q}, \leq)$.*

Dimostrazione. Siano $X = \{x_n \mid n \in \mathbb{N}\}$ e $\mathbb{Q} = \{q_n \mid n \in \mathbb{N}\}$ enumerazioni senza ripetizioni. Costruiremo induttivamente delle funzioni p_n tali che

(a) $p_0 \subseteq p_1 \subseteq \ldots$,

(b) $x_n \in \mathrm{dom}(p_{2n}) \subset X$ e $q_n \in \mathrm{ran}(p_{2n+1}) \subset \mathbb{Q}$,

(c) $\mathrm{dom}(p_n)$ è finito e $p_n\colon \mathrm{dom}(p_n) \to \mathrm{ran}(p_n)$ è una biezione che preserva l'ordine, vale a dire

$$\forall x, y \in \mathrm{dom}(p_n)\, (x \trianglelefteq y \Leftrightarrow p_n(x) \leq p_n(y))\,.$$

Una volta ottenuta la successione delle p_n, è possibile definire

$$F = \bigcup_n p_n.$$

La condizione (a) ci garantisce che F è una funzione, la (b) che $\mathrm{dom}(F) = X$ e $\mathrm{ran}(F) = \mathbb{Q}$ e la (c) che F preserva l'ordine in quanto per ogni $x_n, x_m \in X$, i valori $F(x_n)$ e $F(x_m)$ sono dati da $p_N(x_n)$ e $p_N(x_m)$, per ogni $N \geq 2\max(n,m)$. Resta soltanto da costruire le p_n.

La funzione $p_0 = \{(x_0, q_0)\}$ soddisfa le condizioni (a)–(c). Supponiamo che p_n sia definita e che (a)–(c) siano soddisfatte.

Se $n{+}1 = 2m$ e se $x_m \in \mathrm{dom}(p_n)$ oppure $n{+}1 = 2m{+}1$ e se $y_m \in \mathrm{ran}(p_n)$, allora poniamo $p_{n+1} = p_n$: è facile verificare che p_{n+1} soddisfa (a)–(c).

Supponiamo invece che $n + 1 = 2m$ e $x_m \notin \mathrm{dom}(p_n)$. Consideriamo tre casi:

Caso 1: $x_m \lhd \min(\mathrm{dom}(p_n))$. Sia $q = \min(\mathrm{ran}(p_n)) - 1$ e poniamo $p_{n+1} = p_n \cup \{(x_m, q)\}$.

Caso 2: $\max(\mathrm{dom}(p_n)) \lhd x_m$. Sia $q = \max(\mathrm{ran}(p_n)) + 1$ e poniamo $p_{n+1} = p_n \cup \{(x_m, q)\}$.

Caso 3: esistono $x, x' \in \mathrm{dom}(p_n)$ tali che $x \lhd x_m \lhd x'$, dove x e x' sono elementi consecutivi di $\mathrm{dom}(p_n)$, cioè non esiste alcun $x'' \in \mathrm{dom}(p_n)$ per cui $x \lhd x'' \lhd x'$. Sia $q = \frac{1}{2}(p_n(x') + p_n(x))$ e poniamo $p_{n+1} = p_n \cup \{(x_m, q)\}$.

In tutti e tre i casi è immediato verificare che p_{n+1} soddisfa (a)–(c).

Supponiamo infine che $n + 1 = 2m + 1$ e $q_m \notin \mathrm{ran}(p_n)$. Nuovamente ci sono tre casi da considerare: $q_m < \min(\mathrm{ran}(p_n))$, o $\max(\mathrm{ran}(p_n)) < q_m$, oppure $q < q_m < q'$, per qualche $q, q' \in \mathrm{ran}(p_n)$. In ciascuno dei casi si procede come sopra sfruttando il fatto che X non ha minimo (Caso 1), non ha massimo (Caso 2) ed è denso (Caso 3). □

La costruzione nella dimostrazione del Teorema 10.32 è nota come metodo del *back-and-forth*, in quanto dobbiamo assicurarci che la funzione F sia definita su tutti gli x_n (*back*) e che assuma tutti i valori y_n (*forth*). Usando solo una delle due parti della costruzione possiamo dimostrare che ogni ordine lineare numerabile è immergibile in $\mathbb{Q}$.

Teorema 10.33. *Se $(X, \trianglelefteq)$ è un ordine lineare numerabile, allora c'è una funzione strettamente crescente $F\colon X \to \mathbb{Q}$. In particolare, due ordini lineari, numerabili, densi, senza primo o ultimo elemento, sono isomorfi.*

Dimostrazione. Sia $\{x_n \mid n \in \mathbb{N}\}$ un'enumerazione di X. È sufficiente costruire una successione di funzioni p_n tali che

(a) $p_0 \subseteq p_1 \subseteq \ldots$,

(b) $\mathrm{dom}(p_n) = \{x_0, \ldots, x_n\}$,

(c) $\mathrm{dom}(p_n)$ è finito e $p_n\colon \mathrm{dom}(p_n) \to \mathrm{ran}(p_n)$ è una biezione che preserva l'ordine, vale a dire

$$\forall i, j < n\, (x_i \lhd x_j \Leftrightarrow p_n(x_i) < p_n(x_j))\,.$$

$F = \bigcup_n p_n\colon X \to \mathbb{Q}$ è la funzione cercata. La costruzione delle p_n segue la falsariga della dimostrazione del Teorema 10.32. Poniamo $p_0 = \{(x_0, 0)\}$ e supponiamo p_n è data e soddisfa (a)–(c). Consideriamo i tre casi: $x_{n+1} \lhd \min\{x_0, \ldots, x_n\}$, $\max\{x_0, \ldots, x_n\} \lhd x_{n+1}$ e x_{n+1} si trova tra due elementi $\lhd$-consecutivi x_i e x_j di $\{x_0, \ldots, x_n\}$. In tutti e tre i casi è possibile trovare un razionale q per cui $p_{n+1} = p_n \cup \{(x_{n+1}, q)\}$ soddisfa (a)–(c). □

Sempre utilizzando il metodo del *back-and-forth* è possibile dimostrare che l'ordine $\mathbb{Q}$ ha molti automorfismi:

Teorema 10.34. *Se $A, B \subset \mathbb{Q}$ sono insiemi finiti di ugual cardinalità, allora c'è un isomorfismo $f\colon (\mathbb{Q}, <) \to (\mathbb{Q}, <)$ tale che $f[A] = B$.*

Ricordiamo (pag. 57) che un ordine lineare $(L, \leq)$ si dice **omogeneo** se per ogni $a, a', b, b' \in L$ con $a < b$ e $a' < b'$ c'è un automorfismo F di L tale che $F(a) = a'$ e $F(b) = b'$. Equivalentemente (Esercizio 10.58) se per ogni coppia di sottoinsiemi finiti $A, B \subseteq L$ di uguale cardinalità, c'è sempre un automorfismo F di L tale che $F[A] = B$. Il Teorema 10.34 mostra quindi che $\mathbb{Q}$ è omogeneo.

Mediante una costruzione *back-and-forth* si dimostra che il grafo aleatorio numerabile R_ω della Sezione 5.H.5 è unico a meno di isomorfismi e che contiene ogni grafo numerabile (Esercizio 10.59).

Teorema 10.35. (a) *Ogni grafo numerabile che soddisfa la proprietà* ρ *della Definizione 5.20 è isomorfo a* R_ω.

(b) *Ogni grafo numerabile è isomorfo ad un sottografo indotto di* R_ω.

(c) *Se $A, B \subseteq \mathrm{R}_\omega$ sono finiti e $f\colon A \to B$ è un isomorfismo tra i sottografi indotti, cioè è una biezione tale che $\forall a_1, a_2 \in A\ (a_1\ E\ a_2 \Rightarrow f(a_1)\ E\ f(a_2))$, allora c'è un automorfismo $\hat{f}$ di R_ω tale che $\hat{f} \restriction A = f$.*

Quindi d'ora in poi R_ω denota un arbitrario grafo numerabile aleatorio. Nel prossimo esempio vedremo un altra costruzione esplicita di R_ω. La costruzione richiede conoscenze più avanzate di teoria dei numeri e non sarà usato in seguito.

Esempio 10.36. Se $a \in \mathbb{N}$ e $p \neq 2$ è primo, la quantità

$$\left(\frac{a}{p}\right) \stackrel{\text{def}}{=} \begin{cases} 1 & \text{se } p \nmid a \text{ e } \exists k \in \mathbb{N}\ \left(p \mid (a - k^2)\right), \\ -1 & \text{se } \neg\exists k \in \mathbb{N}\ \left(p \mid (a - k^2)\right), \\ 0 & \text{se } p \mid a \end{cases}$$

è nota come **simbolo di Legendre** di$a$ e p. Il Teorema di reciprocità quadratica di Gauß asserisce che se p, q sono primi dispari

$$\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right).$$

Per il Teorema di Dirichlet sulle progressioni aritmetiche (vedi Esercizio 2.8(vi)) l'insieme $P = \{p \mid p\text{primo e } p \equiv 1 \mod 4\}$ è infinito e se $p, q \in P$, allora $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$. Quindi la relazione $E \subseteq P \times P$

$$p\ E\ q \Leftrightarrow \left(\frac{p}{q}\right) = 1$$

è irriflessiva e simmetrica, cioè (P, E) è un grafo. Per dimostrare che si tratta di un grafo aleatorio, fissiamo $p_0, \ldots, p_n, q_0, \ldots, q_m \in P$ distinti: vogliamo

un $p \in P$ tale che $\left(\frac{p}{p_i}\right) = 1$ e $\left(\frac{p}{q_i}\right) = -1$ per tutti gli $i \leq n$ e $j \leq m$. Fissiamo a_i e b_j tali che $\left(\frac{a_i}{p_i}\right) = 1$ e $\left(\frac{b_j}{q_j}\right) = -1$. Per il Teorema cinese del resto 6.29 c'è un $x \in \mathbb{N}$ tale che

$$\begin{cases} x \equiv 1 \mod 4 \\ x \equiv a_i \mod p_i i \leq n \\ x \equiv b_j \mod q_i j \leq m \end{cases} \tag{10.13}$$

Sia $M = 4p_0 \cdots p_n \cdot q_1 \cdots q_m$. Nuovamente per il Teorema di Dirichlet c'è un primo p tale che $p \equiv x \mod M$. Quindi p è soluzione del sistema (10.13) ed è il primo cercato.

10.I. Costruzioni ricorsive. Come abbiamo già visto nelle precedenti Sezioni 6.B, 7 e 9, le definizioni induttive sono di interesse per la logica e sono molto comuni in matematica. Certe costruzioni induttive possono essere estese al transfinito.

10.I.1. *Ricorsione transfinita e insiemi derivati.*

Definizione 10.37. Il **derivato** di uno spazio topologico X è

$$X' = \{x \in X \mid x \text{ non è isolato in } X\}.$$

Poiché

$$X \setminus X' = \bigcup \{\{x\} \mid \{x\} \text{ aperto in } X\}$$

ne segue che X' è chiuso in X.

Uno spazio topologico si dice **perfetto** se non contiene punti isolati, cioè se coincide col suo derivato. L'insieme vuoto e gli intervalli (non degeneri) di $\mathbb{R}$ sono esempi di spazi perfetti, mentre $\mathbb{N}$ con la topologia discreta (cioè quella indotta come sottoinsieme di $\mathbb{R}$) non è perfetto, dato che il suo derivato è vuoto. Anche l'insieme $\{1 - 2^{-n} \mid n \in \mathbb{N}\} \cup \{1\}$, che ha tipo d'ordine $\omega + 1$, non è perfetto, dato che il suo derivato è $\{1\}$, che a sua volta non è un insieme perfetto, dato che il suo derivato è vuoto.

A partire da X si definisce $X^{(n)}$ applicando n-volte l'operazione di derivazione a X. L'insieme $X^{(\omega)} = \bigcap_n X^{(n)}$ non è necessariamente perfetto, quindi la procedura di iterazione può essere iterata nel transfinito ponendo

$$\begin{aligned} X^{(0)} &= X \\ X^{(\alpha+1)} &= (X^{(\alpha)})' \\ X^{(\lambda)} &= \bigcap_{\alpha<\lambda} X^{(\alpha)} \qquad \text{se } \lambda \text{ è limite.} \end{aligned}$$

Quindi gli $X^{(\alpha)}$ formano una successione decrescente di chiusi, nel senso che $X^{(\beta)} \subseteq X^{(\alpha)}$ se $\alpha < \beta$; se $X^{(\bar{\alpha})} = X^{(\bar{\alpha}+1)}$ allora $X^{(\bar{\alpha})} = X^{(\beta)}$ per ogni $\beta > \bar{\alpha}$ e diremo che l'operazione di derivazione termina. Il più piccolo di

questi ordinali $\bar{\alpha}$ si dice **rango di Cantor-Bendixson** di X e lo si indica con $\|X\|_{\mathrm{CB}}$.

Gli insiemi $X^{(\|X\|_{\mathrm{CB}})} = \bigcap_\nu X^{(\nu)}$ e $X \setminus X^{(\|X\|_{\mathrm{CB}})}$ sono, rispettivamente, la **parte perfetta** e la **parte sparsa**[10] di X. Uno spazio che non ha punti isolati coincide con la sua parte perfetta. All'estremo opposto ci sono gli **spazi sparsi**, in cui la parte perfetta è vuota. La funzione o^X definita su $X \setminus X^{(\|X\|_{\mathrm{CB}})}$ come

$$o^X(x) = o(x) = \text{l'unico } \alpha < \|X\|_{\mathrm{CB}} \text{ tale che } x \in X^{(\alpha)} \setminus X^{(\alpha+1)}$$

è l'**ordine di isolamento** di x in X. Quindi

$$X^{(\alpha)} = X \setminus \{x \in X \mid o(x) < \alpha\}\,.$$

Proposizione 10.38. *In uno spazio secondo numerabile non esiste nessuna successione crescente di aperti di lunghezza ω_1, cioè non ci sono aperti U_α ($\alpha < \omega_1$) tali che*

$$\alpha < \beta \Rightarrow U_\alpha \subset U_\beta.$$

Analogamente non esiste nessuna successione decrescente di chiusi di lunghezza ω_1, cioè non ci sono chiusi C_α ($\alpha < \omega_1$) tali che

$$\alpha < \beta \Rightarrow C_\alpha \supset C_\beta.$$

Dimostrazione. Sia X uno spazio topologico e $\{V_n \mid n \in \mathbb{N}\}$ una sua base. Se, per assurdo, esistessero U_α ($\alpha < \omega_1$) come sopra, allora la funzione $\{\alpha \mid \alpha < \omega_1\} \to \mathbb{N}$

$$\alpha \mapsto \min\{n \in \mathbb{N} \mid V_n \subseteq U_{\alpha+1} \wedge V_n \nsubseteq U_\alpha\}$$

sarebbe un'iniezione, contro la definizione di ω_1.

Il caso dei chiusi si ottiene prendendo i complementi. □

Fissiamo uno spazio topologico X secondo numerabile e fissiamo una sua base $\{U_n \mid n \in \mathbb{N}\}$. Per ogni sottospazio $C \subseteq X$ possiamo definire il suo derivato C' prendendo C come spazio ambiente e la funzione $F_C \colon C \setminus C' \rightarrowtail \mathbb{N}$

$$F_C(x) = \min\{n \in \mathbb{N} \mid U_n \cap C = \{x\}\}$$

è iniettiva. In particolare, se $C_0 = X$ e $C_\alpha = X^{(\alpha)}$, allora i C_α sono una sequenza decrescente di chiusi quindi $\|X\|_{\mathrm{CB}} < \omega_1$ per la Proposizione 10.38, e quindi $X^{(\|X\|_{\mathrm{CB}})}$ è perfetto. Inoltre, se $P \subseteq X$ è perfetto, allora $P \subseteq X^{(\alpha)}$ per tutti gli α e in particolare $P \subseteq X^{(\|X\|_{\mathrm{CB}})}$. La funzione $F \colon \bigcup_{\alpha<\|X\|_{\mathrm{CB}}} X^{(\alpha)} \setminus X^{(\alpha+1)} \to \{\alpha \mid \alpha < \|X\|_{\mathrm{CB}}\} \times \mathbb{N}$ definita da

$$F(x) = (o(x), F_{C^{(o(x))}}(x))$$

[10] In inglese: *scattered*.

è un'iniezione. Poiché $\|X\|_{\mathrm{CB}} < \omega_1$, c'è un'iniezione $g\colon \{\alpha \mid \alpha < \|X\|_{\mathrm{CB}}\} \rightarrowtail \mathbb{N}$: componendo F con la mappa $\{\alpha \mid \alpha < \|X\|_{\mathrm{CB}}\} \times \mathbb{N} \rightarrowtail \mathbb{N} \times \mathbb{N}$, $(\nu, i) \mapsto (g(\nu), i)$, otteniamo che

$$X \setminus X^{(\|X\|_{\mathrm{CB}})} = \bigcup_{\alpha<\|X\|_{\mathrm{CB}}} X^{(\alpha)} \setminus X^{(\alpha+1)} \precsim \mathbb{N} \times \mathbb{N} \approx \mathbb{N}.$$

Abbiamo quindi dimostrato il

Teorema 10.39 (Cantor-Bendixson)**.** *Ogni spazio secondo numerabile X può essere partizionato come $X = P \cup S$, dove P è chiuso e perfetto e S è aperto e numerabile.*

In particolare, ogni chiuso C di $\mathbb{R}$ può essere decomposto in $C = P \cup S$, con P perfetto e S numerabile. Dimostreremo nella Sezione 21 che ogni insieme perfetto non vuoto $P \subseteq \mathbb{R}$ contiene una copia di $2^{\mathbb{N}}$ e quindi è equipotente ad $\mathbb{R}$.

La costruzione degli $X^{(\alpha)}$ è una definizione ricorsiva, ma di un tipo più generale di quelle viste finora,[11] visto che dobbiamo tener conto dei livelli limite. Una funzione $f\colon \mathrm{Ord} \to A$, dove Ord è la famiglia degli ordinali, è definita per ricorsione se è l'unica soluzione del seguente sistema

$$\begin{aligned} f(0) &= a \\ f(\alpha+1) &= F(\alpha, f(\alpha)) \\ f(\lambda) &= G(\lambda, (f(\alpha))_{\alpha<\lambda}) \qquad\qquad \text{se } \lambda \text{ è limite,} \end{aligned}$$

dove $a \in A$, $F\colon \mathrm{Ord} \times A \to A$, e G è definita per coppie della forma $(\lambda, (x_\alpha)_{\alpha<\lambda})$ con λ limite e $x_\alpha \in A$. In molti casi possiamo supporre che F non dipenda da α, cioè che $F\colon A \to A$. Per esempio, se X è uno spazio topologico e

$$A = \mathscr{P}(X), \quad a = X, \quad F(Y) = Y', \quad G(\lambda, (Y_\alpha)_{\alpha<\lambda}) = \bigcap_{\alpha<\lambda} Y_\alpha,$$

si ottiene la costruzione degli $X^{(\alpha)}$.

Lo studio delle definizioni ricorsive sugli ordinali sarà affrontato nella Sezione 13 del Capitolo IV.

10.I.2. *La topologia degli ordinali.* Ogni ordine lineare dotato della topologia dell'ordine è uno spazio topologico e ordini isomorfi generano spazi omeomorfi. Quindi ogni ordinale individua uno spazio topologico. Poiché un ordinale è un insieme bene ordinato a meno di isomorfismo, vorremmo selezionare un insieme bene ordinato canonico il cui tipo d'ordine è l'ordinale dato.

[11] *È vita, Jim, ma non del tipo che conosciamo.* — Mr. Spock, *Star Trek*

Seguendo von Neumann, *definiamo* un ordinale come uno specifico insieme bene ordinato, ponendo

$$0 = \emptyset, \quad 1 = \{0\}, \quad 2 = \{0, 1\}, \ldots \quad \omega = \mathbb{N} = \{0, 1, 2, \ldots\}$$

e più in generale $\alpha = \{\beta \mid \beta < \alpha\}$, così che $\alpha < \beta$ sta per $\alpha \in \beta$. Nel Capitolo IV dimostreremo che, con questa definizione, ogni ordinale è bene ordinato e che ogni insieme bene ordinato è isomorfo ad un unico ordinale.

I punti non isolati dello spazio topologico α sono esattamente gli ordinali limite minori di α. Gli spazi $\omega+1$ e $\omega+n$ sono omeomorfi per ogni $1 \leq n < \omega$ (Esercizio 10.85), mentre gli spazi $\omega + 1$ e $\omega + \omega + 1$ non sono omeomorfi, dato che

$$(\omega + 1)' = \{\omega\} \quad \text{e} \quad (\omega + \omega + 1)' = \{\omega, \omega + \omega\}.$$

Proposizione 10.40. *Un ordinale è uno spazio compatto se e solo se è zero oppure è un ordinale successore.*

Dimostrazione. Dimostreremo per induzione su α, che ogni ricoprimento aperto $\mathcal{U}$ di $\alpha + 1$ ammette un sotto-ricoprimento finito. (Per la Proposizione 10.10 possiamo applicare l'induzione agli ordinali, come descritto nella Sezione 10.B.1.) Se $\alpha = 0$ il risultato è immediato, quindi possiamo supporre che $\alpha > 0$ e che $\beta + 1$ sia compatto, per ogni $\beta < \alpha$. Sia $\mathcal{U}$ un ricoprimento aperto di $\alpha + 1$ e sia $U \in \mathcal{U}$ tale che $\alpha \in U$. Scegliamo $\beta < \alpha$ tale che $[\beta + 1, \alpha] \subseteq U$: per ipotesi induttiva c'è un $\mathcal{U}_0 \subseteq \mathcal{U}$ finito che ricopre $\beta + 1 \leq \alpha$, quindi $\mathcal{U}_0 \cup \{U\}$ è un ricoprimento aperto finito di $\alpha + 1$.

Viceversa, supponiamo λ sia un ordinale limite: allora $\{[0; \alpha) \mid \alpha < \lambda\}$ è un ricoprimento aperto di λ che non ha sotto-ricoprimenti aperti. □

Definizione 10.41. Uno spazio topologico di Hausdorff si dice **totalmente sconnesso** o **zero dimensionale** se ogni punto ha una base di intorni chiusi-aperti.

Uno spazio topologico si dice **completamente regolare**, se

$$\forall C \subseteq X \, \forall x \in X \, \big(C \text{ chiuso} \wedge x \notin C \Rightarrow \exists f \colon X \to [0; 1] \text{ continua} \\ \wedge f(x) = 1 \wedge \forall y \in C \, (f(y) = 0)\big)$$

Uno spazio metrico è completamente regolare (Teorema di Tietze), e uno spazio completamente regolare è di Hausdorff. Un ordinale è uno spazio totalmente sconnesso e completamente regolare (Esercizio 10.86).

Proposizione 10.42. *Sia X è uno spazio topologico completamente regolare che non si surietta su $\mathbb{R}$. Allora X è totalmente sconnesso.*

Dimostrazione. Fissato un $x \in X$ e V un suo intorno aperto, sia f una funzione continua tale che $f(x) = 0$ e $f(y) = 1$ per ogni $y \in X \setminus V$. Per

ipotesi c'è un $r \in (0;1) \setminus \mathrm{ran}(f)$. Allora $f^{-1}[0;r] = f^{-1}[0;r)$ è un intorno chiuso-aperto di x contenuto in V. □

Corollario 10.43. *Uno spazio metrico numerabile è totalmente sconnesso.*

Per l'Esercizio 10.78, ogni ordinale numerabile è omeomorfo ad un chiuso numerabile di $\mathbb{R}$, quindi per la Proposizione 10.40 ogni ordinale successore è omeomorfo ad un compatto numerabile di $\mathbb{R}$. Nella Sezione 24 del Capitolo V dimostreremo il converso: ogni compatto numerabile è omeomorfo ad un ordinale e quindi ad un compatto numerabile di $\mathbb{R}$.

Se $\beta \in \alpha$ allora β è un punto isolato di α se e solo se β è un ordinale successore. Quindi, fissato uno spazio topologico X, una funzione $f\colon \alpha \to X$ è continua se e solo se per ogni ordinale limite $\lambda \in \alpha$ e per ogni aperto $U \subseteq X$ con $f(\lambda) \in U$ c'è $\gamma < \lambda$ tale che $(\gamma;\lambda] \subseteq f^{-1}[U]$.

Proposizione 10.44. *Sia $f\colon \alpha \to \beta$ crescente e sia $\lambda \in \alpha$ limite. Allora*

$$f \text{ è continua in } \lambda \Leftrightarrow f(\lambda) = \sup_{\nu<\lambda} f(\nu).$$

Dimostrazione. ($\Rightarrow$) Dimostriamo il contrapositivo. Poiché f è crescente, $\sup_{\nu<\lambda} f(\nu) \leq f(\lambda)$. Se la disuguaglianza fosse stretta, allora $U = (\sup_{\nu<\lambda} f(\nu); f(\lambda)]$ sarebbe aperto, mentre $f^{-1}[U] = \{\lambda\}$ non è aperto.

($\Leftarrow$) Poiché $\sup_{\nu<\lambda} f(\nu) = f(\lambda)$ allora $f(\lambda)$ è limite, quindi è sufficiente dimostrare che per ogni $\eta < f(\lambda)$ c'è un $\gamma < \lambda$ tale che $\gamma < \nu < \lambda \Rightarrow \eta < f(\nu) < f(\lambda)$, il che è immediato dato che f è crescente. □

10.J. Dalla teoria ingenua alla teoria assiomatica degli insiemi. Finora non abbiamo definito con precisione che cosa sia un ordinale o una cardinalità — abbiamo semplicemente detto che un ordinale è un buon ordine a meno di isomorfismo e una cardinalità è un insieme a meno di biezioni. Potremmo quindi definire un ordinale come la classe di equivalenza di un buon ordine mediante la relazione $\cong$ di isomorfismo e una cardinalità come la classe di equivalenza di un insieme mediante la relazione $\approx$ di equipotenza. L'ordinale 3 risulterebbe la famiglia di tutti i buoni ordini che hanno per diagramma $\circ\!\!\rightarrow\!\!\circ\!\!\rightarrow\!\!\circ$, e la cardinalità 3 come la collezione di tutti gli insiemi equipotenti a $\{0,1,2\}$ ovvero la collezione di tutti gli insiemi che soddisfano l'enunciato $\boldsymbol{\varepsilon}_3$ di pagina 15. Le classi di equivalenza così ottenute sono immense: se $A \neq \emptyset$ e B è un insieme arbitrario, allora $\{B\} \times A$ è equipotente ad A mediante la biezione $A \ni a \mapsto (B,a) \in \{B\} \times A$. In altre parole, se $A \neq \emptyset$ allora $|A|$ è equipotente con l'insieme di tutti gli insiemi; un discorso analogo vale per gli ordinali. (L'unico insieme equipotente all'insieme vuoto è l'insieme stesso). Nella teoria ingenua degli insiemi, vale a dire nelle presentazioni elementari, non assiomatiche, della teoria degli insiemi, come usualmente viene esposta nei libri di matematica, non si dà molto

peso a questo tipo di problemi. Tuttavia l'uso indiscriminato di insiemi molto grandi comporta seri problemi che impediscono lo sviluppo tecnico della disciplina. Questi problemi si manifestano sotto forma di *antinomie* o *paradossi*. Vediamone due, una relativa alla nozione di ordinale, l'altra relativa alla nozione di cardinalità .

10.J.1. *Antinomia di Burali-Forti.* Per la Proposizione 10.10, $(\mathrm{Ord}, \leq)$ è un buon ordine, dove Ord è l'insieme degli ordinali. Osserviamo che se $(P, \leq_P)$ è un buon ordine di tipo d'ordine $\alpha \in \mathrm{Ord}$, allora P è isomorfo a $\{\beta \in \mathrm{Ord} \mid \beta < \alpha\}$ mediante la mappa che manda x nel tipo d'ordine del segmento iniziale $\{y \in P \mid y <_P x\}$. Quindi, se $\Omega \in \mathrm{Ord}$ è il tipo d'ordine di $(\mathrm{Ord}, \leq)$, allora il buon ordine Ord è isomorfo al suo segmento iniziale $\{\alpha \in \mathrm{Ord} \mid \alpha < \Omega\}$, contro il Corollario 10.7.

10.J.2. *Antinomia di Cantor.* Se X è l'insieme di tutti gli insiemi, allora $\mathscr{P}(X) \subseteq X$, da cui si ottiene subito una suriezione da X su $\mathscr{P}(X)$, contro il Teorema 10.23.

Visto che l'uso indiscriminato di totalità molto grandi (l'insieme di tutti gli insiemi, l'insieme di tutti gli ordinali, ...) porta a contraddizioni logiche, è necessario porre su basi solide le costruzioni viste nelle pagine precedenti, a cominciare dalla stessa teoria degli insiemi. Il piano è suddividere gli aggregati di oggetti in due regioni: le *collezioni piccole* dette *insiemi* e *collezioni grandi* dette *classi proprie*. Nella prima regione ritroveremo gli insiemi usuali della matematica ($\mathbb{N}$, $\mathbb{R}$, le varietà differenziabili, ecc), mentre nelle seconde saranno relegate le totalità troppo grandi (l'insieme di tutti gli insiemi, l'insieme di tutti gli ordinali, ...). Nel Capitolo IV vedremo come la teoria assiomatica degli insiemi sia in grado di delimitare l'ambito di applicabilità dei suoi risultati, neutralizzando così le antinomie logiche.

10.K. Un bignamino di teoria degli insiemi. Per il lettore che scalpita per sapere come andrà a finire nel prossimo Capitolo (o, più probabilmente, per il lettore che è troppo pigro per leggerlo tutto), elenchiamo ora le idee principali.

I numeri naturali si definiscono come $0 = \emptyset$, $1 = \{0\}$, $2 = \{0, 1\}$, ..., e l'insieme dei numeri naturali $\{0, 1, \ldots\}$ lo si denota con ω. I numeri naturali sono degli ordinali ed un ordinale è identificato con l'insieme degli ordinali più piccoli,

$$\alpha = \{\beta \mid \beta < \alpha\}$$

dove la relazione di ordine è semplicemente la relazione di appartenenza. Ogni insieme bene ordinato è isomorfo ad un unico ordinale. In altre parole: in ogni classe di equivalenza di *insiemi* bene ordinati è possibile individuare un buon ordine canonico. (La totalità Ord degli ordinali è una classe propria, e non è un ordinale.) Un ordinale è un **cardinale** se non è equipotente ad

un ordinale più piccolo. Ogni numero naturale è un cardinale, l'ordinale ω è un cardinale, mentre $\omega + 1 = \{0, 1, \ldots, \omega\}$ è equipotente a ω e quindi non è un cardinale. Il Teorema 10.18 dice che $\omega \times \omega$ è equipotente a ω, e questo fatto si generalizza a tutti i cardinali infiniti, cioè (Teorema 14.13)

Se κ è un cardinale infinito, allora $\kappa \times \kappa \approx \kappa$.

L'**assioma di scelta** AC asserisce che per ogni insieme non vuoto X c'è una funzione f che sceglie un elemento $f(Y) \in Y$ per ogni sottoinsieme non vuoto $Y \subseteq X$. Ammette molte formulazioni equivalenti, apparentemente non correlate, per esempio (Teorema 14.9):

Le seguenti affermazioni sono equivalenti • AC, • ogni insieme è bene ordinabile, • il Lemma di Zorn.

Il Lemma di Zorn asserisce che un insieme ordinato in cui tutte le catene hanno un estremo superiore ha un elemento massimale.

L'assioma della scelta ha importanti applicazioni in matematica (Sezione 25), ma per la sua natura non costruttiva può essere usato per costruire sottoinsiemi patologici di $\mathbb{R}^n$ (Sezione 25.C). Per evitare ciò sono stati introdotti numerosi indebolimenti di AC. Una di queste è l'**assioma di scelta numerabile** AC_ω, che asserisce che data una famiglia $\{A_n \mid n \in \mathbb{N}\}$ di insiemi non vuoti, c'è una successione $(a_n)_n$ tale che $a_n \in A_n$ per ogni n. Questo principio è indispensabile per dimostrare fatti elementari quali: un insieme infinito contiene una copia di $\mathbb{N}$, l'unione numerabile di insiemi numerabili è numerabile, l'esistenza della misura di Lebesgue, ... Un'altra forma debole di AC è BPI, l'affermazione che ogni ideale proprio in un'algebra di Boole può essere esteso ad un ideale massimale. Il principio BPI discende facilmente dal Lemma di Zorn. Più precisamente (Corollario 23.23)

Se B è un'algebra Boole bene ordinabile, ogni ideale proprio di B può essere esteso ad un ideale massimale.

Se A è un insieme bene ordinabile, sia

$$|A| = \text{il più piccolo ordinale } \alpha \text{ in biezione con } A.$$

Quindi in presenza dell'Assioma della Scelta, la nozione di 'cardinalità di un insieme' è ben definita. Se si abbandona AC la definizione di cardinalità richiede qualche nozione aggiuntiva di teoria degli insiemi (Sezione 14.F). Le operazioni sui cardinali sono definite come sopra, cioè $\kappa + \lambda$ è il cardinale equipotente all'insieme (bene-ordinabile) $\kappa \cup \lambda$ e $\kappa \cdot \lambda$ è il cardinale equipotente all'insieme (bene-ordinabile) $\kappa \times \lambda$. Quindi se κ e λ sono cardinali infiniti

la (10.5) e il Teorema 14.13 implicano che

$$\kappa + \lambda = \kappa \cdot \lambda = \max\{\kappa, \lambda\}.$$

(Poiché i cardinali sono tipi particolari di ordinali, potrebbe sorgere confusione dato che abbiamo già definito le operazioni di somma e prodotto di *ordinali*. Per evitare queste ambiguità è opportuno usare simboli diversi per i due tipi di operazioni. Noi useremo i simboli $\dot{+}$ e $\dot{\cdot}$ per le operazioni sugli ordinali.)

Anche la (10.6) si generalizza a tutti i cardinali infiniti (Teorema 14.18)

$$|X| = \kappa \geq \aleph_0 \Rightarrow |X^{<\mathbb{N}}| = \kappa$$

ovvero:

$$X \text{ infinito e bene ordinabile } \Rightarrow X \approx X^{<\mathbb{N}}.$$

Se non assumiamo qualche forma di assioma di scelta, non possiamo escludere che X sia un insieme infinito, cioè $n \precsim X$ per ogni $n \in \mathbb{N}$, ma tuttavia $\omega \not\precsim X$. In altre parole: X avrebbe più di n elementi, per ogni $n \in \mathbb{N}$, ma non conterrebbe una successione di elementi distinti. Poiché $\mathbb{N} \precsim X^{<\mathbb{N}}$, un X siffatto violerebbe la formula qui sopra. In assenza di scelta possiamo soltanto dimostrare che

$$\emptyset \neq X \Rightarrow X^{<\mathbb{N}} \approx (X^{<\mathbb{N}})^{<\mathbb{N}}$$

Questo risultati saranno utili quando considereremo linguaggi del prim'ordine arbitrari. Per esempio: se l'insieme dei simboli non logici di L ha taglia $\leq \kappa$, allora l'insieme degli L-termini e delle L-formule sono bene-ordinabili e di taglia $\leq \kappa$.

Una funzione finitaria su X è una $f\colon X^n \to X$ per qualche $n > 0$. Data una famiglia $\mathcal{F}$ di funzioni finitarie su un insieme non vuoto X, la chiusura di $Y \subseteq X$ è il più piccolo $\bar{Y} \subseteq X$ tale che $Y \subseteq \bar{Y}$ e $\bar{Y}$ è chiuso per le $f \in \mathcal{F}$, ed è indicato con $\mathrm{Cl}_{\mathcal{F}}(Y)$. Per esempio, se X è un anello, $\mathcal{F} = \{+, -, \cdot\}$, e $0_X \in Y \subseteq X$, allora $\bar{Y} = \mathrm{Cl}_{\mathcal{F}}(Y)$ è il più piccolo sottoanello di X contenente Y. Se Xè bene ordinabile, allora $\bar{Y}$ è di taglia $\leq \max(\aleph_0, |Y|)$. (Dobbiamo considerare $\aleph_0$ dato che Y potrebbe essere finito e tuttavia $\bar{Y}$ infinito.) Più in generale (Teorema 16.5)

Se $\mathcal{F}$ è una famiglia di funzioni finitarie su X, e X e $\mathcal{F}$ sono bene ordinabili con $|\mathcal{F}| \leq |X|$, allora $\mathrm{Cl}_{\mathcal{F}}(Y)$ è bene ordinabile e

$$|\mathrm{Cl}_{\mathcal{F}}(Y)| = \max(\aleph_0, |Y|, |\mathcal{F}|)$$

per ogni $Y \subseteq X$.

Esercizi

Esercizio 10.45. Dimostrare che $P + P \cong P \times 2$.

Esercizio 10.46. Dimostrare che se $(P, \leq)$ è un buon ordine e $Q \subseteq P$, allora Q con l'ordinamento indotto è un buon ordine.

Esercizio 10.47. Dimostrare che gli enunciati delle Proposizioni 10.3, 10.4 e 10.5 non valgono se il buon ordine $(P, \leq)$ è sostituito da $\mathbb{Q}$ o $\mathbb{R}$.

Esercizio 10.48. Dimostrare che $\mathrm{Down}(\mathbb{Q}) \setminus \{\emptyset, \mathbb{Q}\}$ e $\mathbb{R}$ non sono né isomorfi (come insiemi ordinati) né omeomorfi come spazi topologici.

Nei due esercizi seguenti, con **1** e **2** indichiamo, rispettivamente, gli ordini lineari con uno e due elementi.

Esercizio 10.49. Consideriamo il seguente elenco di ordini lineari di cardinalità del continuo:

$\mathbb{R} + \mathbb{R}$	$\mathbb{R} \times \mathbb{R}$	$\bigcup_{n\in\mathbb{Z}}(2n; 2n+1)$
$\mathbb{R} + \mathbf{1} + \mathbb{R}$	$\mathbb{R} + \mathbf{2} + \mathbb{R}$	$\mathbb{R} + (\omega + 1) + \mathbb{R}$
$\mathbb{R} \setminus \mathbb{Q}$	$\mathbb{R} \times \mathbb{Q}$	$\mathbb{Q} \times \mathbb{R}$
$(0;1] \cup (2;3)$	$(0;1] \cup [2;3)$	$(0;1] \cup \left\{2 - (n+1)^{-1} \mid n \in \mathbb{N}\right\} \cup [2;3)$
$[0;1) \times \mathbb{Z}$	$(0;1] \times \mathbb{Z}$	$(0;1] \times \mathbb{N}$
$[0;1) \times \mathbb{N}$	$[0;1] \times \mathbb{Z}$	$(0;1) \times \mathbb{Z}$
$[0;1)$	$(0;1) \cup (1;2)$	$\mathbb{R} \setminus \mathbb{Z}$.

Per ciascuna coppia, stabilire se sono isomorfi o meno.

Esercizio 10.50. Consideriamo il seguente elenco di ordini lineari numerabili:

$\mathbb{Q}$	$\mathbb{Q} + \mathbb{Q}$	$\mathbb{Q} + \mathbf{1} + \mathbb{Q}$
$\mathbb{Q} + \mathbf{2} + \mathbb{Q}$	$\mathbb{Q} \times \mathbb{Z}$	$\mathbb{Z} \times \mathbb{Q}$
$\mathbb{Q} \setminus \mathbb{Z}$		

Per ciascuna coppia, stabilire se sono isomorfi o meno.

Esercizio 10.51. Dimostrare direttamente, senza usare il Teorema 10.32, che $(a; b) \cap \mathbb{Q}$ e $\mathbb{Q}$ sono isomorfi, per ogni coppia di reali $a < b$.

Esercizio 10.52. Dimostrare che c'è una funzione crescente e continua $f\colon \mathbb{R} \to \mathbb{R}$ che mappa i numeri irrazionali sui numeri trascendenti.

Esercizio 10.53. Dimostrare che, a meno di isomorfismi, gli ordini lineari densi numerabili sono quattro:

$$\mathbb{Q}, \quad [0;1] \cap \mathbb{Q}, \quad [0;1) \cap \mathbb{Q}, \quad (0;1] \cap \mathbb{Q}.$$

Esercizio 10.54. Sia

$$\mathcal{I} = \left\{ \left(\frac{j}{3^{k+1}}; \frac{j+1}{3^{k+1}}\right) \mid j, k \in \mathbb{N} \wedge j \equiv 1 \mod 3 \right\}.$$

Verificare che gli intervalli in $\mathcal{I}$ sono le componenti connesse di $[0;1] \setminus E_{1/3}$.

Sia $\lhd$ l'ordinamento su $\mathcal{I}$ definito da $I \lhd J \Leftrightarrow \sup I < \inf J$. Verificare $(\mathcal{I}, \lhd)$ è isomorfo a $(\mathbb{Q}, <)$.

Esercizio 10.55. Dimostrare il Teorema 10.34.

Il prossimo esercizio dimostra che nessun intervallo aperto di $\mathbb{R}$ può essere decomposto in un unione numerabile di intervalli chiusi e disgiunti.

Esercizio 10.56. (i) Sia $\mathcal{I}$ una famiglia numerabile di intervalli chiusi a due a due disgiunti tali che $\bigcup \mathcal{I} = (a; b) \subset \mathbb{R}$. Definiamo l'ordine $\lhd$ su $\mathcal{I}$

$$\forall I, J \in \mathcal{I}\, (I \lhd J \Leftrightarrow \forall x \in I\, \forall y \in J\, (x < y))\,.$$

Dimostrare che $(\mathcal{I}, \lhd)$ è isomorfo a $(\mathbb{Q}, <)$.

(ii) Sia $F\colon (\mathcal{I}, \lhd) \to (\mathbb{Q}, <)$ un isomorfismo e sia $z \in \mathbb{R} \setminus \mathbb{Q}$. Allora gli insiemi $\bigcup\{I \in \mathcal{I} \mid F(I) < z\}$ e $\bigcup\{I \in \mathcal{I} \mid F(I) > z\}$ mostrano che $(a; b)$ è sconnesso. Concludere che una famiglia $\mathcal{I}$ come in (i) non esiste.

(iii) Generalizzare il risultato precedente ad ogni intervallo semi-aperto $[a; b)$ o $(a; b]$.

Esercizio 10.57. Sia L un ordine lineare numerabile non vuoto e sia Q uno tra $\mathbb{Q}$, $\mathbb{Q} \cap [0; 1)$ e $\mathbb{Q} \cap (0; 1]$ Verificare che $Q \times L$ è un ordine lineare denso e numerabile e in ciascun caso individuare il tipo d'ordine.

Esercizio 10.58. Dimostrare che $(L, \leq)$ è omogeneo se e solo se per ogni coppia di sottoinsiemi finiti $A, B \subseteq L$ di uguale cardinalità, c'è sempre un automorfismo F di L tale che $F[A] = B$.

Esercizio 10.59. Dimostrare il Teorema 10.35.

Esercizio 10.60. Dimostrare che

(i) se $\{X_1, \ldots, X_n\}$ è una partizione di $\mathbb{Q}$, allora qualche X_i contiene una copia isomorfa di $\mathbb{Q}$;

(ii) se $\{X_1, \ldots, X_n\}$ è una partizione di R_ω, allora qualche X_i contiene una copia isomorfa di R_ω.

Esercizio 10.61. Dimostrare che due ordini aleatori numerabili sono isomorfi e che ogni ordine numerabile si immerge in un ordine aleatorio numerabile.

Esercizio 10.62. In analogia con quanto fatto per il grafo e l'ordine aleatorio, definire e costruire un oggetto aleatorio per ciascun tipo di struttura:

(i) grafo diretto,

(ii) relazione transitiva,

(iii) relazione irriflessiva,

(iv) relazione binaria.

In tutti i casi enunciare e dimostrare un risultato analogo al Teorema 10.35.

Esercizio 10.63. Dimostrare che esiste un $\mathcal{C} \subseteq \mathscr{P}(\mathbb{N})$ tale che $(\mathcal{C}, \subset)$ è isomorfo ad $(\mathbb{R}, <)$.

Esercizio 10.64. Dimostrare mediante controesempi che le seguenti equazioni non valgono per tutti gli ordinali:

(i) $(\alpha + \beta) \cdot \gamma = \alpha \cdot \gamma + \beta \cdot \gamma$;

(ii) $(\alpha \cdot \beta)^\gamma = \alpha^\gamma \cdot \beta^\gamma$.

Esercizio 10.65. Calcolare il tipo d'ordine dei seguenti insiemi bene ordinati:

(i) $\{\frac{n}{n+1} \mid n \in \mathbb{N}\} \cup \{\frac{2n+1}{n+1} \mid n \in \mathbb{N}\} \cup \{2\}$;

(ii) $\{\frac{n \cdot m - 1}{n} \mid n, m \in \mathbb{N} \setminus \{0\}\}$.

Esercizio 10.66. Consideriamo l'insieme $\mathbb{N}[X]$ dei polinomi in una variabile X con coefficienti in $\mathbb{N}$ ordinato mediante la relazione di maggiorazione definitiva

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

Dimostrare che $\prec$ è un buon ordine di tipo ω^ω e descrivere esplicitamente l'isomorfismo $F\colon (\mathbb{N}[X], \prec) \to (\omega^\omega, <)$.

Esercizio 10.67. Dimostrare che se $\omega \leq \alpha$, $0 \leq n < \omega$ e $0 < m < \omega$ allora $(\alpha + n) \cdot m = \alpha \cdot m + n$.

Esercizio 10.68. Dimostrare che se λ è un ordinale limite, $0 \leq n < \omega$ e $1 \leq m < \omega$, allora $(\lambda + n)^m < \lambda^m \cdot 2$. Dedurre che $(\lambda + n)^\omega = \lambda^\omega$.

Esercizio 10.69. Dimostrare che:

(i) se $\alpha < \beta$ allora $\omega^\alpha + \omega^\beta = \omega^\beta$;

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

(iii) se $\alpha < \omega^\beta$ allora $\alpha + \omega^\beta = \omega^\beta$.

Esercizio 10.70. Dimostrare che un ordinale limite se e solo se è della forma $\omega \cdot \nu$, per qualche $\nu > 0$.

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

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

Esercizio 10.71. Dimostrare per ogni ordinale α sono equivalenti le seguenti affermazioni:

(i) α è additivamente indecomponibile;

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

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

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

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

Esercizio 10.72. Dimostrare per ogni ordinale α sono equivalenti le seguenti affermazioni:

(i) α è moltiplicativamente indecomponibile;

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

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

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

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

Esercizio 10.73. Dimostrare per ogni ordinale α sono equivalenti le seguenti affermazioni:

(i) α è esponenzialmente indecomponibile;

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

Esercizio 10.74. (i) Dimostrare che $\forall \alpha > 2 \, (\alpha + \alpha < \alpha \cdot \alpha < \alpha^\alpha)$.

(ii) Definiamo

$$E(0, \alpha) = \alpha$$
$$E(n+1, \alpha) = E(n, \alpha)^{E(n,\alpha)}.$$

Dimostrare che

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

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

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

$$\epsilon_0 = \sup\{\omega, \omega^\omega, \omega^{\omega^\omega}, \omega^{\omega^{\omega^\omega}}, \ldots\},$$

Esercizio 10.75. Dimostrare che la somma e il prodotto di cardinalità sono operazioni commutative, associative, e che vale la proprietà distributiva del prodotto rispetto alla somma.

Esercizio 10.76. Se $x, y \in \mathbb{R}$ e $x, y > 0$ definiamo

$$x \cdot y = \{p \in \mathbb{Q} \mid \exists q, r \in \mathbb{Q}\,(0 < q \in x \wedge 0 < r \in y \wedge p \leq q \cdot r)\}$$

e se x, y non sono entrambi positivi,

$$x \cdot y = \begin{cases} 0 & \text{se } x = 0 \text{ o } y = 0, \\ -\big((-x) \cdot y\big) & \text{se } x < 0 \text{ e } y > 0, \\ -\big(x \cdot (-y)\big) & \text{se } x > 0 \text{ e } y < 0, \\ (-x) \cdot (-y) & \text{se } x < 0 \text{ e } y < 0, \end{cases}$$

dove

$$-x = \{p \in \mathbb{Q} \mid \exists s \in \mathbb{Q}\, \forall q \in x\,(p + q < s < 0)\}.$$

Verificare che l'operazione è ben definita e che $(\mathbb{R}, +, \cdot, <)$ è un campo ordinato archimedeo.

Esercizio 10.77. Dimostrare che ogni intervallo di $\mathbb{R}$ aperto, chiuso, o semiaperto non degenere (cioè non vuoto oppure un singoletto) è equipotente ad $\mathbb{R}$.

Esercizio 10.78. Verificare che la dimostrazione del Teorema 10.33 prova che ogni ordinale numerabile è immergibile come sottoinsieme chiuso di $\mathbb{R}$. In altre parole, per ogni $\alpha < \omega_1$ c'è una $f\colon \alpha \to \mathbb{Q}$ che preserva l'ordine e tale che $\operatorname{ran}(f)$ è un chiuso di $\mathbb{R}$.

Esercizio 10.79. Verificare che la biezione definita in (10.8) è un isomorfismo di gruppi $(\mathbb{Q}_+, \cdot) \to (\mathbb{Z}[X], +)$.

Esercizio 10.80. Dimostrare che i seguenti sottoinsiemi di $\mathbb{N}^\mathbb{N}$ sono equipotenti ad $\mathbb{R}$:

$\mathcal{F}_0 = \{f \mid f \text{ è biettiva}\}$ $\quad$ $\mathcal{F}_1 = \{f \mid f \text{ è iniettiva}\}$

$\mathcal{F}_2 = \{f \mid f \text{ è suriettiva}\}$ $\quad$ $\mathcal{F}_3 = \{f \mid f \text{ è non decrescente}\}$

$\mathcal{F}_4 = \{f \mid f \text{ è strettamente crescente}\}$.

Esercizio 10.81. Dimostrare che $\{f \mid f\colon \mathbb{N} \to \mathbb{N} \times \mathbb{N} \text{ è una biezione}\}$ è equipotente a $\mathbb{R}$.

Esercizio 10.82. Per ogni $f \in 2^\mathbb{N}$ considerare l'ordine lineare

$$\mathbb{Z} + f(0) + \mathbb{Z} + f(1) + \mathbb{Z} + f(2) + \mathbb{Z} + \dots$$

ottenuto prendendo ω copie di $\mathbb{Z}$ in cui la n-esima copia è separata dalla $n+1$ esima mediante un unico punto se e solo se $f(n) = 1$. Dimostrare che ci sono $2^{\aleph_0}$ ordini lineari numerabili a due a due non isomorfi.

Esercizio 10.83. Per ogni $n \geq 2$ costruire un grafo G_n su $\mathbb{N}$ che soddisfi $\neg\rho_n \wedge \bigwedge_{j<n} \rho_j$ definiti a pagina 97. Concludere che $\Sigma_{\text{GRAFO ALEATORIO}}$ non è finitamente assiomatizzabile.

Esercizio 10.84. Un insieme ordinato $(A, <)$ si dice separabile se contiene un sottoinsieme denso e numerabile. Dimostrare che se A è separabile, allora $A \precsim \mathscr{P}(\mathbb{N})$.

Esercizio 10.85. Dimostrare che se λ è un ordinale limite, allora $\lambda + 1$ e $\lambda + n$ sono omeomorfi, per ogni $1 \leq n < \omega$.

Esercizio 10.86. Dimostrare che se un ordinale è uno spazio totalmente sconnesso e completamente regolare.

Negli esercizi che seguono vedremo alcune dimostrazioni alternative del Teorema di Cantor-Schröder-Bernstein 10.14.

Esercizio 10.87. Supponiamo che $f\colon A \to B$ sia iniettiva e che $B \subseteq A$. Sia $C_0 = A \setminus B$ e $C_{n+1} = f[C_n]$.

(i) Verificare che la funzione $h\colon A \to B$

$$h(x) = \begin{cases} f(x) & \text{se } x \in \bigcup_n C_n \\ x & \text{altrimenti} \end{cases}$$

è una biezione.

(ii) Usare la parte (i) per dedurre il Teorema di Cantor-Schröder-Bernstein.

Esercizio 10.88. Date due funzioni iniettive $f\colon A \to B$ e $g\colon B \to A$ consideriamo gli insiemi

$$A_0 = A \qquad B_0 = B$$
$$A_{n+1} = g[B_n] \qquad B_{n+1} = f[A_n].$$

Verificare che $h\colon A \to B$

$$h(x) = \begin{cases} g^{-1}(x) & \text{se } x \in \bigcup_n A_{2n+1} \setminus A_{2n+2}, \\ f(x) & \text{altrimenti,} \end{cases}$$

è una biezione.

Esercizio 10.89. Supponiamo che $f\colon A \to B$ e $g\colon B \to A$ siano funzioni iniettive e che $A \cap B = \emptyset$. Se $a' = g(f(a))$ diremo che a' è un successore immediato di a e che a è un predecessore immediato di a'. Fissiamo un $a \in A$. Definiamo a_n per $n \geq 0$, ponendo $a_0 = a$ e $a_{n+1} =$ il successore immediato di a_n. Se il predecessore immediato di a esiste, lo indichiamo con a_{-1}; se il predecessore immediato di a_{-1} esiste, lo indichiamo con a_{-2}; se il predecessore immediato di a_{-2} esiste, lo indichiamo con a_{-3}; e così via. Supponiamo a sia tale che c'è un $n < 0$ minimo per cui a_n è definito: allora o

$$a_n \notin \operatorname{ran}(g) \tag{10.14a}$$

oppure

$$a_n \in \operatorname{ran}(g) \text{ e } g^{-1}(a_n) \notin \operatorname{ran}(f) \tag{10.14b}$$

Sia A_0 l'insieme degli a che soddisfano (10.14b).

Verificare che $h\colon A \to B$

$$h(a) = \begin{cases} f(a) & \text{se } a \in A_0, \\ g^{-1}(a) & \text{altrimenti} \end{cases}$$

è una biezione.

Esercizio 10.90. In un semianello commutativo unitario $(R, +, \cdot, 0, 1)$ (vedi Definizione 5.5 a pagina 81) definiamo la relazione

$$x \leq y \Leftrightarrow \exists z\,(x + z = y)\,.$$

Supponiamo $a \in R$ sia tale che

$$a + 1 = a \tag{10.15a}$$
$$x + y \leq x \Rightarrow y \cdot a \leq x. \tag{10.15b}$$

Dimostrare che

(i) $x + y \leq x \Rightarrow x + y = x$;

(ii) $x \leq$ Â $y \wedge y \leq x \Rightarrow x = y$, cioè $\leq$ è un ordine su R;

(iii) la congiunzione di (10.15a) e (10.15b) è equivalente a

$$x + y = x \Leftrightarrow y \cdot a \leq x. \tag{10.15c}$$

Inoltre a è l'unico elemento di R che soddisfa (10.15c).

(iv) $a + a = a$ e $a \cdot a = a$;

Esercizio 10.91. (i) Dimostrare che se $X \cup Y \precsim X$ allora $Y \times \mathbb{N} \precsim X$.

(ii) Sia R la collezione di tutte le classi di equivalenza della relazione $\approx$ di equipotenza sugli insiemi.[12] Usare la parte (i) e l'Esercizio 10.90 per dare una dimostrazione alternativa del Teorema di Schröder-Bernstein 10.14 e del Teorema 10.18.

[12]Come abbiamo detto nella Sezione 10.J, R è la versione ingenua della totalità dei cardinali e questo oggetto non avrebbe diritto di cittadinanza nella teoria degli insiemi; tuttavia nella Sezione 14.F vedremo come modificare la costruzione di $\mathbb{R}$ e renderla una classe legittima.

Esercizio 10.92. Dimostrare che $E_{1/3}$ definito in (10.12) è un insieme compatto, non-vuoto, privo di interno.

Esercizio 10.93. Sia $(A, \trianglelefteq)$ un insieme ordinato. Verificare che $(A^{\mathbb{N}}, \leq_{\text{lex}})$ è un ordine lineare se e solo se $(A, \trianglelefteq)$ è un ordine lineare.

Esercizio 10.94. Dimostrare che:

(i) la serie (10.10) converge ad un reale in $[0; 1]$;

(ii) se $\forall i < n\ (x(i) = y(i))$, mentre $x(n) = 0$ e $y(n) = 1$, allora $\Phi(x) < \Phi(y) \leq \Phi(x) + 3^{-n}$.

Esercizio 10.95. Fissiamo un numero naturale $b > 1$. L'**espansione di** $x \in [0, 1]$ **in base** b è la sequenza $(n_0, n_1, n_2, \dots) \in b^{\mathbb{N}}$ tale che

$$x = \sum_{i=0}^{\infty} \frac{n_i}{b^{i+1}}.$$

(i) Verificare che se
- $\forall i < k\,(n_i = m_i)$,
- $n_k = m_k + 1$,
- $\forall i > k\,(n_i = 0 \wedge m_i = b - 1)$,

allora

$$\sum_{i=0}^{\infty} \frac{n_i}{b^{i+1}} = \sum_{i=0}^{\infty} \frac{m_i}{b^{i+1}} \in [0, 1]$$

e quindi l'espansione in base b di un $x \in [0, 1]$ non è unica.

(ii) Dimostrare che se x ammette un'espansione che non è definitivamente uguale a 0 o definitivamente uguale a $b - 1$, allora tale espansione è unica.

(iii) Dimostrare che $E_{1/3}$, l'insieme di Cantor, è l'insieme dei reali in $[0, 1]$ che ammettono un'espansione in base 3 in cui non compare mai la cifra 1 e che $E_{1/3} = \text{ran}(\Phi)$.

Esercizio 10.96. Dimostrare che $C \subseteq \alpha$ è chiuso nello spazio topologico α se e solo se $\forall \lambda \in \alpha\,[\lambda$ limite $\wedge$ $\forall \nu < \lambda\, \exists \gamma \in C\,(\nu \leq \gamma) \Rightarrow \lambda \in C]$.

Note e osservazioni

La teoria degli insiemi è stata inventata da Cantor verso il 1870 per risolvere un problema sulle serie trigonometriche formulato da Riemann, si veda [**Coo93**].

Il Teorema di Cantor-Schröder-Bernstein 10.14 fu enunciato (senza dimostrazione) da Cantor nel 1887 e nel 1895 ottenne questo risultato come corollario del Teorema del buon ordinamento 14.4, un risultato che dipende da (anzi: è equivalente a) l'Assioma di Scelta. Schröder nel 1896 pubblicò una dimostrazione incorretta del Teorema 10.14 mentre Bernstein un anno dopo ottenne una dimostrazione corretta. Tuttavia la prima dimostrazione corretta del teorema risale al 1887 ed è dovuta a Dedekind anche se, purtroppo, il suo nome non è associato a questo risultato. La dimostrazione del Teorema 10.14 riportata nell'Esercizio 10.14 è attribuita a König, mentre gli Esercizi 10.90 e 10.91 sono tratti da [**Cra11**].

Il risultato citato nell'Esempio 10.11 è dovuto a Thurston, e si basa su risultati di Gromov e Jørgensen [**Thu82**]. La funzione dell'Esempio 10.13 è nota come la funzione 91 di McCarthy dal nome dell'informatico che la definì nel 1970. Questa funzione (e altre generalizzazioni introdotte da Knuth) sono importanti nell'informatica teorica, in particolare negli studi sulla terminazione dei programmi [**Man03**].

Capitolo IV

Teoria elementare degli insiemi

11. Gli assiomi

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 principio 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 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

$$\mathrm{R} = \{x \mid x \notin x\}. \tag{11.1}$$

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

(11.2a) $\mathrm{R} \in \mathrm{R}$ implica che $\mathrm{R} \notin \mathrm{R}$ e

(11.2b) $\mathrm{R} \notin \mathrm{R}$ implica che $\mathrm{R} \in \mathrm{R}$,

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 così come le antinomie di Burali-Forti e di Cantor (Sezioni 10.J.1 e 10.J.2 del Capitolo I) si basano sul principio (∗∗) per definire collezioni molto "grandi". In altre parole, le antinomie della teoria ingenua degli insiemi non coinvolgono mai gli insiemi 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 nota come teoria Morse-Kelly o Kelly-Morse e si indica con MK.

11.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 $A = B$.*

11.B. Le formule della teoria degli insiemi. Se vogliamo formalizzare adeguatamente l'enunciato in (∗∗) dobbiamo rimpiazzare la nozione un po' ambigua di *proprietà* con quella rigorosa di **formula della teoria degli insiemi**. Il **linguaggio della teoria degli insiemi** (LST) è un linguaggio del prim'ordine che ha un unico simbolo non logico $\in$. Quindi le sue formule atomiche sono della forma

$$x \in y \quad \text{e} \quad x = y.$$

Abbrevieremo $\neg(x \in y)$ e $\neg(x = y)$ con $x \notin y$ e $x \neq y$. L'Assioma di Estensionalità si formalizza come

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

Sia poi $\mathrm{Set}(x)$ la formula che asserisce che x è un insieme

$$(\mathrm{Set}(x)) \qquad \exists y\,(x \in y)\,.$$

11.C. Classi definite da formule. Il seguente schema di assiomi rende rigoroso il principio enunciato in $(**)$.

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

$$\forall y_1 \ldots \forall y_n \exists A\, \forall x \Big(x \in A \Leftrightarrow (\mathrm{Set}(x) \wedge \varphi(x, y_1, \ldots, y_n)) \Big).$$

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

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

Osservazione 11.1. In matematica, ogni qual volta si dimostra che

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

si introduce un nuovo simbolo $\mathtt{t}(x_1, \ldots, x_n)$ che denota l'unico y per cui vale $\varphi(x_1, \ldots, x_n, y)$. Questo $\mathtt{t}(x_1, \ldots, x_n)$ è un **termine definito**, vale a dire è un termine di un linguaggio che *estende* LST — ricordiamo che gli unici termini di LST sono le variabili. Capita quindi spesso di imbattersi in classi della forma

$$\{\mathtt{t}(x_1, \ldots, x_n) \mid x_1 \in X_1, \ldots, x_n \in X_n\}. \tag{11.3}$$

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

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

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

Riguardiamo il paradosso di Russell: per l'Assioma di Comprensione, la classe $\mathrm{R} = \{x \mid x \notin x\}$ esiste e l'implicazione in (11.2a) dimostra che $\mathrm{R} \in \mathrm{R}$ non può valere e quindi $\mathrm{R} \notin \mathrm{R}$. Se R fosse un insieme, potremmo applicare (11.2b) 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,

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

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

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

Le usuali operazioni insiemistiche si applicano anche alle classi: se A e B sono classi, allora $A \cap B = \{x \mid x \in A \wedge x \in B\}$, $A \cup B = \{x \mid x \in A \vee x \in B\}$, $A \setminus B = \{x \mid x \in A \wedge x \notin B\}$ e $A \triangle B = (A \setminus B) \cup (B \setminus A)$ sono classi.

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. $\exists x \, \mathrm{Set}(x)$.

11.D. Insieme potenza. Diremo che la classe A è contenuta in B, ovvero che A è una **sottoclasse** di B,

$$A \subseteq B,$$

se $\forall x \, (x \in A \Rightarrow x \in B)$. Se $A \subseteq B$ e $A \neq B$, diremo che A è contenuta propriamente in 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 11.2. *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

$$A^{\neq} = \{x \in A \mid x \neq x\}$$

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

11.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 — per l'Assioma di Estensionalità $\{x, y\} = \{y, x\}$. 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 — se x e y coincidono, indicheremo $\{x, x\}$ con $\{x\}$, che si dice **singoletto** di x.

Esercizio 11.3. Dimostrare che $\{x, y\} = \{z, w\}$ implica che

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

L'Assioma di Comprensione applicato alla formula $\varphi(x, x_1, \ldots, x_n)$

$$x = x_1 \vee \cdots \vee x = x_n$$

garantisce l'esistenza della classe $\{x_1, \ldots, x_n\}$ che ha per elementi esattamente gli insiemi $x_1, \ldots, x_n$; mediante l'Assioma dell'Unione che vedremo tra poco, si dimostra che $\{x_1, \ldots, x_n\}$ è un insieme (Esercizio 11.19(iii)).

In matematica è necessario considerare le **coppie ordinate** (x, y). The set (x, y) deve codificare gli insiemi x e y e deve essere sufficientemente asimmetrico per poter distinguere questi due insiemi. Se x e y sono insiemi poniamo

$$(x, y) \stackrel{\text{def}}{=} \{\{x\}, \{x, y\}\}. \tag{11.4}$$

Il risultato seguente giustifica questa definizione.

Proposizione 11.4. *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 $\{\{x\}\} = (x, y) = (z, w) = \{\{z\}, \{z, w\}\}$, 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

$$x \neq y \quad \text{e} \quad z \neq w. \tag{11.5}$$

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 (11.5), 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 (11.5) e dalla seconda otteniamo $y \in \{x,w\}$, cioè $y = x$ oppure $y = w$: nuovamente per (11.5) otteniamo

$$y = w.$$

L'implicazione inversa è immediata. □

Osservazione 11.5. La definizione di coppia ordinata data in (11.4) è dovuta a Kuratowski; non è l'unica possibile, ma è probabilmente la più semplice. La prima definizione di coppia ordinata è stata data da Norbert Wiener nel 1914:

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

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

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

Lo svantaggio di quest'ultima definizione è che richiede l'Assioma di Fondazione (definito qui sotto) per dimostrarne la sua adeguatezza — si veda l'Esercizio 11.21.

11.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 $A \cap B = \emptyset$.*

Osservazione 11.6. Se $A \in A$ per qualche classe 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.

Analogamente non esistono A e B tali che $A \in B$ e $B \in A$

Poiché nessun insieme appartiene a sé stesso, la classe di Russell R in (11.1) a pagina 257 è la classe di *tutti* gli insiemi e solitamente è denotata con V:

$$\mathrm{V} \stackrel{\mathrm{def}}{=} \{x \mid x = x\}. \tag{11.6}$$

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

11.G. Unioni e intersezioni. Le operazioni di unione generalizzata e di intersezione generalizzata sono definite così:

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

con la convenzione che se $A = \emptyset$ allora $\bigcap A = \emptyset$. Poiché $\bigcap A \subseteq x$, per ogni $x \in A$, il Corollario 11.2 a pagina 260 implica che $\bigcap A$ è sempre un insieme. (L'analogo risultato per $\bigcup A$ non vale — Esercizio 11.26.) Tuttavia, se A è 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, per l'Assioma della Coppia $\{x, y\}$ è un insieme, quindi anche $x \cup y \stackrel{\text{def}}{=} \bigcup\{x, y\}$ è un insieme.

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

$$A \times B = \{(x, y) \mid x \in A, y \in B\},$$

che esiste per l'Assioma di Comprensione.

Proposizione 11.7. *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. □

11.H. Insiemi infiniti. Le varie costruzioni insiemistiche introdotte fin'ora ci consentono di costruire molti insiemi: a partire da $\emptyset$ e usando coppie ed unioni si ottengono

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

dove

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

è il **successore** di x. Non è difficile convincersi che gli insiemi nella lista qui sopra sono tutti distinti. Vorremmo dire che esiste la classe A di tutti questi insiemi e poi stabilire che A è un insieme. Tuttavia non è chiaro quale sia la formula φ che caratterizza tutti e soli gli insiemi nella lista per poter applicare l'Assioma di Comprensione. Introduciamo quindi la seguente definizione: una classe I si dice **induttiva** se

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

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

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

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

$$\mathbb{N} \stackrel{\text{def}}{=} \bigcap \mathcal{I}. \tag{11.7}$$

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

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

Proposizione 11.8. $\mathbb{N} \in \mathcal{I}$ *e se* $n \in \mathbb{N}$, *allora* $n = 0$ *oppure* $n = \mathbf{S}(m)$ *per qualche* $m \in \mathbb{N}$.

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

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

Siamo ora in grado di dimostrare Ind^2 il principio di induzione al second'ordine per $\mathbb{N}$ introdotto a pagina 130 nella Sezione 7.A.

Proposizione 11.9. *Sia* $I \subseteq \mathbb{N}$ *tale che* $0 \in I$ *e tale che* $\forall n\,(n \in I \Rightarrow \mathbf{S}(n) \in I)$. *Allora* $I = \mathbb{N}$.

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

11.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. Una relazione funzionale che sia un insieme si dice **funzione**. Spesso scriveremo $x\ R\ y$ invece di $(x, y) \in R$ e, nel caso in cui R sia una relazione funzionale, $R(x)$ denota l'unico y (se esiste) tale che $(x, y) \in R$.

La **composizione di** R **con** S è la classe

$$R \circ S \stackrel{\text{def}}{=} \{(x, z) \mid \exists y\,((x, y) \in S \wedge (y, z) \in R)\}.$$

Benché la definizione di $R \circ S$ abbia senso per ogni classe R e S, è particolarmente significativa quando si ha a che fare con relazioni funzionali: in quel caso anche $R \circ S$ è una relazione funzionale e $R \circ S(x) = R(S(x))$.

Il **dominio**, l'**immagine**[1] e il **campo** di una classe R sono, rispettivamente,

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

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 11.20). 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 11.10. *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. □

Il prossimo risultato estende i risultati contenuti nell'Osservazione 11.6.

Teorema 11.11. *Non esiste nessuna funzione f tale che* $\mathrm{dom}(f) = \mathbb{N}$ *e*

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

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

Se F è una relazione funzionale e A una classe, l'**immagine** di A mediante F è la classe

$$F[A] = \{F(x) \mid x \in A \cap \mathrm{dom}(F)\},$$

la **controimmagine** di A mediante F è

$$F^{-1}[A] = \{x \mid F(x) \in A\},$$

mentre

$$F \restriction A = \{(x,y) \in F \mid x \in A\}$$

è la **restrizione di F ad A**. Si noti che non si richiede che A sia contenuto in $\mathrm{dom}(F)$ o $\mathrm{ran}(F)$. Se entrambe F ed A sono classi proprie può accadere

[1] In inglese l'immagine di una funzione si dice *range*, da cui il simbolo ran.

che $F[A]$ sia una classe propria: per esempio, se F è la relazione funzionale identica

$$\mathrm{id} \stackrel{\mathrm{def}}{=} \{(x, x) \mid x \in \mathrm{V}\}$$

allora $\mathrm{id}[A] = A$ non è un insieme.

Notazione. In accordo con quanto fatto sinora, scriveremo id_A per $\mathrm{id} \restriction A$ quando A è un insieme.

È facile verificare (Esercizio 11.25) 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.

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

$$^A B \quad \text{oppure} \quad B^A.$$

(Per l'Esercizio 11.27 questa nozione è interessante soltanto quando A è un insieme.)

Osservazione 11.12. 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 11.13) di tutte le funzioni dall'insieme $2 = \{0, 1\}$ nell'insieme $3 = \{0, 1, 2\}$, mentre 3^2 è il numero 9. Quando non c'è pericolo di confusione useremo liberamente B^A.

Proposizione 11.13. *Se A e B sono insiemi, allora B^A è un insieme.*

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

Se F è una (classe-)funzione iniettiva

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

è una (classe-)funzione e si dice (classe-)funzione inversa. In questo caso $F\colon \mathrm{dom}(F) \to \mathrm{ran}(F)$ e $F^{-1}\colon \mathrm{ran}(F) \to \mathrm{dom}(F)$ sono biezioni e sono inverse l'una all'altra, cioè

$$\forall x \in \mathrm{dom}(F)\, (F^{-1} \circ F(x) = x) \quad \text{e} \quad \forall x \in \mathrm{ran}(F)\, (F \circ F^{-1}(x) = x).$$

Osserviamo che l'immagine di A mediante F^{-1} coincide con la controimmagine di A mediante F, quindi non c'è ambiguità nella notazione $F^{-1}[A]$.

Esercizio 11.14. Dimostrare che se A è una classe propria e B un insieme, allora non esiste nessuna $F\colon A \to B$ iniettiva.

Richiamiamo alcune nozioni viste nella Sezione 10.C: date due classi A e B diremo che A **si inietta in** B, in simboli

$$A \precsim B$$

se c'è una relazione funzionale iniettiva $F\colon A \to B$; se F è biettiva diremo che A e B sono **equipotenti**, in simboli

$$A \approx B.$$

11.J. Successioni e stringhe. 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 $\mathrm{lh}(s)$. In matematica per **successione** si intende usualmente una funzione di dominio $\mathbb{N}$, ma in teoria degli insiemi la parola successione è sinonimo di funzione, quindi diremo che $\langle a_i \mid i \in I\rangle$ è una I-successione di insiemi. Con abuso di linguaggio parleremo di successioni anche quando I è una classe propria e quindi $\langle a_i \mid i \in I\rangle$ è una classe-funzione.

Benché la sequenza $\langle a, b\rangle$ di lunghezza 2 e la coppia ordinata (a, b) possano essere identificate, si tratta di insiemi distinti. Il vantaggio di usare le sequenze invece delle coppie è evidente quando vogliamo parlare di 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 $\mathbb{R} \times (\mathbb{R} \times \mathbb{R})$? Quindi per evitare fastidiose (e banali) ambiguità, conviene assumere implicitamente che X^n sia la classe delle funzioni da n in X piuttosto che il prodotto cartesiano $X \times \cdots \times X$ e che $X^n \times X^m$ denoti, in realtà, l'insieme X^{n+m}. Se X è una classe

$$X^{<\mathbb{N}} = \{s \mid s \text{ è una stringa finita e } \mathrm{ran}(s) \subseteq X\}. \tag{11.8}$$

Esercizio 11.15. Dimostrare che se X è un insieme, allora

$$X^{<\mathbb{N}} = \bigcup \{X^n \mid n \in \mathbb{N}\}$$

è un insieme.

Una **funzione finitaria** o **operazione** su una classe X è una

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

dove $n = \mathrm{ar}(f) \in \mathbb{N}$ 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.

Se f è un'operazione su X, per semplicità notazionale scriveremo $f(\vec{x})$ o $f(x_0, \dots, x_{n-1})$ invece del più corretto, ma barocco, $f(\langle x_0, \dots, x_{n-1}\rangle)$.

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 id_I. Questa notazione è molto comoda quando si deve parlare di unione disgiunta degli A_i: l'idea è di sostituire ciascun A_i con un insieme equipotente A'_i di modo che questi nuovi insiemi siano a due a due disgiunti, infine considerare l'unione degli A'_i. Dato che $\{i\} \times A_i \cap \{j\} \times A_j = \emptyset$ possiamo definire l'**unione disgiunta degli insiemi** A_i come

$$\cup_{i\in I}\, A_i = \bigcup_{i\in I} \{i\} \times A_i. \tag{11.9a}$$

Nel caso di due insiemi o classi A e B, la loro unione disgiunta è usualmente definita da

$$A \cup B = (\{0\} \times A) \cup (\{1\} \times B). \tag{11.9b}$$

La definizione di coppia ordinata (introdotta a pagina 261 per gli insiemi) può essere estesa alle classi proprie: se A e B sono classi e almeno una tra A e B è una classe propria, poniamo

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

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 ad ogni $i \in I$ associamo una classe A_i e almeno una delle A_i è una classe propria, definiamo la successione $\langle A_i \mid i \in I\rangle$ come la classe

$$A = \{(i, a) \mid i \in I \wedge a \in A_i\}$$

e, con abuso di linguaggio, scriveremo che $I = \mathrm{dom}(A)$.

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 "$\forall i \in I \exists x\, (x \in A_i)$" 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 $\forall A \in \mathcal{A}\, (f(A) \in A)$.*

Una f come sopra si dice **funzione di scelta per** $\mathcal{A}$; una **funzione di scelta su** X, dove X è un insieme non vuoto, è una $f\colon \mathscr{P}(X) \to X$ tale che $f \restriction \mathscr{P}(X) \setminus \{\emptyset\}$ è una funzione di scelta per $\mathscr{P}(X) \setminus \{\emptyset\}$.

Ponendo $X = \bigcup \mathcal{A}$ possiamo riformulare AC così

Per ogni insieme $X \neq \emptyset$ c'è una funzione di scelta su X.

La teoria ottenuta aggiungendo ad MK l'Assioma di Scelta viene indicata con MK + AC o MKC. L'Assioma di Scelta asserisce l'esistenza di funzioni di scelta, ma non dà indicazioni su come costruirle. Se richiediamo che ci sia un metodo uniforme per estrarre un elemento da un insieme non vuoto si ottiene un rafforzamento di AC noto come **Assioma di Scelta Globale**

$$\text{(GAC)} \qquad \exists F\, (F\colon \mathrm{V} \setminus \{\emptyset\} \to \mathrm{V} \wedge \forall x\, (x \neq \emptyset \Rightarrow F(x) \in x))\,.$$

Non useremo quasi mai questo principio e, salvo indicazione contraria, in questo libro quando utilizziamo la scelta si intende che si utilizza la versione "locale " AC, o un suo indebolimento, e non la versione "globale" GAC.

L'Assioma di Scelta ha molte applicazioni nella matematica ed è centrale nella moderna teoria degli insiemi, ma per via della sua natura non-costruttiva segnaleremo sempre quando viene usato in una dimostrazione. Lo studio sistematico dell'Assioma di Scelta è rimandato alla alla Sezione 14.

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

$$\text{(11.10)} \quad \bigtimes_{i\in I} A_i = \{f \mid f \text{ è una funzione, } \mathrm{dom}(f) = I \text{ e } \forall i \in I\, (f(i) \in A_i)\}.$$

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

Esercizio 11.16. 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 biezione) con $A_0 \times A_1$.

Se $A_{i_0} = \emptyset$ per qualche $i_0 \in I$, allora $\bigtimes_{i\in I} A_i = \emptyset$. Per dimostrare il converso:

$$\text{(11.11)} \quad \text{se } I \neq \emptyset \text{ è un insieme e } A_i \neq \emptyset \text{ per ogni } i \in I, \text{ allora } \bigtimes_{i\in I} A_i \neq \emptyset.$$

dobbiamo ricorrere all'Assioma di Scelta.

Esercizio 11.17. Dimostrare che le seguenti affermazioni sono equivalenti:

(i) AC;

(ii) l'Assioma di Scelta per famiglie di insiemi disgiunti: se $\mathcal{A} \neq \emptyset$ è un insieme tale che $\forall A \in \mathcal{A}\,(A \neq \emptyset)$ e $\forall A, B \in \mathcal{A}\,(A \neq B \Rightarrow A \cap B = \emptyset)$, allora
$$\exists f \colon \mathcal{A} \to \bigcup \mathcal{A}\, \forall A \in \mathcal{A}\,(f(A) \in A);$$

(iii) se $\mathcal{A} \neq \emptyset$ è un insieme tale che $\forall A \in \mathcal{A}\,(A \neq \emptyset)$ e $\forall A, B \in \mathcal{A}\,(A \neq B \Rightarrow A \cap B = \emptyset)$, allora
$$\exists T \subseteq \bigcup \mathcal{A}\,(A \cap T \text{ è un singoletto})\,;$$

(iv) la formula (11.11).

Osserviamo che se gli A_i sono tutti uguali ad un insieme $A \neq \emptyset$, allora non c'è bisogno di usare AC per dimostrare che $\bigtimes_{i\in I} A_i = A^I$ è non vuoto, dato che posso considerare una funzione costante $i \mapsto a \in A$.

11.K. Operazioni. Se f è un'operazione su una classe X diremo che $Y \subseteq X$ è **chiusa per** f se $f[Y^n] \subseteq Y$.

Esercizio 11.18. Supponiamo X sia un insieme e che $Y \subseteq X$. Sia
$$\mathcal{C} = \{Z \subseteq X \mid Y \subseteq Z \wedge Z \text{ è chiuso per } f\}.$$
Dimostrare che $\mathcal{C} \neq \emptyset$ e che $\bigcap \mathcal{C}$ è il più piccolo sottoinsieme di X chiuso per f e contenente Y.

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 $\mathcal{F}$ è
$$\begin{aligned}\mathrm{Cl}_{\mathcal{F}}(Y) &\stackrel{\text{def}}{=} \bigcap \{Z \subseteq X \mid Y \subseteq Z \wedge \forall f \in \mathcal{F}\,(Z \text{ è chiuso per } f)\} \\ &= \bigcap_{f\in\mathcal{F}} \mathrm{Cl}_f(Y).\end{aligned}$$

11.L. 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 MK — che parla di certi 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 $x, y_1, \ldots, y_n$,

$$\forall y_1 \ldots \forall y_n \exists A \, \forall x \, (x \in A \Leftrightarrow \mathrm{Set}(x) \wedge \varphi(x, y_1, \ldots, y_n)) \, .$$

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

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

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: $\forall x \, (\mathrm{Set}(x) \Rightarrow \exists u \, (\mathrm{Set}(u) \wedge u = \bigcup x))$.

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

Rimpiazzamento:

$$\forall F \forall A \, \big((\forall x \in \mathrm{dom}(F) \, \exists! y (x, y) \in F \wedge \mathrm{Set}(A)) \Rightarrow \mathrm{Set}(F[A])\big) \, . \tag{11.12}$$

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

Gli assiomi qui sopra sono solo parzialmente formalizzati nel linguaggio LST dato che abbiamo usato termini definiti quali $\subseteq$, $\{x, y\}$, $\cap$, $\emptyset$, $\bigcup$, $\mathbf{S}$, $F[A]$, e la formula $\mathrm{Set}(x)$. Lasciamo al lettore l'ulteriore sforzo di eliminare questi simboli definiti (Esercizio 11.22). Inoltre abbiamo usato varie lettere maiuscole e minuscole nel tentativo di rendere più trasparente il significato degli assiomi. Per esempio, nel caso dell'Assioma di Rimpiazzamento, la lettera F suggerisce che si sta parlando di una funzione, anzi: di una relazione funzionale. Nell'Assioma di Comprensione le lettere (vale a dire: le variabili) $y_1, \ldots, y_n$ denotano dei parametri, mentre la lettera maiuscola A indica la classe $\{x \mid \varphi(x, y_1, \ldots, y_n)\}$ la cui esistenza è postulata dall'assioma.

Un'altra assiomatizzazione della teoria degli insiemi è dovuta a Ernst Zermelo e Abraham 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 non ha diritto di cittadinanza in ZF. Gli assiomi di Estensionalità e Fondazione sono esattamente come in MK; gli

assiomi della Coppia, Potenza, Unione e Infinito sono *essenzialmente* come in MK, eccetto che non è necessario asserire che si sta parlando di insiemi:

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

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

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

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

Lo Schema di Assiomi di Comprensione è sostituito da

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

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

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

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

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

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

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

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

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

$$\begin{aligned}(11.13)\quad \forall A \forall z_1 \ldots \forall z_n\, (\forall x\, (x \in A \Rightarrow \exists! y \varphi(x, y, A, z_1, \ldots, z_n)) \Rightarrow \\ \exists B \forall y\, (y \in B \Leftrightarrow \exists x\, (x \in A \wedge \varphi(x, y, A, z_1, \ldots, z_n))))\,.\end{aligned}$$

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 (11.12) è un singolo assioma, mentre lo Schema di Assiomi del Rimpiazzamento[2] di ZF è una lista infinita di enunciati. 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.[3] Il paradosso di Russell è neutralizzato da ZF nel seguente modo. Innanzitutto la collezione R

[2]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.

[3]Per fare ciò il programma lavora in simultanea sulle due liste di assiomi, si veda il Teorema 9.47.

in (11.1) a pagina 257 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 (11.2a) e (11.2b) continuano a valere portandoci quindi ad una contraddizione. Ne segue che R *non* è un insieme e quindi il paradosso di Russell non sussiste più.

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

Benché la stragrande maggioranza degli oggetti studiati dai matematici siano insiemi, è spesso utile poter parlare della classe di tutti i gruppi, o della classe degli spazi topologici, o della classe degli insiemi finiti — questo è particolarmente vero quando si utilizza il linguaggio della teoria delle categorie (Sezione 18). Per questo motivo taluni matematici preferiscono MK o NGB a ZF. 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 o in qualche sua estensione.

Le classi proprie in ZF sono solo degli oggetti meta-matematici, delle formule che descrivono una totalità a cui non corrisponde una controparte nella teoria. Per esempio: invece della classe di tutti i gruppi si considera la formula $\boldsymbol{\gamma}(x)$ che asserisce che x è un gruppo, ovverosia $x = \langle G, * \rangle$ è una sequenza di lunghezza 2, 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 $\boldsymbol{\tau}(x)$ che asserisce che x è uno spazio topologico, ovverosia x è una coppia ordinata $\langle Y, \mathcal{O} \rangle$ dove Y è un insieme non vuoto e $\mathcal{O}$ è una topologia su Y. Nella teoria MK è possibile dimostrare teoremi della forma

$$\exists X \, (\neg \, \mathrm{Set}(X) \wedge \ldots X \ldots) \tag{11.14}$$

e

$$\forall X \, (\neg \, \mathrm{Set}(X) \Rightarrow \ldots X \ldots) \tag{11.15}$$

cioè affermazioni del tipo: "Esiste una classe propria X tale che..." e "Per ogni classe propria X succede che ...". Naturalmente in MK possiamo dimostrare enunciati ancora più complessi, del tipo: "Per ogni classe propria X c'è una classe propria Y tale che ...". In ZF capita di dimostrare affermazioni esistenziali come in (11.14): in questo caso dobbiamo *esibire esplicitamente una formula* che definisce la classe propria X con le proprietà richieste. In MK la richiesta è più modesta e potremmo, per esempio, dimostrare (11.14) per assurdo: si parte dall'assunzione che nessuna classe propria X soddisfi la proprietà in questione, e da ciò si ottiene una contraddizione in MK. Le affermazioni del tipo (11.15) in ZF sono 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 di *metateorema*.

La discussione precedente può far sorgere il sospetto che la differenza tra MK e ZF riguardi solo risultati sulle classi proprie, e che i risultati sugli insiemi siano i medesimi nelle due teorie. Ogni affermazione sugli insiemi dimostrabile in ZF è anche un teorema di MK, ma non vale il viceversa: ci sono affermazioni 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 P è un predicato ricorsivo. Tuttavia enunciati di questo genere sono molto rari e, nella maggioranza dei casi, un risultato sugli *insiemi* dimostrato in MK è anche dimostrabile in ZF, essenzialmente con la stessa dimostrazione.

11.M. La teoria degli insiemi come fondamento della matematica. Nelle sezioni che verranno vedremo come ricostruire la matematica all'interno della teoria assiomatica degli insiemi, dimostrando rigorosamente anche i risultati più elementari. In particolare, verificheremo che i risultati dei Capitoli I e II sono dimostrabili in MK e in ZF. Vediamo come.

I Teoremi 7.3, 7.4 e 7.11 si traducono facilmente nella teoria assiomatica degli insiemi, consentendoci quindi di definire le operazioni di somma, prodotto, esponenziazione sui naturali. In particolare possiamo definire gli insiemi $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$. Poiché $\mathbb{N}$ soddisfa gli assiomi di Peano, possiamo considerare assodati i risultati delle Sezioni 7–9.

I numeri ordinali e cardinali verranno definiti rigorosamente nella Sezione 12. In particolare, un insieme si dirà finito se è equipotente ad un $n \in \mathbb{N}$.

Le definizioni di linguaggio, termine, formula verranno date nella Sezione 28, quindi definiremo la nozione di soddisfazione nella Sezione 29: le nozioni ausiliarie (quali: occorrenze libere/vincolate, ecc) sono casi particolari di risultati sulle stringhe finite che vedremo nella Sezione 20.

Esercizi

Esercizio 11.19. Dimostrare che:

(i) se A è un insieme allora $A \cap B$ è un insieme,

(ii) se B è una classe propria allora $A \cup B$ è una classe propria,

(iii) se $x_1, \ldots, x_n$ sono insiemi, anche $\{x_1, \ldots, x_n\}$ è un insieme,

(iv) $\mathrm{V} \setminus x$ è una classe propria, per ogni insieme x.

Esercizio 11.20. Dare formule $\varphi(x, y, z)$ e $\psi(x, y, z)$ che asseriscono, rispettivamente, "$z = \{x, y\}$" e "$z = (x, y)$."

Esercizio 11.21. 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 11.5 sono adeguate.

Esercizio 11.22. Formalizzare nel linguaggio LST i seguenti assiomi di MK: Potenza, Coppia, Fondazione, Unione, Infinito e Rimpiazzamento. Analogamente per gli assiomi di ZF.

Esercizio 11.23. Per ciascuna classe qui sotto trovare una formula di LST che la definisce mediante l'Assioma di Comprensione:

$$F \circ G, \qquad F[A], \qquad F^{-1}[A], \qquad F \restriction A.$$

Esercizio 11.24. Dimostrare che per ogni insieme x non esiste alcun y tale che $x \in y$ e $y \in \mathbf{S}(x)$.

Esercizio 11.25. Dimostrare che se f è un insieme anche $f[A]$ è un insieme.

Esercizio 11.26. Dimostrare che:

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

(ii) se $y \neq \emptyset$, allora la classe degli insiemi $x \approx y$

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

è una classe propria.

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

Esercizio 11.27. 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 11.28. Sia σ l'affermazione che la classe vuota esiste, cioè

$$\exists x \forall y (y \notin x)$$

che è chiaramente un teorema di ZF e di MK. Consideriamo le seguenti teorie

T_1: σ + Assioma della Coppia + Assioma dell'Insieme Potenza,

T_2: σ + Assioma dell'Unione + Assioma dell'Insieme Potenza,

T_3: σ + Assioma della Coppia + Assioma dell'Unione + Assioma dell'Insieme Potenza.

Quali di queste teorie dimostrare l'esistenza di un insieme con 5 elementi?

Esercizio 11.29. Siano $F_{i,j}$ degli insiemi non vuoti, con $(i, j) \in I \times J$. Dimostrare che:

(i) $\bigcap_{i\in I}\bigcup_{j\in J} F_{i,j} \supseteq \bigcup_{f\in {}^I J}\bigcap_{i\in I} F_{i,f(i)}$ e $\bigtimes_{i\in I}\bigcup_{j\in J} F_{i,j} \supseteq \bigcup_{f\in {}^I J}\bigtimes_{i\in I} F_{i,f(i)}$;

(ii) AC implica che

$$\bigcap_{i\in I}\bigcup_{j\in J} F_{i,j} = \bigcup_{f\in {}^I J}\bigcap_{i\in I} F_{i,f(i)} \quad \text{e} \quad \bigtimes_{i\in I}\bigcup_{j\in J} F_{i,j} = \bigcup_{f\in {}^I J}\bigtimes_{i\in I} F_{i,f(i)};$$

(iii) entrambi gli enunciati, per $I, J, F_{i,j}$ arbitrari,

$$\bigcap_{i\in I}\bigcup_{j\in J} F_{i,j} \subseteq \bigcup_{f\in {}^I J}\bigcap_{i\in I} F_{i,f(i)} \quad \text{e} \quad \bigtimes_{i\in I}\bigcup_{j\in J} F_{i,j} \subseteq \bigcup_{f\in {}^I J}\bigtimes_{i\in I} F_{i,f(i)}$$

implicano AC.

Esercizio 11.30. Dimostrare che i seguenti enunciati sono equivalenti all'Assioma di Scelta:

(i) Se $f\colon X \twoheadrightarrow Y$ allora esiste un'inversa sinistra per f, cioè esiste $g\colon Y \rightarrowtail X$ tale che $\forall y \in Y\,(f \circ g(y) = y)$.

(ii) Ogni insieme X è **proiettivo**, vale a dire: per ogni $f\colon X \to Y$ e ogni suriezione $g\colon Z \twoheadrightarrow Y$ c'è una $h\colon X \to Z$ tale che $f = g \circ h$.

(iii) Ogni insieme è contenuto in un insieme proiettivo.

(iv) Se un insieme R è una relazione binaria, allora c'è una funzione f tale che $\mathrm{dom}(f) = \mathrm{dom}(R)$ e $\forall x \in \mathrm{dom}(R)\,(x, f(x)) \in R$.

Esercizio 11.31. Dimostrare che se C è una classe propria, anche C^n $(n \neq 0)$ e $C^{<\mathbb{N}}$ sono classi proprie.

Esercizio 11.32. Dimostrare che se $\langle A_i \mid i \in I\rangle$ è una sequenza di classi non-vuote e I è in biezione con un numero naturale, allora $\bigtimes_{i\in I} A_i \neq \emptyset$.

Esercizio 11.33. Dimostrare che:

(i) In presenza degli altri assiomi di MK, l'Assioma di Rimpiazzamento (11.12) a pagina 271 è equivalente alla sua versione iniettiva:

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

(ii) Analogamente, in presenza degli altri assiomi di ZF, l'Assioma di Rimpiazzamento (11.13) a pagina 272 è equivalente alla sua versione iniettiva:

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

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

e se

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

allora

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

(iii) In presenza degli altri assiomi di ZF, l'Assioma di Rimpiazzamento (11.13) implica l'Assioma di Separazione.

Note e osservazioni

L'assiomatizzazione della teoria degli insiemi è stata portata a termine solo nella prima metà del secolo scorso ad opera di molti matematici tra cui Zermelo, Frænkel, von Neumann, Gödel, Bernays, Kelley e Morse. In particolare, la teoria MK qui esposta è stata sviluppata indipendentemente da Kelley e Morse: una lista di assiomi essenzialmente equivalenti a quelli qui presentati si trova nell'appendice del libro di Kelley di topologia generale [**Kel55**], mentre la monografia di Morse [**Mor65**] presenta (in modo assai idiosincratico) una trattazione dettagliata della teoria degli insiemi MK. L'esposizione in questo libro segue abbastanza fedelmente [**Mon69**]. Un ottimo testo di teoria degli insiemi in cui viene sviluppata ZF è [**Lev02**].

12. Insiemi ordinati e ordinali

Molte delle nozioni viste nella Sezione 8 (ordini, relazioni di equivalenza, ...) possono essere tradotte nel linguaggio delle classi. Per esempio, diremo che $R \subseteq X \times X$ è riflessiva sulla classe X se $x\ R\ x$ cioè $(x, x) \in R$ per ogni $x \in X$, ma eviteremo di scrivere

$$\langle X, R\rangle \vDash \forall x\,(x\ R\ x)$$

dato che, come vedremo nella Sezione 29, la relazione di soddisfazione è definita solamente per strutture che siano *insiemi*.

Una nozione che è significativa soltanto quando si ha a che fare con classi proprie è la seguente.

Definizione 12.1. $R \subseteq X \times X$ è **regolare (a sinistra)** se $\{y \in X \mid y\ R\ x\}$ è un insieme, per ogni $x \in X$.

Quindi un ordine $\leq$ su una classe propria X è regolare se $\mathrm{pred}(x)$ è un insieme, per ogni $x \in X$. Analogamente, una relazione di equivalenza E su una classe propria X è regolare se ogni classe di equivalenza è un insieme, nel qual caso è possibile costruire il quoziente[4]

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

Esercizio 12.2. 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 $\sim$ è una relazione di equivalenza su un insieme X, allora $X/\!\sim$ è un insieme.

(iii) La relazione di equipotenza tra insiemi (vedi pagina 267) è una relazione di equivalenza non regolare su V.

[4]Nella Sezione 14.F vedremo un metodo per definire il quoziente X/E quando E non regolare.

Proposizione 12.3. *Sia $\mathcal{F}$ una classe di funzioni e supponiamo sia diretto superiormente sotto $\subseteq$. 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 $y = z$. □

12.A. Esempi di ordini. Come abbiamo detto nella Sezione 10.A se $\langle X_0, \leq_0 \rangle$ e $\langle X_1, \leq_1 \rangle$ sono classi ordinate, possiamo definire due ordinamenti su $X_0 \times X_1$. L'**ordine prodotto** è definito da

$$(x_0, x_1) \trianglelefteq (y_0, y_1) \Leftrightarrow (x_0 \leq_0 y_0 \wedge x_1 \leq_1 y_1).$$

L'**ordine lessicografico** è definito da

$$(x_0, x_1) \leq_{\text{lex}} (y_0, y_1) \Leftrightarrow (x_0 <_0 y_0 \vee (x_0 = y_0 \wedge x_1 \leq_1 y_1)).$$

Se ordiniamo $X_0 \cup X_1$, l'unione disgiunta di X_0 e X_1 imponendo che gli elementi di X_0 vengono prima di quelli di X_1, l'ordinamento così ottenuto si chiama ancora ordinamento lessicografico, dato che

$$(i, x) \leq_{\text{lex}} (j, y) \Leftrightarrow (i < j \vee (i = j \wedge x \leq_i y)).$$

Queste costruzioni possono essere generalizzate: supponiamo $\langle I, \preccurlyeq \rangle$ e $\langle X_i, \leq_i \rangle$ con $i \in I$ siano classi ordinate. L'ordine prodotto su $\bigtimes_{i \in I} X_i$ è definito da

$$f \trianglelefteq g \Leftrightarrow \forall i \in I\, (f(i) \leq_i g(i))$$

e l'ordine lessicografico è definito da

$$f \leq_{\text{lex}} g \Leftrightarrow \exists i \in I \Big(\forall j \in I\, (j \prec i \Rightarrow f(j) = g(j)) \wedge f(i) \leq_i g(i)\Big),$$

dove '$j \prec i$' significa '$j \preccurlyeq i \wedge j \neq i$'. L'ordinamento lessicografico su $\biguplus_{i \in I} X_i = \bigcup_{i \in I} \{i\} \times X_i$, l'unione disgiunta delle X_i, è definito da

$$(i, x) \leq_{\text{lex}} (j, y) \Leftrightarrow (i \prec j \vee (i = j \wedge x \leq_i y)).$$

Definizione 12.4. Sia X una classe e $R \subseteq X \times X$ una relazione su X. Diremo che R è **ben-fondata** se ogni sottoclasse 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 12.5. 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 $<$.

Ricordiamo (pag. 269) che l'assioma di scelta AC asserisce che per ogni famiglia $\emptyset \neq \mathcal{A}$ di insiemi nonvuoti esiste sempre una funzione di scelta, cioè una f tale che $f(A) \in A$. I buoni ordini permettono di effettuare scelte canoniche.

Teorema 12.6. *Se l'insieme X è bene ordinabile, allora c'è una funzione di scelta su X. In particolare, se ogni insieme è bene ordinabile, allora vale* AC.

Dimostrazione. Sia $f(A) = \lhd\text{-}\min A$ dove $\lhd$ è un buon ordine su X. □

I seguenti risultati sono generalizzazioni immediate delle Proposizioni 10.4 e 10.5 e dei Corollari 10.6 e 10.7.

Proposizione 12.7. *Se $\langle A, < \rangle$ è una classe bene ordinata e $f\colon A \to A$ è strettamente crescente, allora*

$$\forall a \in A\, (a \leq f(a))\,.$$

Proposizione 12.8. *Se $\langle A, < \rangle$ è una classe bene ordinata e $f\colon A \to A$ è una biezione strettamente crescente, allora $f = \mathrm{id} \restriction A$.*

Corollario 12.9. *Se $\langle A, < \rangle$ e $\langle B, \lhd \rangle$ sono classi bene ordinate isomorfe, allora l'isomorfismo $f\colon A \to B$ è unico.*

Corollario 12.10. *Se $\langle A, < \rangle$ è una classe bene ordinata e $a \in A$, allora $\langle \mathrm{pred}(a, A; <), < \rangle$ e $\langle A, < \rangle$ non sono isomorfi.*

Il Teorema 10.8 si generalizza alle classi.

Teorema 12.11. *Se $\langle A, < \rangle$ e $\langle B, \prec \rangle$ sono classi bene ordinate, allora una ed una sola delle tre seguenti proprietà vale:*

(1) $\exists a \in A\, (\langle \mathrm{pred}\, a, < \rangle \cong \langle B, \prec \rangle)$

(2) $\exists b \in B\, (\langle \mathrm{pred}\, b, \prec \rangle \cong \langle A, < \rangle)$

(3) $\langle A, < \rangle \cong \langle B, \prec \rangle$.

In particolare, due classi proprie bene ordinate sono isomorfe.

12.B. Ordinali. Gli ordinali sono esempi canonici di buoni ordini.

Definizione 12.12. 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

$$\mathrm{Ord}$$

è la classe degli ordinali.

Esercizio 12.13. (i) Il singoletto $\{x\}$ è transitivo se e solo se $x = \emptyset$. Nessuna coppia ordinata (x, y) è un insieme transitivo.

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

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

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

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

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

Proposizione 12.14. Ord *è una classe propria.*

Dimostrazione. Se $\alpha \in \mathrm{Ord}$ e $\beta \in \alpha$, allora $\beta \in \mathrm{Ord}$ per la parte (v) dell'Esercizio 12.13. Quindi Ord è una classe transitiva. Se Ord fosse un insieme, allora sarebbe un ordinale e quindi $\mathrm{Ord} \in \mathrm{Ord}$, contro l'Assioma di Fondazione. □

Teorema 12.15. *Due ordinali sono sempre confrontabili mediante* $\in$*, cioè se* $\alpha, \beta \in \mathrm{Ord}$

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

Dimostrazione. Dobbiamo dimostrare che

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

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

$$\bar{\alpha} \cap A = \emptyset. \tag{12.1}$$

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 (12.1), $\gamma \notin A$, quindi, in particolare

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

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 12.16. *La relazione di appartenenza* $\in$ *è un buon ordine stretto su* Ord *e quindi su ogni ordinale* α*.*

Per questo motivo spesso 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 $\in$-minimale di A è il minimo di A.

Notazione. Abbrevieremo l'espressione "$A \in \mathrm{Ord} \vee A = \mathrm{Ord}$" con

$$A \leq \mathrm{Ord}$$

e useremo la lettera Ω per indicare una classe A siffatta, vale a dire un generico ordinale, oppure Ord.

Ogni ordinale α definisce un buon ordine $\langle \alpha, \in \rangle$ e se $\beta \in \alpha$, allora β è l'insieme dei predecessori di β in α, cioè

$$\beta = \mathrm{pred}(\beta, \alpha; \in).$$

Quindi per il Corollario 12.10 a pagina 279

$$\langle \alpha, < \rangle \cong \langle \beta, < \rangle \Leftrightarrow \alpha = \beta.$$

Sia $\langle X, < \rangle$ una classe bene ordinata e sia

$$A = \{\alpha \in \mathrm{Ord} \mid \exists x \in X \, (\langle \alpha, \in \rangle \cong \langle \mathrm{pred}(x), < \rangle)\}$$

la classe degli ordinali isomorfi ad un qualche segmento iniziale di X. Supponiamo $f \colon \langle \alpha, \in \rangle \to \langle \mathrm{pred}(x), < \rangle$ sia l'isomorfismo che testimonia che $\alpha \in A$. Se $\beta \in \alpha$ allora $f \restriction \beta \colon \langle \beta, < \rangle \to \langle \mathrm{pred}(f(\beta)), < \rangle$ è un isomorfismo e quindi $\beta \in A$. Segue che A è una classe transitiva di ordinali e quindi $A \leq \mathrm{Ord}$. Sia $f \colon A \to X$ la relazione funzionale che associa ad un $\alpha \in A$ l'unico $x \in X$ tale che $\langle \alpha, \in \rangle \cong \langle \mathrm{pred}(x), < \rangle$. È immediato verificare che $\mathrm{ran}(f)$ è un segmento iniziale di X. Se, per assurdo, $\mathrm{ran}(f) \neq X$, allora $\mathrm{ran}(f) = \mathrm{pred}(\bar{x})$, per un qualche $\bar{x} \in X$. Poiché A è in biezione con l'insieme $\mathrm{pred}(\bar{x})$, segue che $A \in \mathrm{Ord}$ e quindi $A \in A$ per definizione della classe A: una contraddizione. Quindi f è suriettiva. Abbiamo quindi dimostrato il seguente

Teorema 12.17. *Ogni insieme bene ordinato è isomorfo ad un ordinale ed ogni classe propria bene ordinata è isomorfa ad* Ord. *Inoltre per i Corollari 12.9 e 12.10 l'ordinale e l'isomorfismo sono unici.*

Se $\langle X, < \rangle$ è una classe bene ordinata, il suo **tipo d'ordine** è l'unico $\Omega \leq \mathrm{Ord}$ isomorfo a $\langle X, < \rangle$ e lo si indica con $\mathrm{ot}\,\langle X, < \rangle$ o semplicemente con $\mathrm{ot}(X)$ se l'ordinamento è chiaro dal contesto. In particolare $\mathrm{ot}(A) = \mathrm{Ord}$ per ogni classe propria $A \subseteq \mathrm{Ord}$. L'unico isomorfismo $\langle \Omega, \in \rangle \to \langle X, < \rangle$ si dice **funzione enumerante**.

Proposizione 12.18. *Se A 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 11.11 a pagina 265 otteniamo

Corollario 12.19. *Non esiste nessuna catena discendente di ordinali, vale a dire*

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

Lemma 12.20. (a) *Ogni numero naturale è un ordinale.*
(b) *Se $n \in \mathbb{N}$ e $x \in n$ allora $x \in \mathbb{N}$.*

Dimostrazione. (a) Per assurdo, supponiamo $X = \mathbb{N} \setminus \mathrm{Ord}$ sia non vuoto e sia $n \in X$ tale che $n \cap X = \emptyset$. Poiché 0 è un ordinale, ne segue che $n \neq 0$ e quindi, per la Proposizione 11.8 a pagina 264, $n = \mathbf{S}(m)$ per qualche $m \in \mathbb{N}$. Allora $m \in \mathrm{Ord}$ e quindi $\mathbf{S}(m) \in \mathrm{Ord} \cap \mathbb{N}$: una contraddizione.

(b) Per assurdo supponiamo che $X = \{n \in \mathbb{N} \mid \exists x \in n\,(x \notin \mathbb{N})\}$ sia non vuoto e sia $\bar{n} \in X$ tale che $\bar{n} \cap X = \emptyset$. Fissiamo $\bar{x} \in \bar{n}$ tale che $\bar{x} \in \bar{n} \setminus \mathbb{N}$. Per la Proposizione 11.8, $\bar{n} = \mathbf{S}(\bar{m})$, per qualche $\bar{m} \in \mathbb{N}$, quindi $\bar{x} \in \bar{m}$ o $\bar{x} = \bar{m}$. È immediato verificare che entrambe le possibilità portano ad un assurdo. □

Un ordinale α è **successore** se $\alpha = \mathbf{S}(\beta)$, per qualche β. Chiaramente $\alpha < \mathbf{S}(\alpha)$ e per l'Esercizio 11.24 a pagina 275, non esiste alcun β tale che $\alpha < \beta < \mathbf{S}(\alpha)$. In altre parole $\mathbf{S}(\alpha)$ è il successore immediato di α nell'ordinamento dato da $\in$. Se un ordinale non è successore e non è 0, allora si dice **limite**.

Teorema 12.21. *$\mathbb{N}$ è il più piccolo ordinale limite.*

Dimostrazione. $\mathbb{N}$ è un ordinale per il Lemma 12.20 e per la Proposizione 11.8 a pagina 264 non esistono ordinali limite minori di $\mathbb{N}$. Basta quindi verificare che $\mathbb{N}$ non è successore. Se, per assurdo, $\mathbb{N} = \mathbf{S}(\alpha)$, allora $\alpha \in \mathbb{N}$, da cui $\mathbf{S}(\alpha) \in \mathbb{N}$, cioè $\mathbb{N} \in \mathbb{N}$: contraddizione. □

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

$$\omega.$$

Esercizio 12.22. Se $\langle A, <\rangle$ è una classe bene ordinata in cui ogni elemento diverso dal minimo ha un predecessore immediato, allora il suo tipo d'ordine è $\leq \omega$ e quindi A è un insieme.

Proposizione 12.23. (a) *$\alpha < \beta \Leftrightarrow \alpha \subset \beta$;*
(b) *$\alpha \leq \beta \Leftrightarrow \alpha \subseteq \beta$;*

(c) $\alpha < \beta \Leftrightarrow \mathbf{S}(\alpha) \leq \beta$;
(d) $\alpha < \beta \Leftrightarrow \mathbf{S}(\alpha) < \mathbf{S}(\beta)$;
(e) $x \subseteq \alpha \Rightarrow (\bigcup x = \alpha \vee \bigcup x < \alpha)$;
(f) $\bigcup(\mathbf{S}(\alpha)) = \alpha$;
(g) $\alpha = \mathbf{S}(\bigcup \alpha) \vee \alpha = \bigcup \alpha$;
(h) $\bigcup \alpha = \alpha \Leftrightarrow (\alpha = 0 \vee \alpha$ *limite*$) \Leftrightarrow \langle \alpha, < \rangle$ *non ha massimo.*

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

(b) è analogo ad (a).

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

(d) è simile a (c).

(e) $\bigcup x$ è un ordinale per l'Esercizio 12.13 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 $\bigcup x \leq \alpha$.

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

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

(h) segue da (f) e (g). □

Proposizione 12.24. *Se A è un insieme di ordinali, allora $\bigcup A = \sup A$.*

Dimostrazione. Sia A sia un insieme di ordinali. L'insieme $\bigcup A$ è il più piccolo insieme contenente ogni $\alpha \in A$ e dato che $\bigcup A$ è un ordinale (Esercizio 12.13) e che l'inclusione coincide con $\leq$ sugli ordinali (Proposizione 12.23), ne segue che $\bigcup A = \sup A$. □

Esercizio 12.25. Sia $I \subseteq \Omega \leq \mathrm{Ord}$.

(i) Supponiamo che
$$(\forall \beta \in \Omega\, (\beta < \alpha \Rightarrow \beta \in I)) \Rightarrow \alpha \in I,$$
per ogni $\alpha \in \Omega$. Dimostrare che $I = \Omega$.

(ii) Supponiamo che
- $0 \in I$,
- $\forall \alpha \in \Omega (\exists \beta (\alpha = \mathbf{S}(\beta) \wedge \beta \in I) \Rightarrow \alpha \in I)$,

• $\forall\alpha \in \Omega\big((\alpha \text{ limite e } \forall\beta < \alpha\ \beta \in I) \Rightarrow \alpha \in I\big)$.
Dimostrare che $I = \Omega$.

Il prossimo risultato è dimostrato come la Proposizione 12.7 (e quindi la Proposizione 10.4) e utilizzando il Corollario 12.9.

Proposizione 12.26. (a) *Sia $f\colon \alpha \to \beta$ strettamente crescente. Allora*

$$\forall\gamma \in \alpha\,(\gamma \leq f(\gamma)) \tag{12.2}$$

e $\alpha \leq \beta$.

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

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

12.C. Cardinali.

12.C.1. *Insiemi finiti.* Una classe si dice **finita** se è in biezione con un numero naturale, altrimenti si dice **infinita**.. Poiché i numeri naturali sono insiemi, le classi finite sono insiemi e le classi proprie sono infinite.

La struttura

$$\langle \mathbb{N}, \mathbf{S}, 0\rangle$$

è induttiva per la Proposizione 11.9, quindi per quanto detto al fondo della Sezione 7.A risultano definite due operazioni $+$ e $\cdot$ su $\mathbb{N}$ che soddisfano le definizioni ricorsive di somma e prodotto (7.4)–(7.7). Poiché la struttura $\langle \mathbb{N}, \mathbf{S}, 0, +, \cdot, <\rangle$ soddisfa gli assiomi di PA, ne segue che le operazioni di somma e prodotto soddisfano le usuali proprietà aritmetiche (Proposizione 7.14). In particolare, possiamo definire la biezione $\boldsymbol{J}\colon \mathbb{N}\times\mathbb{N} \to \mathbb{N}$ di (6.6) a pagina 118 e quindi dimostrare che $\mathbb{N}\times\mathbb{N} \approx \mathbb{N}$ sono equipotenti (Teorema 10.18).

Definizione 12.27. Un **cardinale** è un ordinale κ che non è in biezione con nessun $\alpha < \kappa$. I cardinali sono generalmente denotati con lettere greche κ, λ, ... e Card è la classe dei cardinali.

Una classe X è **bene ordinabile** se esiste un buon ordine su X — equivalentemente, per il Teorema 12.17, se X è in biezione con un $\Omega \leq \mathrm{Ord}$.

Esercizio 12.28. Dimostrare che per una classe X le seguenti condizioni sono equivalenti:

- X è bene ordinabile
- X è immagine suriettiva di un ordinale o di Ord, cioè
$$\exists\Omega \leq \mathrm{Ord}\,\exists f\,(f\colon \Omega \twoheadrightarrow X),$$
- $X \precsim \mathrm{Ord}$, cioè $\exists f\,(f\colon X \rightarrowtail \Omega)$.

Quindi se X è bene ordinabile e Y è in biezione con (o anche solo: immagine suriettiva di) X, allora Y è bene ordinabile. Viceversa, se Y è bene ordinabile e $X \precsim Y$, allora X è bene ordinabile.

Definizione 12.29. Se X è un *insieme* bene ordinabile la **cardinalità di** X è il più piccolo ordinale $|X|$ in biezione con X.

In particolare $|\alpha|$, è il più piccolo ordinale $\beta \approx \alpha$ da cui $|\alpha| \leq \alpha$.

Quindi, la cardinalità di un insieme (se esiste, cioè se l'insieme è bene ordinabile) è un cardinale. Vedremo tra poco (Sezione 14.B) che l'Assioma di Scelta AC è equivalente all'affermazione che ogni insieme è bene ordinabile; quindi assumendo AC, $|X|$ è definito per *ogni insieme* X.

Il Teorema 10.19 implica che ogni numero naturale è un cardinale e che ω è il primo cardinale infinito. Invece $\mathbf{S}(\omega)$, $\mathbf{S}(\mathbf{S}(\omega))$, $\mathbf{S}(\mathbf{S}(\mathbf{S}(\omega)))$, ... non sono cardinali (Proposizione 12.31).

Proposizione 12.30. *Se κ e λ sono cardinali,*

(a) $\kappa = \lambda$ *se e solo se* $\kappa \approx \lambda$,

(b) $\kappa \leq \lambda$ *se e solo se* $\kappa \precsim \lambda$. *In particolare: se X e Y sono bene ordinabili, allora*

$$|X| \leq |Y| \Leftrightarrow \exists f(f\colon X \rightarrowtail Y).$$

Dimostrazione. (a) Supponiamo che $\kappa \approx \lambda$ e che $\kappa \neq \lambda$, per esempio $\kappa < \lambda$. Allora λ sarebbe in biezione con un ordinale più piccolo, una contraddizione.

(b) Per assurdo supponiamo $\kappa \precsim \lambda$ e $\lambda < \kappa$. Allora $\mathrm{id}_\lambda\colon \lambda \rightarrowtail \kappa$ e per il Teorema di Cantor-Schröder-Bernstein 10.14 a pagina 226, $\kappa \approx \lambda$, quindi $\kappa = \lambda$ per la parte (a), una contraddizione. □

Proposizione 12.31. (a) *Se $\alpha \geq \omega$ allora* $|\alpha| = |\mathbf{S}(\alpha)|$,

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

(c) $|\alpha| = |\beta|$ *se e solo se* $\alpha \approx \beta$,

(d) $|\alpha| \leq |\beta|$ *se e solo se esiste* $\alpha \precsim \beta$.

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

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

è una biezione.

(b) Sia $f\colon \alpha \to |\alpha|$ una biezione. Poiché $f\colon \alpha \to \beta$ è iniettiva e β si inietta in α, $|\alpha| = |\beta|$ per il Teorema di Cantor-Schröder-Bernstein 10.14 e la Proposizione 12.30.

(c) e (d) discendono dalla Proposizione 12.30. □

Gli unici esempi di cardinali visti finora sono i numeri naturali e ω, quindi è naturale chiedersi se esistano cardinali più grandi. Fissato un insieme X sia

$$A = \{(\alpha, f) \mid \alpha \in \mathrm{Ord} \wedge f\colon \alpha \rightarrowtail X\}.$$

Ad ogni $(\alpha, f) \in A$ associamo il buon ordine $W_{(\alpha,f)}$ su $\mathrm{ran}(f) \subseteq X$ indotto da f, cioè

$$x\ W_{(\alpha,f)}\ y \Leftrightarrow f^{-1}(x) \leq f^{-1}(y).$$

Quindi $f\colon \langle \alpha, \leq\rangle \to \left\langle \mathrm{ran}(f), W_{(\alpha,f)}\right\rangle$ è un isomorfismo. Se $(\alpha, f), (\beta, g) \in A$ e $W_{(\alpha,f)} = W_{(\beta,g)}$ allora $g^{-1} \circ f\colon \langle \alpha, \leq\rangle \to \langle \beta, \leq\rangle$ è un isomorfismo e quindi $\alpha = \beta$ e $f = g$ per la Proposizione 12.26. In altre parole: la funzione

$$A \to \mathscr{P}(X \times X), \qquad (\alpha, f) \mapsto W_{(\alpha,f)} \tag{12.3}$$

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

$$B = \{\alpha \in \mathrm{Ord} \mid \exists f\colon \alpha \rightarrowtail X\}$$

è un insieme transitivo, quindi è un ordinale. L'ordinale B è il più piccolo ordinale che non si inietta in X e si dice **numero di Hartogs** dell'insieme X, in simboli

$$\mathrm{Hrtg}(X).$$

Invertendo la funzione in (12.3) si ottiene una suriezione $\mathscr{P}(X \times X) \twoheadrightarrow A$, e componendo quest'ultima con la proiezione $A \twoheadrightarrow B$ si ottiene una suriezione

$$\mathscr{P}(X \times X) \twoheadrightarrow \mathrm{Hrtg}(X).$$

Se, per assurdo, $|\mathrm{Hrtg}(X)| \in \mathrm{Hrtg}(X)$, allora $\mathrm{Hrtg}(X) \rightarrowtail |\mathrm{Hrtg}(X)| \rightarrowtail X$, una contraddizione. Abbiamo quindi dimostrato il seguente

Teorema 12.32. $\mathrm{Hrtg}(X)$ *è il più piccolo ordinale che non si inietta in* X*, ed è un cardinale. Inoltre* $\mathscr{P}(X \times X)$ *si surietta su* $\mathrm{Hrtg}(X)$*.*

Nel caso in cui X sia un ordinale $\alpha \geq \omega$, allora $\mathrm{Hrtg}(\alpha) = \bigcup\{\beta \mid |\beta| = |\alpha|\} = \{\beta \mid |\beta| \leq |\alpha|\}$ è il più piccolo cardinale strettamente maggiore di α e lo si denota con

$$\alpha^+.$$

Nella Sezione 14.D dimostreremo (Teorema 14.13) che $\alpha \times \alpha \approx \alpha$, per ogni $\alpha \geq \omega$ e quindi

$$\forall \alpha \geq \omega \left(\mathscr{P}(\alpha) \twoheadrightarrow \alpha^+\right). \tag{12.4}$$

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

Esercizio 12.33. Dimostrare che un insieme non vuoto è numerabile se e solo se è immagine suriettiva di ω.

Il cardinale ω^+ viene denotato con

$$\omega_1$$

ed è il primo cardinale più che numerabile.

Teorema 12.34. *Se X è un insieme di cardinali, allora* $\sup X$ *è un cardinale.*

Dimostrazione. Se $\lambda = \bigcup X$ non fosse un cardinale allora λ sarebbe in biezione 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 12.35. Card *è una classe propria.*

Esercizi

Esercizio 12.36. 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 12.37. (i) Se $\langle X, \leq\rangle$ e $\langle Y, \preccurlyeq\rangle$ sono classi bene ordinate, quali delle proprietà viste (essere diretto, avere massimi, minimi, etc.) si preservano passando agli ordini prodotto e lessicografico su $X \times Y$? Ripetere l'esercizio quando $\langle I, \preccurlyeq\rangle$ e $\langle X_i, \leq_i\rangle$ con $i \in I$ sono classi bene ordinate.

(ii) Dimostrare che se $\langle X, \leq\rangle$ e $\langle Y, \preccurlyeq\rangle$ sono classi bene ordinate, allora $<_{\text{lex}}$ è un buon ordine su $X \times Y$ e l'ordine prodotto $\lhd$ è una relazione ben fondata su $X \times Y$. Sotto quali ipotesi $\lhd$ è un buon-ordine?

(iii) Dimostrare che se $\langle I, \preccurlyeq\rangle$ e $\langle X_i, \leq_i\rangle$ (per $i \in I$) sono insiemi bene ordinati, allora $\leq_{\text{lex}}$ è un buon ordine sull'unione disgiunta $\cup_{i\in I} X_i$. In particolare, se A e B sono insiemi bene ordinati, l'ordinamento lessicografico su $A \cup B$ è il buon ordine che elenca gli elementi di A e poi quelli di B.

Esercizio 12.38. Sia $R \subseteq X \times X$ una relazione transitiva[5] e regolare. Allora R è ben-fondata se e solo se ogni sotto-*insieme* non-vuoto di X ha un elemento R-minimale.

Esercizio 12.39. Dimostrare che non esiste nessuna funzione $f\colon \omega_1 \to \mathbb{R}$ strettamente crescente o strettamente decrescente.

[5]Vedremo nell'Esercizio 13.26 che l'ipotesi di transitività può essere rimossa.

Note e osservazioni

La letteratura sugli ordini è vastissima. I buoni ordini (e i loro rappresentanti canonici, gli ordinali, che vedremo nella sezione successiva) sono gli unici tipi di ordini che ammettono dei teoremi generali di struttura — per gli altri tipi di ordini ci sono pochi risultati generali. Nel caso degli ordini lineari numerabili vale il seguente risultato, congetturato da Fraïssé e dimostrato nel 1971 da Laver: Per ogni successione $\langle X_n, \trianglelefteq_n\rangle$ di ordini lineari numerabili esistono $n < m$ tali che $\langle X_n, \trianglelefteq_n\rangle$ si immerge in $\langle X_m, \trianglelefteq_m\rangle$. In altre parole: se $\langle X, \leq\rangle \preceq \langle Y, \trianglelefteq\rangle$ denota il fatto che $\langle X, \leq\rangle$ si immerge in $\langle Y, \trianglelefteq\rangle$ e $\langle X, \leq\rangle \prec \langle Y, \trianglelefteq\rangle$ significa che $\langle X, \leq\rangle \preceq \langle Y, \trianglelefteq\rangle$ ma $\langle Y, \trianglelefteq\rangle \not\preceq \langle X, \leq\rangle$, allora nella classe degli ordini lineari numerabili non esistono catene $\prec$-discendenti infinite e non esistono famiglie infinite di ordini reciprocamente non immergibili l'uno nell'altro. Per una trattazione completa della teoria degli ordini lineari e per una dimostrazione di questo profondo risultato di Laver, si veda il libro [**Ros82**].

La definizione originaria di ordinale (dovuta a Cantor) come classe di isomorfismo di buoni ordini ha lo svantaggio che un ordinale non nullo risulta essere una classe propria — questo è lo stesso difetto della definizione ingenua di cardinalità, come classe di equivalenza di insiemi equipotenti (si veda la Sezione 14.F). La definizione moderna di ordinale come insieme transitivo di insiemi transitivi è dovuta a von Neuman.

13. Costruzioni per ricorsione

Incominciamo ora uno studio sistematico delle costruzioni recursive, un argomento che è stato introdotto nella Sezione 7.B. Per il Teorema 7.4, dati due insiemi non vuoti A e B, e funzioni $g\colon B \to A$ e $F\colon \mathbb{N} \times B \times A \to A$, c'è un'unica $f\colon \mathbb{N} \times B \to A$ tale che

$$\begin{cases} f(0, b) = g(b) \\ f(n+1, b) = F(n, b, f(n, b)). \end{cases}$$

Nella dimostrazione del Teorema 7.4, la funzione f è ottenuta considerando l'intersezione di un'opportuna famiglia di sottoinsiemi di $(\mathbb{N} \times B) \times A$. Questo ragionamento funziona fin tanto che A e B sono *insiemi*, ma non può essere formalizzato in MK o in ZF se A o B sono *classi proprie*. In questo caso ogni funzione $f_n\colon B \to A$, $b \mapsto f(n, b)$, può essere definita mediante l'assioma di comprensione; per esempio

$$f_2 = \{(b, a) \in B \times A \mid \exists a_0, a_1 \in A\,[((1, b, a_1), a) \in F \\ \wedge ((0, b, a_0), a_1) \in F \wedge (b, a_0) \in g]\}$$

Il punto dolente è definire la sequenza delle f_n, ovvero — equivalentemente — la funzione f. Invece di approssimare la funzione f *dal di sopra* come nella dimostrazione del Teorema 7.4, approssimeremo f *dal di sotto*, in modo piuttosto simile a quanto è stato fatto nell'Esempio 7.10 per costruire il sottogruppo generato da un insieme.

Una dimostrazione alternativa del Teorema 7.4. Sia

$$\mathcal{G} = \{p \mid \exists m \in \omega\, \forall b \in B\, [p\colon m \times B \to A \wedge (0 < m \Rightarrow p(0,b) = g(b)) \\ \wedge \forall n\ (n+1 < m \Rightarrow p(n+1,b) = F(n,b,p(n,b)))]\}$$

Fatto 13.0.1. *Se $p, q \in \mathcal{G}$ allora $p \cup q$ è una funzione.*

Dimostrazione. Supponiamo che $p, q \in \mathcal{G}$ ma $p \cup q$ non sia una funzione. Allora c'è un $(n, b) \in \mathrm{dom}(p) \cap \mathrm{dom}(q)$ che testimonia $p(n,b) \neq q(n,b)$. Scegliamo un testimone siffatto con n minimo. Chiaramente $n \neq 0$, dato che $p(0,b) = g(b) = q(0,b)$ per ogni $b \in B$, quindi $n = k+1$. Allora

$$\begin{aligned} p(n,b) &= F(k,b,p(k,b)) \\ &= F(k,b,q(k,b)) && \text{per la minimalità di } n, \\ &= q(n,b). && \square \end{aligned}$$

Per la Proposizione 12.3 a pagina 278, $G = \bigcup \mathcal{G} \subseteq \omega \times A$ è una funzione.

Fatto 13.0.2. *$G \neq \emptyset$ e $G \in \mathcal{G}$.*

Dimostrazione. Poiché $\{((0,b), g(b)) \mid b \in B\} \in \mathcal{G}$, ne segue che $G \neq \emptyset$ e $G(0,b) = g(b)$. Se $\mathbf{S}(n) \in \mathrm{dom}(G)$ allora $G(\mathbf{S}(n)) = p(\mathbf{S}(n))$ per qualche $p \in \mathcal{G}$ e quindi $G(\mathbf{S}(n)) = F(p(n)) = F(G(n))$. $\square$

Vogliamo verificare che $\mathrm{dom}(G) = \omega \times B$. Per assurdo supponiamo che $\bar{n}$ sia minimo tale che $(\bar{n}, b) \notin \mathrm{dom}(G)$ per qualche $b \in B$, quindi $\bar{n} = \mathbf{S}(\bar{m})$ per qualche $\bar{m}$. È facile verificare che

$$p \stackrel{\text{def}}{=} G \cup \{((\bar{n}, b), F(G(\bar{m}, b)))\} \in \mathcal{G}$$

quindi $p \subseteq G$, da cui $(\bar{n}, b) \in \mathrm{dom}(G)$ per ogni $b \in B$: una contraddizione.

Resta infine da dimostrare che la funzione G è unica: se G' fosse un'altra funzione che soddisfa l'enunciato del teorema, allora sia $\bar{n}$ minimo per cui $G(\bar{n}, b) \neq G'(\bar{n}, b)$ per qualche $b \in B$. Chiaramente $\bar{n} \neq 0$ quindi $\bar{n} = \mathbf{S}(\bar{m})$ per qualche $\bar{m}$, e quindi

$$\begin{aligned} G(\bar{n},b) &= F(\bar{m},b,G(\bar{m},b)) \\ &= F(\bar{m},b,G'(\bar{m},b)) && \text{per la minimalità di } \bar{n}, \\ &= G'(\bar{n},b), \end{aligned}$$

contraddizione! $\square$

13.A. Esempi.

13.A.1. *Chiusura transitiva.* La **chiusura transitiva** di una relazione R su X è la relazione

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

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

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

Esercizio 13.1. Dimostrare che la relazione $\tilde{R}$ è transitiva su X.

Proposizione 13.2. *R è ben fondata su X se e solo se $\tilde{R}$ è ben fondata su X.*

Dimostrazione. Poiché $R \subseteq \tilde{R}$ è sufficiente verificare che $\tilde{R}$ è ben fondata se R lo è. Fissiamo $\emptyset \neq Y \subseteq X$ e dimostriamo che c'è un elemento $\tilde{R}$-minimale in Y. Un cammino da Y in sé stesso è una successione $\langle z_0, \dots, z_n, z_{n+1}\rangle$ in X di lunghezza ≥ 2 tale che $z_0, z_{n+1} \in Y$ e $z_i\ R\ z_{i+1}$ per $i = 0, \dots, n$. Sia

$$\bar{Y} = \{x \in X \mid \exists s\, (s \text{ è un cammino da } Y \text{ in sé stesso e } x \in \operatorname{ran} s)\}$$

l'insieme dei punti visitati da un cammino da Y in sé stesso. Per costruzione $Y \subseteq \bar{Y}$ e sia $\bar{y}$ un elemento R-minimale di $\bar{Y}$. Per costruzione nessun elemento di $\bar{Y} \setminus Y$ è R-minimale, quindi $\bar{y} \in Y$. Verifichiamo che $\bar{y}$ è $\tilde{R}$-minimale in Y. Se, per assurdo, $\bar{x}\ \tilde{R}\ \bar{y}$ per qualche $\bar{x} \in Y$ distinto da $\bar{y}$, allora c'è un cammino $\langle z_0, \dots, z_{n+1}\rangle$ da Y in sé stesso con $z_0 = \bar{x}$ e $z_{n+1} = \bar{y}$ e quindi $z_n\ R\ \bar{y}$, contro la R-minimalità di $\bar{y}$. □

La Proposizione 13.2 e l'Esercizio 13.1 non fanno uso di definizioni induttive, ma la dimostrazione del prossimo risultato sì.

Proposizione 13.3. *R è regolare su X se e solo se $\tilde{R}$ è regolare su X.*

Dimostrazione. Poiché $R \subseteq \tilde{R}$ è sufficiente verificare che $\tilde{R}$ è regolare se R lo è. Fissato un $\bar{x} \in X$, definiamo per ricorsione gli insiemi Z_n

$$\begin{aligned} Z_0 &= \{y \in X \mid y\ R\ \bar{x}\} \\ Z_{n+1} &= \{y \in X \mid \exists z \in Z_n\, (y\ R\ z)\} \\ &= \bigcup_{z \in Z_n} \{y \in X \mid y\ R\ z\}. \end{aligned}$$

Allora $\{y \in X \mid y\ \tilde{R}\ \bar{x}\} = \bigcup_{n\in\omega} Z_n$ è un insieme. □

Esercizio 13.4. Verificare che l'esistenza della $\langle Z_n \mid n \in \omega\rangle$ nella dimostrazione qui sopra discende dal Teorema **??**.

13.A.2. *Sottogruppo generato da un insieme.* Il sottogruppo di un gruppo G generato da $X \subseteq G$ è $\bigcup_n H_n$ dove

$$H_0 = X \cup \{e\}$$
$$H_{n+1} = \left\{x \cdot y^{-1} \mid x, y \in H_n\right\} \cup H_n.$$

La sequenza $\langle H_n \mid n \in \omega\rangle$ è ottenuta dal Teorema **??** ponendo $A = \mathscr{P}(G)$, $\bar{a} = X \cup \{e\}$ e $F(Z) = Z \cup \{x \cdot y^{-1} \mid x, y \in Z\}$.

Più in generale, ricordiamo dalla Sezione 11.K che se $\mathcal{F}$ è una famiglia di funzioni finitarie su un insieme X e $Y \subseteq X$, la chiusura $\mathrm{Cl}_{\mathcal{F}}(Y)$ di Y sotto $\mathcal{F}$ è il più piccolo sottoinsieme di X che contiene Y ed è chiuso sotto ogni $f \in \mathcal{F}$.

Applicando il Teorema **??** ad $A = \mathscr{P}(X)$, $\bar{a} = Y$ e $F(Z) = Z \cup \{f(z_1, \dots, z_m) \mid z_1, \dots, z_m \in Z \wedge m = \mathrm{ar}(f) \wedge f \in \mathcal{F}\}$ otteniamo una successione $\langle Y_n \mid n \in \omega\rangle$ tale che

$$Y_0 = Y$$
$$Y_{n+1} = Y_n \cup \{f(z_1, \dots, z_m) \mid z_1, \dots, z_m \in Y_n \wedge m = \mathrm{ar}(f) \wedge f \in \mathcal{F}\}.$$

Chiaramente $Y_n \subseteq Y_{n+1}$ e $Y_n \subseteq \mathrm{Cl}_{\mathcal{F}}(Y)$ per ogni n. Inoltre, se $f \in \mathcal{F}$ è m-aria e $z_1, \dots, z_m \in \bigcup_k Y_k$, allora $z_1, \dots, z_m \in Y_n$ per qualche n, quindi $f(z_1, \dots, z_m) \in Y_{n+1}$. Abbiamo quindi dimostrato che $\mathrm{Cl}_{\mathcal{F}}(Y) = \bigcup_k Y_k$.

Grazie al Teorema **??** e al Teorema 13.5 qui sotto, è possibile tradurre nel linguaggio della teoria degli insiemi ogni funzione definita ricorsivamente. Per esempio, supponiamo di voler formalizzare nel linguaggio LST la formula

$$\forall n, m \in \omega\,(n + m = m + n)\,. \tag{13.1}$$

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

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

dove $\varphi(u)$ è la formula che asserisce che u è un ordinale limite ed è il più piccolo siffatto. Per eliminare il simbolo $+$ possiamo ricorrere alla perifrasi: c'è una funzione $f\colon \omega \times \omega \to \omega$ che soddisfa gli assiomi della somma e tale che $f(n, m) = f(m, n)$, per tutti gli n, m. Il Teorema **??** ci garantisce che tale funzione esiste ed è unica. Quindi la formula (13.1) diventa

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

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

13.B. Il Teorema di Ricorsione. Il Teorema **??** benché molto utile non è sufficiente per molte applicazioni. Un primo per problema è che per calcolare $G(\mathbf{S}(n))$ potrebbe aver bisogno tanto di $G(n)$ quanto di n — per esempio, se G è la funzione fattoriale, allora $G(\mathbf{S}(n)) = G(n) \cdot \mathbf{S}(n)$. Un altro problema è che il valore $G(\mathbf{S}(n))$ potrebbe dipendere da alcuni (o tutti) i valori $G(k)$ con $k \leq n$. Infine è spesso necessario definire una funzione per ricorsione non solo su ω ma anche su un buon ordine generale o su una relazione ben fondata. Estenderemo il Teorema **??** rimpiazzando ω ed il suo ordinamento con una classe (eventualmente propria) X ed una relazione R ben-fondata e regolare su di essa.

Teorema 13.5. *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 $(z, x) \in Z \times X$*

$$G(z, x) = F(z, x, G \restriction \{(z, y) \mid y \mathrel{R} x\}). \tag{13.2}$$

Dimostrazione. Supponiamo che $G, G'\colon Z \times X \to \mathrm{V}$ soddisfino (13.2) 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 di Y. Allora

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

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

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

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

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

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

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

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

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

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

e per la R-minimalità di $\bar{x}$

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

da cui, utilizzando (iii) $p(\bar{z}, \bar{x}) = F(\bar{z}, \bar{x}, \bar{r}) = q(\bar{z}, \bar{x})$, contrariamente alla nostra ipotesi. È facile verificare che $p \cup q \in \mathcal{G}$, e quindi $\mathcal{G}$ è un semi-reticolo superiore rispetto all'inclusione. Per la Proposizione 12.3 a pagina 278, $G =$

$\bigcup \mathcal{G}$ è una relazione funzionale di dominio $\subseteq Z \times X$. Se $Z \times X \setminus \mathrm{dom}(G) \neq \emptyset$, sia $\bar{x}$ un elemento R-minimale di $\{x \in X \mid \exists z \in Z\ (z, x) \notin \mathrm{dom}(G)\}$ e sia $\bar{z} \in Z$ tale che $(\bar{z}, \bar{x}) \notin \mathrm{dom}(G)$. Per la Proposizione 13.3 $\tilde{R}$, la chiusura transitiva di R su X, è regolare, quindi

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

è un insieme per l'Assioma del Rimpiazzamento. È facile verificare che $\bar{p} \cup \{((\bar{z}, \bar{x}), F(\bar{z}, \bar{x}, \bar{p}))\} \in \mathcal{G}$ — le condizioni (i) e (iii) sono immediate, la (ii) si basa sulla transitività di $\tilde{R}$. Quindi $(\bar{z}, \bar{x}) \in \mathrm{dom}(G)$, contrariamente alla nostra assunzione. Ne segue che G è la relazione funzionale cercata. □

Osservazione 13.6. Il teorema così formulato è un enunciato di MK che asserisce che per ogni classe-funzione F c'è una ed una sola classe-funzione G con certe proprietà. Se vogliamo formulare (e dimostrare) il Teorema 13.5 in ZF, dobbiamo usare la perifrasi: date delle formule φ_X, φ_Z, φ_R e φ_F che definiscono rispettivamente le classi X, Z, la relazione $R \subseteq X \times X$ e la classe-funzione $F\colon Z \times X \times \mathrm{V} \to \mathrm{V}$ come nell'enunciato, allora c'è una formula φ_G che definisce la classe-funzione G che soddisfa (13.2). Inoltre, se ψ è un'altra formula che definisce una classe-funzione G' che soddisfa (13.2) allora $G = G'$, cioè le formule φ_G e ψ sono equivalenti.

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

Vediamo alcuni corollari immediati del Teorema 13.5. Se la funzione F non dipende dalla prima coordinata, otteniamo come caso particolare

Teorema 13.7. *Sia R una relazione irriflessiva, regolare e ben-fondata su X e sia $F\colon X \times \mathrm{V} \to \mathrm{V}$. Allora esiste un'unica $G\colon X \to \mathrm{V}$ tale che*

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

Se X un ordinale oppure $X = \mathrm{Ord}$ e R è l'ordinamento sugli ordinali otteniamo:

Corollario 13.8. *Sia $\Omega \leq \mathrm{Ord}$ e sia Z una classe. Siano H, K e L funzioni di dominio Z, $Z \times \{\alpha \in \Omega \mid \alpha$ successore$\} \times \mathrm{V}$ e $Z \times \{\alpha \in \Omega \mid \alpha$ limite$\} \times \mathrm{V}$, rispettivamente. Allora esiste un'unica $G\colon Z \times \Omega \to \mathrm{V}$ tale che*

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

Dimostrazione. Basta porre $F\colon Z \times \Omega \times \mathrm{V} \to \mathrm{V}$,

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

Quando la classe Z è irrilevante otteniamo

Corollario 13.9. *Sia $\Omega \leq \mathrm{Ord}$, sia $\bar{a}$ un insieme e siano K e L funzioni di dominio $\{\alpha \in \Omega \mid \alpha \text{ successore}\}\times\mathrm{V}$ e $\{\alpha \in \Omega \mid \alpha \text{ limite}\}\times\mathrm{V}$, rispettivamente. Allora esiste un'unica $G\colon \Omega \to \mathrm{V}$ tale che*

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

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

13.C. Applicazioni ed esempi. Vediamo alcuni esempi di funzioni costruite mediante il Teorema 13.5.

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

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

che soddisfa

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

si dice **rango di R su X**. Osserviamo innanzitutto che $\mathrm{ran}(\boldsymbol{\varrho}_{R,X}) \subseteq \mathrm{Ord}$: se $\boldsymbol{\varrho}_{R,X}(y) \in \mathrm{Ord}$ per ogni y tale che $y\ R\ x$, allora $\boldsymbol{\varrho}_{R,X}(x) \in \mathrm{Ord}$ per l'Esercizio 12.13. Inoltre $\mathrm{ran}(\boldsymbol{\varrho}_{R,X})$ è un segmento iniziale di Ord, cioè

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

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

Esercizio 13.10. Verificare che l'esistenza di $\boldsymbol{\varrho}_{R,X}$ discende dal Teorema 13.7 e dimostrare che:

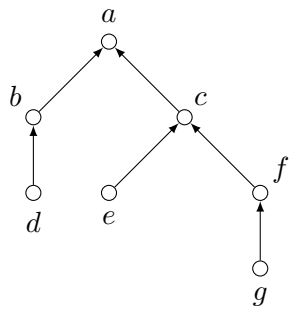
(i) $x\ R\ y \Rightarrow \boldsymbol{\varrho}_{R,X}(x) < \boldsymbol{\varrho}_{R,X}(y)$,

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

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

Esercizio 13.11. Verificare che se R è un buon ordine su X allora $\mathrm{ran}(\boldsymbol{\varrho}_{R,X}) = \mathrm{ot}(X, R)$ e $\boldsymbol{\varrho}_{R,X} \colon X \to \mathrm{ot}(X, R)$ è l'inversa della funzione enumerante (vedi pagina 281).

La funzione rango associa ad ogni elemento $x \in X$ una complessità — la complessità di un x è il minimo valore maggiore della complessità degli y tali che $y \mathrel{R} x$. Gli elementi di complessità minima sono quegli x tali che $\boldsymbol{\varrho}_{R,X}(x) = 0$, cioè gli elementi R-minimali. Per esempio, se R è la relazione su $\{a, b, c, d, e, f, g\}$ descritta dal grafo diretto (si veda la Sezione 8.B)



allora $\boldsymbol{\varrho}_{R,X}(d) = \boldsymbol{\varrho}_{R,X}(e) = \boldsymbol{\varrho}_{R,X}(g) = 0$, $\boldsymbol{\varrho}_{R,X}(b) = \boldsymbol{\varrho}_{R,X}(f) = 1$, $\boldsymbol{\varrho}_{R,X}(c) = 2$ e $\boldsymbol{\varrho}_{R,X}(a) = 3$.

13.C.2. *Collasso di Mostowski.* 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**.

Per esempio, se R e X sono come sopra, $\boldsymbol{\pi}_{R,X}(d) = \boldsymbol{\pi}_{R,X}(e) = \boldsymbol{\pi}_{R,X}(g) = \emptyset$, $\boldsymbol{\pi}_{R,X}(b) = \boldsymbol{\pi}_{R,X}(f) = \{\emptyset\} = 1$ e $\boldsymbol{\pi}_{R,X}(c) = \{0, 1\} = 2$ e $\boldsymbol{\pi}_{R,X}(a) = \{1, 2\}$.

Esercizio 13.12. 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 13.13. 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 13.14. Dimostrare che:

(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 ordine lineare (stretto o meno) su X, allora R è estensionale su X.

Proposizione 13.15. *Sia R una relazione irriflessiva, regolare e ben fondata sulla classe X.*

(a) *Se R è estensionale su X, allora $\boldsymbol{\pi}_{R,X}$ è iniettiva e $\boldsymbol{\pi}_{R,X}\colon \langle X, R\rangle \to \left\langle \overline{X}, \in \right\rangle$ è un isomorfismo.*

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

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

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

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

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

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

Se $\boldsymbol{\pi}_{R,X}(x) \in \boldsymbol{\pi}_{R,X}(y) = \{\boldsymbol{\pi}_{R,X}(z) \mid z\ R\ y\}$, allora per l'iniettività, $x\ R\ y$. Quindi per l'Esercizio 13.12,

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

vale.

(b) Supponiamo che $\boldsymbol{\varrho}_{R,X}(y) = \boldsymbol{\pi}_{R,X}(y)$, per ogni $y\ R\ x$. Allora $\boldsymbol{\pi}_{R,X}(x) = \{\boldsymbol{\pi}_{R,X}(y) \mid y\ R\ x\} = \{\boldsymbol{\varrho}_{R,X}(y) \mid y\ R\ x\}$ è un insieme di ordinali. Se $\boldsymbol{\pi}_{R,X}(z) \in \boldsymbol{\pi}_{R,X}(y) \in \boldsymbol{\pi}_{R,X}(x)$, allora $z\ R\ y\ R\ x$, da cui $z\ R\ x$, cioè $\boldsymbol{\pi}_{R,X}(x)$ è transitivo e quindi è un ordinale. Per costruzione $\boldsymbol{\pi}_{R,X}(x)$ è l'estremo superiore degli ordinali $\mathbf{S}(\boldsymbol{\pi}_{R,X}(y)) = \mathbf{S}(\boldsymbol{\varrho}_{R,X}(y))$ con $y\ R\ x$, vale a dire $\boldsymbol{\pi}_{R,X}(x) = \boldsymbol{\varrho}_{R,X}(x)$. □

13.C.3. *Punti fissi di funzioni continue.* Una funzione debolmente crescente $f\colon \Omega \to \mathrm{Ord}$, dove $\Omega \leq \mathrm{Ord}$, si dice **continua** se

$$\forall \lambda \in \Omega(\lambda \text{ limite } \Rightarrow f(\lambda) = \sup_{\alpha<\lambda} f(\alpha)). \tag{13.3}$$

Esercizio 13.16. 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 13.17. *Se* $f\colon \mathrm{Ord} \to \mathrm{Ord}$ *è strettamente crescente e continua, allora*

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

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

$$\begin{aligned} f(\bar{\alpha}) &= \sup_{\nu < \bar{\alpha}} f(\nu) \\ &= \sup_n f(\alpha_n) && \text{(per l'Esercizio 13.16)} \\ &= \sup_n \alpha_{\mathbf{S}(n)} \\ &= \bar{\alpha}. \end{aligned}$$

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

Definizione 13.18. $\aleph\colon \mathrm{Ord} \to \mathrm{Card} \setminus \omega$ è la funzione che enumera la classe dei cardinali infiniti, cioè

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

La definizione di $\aleph_\lambda$, per λ limite, è ben posta per il Teorema 12.34. 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

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

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

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

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

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

Esercizio 13.19. Dimostrare che $\mathrm{trcl}(X)$ è la più piccola classe transitiva contenente X. Se X è un insieme anche $\mathrm{trcl}(X)$ lo è e $\mathrm{trcl}(X) = \bigcup_n X_n$, dove $X_0 = X$ e $X_{n+1} = \bigcup X_n$.

13.D. La gerarchia di Von Neuman. 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 13.20. Dimostrare che

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

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

Dimostrazione. (a) Poiché $x \in \mathscr{P}(x)$ si ha che $\mathbf{S}(\mathrm{rank}(x)) \leq \mathrm{rank}(\mathscr{P}(x))$. Viceversa se $y \subseteq x$, allora $\mathbf{S}(\mathrm{rank}(y)) \leq \mathbf{S}(\mathrm{rank}(x))$ per l'Esercizio 13.20 e quindi $\mathrm{rank}(\mathscr{P}(x)) = \sup\{\mathbf{S}(\mathrm{rank}(y)) \mid y \subseteq x\} \leq \mathbf{S}(\mathrm{rank}(x))$.

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

Definizione 13.22. $\mathrm{V}_\alpha = \{x \mid \mathrm{rank}(x) < \alpha\}$.

Teorema 13.23. V_α *è un insieme transitivo e*

$$\mathrm{V}_\alpha = \bigcup_{\beta<\alpha} \mathscr{P}(\mathrm{V}_\beta). \tag{13.4}$$

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 vale (13.4). 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 (13.4). Per l'Esercizio 13.20 $x \subseteq \mathrm{V}_{\mathrm{rank}(x)}$ e quindi $\mathrm{rank}(x) < \alpha \Rightarrow x \in \bigcup_{\beta<\alpha} \mathscr{P}(\mathrm{V}_\beta)$. Viceversa, se $x \in \bigcup_{\beta<\alpha} \mathscr{P}(\mathrm{V}_\beta)$, allora $x \subseteq \mathrm{V}_\beta$, per qualche $\beta < \alpha$ e quindi $\mathrm{rank}(y) < \beta$ per ogni $y \in x$, da cui $\mathrm{rank}(x) \leq \beta < \alpha$. □

Corollario 13.24. (a) $\mathrm{V}_0 = \emptyset$.

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

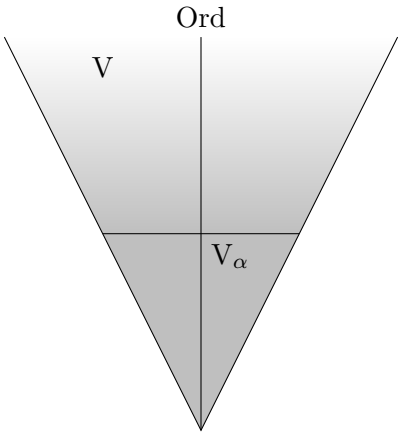
(c) $\mathrm{V}_{\mathbf{S}(\alpha)} = \mathscr{P}(\mathrm{V}_\alpha)$.

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

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

Quindi l'universo V è l'unione di una successione crescente di insiemi transitivi V_α, ognuno dei quali appartiene agli insiemi successivi e il più

piccolo dei quali è l'insieme vuoto:



Gli insiemi V_α sono approssimazioni dell'universo V, per l'Esercizio 13.20 (iii) $V_\alpha \cap \mathrm{Ord} = \alpha$, e l'approssimazione sarà tanto migliore quanto più grande è l'ordinale α. Sorge spontanea la domanda:

Quali assiomi della teoria degli insiemi sono veri in V_α?

Per semplicità ci limitiamo alla teoria ZF rimandando all'Esercizio 13.29 l'analoga questione per MK.

Innanzi tutto osserviamo che gli assiomi di estensionalità e di fondazione valgono in ogni classe transitiva M. Se $x, y \in M$ e $z \in x \triangle y$, allora $z \in M$ per transitività. Analogamente se $x \in M$ è non vuoto, allora c'è un $y \in x$ disgiunto da x: per transitività $y \in M$ e chiaramente non c'è nessun elemento di M che stia tanto in x quanto in y. Se $x \in V_\alpha$, allora $\mathrm{rank}(\bigcup x) \leq \mathrm{rank}(x) < \alpha$ e quindi $\bigcup x \in V_\alpha$. Quindi gli assiomi di estensionalità, di fondazione e di unione valgono in ogni V_α. Supponiamo ora che λ sia limite. Se $x, y \in V_\lambda$, allora $\mathrm{rank}(\{x, y\}) = \mathbf{S}(\max(\mathrm{rank}(x), \mathrm{rank}(y))) < \lambda$ e $\mathrm{rank}(\mathscr{P}(x)) = \mathbf{S}(\mathrm{rank}(x)) < \lambda$, quindi $\{x, y\}, \mathscr{P}(x) \in V_\lambda$. In particolare, dato che V_λ è chiuso sotto l'operazione di insieme potenza $x \mapsto \mathscr{P}(x)$, l'assioma di separazione vale in V_λ. Inoltre, se R è un buon ordine su $x \in V_\lambda$ è facile verificare che $R \in V_\lambda$, quindi se ogni insieme in V_λ è bene ordinabile, allora l'Assioma di Scelta vale in V_λ. Infine $\omega \in V_\lambda$ garantisce che c'è un insieme induttivo in V_λ (vedi pagina 263).

Indichiamo con Z e ZC le teorie ZF e ZFC senza l'Assioma del Rimpiazzamento, e con $\mathsf{ZFC} - \mathsf{Inf}$ la teoria ZFC senza l'Assioma dell'Infinito.

Teorema 13.25. (a) *Tutti gli assiomi di* $\mathsf{ZFC} - \mathsf{Inf}$ *valgono in* V_ω.

(b) *Tutti gli assiomi di* Z *valgono in* V_λ*, se* $\lambda > \omega$ *è limite.*

(c) *Se assumiamo* AC*, allora tutti gli assiomi di* ZC *valgono in* V_λ*, se* $\lambda > \omega$ *è limite.*

Dimostrazione. Per quanto detto è sufficiente dimostrare che rimpiazzamento e scelta valgono in V_ω. Come vedremo in seguito (Esercizio 15.11 a pagina 324), ogni V_n è finito e quindi ogni elemento di V_ω è finito. Ne segue che ogni $x \in \mathrm{V}_\omega$ è bene ordinabile e quindi AC vale per il Teorema 12.6. Inoltre se $A \in \mathrm{V}_\omega$ e $F\colon A \to \mathrm{V}_\omega$, allora $F[A]$ è finito, $F[A] = \{a_0, \dots, a_{n-1}\}$. Per ogni $i < n$ sia $m_i < \omega$ tale che $a_i \in \mathrm{V}_{m_i}$. Allora $F[A] \subseteq \mathrm{V}_m$, dove $m = \max\{m_0, \dots, m_{n-1}\}$, e quindi $F[A] \in \mathrm{V}_{m+1}$. □

Esercizi

Esercizio 13.26. Sia $R \subseteq X \times X$ una relazione regolare. Se $Y \subseteq X$ è un insieme definiamo

$$Y_0 = Y$$
$$Y_{k+1} = \bigcup\{R^{(y)} \mid y \in Y_k\}.$$

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

(ii) Generalizzare l'Esercizio 12.38 dimostrando che se è regolare e tale che ogni sotto-*insieme* non vuoto di X ammette un elemento R-minimale, allora R è ben fondata su X.

Esercizio 13.27. Dimostrare che da una successione di ordinali α_n si può estrarre una sotto-successione α_{n_k} debolmente crescente. In altre parole: per ogni $f\colon \omega \to \mathrm{Ord}$ c'è una $g\colon \omega \to \omega$ strettamente crescente tale che $f \circ g\colon \omega \to \mathrm{Ord}$ è debolmente crescente.

Esercizio 13.28. Dimostrare che se X e Y sono classi transitive e $f\colon X \to Y$ è una relazione funzionale biettiva tale che

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

allora $X = Y$ e $f = \mathrm{id} \restriction X$.

Concludere che le classi $\boldsymbol{\pi}_{R,X}$ e $\overline{X}$ nella parte (a) della Proposizione 13.15 sono uniche:

Se R è una relazione irriflessiva, regolare, ben fondata ed estensionale sulla classe X, allora c'è un'unica classe transitiva Y ed un'unica relazione funzionale $F\colon X \to Y$ tali che $\forall x, y \in X\,(x\ R\ y \Leftrightarrow F(x) \in F(y))$.

Esercizio 13.29. Dimostrare che

(i) tutti gli assiomi di MKC eccetto l'Assioma dell'Infinito valgono in $\mathrm{V}_{\mathbf{S}(\omega)}$,

(ii) se λ è limite, tutti gli assiomi di MK eccetto l'Assioma del Rimpiazzamento valgono in $\mathrm{V}_{\mathbf{S}(\lambda)}$, e se assumiamo la scelta, anche AC vale.

14. Assioma della scelta e cardinalità

14.A. L'assioma della scelta. L'Assioma di Scelta (AC), introdotto a pagina 269, asserisce che data una famiglia non vuota di insiemi non vuoti $\mathcal{A}$ c'è una funzione $f\colon \mathcal{A} \to \bigcup\mathcal{A}$ tale che $\forall A \in \mathcal{A}\,(f(A) \in A)$. La famiglia $\mathcal{A}$ può essere descritta come $\{A_i \mid i \in I\}$ dove $A_i \subseteq X$, per opportuni insiemi I e X. Se si fissano uno o entrambi i parametri I ed X si ottengono degli indebolimenti interessanti di AC.

Se si fissa l'insieme I degli indici della famiglia si ottiene l'enunciato AC_I

(AC_I) per ogni $\langle A_i \mid i \in I\rangle$ tale che $\forall i \in I\ (A_i \neq \emptyset)$ c'è una $\langle a_i \mid i \in I\rangle$ tale che $\forall i \in I\ (a_i \in A_i)$.

Quando I è finito, AC_I è dimostrabile in MK e in ZF, ma se I è infinito si ottiene un enunciato strettamente più debole di AC ma anch'esso indipendente dagli altri assiomi della teoria degli insiemi.

Se si fissa X si ottiene l'enunciato $\mathsf{AC}(X)$:

($\mathsf{AC}(X)$) se $X \neq \emptyset$ è un insieme, allora c'è una funzione di scelta su X (vedi pag. 269).

Infine $\mathsf{AC}_I(X)$ è l'enunciato:

($\mathsf{AC}_I(X)$) se $X \neq \emptyset$ è un insieme, per ogni $\langle A_i \mid i \in I\rangle$ tale che $\forall i \in I\ (\emptyset \neq A_i \subseteq X)$, c'è una $\langle a_i \mid i \in I\rangle$ tale che $\forall i \in I\ (a_i \in A_i)$.

Quindi

$$\begin{aligned} \mathsf{AC}_I &\Leftrightarrow \forall X\, \mathsf{AC}_I(X) \\ \mathsf{AC}(X) &\Leftrightarrow \forall I\, \mathsf{AC}_I(X) \\ \mathsf{AC} &\Leftrightarrow \forall I\, \forall X\, \mathsf{AC}_I(X). \end{aligned}$$

È facile verificare che se $X \twoheadrightarrow Y$ e $J \rightarrowtail I$, allora $\mathsf{AC}_I(X) \Rightarrow \mathsf{AC}_J(Y)$ (Esercizio 14.27).

14.A.1. *Scelte numerabili.* L'**Assioma delle scelte numerabili** AC_ω è una conseguenza di AC e non può essere dimostrata a partire da MK o da ZF. Si tratta di un principio insiemistico così intuitivo che spesso viene usato senza menzione.

Teorema 14.1. *Assumiamo* AC_ω. *Se* X *è infinito allora* $\omega \precsim X$.

Dimostrazione. Poiché X è infinito, $\emptyset \neq \mathcal{G}_n \stackrel{\text{def}}{=} \{g \mid g\colon n \rightarrowtail X\}$ per tutti gli $n \in \omega$. Per AC_ω fissiamo $g_n \in \mathcal{G}_n$ e per ricorsione definiamo $f\colon \omega \to X$

$$\begin{aligned} f(0) &= g_1(0) \\ f(n+1) &= g_{n+2}(i) \end{aligned}$$

dove $i = \min\{k \leq n+1 \mid g_{n+2}(k) \notin \{f(0), \dots, f(n)\}\}$. Poiché $\operatorname{ran}(g_{n+2})$ ha $n+2$ elementi, almeno uno di questi non appartiene all'insieme $\{f(0), \dots, f(n)\}$ e quindi f è ben definita. Una facile induzione mostra che f è iniettiva. □

Quindi AC_ω e la Proposizione 10.15 implicano che un insieme è infinito se e solo se è in biezione con un suo sottoinsieme proprio. Questa è la proprietà usata da Dedekind per definire la nozione di infinito, e per questo motivo gli insiemi che sono equipotenti con un qualche loro sottoinsieme proprio si dicono **Dedekind-infiniti**.

Teorema 14.2. *Assumiamo* AC_ω. *Se* $|X_n| \leq \omega$ *per tutti gli* $n \in \omega$, *allora* $|\bigcup_{n\in\omega} X_n| \leq \omega$, *vale a dire: l'unione numerabile di insiemi numerabili è numerabile.*

Dimostrazione. Sia $N\colon \bigcup_n X_n \to \omega$

$$N(x) = \min\{n \in \omega \mid x \in X_n\}.$$

Per AC_ω possiamo scegliere delle funzioni iniettive $f_n\colon X_n \rightarrowtail \omega$ e quindi definire l'iniezione

$$F\colon \bigcup_n X_n \rightarrowtail \omega \times \omega, \qquad F(x) = (N(x), f_{N(x)}(x)). \qquad \square$$

Osservazione 14.3. Nessuno dei Teoremi 14.1 e 14.2 sono dimostrabili senza scelta.

Per esempio è coerente supporre che esistano insiemi infiniti ma Dedekind-finiti, cioè insiemi X tali che $n \precsim X$ per ogni $n \in \omega$, e tuttavia X non contiene alcuna ω-sequenza di elementi distinti. Infatti, è possibile che insiemi siffatti siano sottoinsiemi di $\mathbb{R}$. Chiaramente, nessun insieme infinito e Dedekind-finito può essere bene ordinabile.

Analogamente, in assenza di scelta, l'unione numerabile di insiemi numerabili non è necessariamente numerabile. Infatti è coerente supporre che $\mathbb{R}$ sia l'unione numerabile di insiemi numerabili!

L'assioma $\mathsf{AC}_\omega(\mathbb{R})$ asserisce che per ogni successione numerabile di insiemi non vuoti di reali $A_0, A_1, \ldots$ c'è un successione di reali $a_0, a_1, \ldots$ tali che $a_n \in A_n$. È usato anche nei primi corsi di analisi, per esempio per dimostrare l'equivalenza tra continuità e continuità sequenziale. Ricordiamo che $f\colon \mathbb{R} \to \mathbb{R}$ è sequenzialmente continua in $\bar{x}$ se $f(x_n) \to f(\bar{x})$ per ogni successione $x_n \to \bar{x}$. Ogni funzione continua è sequenzialmente continua e mediante $\mathsf{AC}_\omega(\mathbb{R})$ si dimostra che

(14.1) Per ogni $f\colon \mathbb{R} \to \mathbb{R}$ e ogni $\bar{x} \in \mathbb{R}$, se f è sequenzialmente continua in $\bar{x}$, allora f è continua in $\bar{x}$.

Infatti l'enunciato (14.1) è *equivalente* ad $\mathsf{AC}_\omega(\mathbb{R})$ — si veda l'Esercizio 22.23. Tuttavia la sua versione globale:

(14.2) Per ogni $f\colon \mathbb{R} \to \mathbb{R}$, se f è sequenzialmente continua in *ogni* punto, allora è continua su $\mathbb{R}$.

è dimostrabile senza scelta [**Her06**, pag. 30]. Questo non è sorprendente: la (14.1) è un'affermazione del tipo

$$\forall f\, \forall \bar{x}\ (\varphi_{\text{seq. cont.}}(f, \bar{x}) \Rightarrow \varphi_{\text{seq. cont.}}(f, \bar{x}))$$

ed è più forte della (14.2) che è della forma

$$\forall f\ (\forall \bar{x}\, \varphi_{\text{seq. cont.}}(f, \bar{x}) \Rightarrow \forall \bar{x}\, \varphi_{\text{seq. cont.}}(f, \bar{x}))$$

14.A.2. *Equivalenti dell'assioma di scelta.* Abbiamo visto alcuni enunciati equivalenti ad AC, introdotto a pagina 269:

- ogni partizione di un insieme non vuoto ammette un selettore (Esercizio 11.17),
- il prodotto cartesiano di insiemi non vuoti è non vuoto (Esercizio 11.17),
- la proprietà distributiva infinitaria dell'intersezione rispetto all'unione (Esercizio 11.29),
- ogni suriezione ammette un'inversa sinistra (Esercizio 11.30),
- ogni insieme è proiettivo (Esercizio 11.30),
- per ogni relazione R c'è una funzione f tale che $\forall x \in \mathrm{dom}(R)\,[x\ R\ f(x)]$ (Esercizio 11.30),

e altri esempi, provenienti da varie parti della matematica, li vedremo nella Sezione 25. Nella prossima sezione vedremo che possiamo aggiungere a questa lista l'enunciato: ogni insieme è bene ordinabile.

14.B. Quali insiemi sono bene ordinabili? Il Teorema 12.6 ci assicura che

$$X \text{ bene ordinabile} \Rightarrow \mathsf{AC}(X)$$

e il Teorema 14.4 qui sotto dimostra il converso. Quindi:

$$\mathsf{AC}(X) \Leftrightarrow X \text{ è bene ordinabile.}$$

Teorema 14.4. $\mathsf{AC}(X)$ *implica che* X *è in biezione con un ordinale.*

Dimostrazione. Se $X = \emptyset$ allora, banalmente, X è bene ordinabile, quindi possiamo supporre X non vuoto e fissiamo una funzione di scelta C per X. Diamo innanzi tutto un'idea informale della dimostrazione: sia x_0 un elemento di X, per esempio $x_0 = C(X)$ e supponiamo di aver costruito $x_0, x_1, \ldots, x_\beta, \ldots$ elementi distinti di X, con $\beta < \alpha$. Se $X = \{x_\beta \mid \beta < \alpha\}$ allora $\alpha \to X$, $\beta \mapsto x_\beta$ è la biezione cercata. Altrimenti scegliamo un nuovo elemento $x_\alpha \in X$ distinto dai precedenti, per esempio $x_\alpha = C(X \setminus \{x_\beta \mid \beta < \alpha\})$. Se la funzione $\alpha \mapsto x_\alpha$ fosse definita per tutti gli $\alpha < \mathrm{Hrtg}(X)$, allora avremmo un'iniezione $\mathrm{Hrtg}(X) \rightarrowtail X$, contro la definizione di numero di Hartogs (pag. 286). Quindi esiste un $\bar\alpha < \mathrm{Hrtg}(X)$ tale che $X = \{x_\beta \mid \beta < \bar\alpha\}$.

Vediamo ora la dimostrazione nei suoi dettagli tecnici. Sia $F\colon \mathrm{V} \to \mathrm{V}$

$$F(h) = \begin{cases} C(X \setminus \mathrm{ran}(h)) & \text{se } h \text{ è una funzione e } \mathrm{ran}(h) \subset X, \\ X & \text{altrimenti.} \end{cases}$$

Per il Teorema 13.5 c'è una $G\colon \mathrm{Ord} \to \mathrm{V}$ tale che $\forall \alpha \in \mathrm{Ord}\,(G(\alpha) = F(G \restriction \alpha))$.

Fatto 14.4.1. *Se* $G(\alpha) = X$ *e* $\alpha < \beta$ *allora* $G(\beta) = X$.

Dimostrazione. $X = G(\alpha) \in \mathrm{ran}(G \restriction \beta)$, quindi $\mathrm{ran}(G \restriction \beta) \not\subset X$. Ne segue che $F(G \restriction \beta) = X$ e quindi $G(\beta) = X$. □

Fatto 14.4.2. *Se $G(\beta) \neq X$ e $\alpha < \beta$, allora $G(\alpha) \neq G(\beta)$.*

Dimostrazione. $G(\alpha) \in \mathrm{ran}(G \restriction \beta) \subseteq X$, quindi $G(\alpha)$ è distinto da $G(\beta) \in X \setminus \mathrm{ran}(G \restriction \beta)$. □

Ne segue che $G(\alpha) = X$ per qualche $\alpha < \mathrm{Hrtg}(X)$, altrimenti si avrebbe una funzione iniettiva $\mathrm{Hrtg}(X) \rightarrowtail X$. Sia $\bar\alpha$ minimo tale che $G(\bar\alpha) = X$. Allora $g = G \restriction \bar\alpha$ è una funzione iniettiva in X. Se $\mathrm{ran}(g) \neq X$, allora

$$X = G(\bar\alpha) = F(g) = C(X \setminus \mathrm{ran}(g)) \in X$$

contraddizione. Quindi $g\colon \bar\alpha \to X$ è una biezione. □

I risultati precedenti possono essere generalizzati alle classi proprie, se si conviene che una funzione di scelta per una classe propria X sia una relazione funzionale F di dominio $\{y \mid \emptyset \neq y \subseteq X\}$ e tale che $F(y) \in y$, per ogni $y \in \mathrm{dom}(F)$.

Teorema 14.5. *Una classe X è bene ordinabile se e solo se c'è una funzione di scelta su X. In particolare, V è bene ordinabile se e solo se vale* GAC*, l'Assioma di Scelta Globale (pag. 269).*

Teorema 14.6. AC *è equivalente all'affermazione*

$$\forall \alpha \in \mathrm{Ord}\ (\mathscr{P}(\alpha) \text{ è bene ordinabile})\,.$$

Dimostrazione. Per il Corollario 13.24 è sufficiente dimostrare che V_α è bene ordinabile, per ogni α. Procediamo per induzione su α.

Chiaramente $\mathrm{V}_0 = \emptyset$ è bene ordinabile, e se V_α è bene ordinabile e $f\colon \mathrm{V}_\alpha \to \gamma$ è una biezione, allora per ipotesi c'è un buon ordine $\prec$ su $\mathscr{P}(\gamma)$ che induce mediante f un buon ordine su $\mathrm{V}_{\alpha+1} = \mathscr{P}(\mathrm{V}_\alpha)$.

Passiamo al caso λ limite, che è il più complesso. Useremo il seguente

Esercizio 14.7. Se λ è limite e $\lhd_\alpha$ è un buon ordine su X_α per ogni $\alpha < \lambda$, allora il seguente è un buon ordine su $\bigcup_{\alpha<\lambda} X_\alpha$:

$$x \lhd_\lambda y \Leftrightarrow \big[\min\{\alpha \mid x \in X_\alpha\} < \min\{\alpha \mid y \in X_\alpha\} \vee \exists \alpha (x, y \in X_\alpha \setminus \bigcup_{\beta<\alpha} X_\beta \wedge x \lhd_\alpha y)\big].$$

Supponiamo V_α sia bene ordinabile per ogni $\alpha < \lambda$: per l'Esercizio 14.7 è sufficiente scegliere (senza usare AC!) un buon ordine $\lhd_\alpha$ su V_α, per ogni $\alpha < \lambda$. Sia γ_α minimo tale che $\mathscr{P}(\alpha)$ è bene ordinabile in tipo d'ordine γ_α, sia γ l'estremo superiore dei γ_α^+, così che ogni buon ordine su V_α ha tipo d'ordine $< \gamma$. Sia $\prec$ un buon ordine su $\mathscr{P}(\gamma)$. Possiamo ora ripetere il

ragionamento precedente che ci ha portati al caso λ limite: poniamo $\lhd_0 = \emptyset$; se $\lhd_\alpha$ è un buon ordine su V_α e $f_\alpha\colon \mathrm{V}_\alpha \to \gamma^+$ è la sua funzione enumerante, allora definiamo $\lhd_{\alpha+1}$ su $\mathrm{V}_{\alpha+1}$ mediante f_α e $\prec$; se $\nu < \lambda$ è un ordinale limite applichiamo l'Esercizio 14.7 e otteniamo $\lhd_\nu$. □

14.C. Il principio del buon ordinamento e il Lemma di Zorn. In questa sezione stabiliremo l'equivalenza tra scelta e alcuni principi insiemistici usati in matematica:

- il **principio di massimalità di Hausdorff:** Ogni insieme parzialmente ordinato contiene una catena massimale;
- il **Lemma di Zorn:** Ogni insieme parzialmente ordinato in cui ogni catena ha un maggiorante, contiene un elemento massimale;
- la **forma debole del Lemma di Zorn:** Ogni insieme parzialmente ordinato in cui ogni sottoinsieme diretto superiormente ha un maggiorante, contiene un elemento massimale.

Questi principi possono essere *localizzati* ad un insieme, analogamente a quanto avviene per AC quando lo si localizza ad un insieme X ottenendo così $\mathsf{AC}(X)$. Per esempio è possibile restringere il principio di massimalità di Hausdorff agli ordinamenti su un insieme fissato, ottenendo così (MaxHaus(X):

se $\leq$ è un ordinamento su X, allora $\exists C \subseteq X$ (C catena massimale).

Quindi il principio di massimalità di Hausdorff diventa $\forall X$ (MaxHaus(X)). Il Lemma di Zorn diventa $\forall X$ Zorn(X), dove Zorn(X) è l'enunciato

se $\leq$ è un ordinamento su X tale che
ogni catena ha un maggiorante, allora $\exists x \in X$ (x massimale).

Analogamente la forma debole del Lemma di Zorn diventa $\forall X$ wZorn(X).

Proposizione 14.8. *Fissiamo un insieme non vuoto X.*

(a) *Se X è bene ordinabile, allora* MaxHaus(X).
(b) MaxHaus(X) $\Rightarrow$ Zorn(X).
(c) Zorn(X) $\Rightarrow$ wZorn(X).

Dimostrazione. (a) Per assurdo, sia $\leq$ un ordinamento su X privo di catene massimali. Se $C \subseteq X$ è una catena, l'insieme

$$K(C) = \{x \in X \setminus C \mid C \cup \{x\} \text{ è una catena}\}$$

è non vuoto. Fissiamo una funzione di scelta $F\colon \mathscr{P}(X) \setminus \{\emptyset\} \to X$. La funzione $g\colon \mathrm{Hrtg}(X) \to X$ definita da

$$g(\alpha) = F\left(K\left(\{g(\beta) \mid \beta < \alpha\}\right)\right).$$

è iniettiva e questo contraddice il Teorema 12.32.

(b) Sia $\leq$ un ordine parziale su X in cui ogni catena ha un maggiorante. Se $C \subseteq X$ è una catena massimale, allora il maggiorante di C deve appartenere a C e quindi è un elemento massimale di X.

(c) è immediato. □

Teorema 14.9. *Sono equivalenti:*

(a) AC.

(b) *Il principio di massimalità di Hausdorff.*

(c) *Il Lemma di Zorn.*

(d) *La forma debole del Lemma di Zorn.*

(e) *Il* **Lemma di Teichmüller-Tukey:** *Sia $\emptyset \neq \mathcal{F} \subseteq \mathscr{P}(X)$ una famiglia di* ***carattere finito****, cioè*

$$\forall Y \subseteq X \, (Y \in \mathcal{F} \Leftrightarrow \forall Z \subseteq Y \, (Z \text{ finito} \Rightarrow Z \in \mathcal{F})) \, .$$

Allora ogni $Y \in \mathcal{F}$ è contenuto in uno $Z \in \mathcal{F}$ massimale.

(f) *L'***Assioma delle Scelte Multiple (AMC):** *Per ogni insieme $X \neq \emptyset$ c'è una funzione $F \colon \mathscr{P}(X) \setminus \{\emptyset\} \to \mathscr{P}(X) \setminus \{\emptyset\}$ tale che $F(A) \subseteq A$ è finito, per ogni $\emptyset \neq A \subseteq X$.*

(g) *Ogni pre-ordine contiene un sottoinsieme A massimale di elementi inconfrontabili, cioè tali che $x \not\leq y$ e $y \not\leq x$ per ogni coppia di elementi distinti $x, y \in A$.*

(h) **Principio di massimalità di Kurepa:** *Ogni ordine parziale contiene un sottoinsieme A massimale di elementi inconfrontabili.*

(i) *Ogni ordine lineare è bene ordinabile.*

Dimostrazione. Le implicazioni (g) $\Rightarrow$ (h) e (a) $\Rightarrow$ (f) sono immediate, mentre (a) $\Rightarrow$ (b) $\Rightarrow$ (c) $\Rightarrow$ (d) seguono dalla Proposizione 14.8.

(d) $\Rightarrow$ (e). In una famiglia $\mathcal{F} \subseteq \mathscr{P}(X)$ di carattere finito ogni famiglia $\mathcal{D}$ di insiemi contenenti Y che è diretta superiormente per inclusione ha un estremo superiore, $\bigcup \mathcal{D} \in \mathcal{F}$, quindi c'è uno $Z \in \mathcal{F}$ massimale contenente Y.

(e) $\Rightarrow$ (g). Sia $\langle X, \leq \rangle$ un insieme pre-ordinato. La famiglia

$$\mathcal{F} = \{A \subseteq X \mid \forall x, y \in A \, (x \neq y \Rightarrow x \not\leq y \wedge y \not\leq x)\}$$

ha carattere finito, e $\emptyset \in \mathcal{F}$, quindi contiene un insieme massimale.

(f) $\Rightarrow$ (i) e (h) $\Rightarrow$ (i). Sia $\langle X, \leq \rangle$ un ordine lineare: dimostreremo che c'è una funzione di scelta per X e quindi il risultato discende dal Teorema 14.4.

Supponiamo valga (f): per ipotesi c'è una $G\colon \mathscr{P}(X)\setminus\{\emptyset\} \to \mathscr{P}(X)\setminus\{\emptyset\}$ tale che $G(A) \subseteq A$ è finito, per ogni $\emptyset \neq A \subseteq X$. Sia $g(A)$ l'elemento minimo di A. Allora g è una funzione di scelta su X.

Supponiamo valga (i): sia $\preceq$ il preordine su $\mathcal{P} = \{(A, a) \mid A \subseteq X \wedge a \in A\}$ definito da

$$(A, a) \preceq (B, b) \Leftrightarrow A = B \wedge a \leq b.$$

Per ipotesi c'è un insieme massimale $\mathcal{A} \subseteq \mathcal{P}$ di elementi inconfrontabili: si verifica immediatamente che $\mathcal{A}$ è una funzione di scelta per X.

(i) $\Rightarrow$ (a). ${}^{\alpha}2$ è linearmente ordinato dall'ordinamento lessicografico $<_{\text{lex}}$, quindi ${}^{\alpha}2$ è bene ordinabile. Poiché ${}^{\alpha}2 \approx \mathscr{P}(\alpha)$ il risultato segue dal Teorema 14.6. □

14.D. Aritmetica cardinale.

Definizione 14.10. La **somma cardinale** ed il **prodotto cardinale** sono le operazioni binarie Card × Card → Card definite da

$$\kappa + \lambda = |\kappa \times \{0\} \cup \lambda \times \{1\}|$$
$$\kappa \cdot \lambda = |\kappa \times \lambda|.$$

La definizione è ben posta dato che $\kappa \times \{0\} \cup \lambda \times \{1\}$ e $\kappa \times \lambda$ sono bene ordinabili (Esercizio 12.37, pag. 287).

Per la (10.5),

$$\kappa + \lambda \leq \kappa \cdot \lambda. \tag{14.3}$$

Osserviamo che per la parte (a) della Proposizione 12.31 a pagina 285, questa formula vale anche quando uno dei due cardinali è 1 e l'altro è $\geq \omega$. Riassumendo: se κ e λ sono cardinali e se $2 \leq \min(\kappa, \lambda)$ oppure $1 = \min(\kappa, \lambda)$ e $\omega \leq \max(\kappa, \lambda)$, allora

$$\max(\kappa, \lambda) \leq \kappa + \lambda \leq \kappa \cdot \lambda \leq \max(\kappa, \lambda) \cdot \max(\kappa, \lambda). \tag{14.4}$$

Vogliamo ora mostrare che il prodotto di numeri naturali è un numero naturale.

Esercizio 14.11. Il **buon ordine di Gödel su** Ord × Ord è definito da

$$(\alpha, \beta) <_{\text{G}} (\gamma, \delta) \Leftrightarrow$$
$$\Big[\max(\alpha, \beta) < \max(\gamma, \delta) \vee \big(\max(\alpha, \beta) = \max(\gamma, \delta) \wedge (\alpha, \beta) <_{\text{lex}} (\gamma, \delta)\big)\Big].$$

Verificare che $<_{\text{G}}$ è un buon-ordine su Ord × Ord e che se $\alpha < \beta$ allora $\alpha \times \alpha$ è un segmento iniziale di $\beta \times \beta$.

Lemma 14.12. *Se X e Y sono insiemi finiti, allora anche $X \times Y$ è finito. In particolare $\forall n, m \in \omega\, (n \cdot m \in \omega)$.*

Dimostrazione. Per l'Esercizio 10.24(i) e la Proposizione 10.21, e poiché $n \times m \subseteq \max(n,m) \times \max(n,m)$, è sufficiente dimostrare che $n \times n$ è finito, per ogni $n \in \omega$.

L'ordine $<_{\mathrm{G}}$ ha $(0,0)$ come minimo e ogni $(i,j) \in n \times n \setminus \{(0,0)\}$ ha un predecessore immediato. Infatti $\max(i,j) > 0$ è della forma $\mathbf{S}(m)$:

- se $i = 0$ allora $j = \mathbf{S}(m)$ quindi (m,m) è il predecessore di (i,j);
- se $0 < i < \max(i,j) = j$ allora $i = \mathbf{S}(k)$ per qualche k e (k,j) è il predecessore di (i,j);
- se $i = \max(i,j)$ e $j = 0$ allora $(m, \mathbf{S}(m))$ è il predecessore di (i,j);
- se $i = \max(i,j)$ e $j \neq 0$ allora $j = \mathbf{S}(k)$ per qualche k e (i,k) è il predecessore di (i,j).

Quindi per l'Esercizio 12.22 a pagina 282 il tipo d'ordine di $n \times n$ è $\leq \omega$. Abbiamo quindi dimostrato che

$$\forall n \in \omega \, (\mathrm{ot} \, \langle n \times n, <_{\mathrm{G}} \rangle \leq \omega) \, .$$

Poiché $n \times n$ è l'insieme dei predecessori di $(0,n)$ in $\langle (n+1) \times (n+1), <_{\mathrm{G}} \rangle$, per il Corollario 12.10 si ha che $\mathrm{ot} \, \langle n \times n, <_{\mathrm{G}} \rangle < \mathrm{ot} \, \langle (n+1) \times (n+1), <_{\mathrm{G}} \rangle \leq \omega$ ed essendo n arbitrario

$$\forall n \in \omega \, (\mathrm{ot} \, \langle n \times n, <_{\mathrm{G}} \rangle < \omega) \, . \qquad \square$$

Teorema 14.13. *Sia κ un cardinale infinito. Allora* $\mathrm{ot}(\kappa \times \kappa, <_{\mathrm{G}}) = \kappa$ *e* $|\kappa \times \kappa| = \kappa$.

Dimostrazione. La funzione

$$\langle \kappa, < \rangle \to \langle \kappa \times \kappa, <_{\mathrm{G}} \rangle \qquad \alpha \mapsto (\alpha, 0)$$

è strettamente crescente da cui $\kappa \leq \mathrm{ot}(\kappa \times \kappa, <_{\mathrm{G}})$. È quindi sufficiente dimostrare per induzione su $\kappa \geq \omega$ che $\mathrm{ot}(\kappa \times \kappa, <_{\mathrm{G}}) \leq \kappa$, e quindi $|\kappa \times \kappa| = \kappa$.

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 biezione 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)

$$\mathrm{pred}(\alpha,\beta) = \mathrm{pred}((\alpha,\beta); <_{\mathrm{G}}) = \{(\alpha', \beta') \in \kappa \times \kappa \mid (\alpha', \beta') <_{\mathrm{G}} (\alpha, \beta)\}$$

è contenuto in $\nu \times \nu$, dove $\nu = \max\{\alpha, \beta\} + 1$, quindi $|\mathrm{pred}(\alpha,\beta)| \leq |\nu \times \nu| < \kappa$. Abbiamo quindi dimostrato che

$$\forall \alpha, \beta < \kappa \, (\mathrm{ot}(\mathrm{pred}(\alpha,\beta), <_{\mathrm{G}}) < \kappa)$$

e quindi $\mathrm{ot}(\kappa \times \kappa, <_{\mathrm{G}}) \leq \kappa$. $\square$

Dalla (14.4) e dal Teorema 14.13 otteniamo

Corollario 14.14. *Se κ e λ sono cardinali diversi da 0 e almeno uno tra κ e λ è infinito, allora*

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

In altre parole: la somma ed il prodotto di cardinali sono operazioni banali.

Proposizione 14.15. *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 biezione.

Dimostrazione. Poiché $^{\lambda}2 \subseteq {}^{\lambda}\kappa \subseteq {}^{\lambda}\lambda$, per il teorema di Cantor-Schröder-Bernstein è sufficiente dare un'iniezione $^{\lambda}\lambda \rightarrowtail {}^{\lambda}2$. Per il Teorema 14.13 e la parte (ii) dell'Esercizio 10.24 $\mathscr{P}(\lambda \times \lambda)$ è in biezione con $\mathscr{P}(\lambda)$, quindi il risultato discende da $^{\lambda}\lambda \subseteq \mathscr{P}(\lambda \times \lambda)$. □

Definizione 14.16. Se X è un insieme e κ un cardinale

$$\mathscr{P}_{\kappa}(X) = \{Y \subseteq X \mid |Y| < \kappa\}$$

è la famiglia dei sottoinsiemi di X che sono bene ordinabili e di cardinalità minore di κ.

La definizione è particolarmente importante quando X è un insieme bene ordinabile, per esempio un cardinale λ. La Proposizione precedente può essere generalizzata così:

Proposizione 14.17. *Se $\kappa \leq \lambda$ sono cardinali, gli insiemi*

$$\mathscr{P}_{\kappa}(\lambda), \quad \{f \in {}^{\kappa}\lambda \mid f \text{ è strettamente crescente}\}, \quad {}^{\kappa}\lambda$$

sono in biezione.

Senza l'Assioma di Scelta non è possibile dimostrare la bene-ordinabilità di $^{\kappa}X$ quando $\kappa \geq \omega$ e X ha almeno due elementi — per esempio se non vale AC non è detto che $^{\omega}2$ sia in biezione con un qualche ordinale. Invece mostreremo ora (senza usare AC) che $^{n}\kappa$ è bene ordinabile per $n < \omega$. 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 biezioni $j_n\colon {}^{n}\kappa \to \kappa$ 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

biezione, possiamo definire j_{n+1} mediante il diagramma

$$\begin{array}{ccccccc} & & & & j_{n+1} & & \\ & \overset{}{\frown} & & \overset{}{\frown} & & \overset{}{\frown} & \\ {}^{n+1}\kappa & \longrightarrow & {}^{n}\kappa \times \kappa & \longrightarrow & \kappa \times \kappa & \longrightarrow & \kappa \\ s & \longmapsto & (s \restriction n, s(n)) & \longmapsto & (j_n(s \restriction n), s(n)) & \longmapsto & f(j_n(s \restriction n), s(n)) \end{array}$$

Quindi, se κ è un cardinale infinito, allora $|{}^{n}\kappa| = \kappa$. Inoltre la funzione $j_\omega \colon {}^{<\omega}\kappa \to \omega \times \kappa$

$$j_\omega(s) = \begin{cases} (0,0) & \text{se } s = \emptyset, \\ (n, j_n(s)) & \text{se } \mathrm{lh}(s) = n > 0, \end{cases}$$

è iniettiva e quindi $|{}^{<\omega}\kappa| = \kappa$. Abbiamo quindi dimostrato che

Teorema 14.18. *Se X è bene ordinabile e infinito, allora $|{}^{<\omega}X| = |X|$.*

La nozione di successione finita di elementi di X è strettamente collegata a quella di sottoinsieme finito di X.

Definizione 14.19. L'insieme dei sottoinsiemi finiti di κ di cardinalità n è

$$[\kappa]^n \stackrel{\text{def}}{=} \{x \subseteq \kappa \mid |x| = n\}.$$

Gli insiemi $[\kappa]^{<n}$ e $[\kappa]^{\leq n}$ dei sottoinsiemi finiti di κ di cardinalità rispettivamente $< n$ e $\leq n$ sono definiti similmente. Infine

$$[\kappa]^{<\omega} \stackrel{\text{def}}{=} \bigcup_n [\kappa]^n$$

è l'insieme dei sottoinsiemi finiti di κ.

Quindi $[\kappa]^0 = \{\emptyset\}$ e $[\kappa]^1$ è l'insieme dei singoletti di κ.

Ogni $x \in [\kappa]^n$ può essere scritto come $x = \{\alpha_0, \dots, \alpha_{n-1}\}$ con $\alpha_0 < \cdots < \alpha_{n-1} < \kappa$ e quindi può essere identificato con la successione $\langle \alpha_0, \dots, \alpha_{n-1} \rangle \in {}^{n}\kappa$. Questa identificazione definisce un'iniezione $[\kappa]^n \rightarrowtail {}^{n}\kappa$ che si estende a $[\kappa]^{<\omega} \rightarrowtail {}^{<\omega}\kappa = \bigcup_n {}^{n}\kappa$. Quindi per $n > 0$

$$\kappa \leq |[\kappa]^n| \leq |[\kappa]^{<\omega}| \leq |{}^{<\omega}\kappa| = \kappa$$

cioè $\kappa = |[\kappa]^n| = |[\kappa]^{<\omega}|$.

Poiché nella Definizione 14.19 possiamo sostituire un insieme infinito bene ordinabile X al posto di κ, otteniamo

Corollario 14.20. *Se X è infinito e bene ordinabile, allora anche $[X]^n$ e $[X]^{<\omega}$ sono bene ordinabili e se $n > 0$*

$$|[X]^n| = |[X]^{<\omega}| = |X|.$$

14.E. Applicazioni. Vediamo qualche applicazione dei risultati precedenti.

14.E.1. *Gruppi liberi.* Una parola su un insieme non vuoto X è un elemento di $(X \times \{1,-1\})^{<\omega}$, cioè una sequenza della forma

$$\langle (x_1,\varepsilon_1),(x_2,\varepsilon_2),\dots,(x_n,\varepsilon_n)\rangle$$

con $x_1,\dots,x_n \in X$ e $\varepsilon_1,\dots,\varepsilon_n \in \{-1,1\}$. Per semplificare la notazione scriveremo una parola come

$$x_1^{\varepsilon_1}\cdot x_2^{\varepsilon_2}\cdots x_n^{\varepsilon_n}$$

con la convenzione che x^1 si indica semplicemente con x. Una parola è riducibile se $x_i = x_{i+1}$ e $\varepsilon_i = -\varepsilon_{i+1}$ per qualche $i+1<n$; altrimenti si dice irriducibile. L'inversa di una parola $w = x_1^{\varepsilon_1}\cdot x_2^{\varepsilon_2}\cdots x_n^{\varepsilon_n}$ è la parola $w^{-1} \stackrel{\text{def}}{=} x_n^{-\varepsilon_n}\cdots x_2^{-\varepsilon_2}\cdot x_1^{\varepsilon_1}$. Per convenzione, la parola vuota $\emptyset$ è l'inversa di sé stessa. Il **gruppo libero** su X è l'insieme $F(X)$ delle parole ridotte su X con la seguente operazione: dati $w_1,w_2 \in F(X)$ sia v la più lunga sequenza tale che $w_1 = z^\frown v$ e $w_2 = v^{-1\frown}u$. (Chiaramente $v=\emptyset$ è possibile.) Per costruzione $z^\frown u$ è una parola irriducibile e poniamo

$$w_1\cdot w_2 = z^\frown u.$$

Si verifica [**Hun80**, p. 65] che l'operazione è associativa, che w^{-1} è proprio l'inverso (nel senso della teoria dei gruppi) di w e che $\emptyset$ è l'elemento neutro e che quindi viene indicato con 1.

Poiché $F(X) \subseteq (X\times\{1,-1\})^{<\omega}$ otteniamo subito che se X è bene ordinabile, anche $F(X)$ lo è, e se $|X| = \kappa \geq \omega$, allora $|F(X)| = \kappa$.

Se X è equipotente a Y allora $F(X)$ è isomorfo a $F(Y)$, quindi se X è bene ordinabile posiamo definire il **rango** di $F(X)$ come la cardinalità di X. Il gruppo libero di rango κ, con κ cardinale non nullo, è unico a meno di isomorfismo e lo si indica con F_κ; inoltre F_κ è isomorfo a F_λ se e solo se $\kappa=\lambda$. È immediato verificare che F_1 è (isomorfo a) $\mathbb{Z}$, e questo è l'unico gruppo libero commutativo. Il gruppo F_2 è generato da due elementi a e b e non è abeliano, dato che $ab \neq ba$. La struttura di F_2 può essere visualizzato mediante un grafo aciclico con ω vertici di valenza 4, e con un vertice privilegiato etichettato con 1 (Figura 1). L'operazione $w \mapsto wa^{\pm 1}$ di moltiplicazione a destra per a o a^{-1} corrisponde ad uno spostamento orizzontale a destra o a sinistra, mentre a $w \mapsto wb^{\pm 1}$ corrisponde ad uno spostamento verticale verso l'alto o verso il basso. Analogamente F_n è descritto da un grafo aciclico su ω vertici, ciascuno di valenza $2n$.

Se $(G,\circ)$ è un gruppo e X è un insieme non vuoto, ogni funzione $f\colon X\to G$ può essere esteso ad un omomorfismo $\hat f\colon F(X)\to G$ ponendo

$$\hat f(x_1^{n_1}\dots x_k^{n_k}) = f(x_1)^{n_1}\circ\cdots\circ f(x_k)^{n_k}.$$

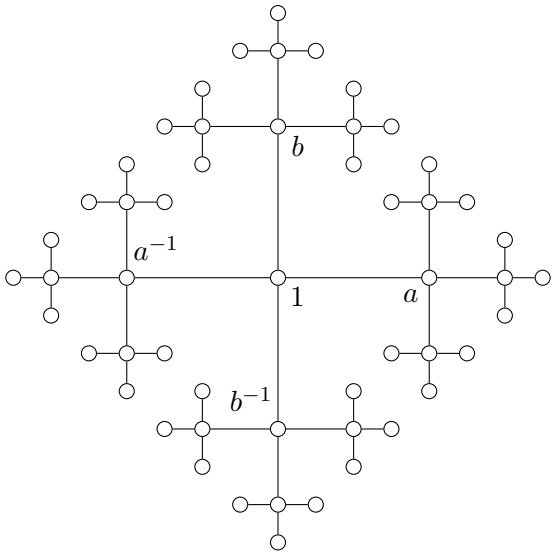


Figura 1. Il gruppo F_2 con due generatori a e b

I gruppi liberi di rango κ sono quindi suriettivamente universali per i gruppi generati da al più κ elementi nel seguente senso: se $X \subseteq G$ è un insieme di al più κ generatori, allora G è immagine omomorfa di $F(X)$.

Se X si inietta in Y allora $F(X)$ è isomorfo ad un sottogruppo di $F(Y)$, ma il viceversa non vale: il gruppo libero F_2 contiene sottogruppi propri isomorfi a F_n per ogni $1 \leq n \leq \omega$; per esempio il sottogruppo generato da $\{a^n b a^{-n} \mid n \in \omega\}$ è isomorfo a F_ω.

Per ogni famiglia di gruppi G_i con $i \in I$, possiamo considerare l'insieme $W = (\cup_{i\in I} G_i \setminus \{1_i\})^{<\omega}$ i cui elementi sono della forma

$$w = \langle (i_0, g_0), \ldots, (i_n, g_{i_n}) \rangle$$

dove $g_k \in G_{i_k}$ e $i_k \in I$. Se $i_j \neq i_{j+1}$ per ogni $j + 1 \leq n$, diremo che w è irriducibile. L'inversa di w è

$$w^{-1} = \langle (i_n, g_{i_n}), \ldots, (i_0, g_0) \rangle$$

dove g_k^{-1} è l'inverso di g_k calcolato in G_{i_k}. L'inversa di una w irriducibile è irriducibile. Il **prodotto libero** di due gruppi G_i, che è solitamente indicato con

$$*_{i\in I} G_i.$$

è l'insieme delle parole ridotte con l'operazione di prodotto $\cdot$ definita in analogia a quanto fatto per $F(X)$, vale a dire: dati $w_1, w_2 \in *_{i\in I} G_i$ sia v la più lunga sequenza tale che $w_1 = z^\frown v$ e $w_2 = v^{-1\frown} u$ e sia

$$w_1 \cdot w_2 = z^\frown u.$$

Il prodotto libero di due gruppi G_0 e G_1 (cioè quando $|I| = 2$) lo si indica con $G_0 * G_1$. Il prodotto libero generalizza la costruzione del gruppo libero, nel senso che se $|X| = \kappa$ allora

$$F(X) = \underbrace{\mathbb{Z} * \mathbb{Z} * \cdots}_{\kappa\text{-volte}}.$$

Supponiamo che i gruppi G_1 e G_2 contengano G_0 come sottogruppo. Sia $W = (G_0 \cup (G_1 \setminus G_0) \cup (G_2 \setminus G_0))^{<\omega}$ i cui elementi sono della forma

$$w = \langle (i_0, g_0), \ldots, (i_n, g_{i_n}) \rangle$$

dove $g_k \in G_{i_k}$ e $i_k \in \{0, 1, 2\}$. Se $i_j \neq i_{j+1}$ per ogni $j + 1 \leq n$, diremo che w è irriducibile. L'insieme delle parole irriducibili si dice **prodotto libero di G_1 e G_2 modulo H** ed è indicato con $G_1 *_{G_0} G_2$: è un gruppo e a definizione di w^{-1} e di prodotto è come nel caso dei prodotti liberi.

Possiamo ora dare un esempio di gruppo contenente due gruppi finitamente generati la cui intersezione non è finitamente generata, come avevamo detto nell'Esempio 8.25(f) a pagina 166.

Esempio 14.21. Sia $G_1 = G_2 = F_2$ e sia H il sottogruppo di F_2 generato da $\{a^n b a^{-n} \mid n \in \mathbb{N}\}$, dove a, b sono i generatori di F_2. Allora G_0 e G_1 sono sottogruppi finitamente generati di $G = F_2 *_H F_2$ la cui intersezione è H non è finitamente generata.

14.E.2. *Spazi vettoriali.* Sia V uno spazio vettoriale su un campo $\Bbbk$ bene ordinabile di cardinalità κ e sia λ la dimensione di V, cioè la cardinalità di una sua base $\{\mathbf{e}_\alpha \mid \alpha \in \lambda\}$. Se V è finito dimensionale, cioè $\lambda < \omega$, allora V è in biezione con $\Bbbk^\lambda$ e quindi

$$|V| = |^\lambda \kappa| = \begin{cases} \kappa & \text{se } \kappa \geq \omega, \\ \kappa^\lambda & \text{altrimenti.} \end{cases}$$

Se V è infinito-dimensionale cioè $\lambda \geq \omega$, allora ogni $\mathbf{v} \in V$ può essere scritto in un unico modo come

$$\mathbf{v} = \sum_{i \in I} r_i \mathbf{e}_i$$

dove $I \subset \lambda$ è finito e $r_i \in \Bbbk \setminus \{0_\Bbbk\}$ — se $\mathbf{v}$ è il vettore nullo $\mathbf{0}$ prendiamo $I = \emptyset$. Quindi V è in biezione con l'insieme

$$\bigcup_{n \in \omega} [\lambda]^n \times (\Bbbk \setminus \{0_\Bbbk\})^n$$

e quindi ha cardinalità λ, se $\kappa < \omega$ cioè se il campo $\Bbbk$ è finito, e ha cardinalità $\max(\kappa, \lambda)$ altrimenti. Quindi

$$|V| = \begin{cases} \kappa^\lambda & \text{se } \kappa, \lambda < \omega, \\ \kappa & \text{se } \lambda < \omega \leq \kappa, \\ \max(\kappa, \lambda) & \text{se } \omega \leq \kappa, \lambda. \end{cases}$$

14.F. Cardinalità senza scelta. Assumendo l'Assioma di Scelta, ogni insieme è in biezione con un ordinale, quindi si definisce la cardinalità (Definizione 12.29 a pag. 285) come

$$|X| = \min \{\alpha \mid \alpha \approx X\}$$

dove $\approx$ è la relazione di equipotenza tra insiemi. Ma che fare se per qualche motivo vogliamo (o siamo costretti a) fare a meno di AC? Nella teoria ingenua degli insiemi (Sezione 10) la cardinalità di un insieme X è definita come

$$\operatorname{card}(X) = [X]_{\approx}.$$

Il confronto tra cardinalità è definito come

$$\operatorname{card}(X) \leq \operatorname{card}(Y) \Leftrightarrow X \precsim Y \tag{14.5}$$

dove $\precsim$ è la relazione di immergibilità. Per il Teorema di Cantor-Schröder-Bernstein 10.14 a pagina 226 la relazione $\leq$ è antisimmetrica, quindi è un ordine parziale sulle cardinalità. Il difetto di questo approccio è che $\operatorname{card}(X)$ è una classe propria se X non è vuoto (Esercizio 12.2). Un problema analogo si presenta quando si lavora con una relazione di equivalenza E su una classe propria $\mathcal{A}$. In molti casi la relazione E non è regolare, cioè le classi di equivalenza sono classi proprie — questa è la situazione tipica quando si studiano classi di strutture a meno di isomorfismo. Data una classe $\mathcal{A}$ ed una relazione d'equivalenza E come sopra, vorremmo una classe funzione $\boldsymbol{C} \colon \mathcal{A} \to \mathcal{A}$ tale che

$$\forall x \in \mathcal{A}\, (\boldsymbol{C}(x) \in [x]_E)$$

e

$$\forall x, y \in \mathcal{A}\, (x \mathrel{E} y \Rightarrow \boldsymbol{C}(x) = \boldsymbol{C}(y)).$$

L'esistenza di una $\boldsymbol{C}$ siffatta è equivalente all'esistenza di un **trasversale** T **per la relazione** E, vale a dire una classe $T \subseteq \mathcal{A}$ tale che $T \cap [x]_E$ è un singoletto, per ogni $x \in \mathcal{A}$.

In alcune situazioni la funzione $\boldsymbol{C}$ può essere descritta esplicitamente, anche se E non è regolare su $\mathcal{A}$:

- Se $\mathcal{A}$ è la classe degli insiemi bene ordinati ed E è la relazione di isomorfismo, allora ogni classe d'equivalenza contiene esattamente un ordinale, quindi possiamo porre $\boldsymbol{C}(A, <) = \operatorname{ot}(A, <)$;

- Se $\mathcal{A}$ è la classe dei compatti numerabili ed E è la relazione di omeomorfismo, allora possiamo definire $\boldsymbol{C}(K)$ come l'unico ordinale della forma $\omega^{\cdot\gamma} \cdot n + 1$, con $\gamma < \omega_1$ (Teorema 24.8);
- Se $\mathcal{A}$ è la classe dei gruppi abeliani finitamente generati ed E è la relazione di isomorfismo, allora possiamo definire $\boldsymbol{C}(G)$ come l'unico gruppo isomorfo a G della forma

$$\mathbb{Z}^n \times \mathbb{Z}/p_1\mathbb{Z} \times \mathbb{Z}/p_2\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k\mathbb{Z}$$

con $n \geq 0$ e $p_1 \leq p_2 \leq \cdots \leq p_k$ primi e $k \geq 0$.

Se si assume qualche forma di assioma di scelta, l'elenco precedente può essere esteso:

- Se assumiamo AC e $\mathcal{A}$ è la classe V di tutti gli insiemi ed E è la relazione di equipotenza, allora possiamo definire $\boldsymbol{C}(A)$ come l'unico cardinale κ equipotente ad A.
- Se assumiamo l'Assioma di Scelta Globale GAC allora V è bene ordinabile (Teorema 14.5) e quindi la classe-funzione $\boldsymbol{C}$ può essere definita per ogni $\mathcal{A}$ e E.

Tuttavia, in assenza di scelta non è possibile, in generale, selezionare un rappresentante canonico in ogni classe di equivalenza di E.

Mediante la gerarchia dei V_α introdotta nella Sezione 13.D, è possibile definire (senza scelta!) una funzione $[\![\cdot]\!]_E \colon \mathcal{A} \to \mathrm{V}$ tale che

$$\emptyset \neq [\![x]\!]_E \subseteq [x]_E$$

e

$$x \mathrel{E} y \Leftrightarrow [\![x]\!]_E = [\![y]\!]_E.$$

L'insieme $[\![x]\!]_E$ si dice classe di E-equivalenza di Scott, ed è definita da

$$[\![x]\!]_E = \{y \mid y \mathrel{E} x \wedge \forall z\,(z \mathrel{E} x \Rightarrow \mathrm{rank}(y) \leq \mathrm{rank}(z))\}$$

o, equivalentemente,

$$[\![x]\!]_E = [x]_E \cap \mathrm{V}_{\bar{\alpha}}, \text{ dove } \bar{\alpha} = \min\{\alpha \mid \mathrm{V}_\alpha \cap [x]_E \neq \emptyset\}.$$

Osservazioni 14.22. (a) Se $[\![x]\!]_E$ è un singoletto per ogni x, allora possiamo porre $\boldsymbol{C}(x) = \bigcup [\![x]\!]_E$.

(b) In generale, $x \notin [\![x]\!]_E$.

Usando le classi di Scott possiamo dare la seguente:

Definizione 14.23. Il **tipo d'ordine** di un insieme ordinato $(A, <)$ è definito come

$$\mathrm{type}(A, <) = \begin{cases} \mathrm{ot}(A, <) & \text{se } (A, <) \text{ è un buon ordine,} \\ [\![(A, <)]\!]_{\cong} & \text{altrimenti,} \end{cases}$$

dove $\cong$ è la relazione di isomorfismo tra insiemi ordinati.

Quindi in assenza di AC, la **cardinalità** di un insieme X è definita come

$$\operatorname{card}(X) = \begin{cases} |X| & \text{se } X \text{ è bene ordinabile,} \\ [\![X]\!]_{\approx} & \text{altrimenti.} \end{cases} \tag{14.6}$$

Le cardinalità sono usualmente indicate con lettere gotiche minuscole, riservando la lettera $\mathfrak{c}$ per la cardinalità del continuo. L'ordinamento sulle cardinalità è dato dalla (14.5), cioè

$$\mathfrak{a} \leq \mathfrak{b} \Leftrightarrow A \preccurlyeq B \text{ per qualche/ogni } A \in \mathfrak{a} \text{ e } B \in \mathfrak{b}.$$

Osservazione 14.24. Con questa definizione ogni cardinale è una cardinalità — il converso (cioè ogni cardinalità è un cardinale) è equivalente all'Assioma di Scelta per la Sezione 14.B.

AC implica che due cardinalità sono sempre confrontabili, visto che si tratta di ordinali. Infatti la confrontabilità delle cardinalità è equivalente all'Assioma di Scelta.

Teorema 14.25. AC *è equivalente all'affermazione:*

$$\forall \mathfrak{a}, \mathfrak{b}\ (\mathfrak{a} \leq \mathfrak{b} \vee \mathfrak{b} \leq \mathfrak{a}),$$

o equivalentemente: $\operatorname{card}(A) \leq \operatorname{card}(B) \vee \operatorname{card}(B) \leq \operatorname{card}(A)$*, per ogni insieme* A, B*.*

Dimostrazione. Per il Teorema 12.6 e per quanto detto qui sopra, è sufficiente dimostrare che la confrontabilità sulle cardinalità implica che ogni insieme sia bene ordinabile. Fissiamo un insieme A: poiché $\operatorname{Hrtg}(A) \rightarrowtail A$ è impossibile per il Teorema di Hartogs 12.32, allora $A \rightarrowtail \operatorname{Hrtg}(A) \subseteq \operatorname{Ord}$. □

14.F.1. *Aritmetica cardinale in assenza di scelta.* La somma e prodotto di cardinalità sono definite da

$$\begin{aligned} \operatorname{card}(A) + \operatorname{card}(B) &= \operatorname{card}(A \cup B) \\ \operatorname{card}(A) \cdot \operatorname{card}(B) &= \operatorname{card}(A \times B), \end{aligned}$$

e questo concorda con la Definizione 14.10 quando A e B sono bene ordinabili. La dimostrazione a pagina 228 mostra che se $2 \leq \mathfrak{a}, \mathfrak{b}$, allora

$$\mathfrak{a} + \mathfrak{b} \leq \mathfrak{a} \cdot \mathfrak{b}.$$

Per quanto visto, $\mathfrak{a}$ è infinito se e solo se $\mathfrak{a} \not< \omega$, quindi in assenza di scelta il Teorema 14.13 può essere riformulato come

$$\mathfrak{a} \not< \omega \Rightarrow \mathfrak{a} \cdot \mathfrak{a}, \tag{14.7}$$

ovvero: se A è infinito, allora $A \approx A \times A$. Assumendo (14.7), se $A \in \mathfrak{a}$ e $B \in \mathfrak{b}$ sono insiemi infiniti e disgiunti allora

$$A \cup B \approx (A \cup B) \times (A \cup B) \approx A \cup (A \times B) \cup (B \times A) \cup B,$$

e quindi $A \times B \rightarrowtail A \cup B$, da cui

$$\mathfrak{a} \cdot \mathfrak{b} = \mathfrak{a} + \mathfrak{b}.$$

Proposizione 14.26. *Le seguenti affermazioni sono equivalenti:*

(a) AC,

(b) $\mathfrak{a} \not< \omega \Rightarrow \mathfrak{a} \cdot \mathfrak{a} = \mathfrak{a}$,

(c) $\mathfrak{a}, \mathfrak{b} \not< \omega \Rightarrow \mathfrak{a} \cdot \mathfrak{b} = \mathfrak{a} + \mathfrak{b}$.

Dimostrazione. È sufficiente dimostrare che (c) implica che ogni insieme A è bene ordinabile. Innanzi tutto possiamo supporre che A non contenga ordinali e che quindi sia disgiunto da $B = \mathrm{Hrtg}(A)$. Per la (**??**) c'è una biezione $F\colon A \times \mathrm{Hrtg}(A) \to A \cup \mathrm{Hrtg}(A)$. Poiché $\mathrm{Hrtg}(A) \preccurlyeq A$ è impossibile,

$$\forall x \in A\, \exists \alpha \in \mathrm{Hrtg}(A)\, (F(x, \alpha) \notin A).$$

Se $\alpha(x)$ è il minimo testimone, allora $A \to \mathrm{Hrtg}(A)$, $x \mapsto F(x, \alpha(x))$, è iniettiva e quindi A è bene ordinabile. □

Esercizi

Esercizio 14.27. Dimostrare che se $X \twoheadrightarrow Y$ e $I \rightarrowtail J$, allora $\mathsf{AC}(X) \Rightarrow \mathsf{AC}(Y)$.

Esercizio 14.28. Dimostrare che le seguenti affermazioni sono equivalenti ad AC.

(i) Per ogni famiglia $\mathcal{A}$ di insiemi c'è una $\mathcal{B} \subseteq \mathcal{A}$ massimale formata da insiemi a due a due disgiunti.

(ii) Per ogni $\langle A_i \mid i \in I\rangle$ c'è una $\langle B_i \mid i \in I\rangle$ tale che $\emptyset \subseteq B_i \subseteq A_i$, $\bigcup_{i\in I} B_i = \bigcup_{i\in I} A_i$ e che $B_i \cap B_j = \emptyset$ per $i \neq j$.

(iii) Ogni insieme parzialmente ordinato in cui ogni catena ha un estremo superiore, contiene un elemento massimale.[6]

(iv) Ogni insieme parzialmente ordinato in cui ogni catena bene ordinata ha un estremo superiore, contiene un elemento massimale.

Esercizio 14.29. Per il Teorema di Cantor 10.23 non esiste nessuna iniezione $F\colon \mathscr{P}(X) \rightarrowtail X$. Per ogni $F\colon \mathscr{P}(X) \to X$ costruiremo esplicitamente insiemi $W, Z \subseteq X$ tali che $F(W) = F(Z)$.

Dimostrare che esiste un unico $W \subseteq X$ ed un unico buon ordine $\lhd$ su W tali che

(a) $F(\{z \in W \mid z \lhd w\}) = w$, per ogni $w \in W$ e

(b) $F(W) \in W$.

[6]Questo è l'enunciato del Lemma di Zorn con *estremo superiore* invece di *maggiorante*.

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.

Esercizio 14.30. Dimostrare il Teorema 14.5.

Esercizio 14.31. Dimostrare la Proposizione 14.17.

Esercizio 14.32. (i) Dimostrare che (14.7) implica il seguente rafforzamento di (**??**): Se X e Y sono non vuoti e almeno uno dei due è infinito, allora $\mathrm{card}(X)+\mathrm{card}(Y) = \mathrm{card}(X)\cdot\mathrm{card}(Y)$.

(ii) Dimostrare che da (**??**) segue che $\mathrm{card}(X) + \mathrm{card}(X) = \mathrm{card}(X)$ per ogni insieme infinito X.

Esercizio 14.33. (i) Dimostrare che se $A_1, \dots, A_n$ sono insiemi finiti, allora anche $A_1 \cup \cdots \cup A_n$ e $A_1 \times \cdots \times A_n$ sono finiti.

(ii) Definire $\prod I$ il prodotto di un insieme finito I di numeri naturali e verificare che $|A_1 \times \cdots \times A_n| = \prod \{|A_1|, \dots |A_n|\}$.

(iii) Definire $\sum I$ la somma di un insieme finito I di numeri naturali e verificare che $|A_1 \cup \cdots \cup A_n| = S_1 - S_2 + S_3 - S_4 + \cdots + (-1)^{n+1} S_n$ dove

$$S_k = \sum \left\{ \sum_{i\in I} |A_i| \mid I \subseteq \{1, \dots, n\} \wedge |I| = k \right\}.$$

Esercizio 14.34. Dimostrare che AC è equivalente a $\forall\alpha(\mathscr{P}(\alpha)$ è bene ordinabile).

Esercizio 14.35. Dimostrare che $\aleph_{\alpha+1} \not\precsim \mathscr{P}(\mathscr{P}(\aleph_\alpha))$.

Esercizio 14.36. Dimostrare che $\forall X\,(X$ infinito $\Rightarrow [X]^2 \approx X)$ implica AC.

Note e osservazioni

La letteratura sull'assioma di scelta è vastissima. A parte i classici libri [**Jec73, RR85**] e il monumentale [**HR98**] segnaliamo tra le più recenti pubblicazioni [**Her06**]. Il Teorema 14.6 è dovuto a Sierpiński.

La proposizione 14.26 è di Tarski. L'enunciato '$\mathrm{card}(X)+\mathrm{card}(X) = \mathrm{card}(X)$ per ogni insieme infinito X' non implica AC [**Sag75**]. L'Esercizio 14.36 è tratto da [].

15. Aritmetica ordinale

Per il Corollario 13.8 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. (Le notazioni $\alpha + \beta$, $\alpha \cdot \beta$ sono già state utilizzate per le operazioni di somma e prodotto *cardinale* nella Sezione 14.D.)

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

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

Proposizione 15.1. (a) $\beta < \beta' \Rightarrow \alpha \dot{+} \beta < \alpha \dot{+} \beta'$.

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

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

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

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

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

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

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

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

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

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

(b) La funzione $\nu \mapsto \alpha \dot{+} \nu$ è strettamente crescente e continua, quindi $\alpha \dot{+} \lambda$ è limite per l'Esercizio 13.16. Se $\lambda = \sup_{i\in I} \lambda_i$, allora $\alpha \dot{+} \lambda_i \leq \alpha \dot{+} \lambda$ e quindi $\sup_{i\in I} \alpha \dot{+} \lambda_i \leq \alpha \dot{+} \lambda$. Viceversa, se $\beta < \alpha \dot{+} \lambda$, allora fissiamo $\gamma < \lambda$ tale che $\beta < \alpha \dot{+} \gamma$ e fissiamo $j \in I$ tale che $\gamma < \lambda_j$. Allora $\beta < \alpha \dot{+} \gamma < \alpha \dot{+} \lambda_j$, da cui segue l'asserto.

(c) Per induzione su γ. Il caso $\gamma = 0$ è banale. Supponiamo che la proprietà valga per un γ e dimostriamola:[7] per $\mathbf{S}(\gamma)$

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

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

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

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

[7] La dimostrazione è analoga alla parte (c) della Proposizione 7.14.

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

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

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

Esercizio 15.2. Dimostrare che

$$\alpha \dot{+} \beta = \{\xi \mid \xi < \alpha \vee \exists! \delta\, (0 < \delta < \beta \wedge \xi = \alpha \dot{+} \delta)\}\,.$$

L'ordine lessicografico (Sezione 12.A) sull'unione disgiunta $\alpha \cup \beta$ è un buon ordine (Esercizio 12.37) e la funzione $f\colon \alpha \dot{+} \beta \to \alpha \cup \beta$

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

è un isomorfismo di buoni ordini. Quindi la somma ordinale di α e β può essere definita come il tipo d'ordine della loro unione disgiunta $\alpha \cup \beta$ con l'ordinamento lessicografico, cioè una copia di α seguita da una copia di β. In particolare

$$|\alpha \dot{+} \beta| = |\alpha \times \{0\} \cup \beta \times \{1\}|. \tag{15.1}$$

Esercizio 15.3. Dimostrare che

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

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

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

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

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

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

Come nell'aritmetica elementare, l'esponenziale lega più strettamente della moltiplicazione, e questa lega più strettamente dell'addizione, cioè $\alpha \cdot \beta^{\cdot\gamma}$ sta per $\alpha \cdot (\beta^{\cdot\gamma})$ e $\alpha \dot{+} \beta \cdot \gamma$ sta per $\alpha \dot{+} (\beta \cdot \gamma)$.

Proposizione 15.4. (a) *Supponiamo* $\alpha \neq 0$. *Allora* $\beta < \beta' \Rightarrow \alpha \cdot \beta < \alpha \cdot \beta'$.

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

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

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

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

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

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

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

Dimostrazione. (a) e (b) si dimostrano come le analoghe affermazioni (a) e (b) della Proposizione 15.1.

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

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

Supponiamo γ limite e che la proprietà valga per tutti i $\gamma' < \gamma$. Poiché $\beta \dot{+} \gamma = \sup_{\gamma'<\gamma} \beta \dot{+} \gamma'$ è limite per la (b) della Proposizione 15.1, per la parte (b) $\alpha \cdot (\beta \dot{+} \gamma) = \sup_{\nu<\gamma} \alpha \cdot (\beta \dot{+} \nu)$ è limite, quindi

$$\begin{aligned}
\alpha \cdot (\beta \dot{+} \gamma) &= \sup_{\nu<\gamma} (\alpha \cdot \beta \dot{+} \alpha \cdot \nu) && \text{(per ipotesi induttiva)} \\
&= \alpha \cdot \beta \dot{+} \sup_{\nu<\gamma} \alpha \cdot \nu && \text{(per la parte (b) della Proposizione 15.1)} \\
&= \alpha \cdot \beta \dot{+} \alpha \cdot \gamma.
\end{aligned}$$

(d)–(g) sono simili alle analoghe dimostrazioni della Proposizione 15.1.

(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 la parte (a)

$$\begin{aligned}
\beta &= \alpha \cdot \gamma \dot{+} \delta \\
&< \alpha \cdot \gamma \dot{+} \alpha && \text{(Proposizione 15.1(a))} \\
&= \alpha \cdot (\gamma \dot{+} 1) \\
&\leq \alpha \cdot \gamma' && \text{(per la parte(a))} \\
&\leq \alpha \cdot \gamma' \dot{+} \delta' && \text{(Proposizione 15.1(a))} \\
&= \beta,
\end{aligned}$$

contraddizione! Quindi $\gamma = \gamma'$. Se, per esempio $\delta < \delta'$ allora argomentando come sopra

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

contraddizione!

Dimostriamo l'esistenza di γ e δ. Se $\alpha > \beta$ poniamo $\gamma = 0$ e $\delta = \beta$, quindi possiamo supporre che $\alpha \leq \beta$. Per (a) esistono ordinali γ tali che $\alpha \cdot \gamma > \beta$ e sia $\bar{\gamma}$ il loro minimo: poiché $\bar{\gamma} = 0$ o $\bar{\gamma}$ limite è impossibile, ne segue che $\bar{\gamma}$ è della forma $\mathbf{S}(\gamma)$. Quindi $\alpha \cdot \gamma \leq \beta$ e $\gamma \leq \beta$ per (g) e (a). Se $\alpha \cdot \gamma = \beta$, allora poniamo $\delta = 0$. Se invece $\alpha \cdot \gamma < \beta$, per la parte (g) della Proposizione 15.1 c'è un δ tale che $\alpha \cdot \gamma \dot{+} \delta = \beta$. Poiché $\alpha \cdot \gamma \dot{+} \alpha > \beta$, ne segue che $\delta < \alpha$. □

Esercizio 15.5. Dimostrare che

$$\alpha \cdot \beta = \{\alpha \cdot \gamma \dot{+} \delta \mid \gamma < \beta \wedge \delta < \alpha\}$$

Supponiamo $\alpha, \beta \neq 0$ e diamo a $\beta \times \alpha$ l'ordinamento lessicografico $<_{\text{lex}}$. Per la Proposizione 15.4, per ogni $\xi < \alpha \cdot \beta$ esistono $\gamma < \beta$ e $\delta < \alpha$ tali che $\alpha \cdot \gamma \dot{+} \delta = \xi$ e la funzione

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

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

$$|\alpha \cdot \beta| = |\alpha \times \beta|. \tag{15.2}$$

Anche l'esponenziale $\alpha^{\cdot\beta}$ può essere definito come il tipo d'ordine di un opportuno insieme bene ordinato — si veda l'Esercizio 15.14.

Esercizio 15.6. Dimostrare che

(i) $\alpha \cdot 2 = \alpha \dot{+} \alpha$ e

(ii) se λ è limite, allora $2 \cdot \lambda = \lambda$. Quindi la moltiplicazione di ordinali non è commutativa.

Per (15.1) e (15.2) la cardinalità della *somma ordinale* e del *prodotto ordinale* di due ordinali è, rispettivamente, la somma e prodotto *cardinale* delle loro cardinalità, cioè

$$|\alpha \dot{+} \beta| = |\alpha| + |\beta| \quad \text{e} \quad |\alpha \cdot \beta| = |\alpha| \cdot |\beta|. \tag{15.3}$$

Il seguente risultato, la cui dimostrazione è lasciata per esercizio, è l'analogo delle Proposizioni 15.1 e 15.4.

Proposizione 15.7. (a) *Se* $\alpha > 1$ *allora* $\beta < \beta' \Rightarrow \alpha^{\cdot\beta} < \alpha^{\cdot\beta'}$.

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

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

Lemma 15.8. (a) $\forall m, n \in \omega \, (m + n = m \dot{+} n \in \omega)$.

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

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

Dimostrazione. Cominciamo col dimostrare per induzione su n che

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

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

Per (15.3) e il Teorema 10.19 si ha

$$m \dot{+} n = |m \dot{+} n| = |m| + |n| = m + n$$

e, analogamente,

$$m \cdot n = |m \cdot n| = |m| \cdot |n| = m \cdot n.$$

Per il Teorema 14.18, ${}^n m$ è bene ordinabile e quindi il suo cardinale m^n è ben definito (anche senza AC). Verifichiamo per induzione su n che $|{}^n m| = n^{\cdot m}$. Se $n = 0$ il risultato segue dal fatto che ${}^n m = \{\emptyset\}$, quindi supponiamo che il risultato valga per n e dimostriamolo per $\mathbf{S}(n)$. Ragionando come nella dimostrazione del Teorema 14.18, la mappa

$${}^{\mathbf{S}(n)} m \to {}^n m \times m, \quad f \mapsto (f \restriction n, f(n))$$

è una biezione e $|{}^n m \times m| = m^{\cdot n} \cdot m = m^{\cdot \mathbf{S}(n)}$, che è quanto dovevamo provare. □

Esercizi

Esercizio 15.9. Dimostrare che

(i) $\forall n, k \in \omega \left(2^{k+1} \mid n \Rightarrow 2^k \mid n\right)$

(ii) $\forall n \in \omega\, (n < 2^n)$ e quindi $\forall n \in \omega \setminus \{0\}\, (2^n \nmid n)$.

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

Esercizio 15.10. Dimostrare che l'ordinamento lessicografico su $2 \times \mathrm{Ord}$ è totale, ogni sottoclasse non vuota ha un minimo, ma non è regolare, quindi non è un buon ordine.

Esercizio 15.11. Dimostrare che se x è finito, allora $\mathscr{P}(x)$ è finito e ha cardinalità $2^{|x|}$.

Concludere che $|\mathrm{V}_n| = k_n$, dove $k_0 = 0$ e $k_{n+1} = 2^{k_n}$.

Esercizio 15.12. Dimostrare che un cardinale $\kappa \geq \omega$ è chiuso sotto somma, prodotto ed esponenziazione ordinale, cioè

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

Esercizio 15.13. Mettere in ordine i seguenti ordinali:

$$\omega^\omega \cdot (\omega \dot{+} \omega), \quad (\omega \dot{+} \omega) \cdot \omega^\omega, \quad \omega^\omega \cdot \omega \dot{+} \omega^\omega \cdot \omega, \quad \omega \cdot \omega^\omega \dot{+} \omega \cdot \omega^\omega, \quad \omega \cdot \omega^\omega \dot{+} \omega^\omega \cdot \omega, \quad \omega^\omega \cdot \omega \dot{+} \omega \cdot \omega^\omega$$

Esercizio 15.14. Il supporto di una funzione $f\colon \beta \to \alpha$ è

$$\mathrm{supt}(f) = \{\nu < \beta \mid f(\nu) \neq 0\}.$$

e sia $F(\alpha, \beta)$ l'insieme delle f a supporto finito. Se $f, g \in F(\alpha, \beta)$ definiamo

$$f \prec g \Leftrightarrow \exists \nu \in \beta\, (f(\nu) < g(\nu) \wedge \forall \xi\, (\nu < \xi < \beta \Rightarrow f(\xi) = g(\xi))).$$

Dimostrare che $\prec$ è un buon ordine su $F(\alpha, \beta)$ di tipo α^β.

Esercizio 15.15. Sia $\beta > 1$. Dimostrare che per ogni α esiste un $m \in \omega$ ed esistono ordinali $\gamma_0, \ldots, \gamma_{m-1}$ e $\delta_0, \ldots, \delta_{m-1}$ con $\alpha \geq \gamma_0 > \gamma_1 > \cdots > \gamma_{m-1}$ e $0 < \delta_i < \beta$ per ogni $i < m$, tali che

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

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

Esercizio 15.16. La somma ordinale di una successione $\langle \alpha_i \mid i < \nu \rangle$ di ordinali è definita mediante l'Esercizio 12.37 da

$$\dot{\sum_{i<\nu}} \alpha_i = \mathrm{ot}\langle \cup_{i<\nu} \alpha_i, \leq_{\mathrm{lex}} \rangle,$$

dove $\cup_{i<\nu}\alpha_i$ è definita in (11.9a) a pagina 268. Dimostrare che:

(i) se $\nu = \xi \dot{+} 1$, allora $\dot{\sum}_{i<\nu}\alpha_i = \dot{\sum}_{i<\xi}\alpha_i \dot{+} \alpha_\xi$. In particolare se $\nu = 2$, $\dot{\sum}_{i<\nu}\alpha_i = \alpha_0 \dot{+} \alpha_1$.

(ii) Se $\xi < \nu$, allora $\dot{\sum}_{i<\xi}\alpha_i \leq \dot{\sum}_{i<\nu}\alpha_i$ e la disuguaglianza è stretta se e solo se $\alpha_j \neq 0$ per qualche $\xi \leq j < \nu$.

(iii) Se ν è limite, allora $\dot{\sum}_{i<\nu}\alpha_i = \sup_{\xi<\nu} \dot{\sum}_{i<\xi}\alpha_i$.

Esercizio 15.17. Se f e g sono funzioni reali di variabile reale, poniamo

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

(Si veda l'Esercizio 10.66 a pagina 251.) Sia $\mathcal{F}$ il più piccolo insieme di funzioni contenente $\mathbb{N}[X]$ e chiuso sotto la somma e l'operazione $f \mapsto X^f$. (Quindi funzioni quali $X^{(X^{3X+2}+5X^X)} + 2X + 4$ sono in $\mathcal{F}$, ma $(X+1)^X$ no.) Dimostrare che l'ordinamento $\prec$ su $\mathcal{F}$ è un buon ordine di tipo ε_0, il primo punto fisso della funzione $\alpha \mapsto \omega^{\cdot \alpha}$.

Esercizio 15.18. Consideriamo il linguaggio L del prim'ordine contenente soltanto il simbolo $<$. Un enunciato σ **caratterizza** un ordinale $\alpha \neq 0$ se α è l'unico ordinale non nullo che soddisfa σ, cioè se $\beta \neq 0$ e $\langle \beta, < \rangle \vDash \sigma$ allora $\alpha = \beta$.

Dimostrare che:

(i) ogni $0 < \alpha < \omega^{\cdot\omega}$ è caratterizzabile mediante un L-enunciato σ,

(ii) se $0 < \alpha < \omega^{\cdot\omega}$ e $0 \neq \beta \neq \alpha$ allora $\langle \alpha, < \rangle$ e $\langle \beta, < \rangle$ non sono elementarmente equivalenti.

(Dimostreremo in **??** che questo risultato è ottimale: gli unici ordinali caratterizzabili sono quelli $< \omega^\omega$.)

Esercizio 15.19. Sia $b > 1$ un numero naturale. 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, ecc.

finché nello sviluppo compaiono solo cifre $\leq b$. Per esempio lo sviluppo di $n = 1931$ in pura base $b = 2, 3, 4$ è

$$\begin{aligned} 1931 &= 2^{2^{2+1}+2} + 2^{2^{2+1}+1} + 2^{2^{2+1}} + 2^{2^2+2+1} + 2^{2+1} + 2 + 1 \\ &= 3^{3\cdot 2} \cdot 2 + 3^{3+2} + 3^{3+1} \cdot 2 + 3^3 \cdot 2 + 3^2 + 3 + 2 \\ &= 4^{4+1} + 4^4 \cdot 3 + 4^3 \cdot 2 + 4 \cdot 2 + 3. \end{aligned}$$

Per ogni $n \in \mathbb{N}$, la sequenza di Goodstein di n

$$G_n(0), \quad G_n(1), \quad G_n(2), \quad G_n(3), \quad \ldots$$

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 $n = 1931$ sono

$$\begin{aligned} &2^{2^{2+1}+2} + 2^{2^{2+1}+1} + 2^{2^{2+1}} + 2^{2^2+2+1} + 2^{2+1} + 2 + 1 \\ &3^{3^{3+1}+3} + 3^{3^{3+1}+1} + 3^{3^{3+1}} + 3^{3^3+3+1} + 3^{3+1} + 3 \\ &4^{4^{4+1}+4} + 4^{4^{4+1}+1} + 4^{4^{4+1}} + 4^{4^4+4+1} + 4^{4+1} + 3 \\ &5^{5^{5+1}+5} + 5^{5^{5+1}+1} + 5^{5^{5+1}} + 5^{5^5+5+1} + 5^{5+1} + 2 \\ &\vdots \end{aligned}$$

Dimostrare che ogni sequenza di Goodstein termina a 0, cioè

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

16. Esponenziazione cardinale

Se si assume AC ogni insieme è bene ordinabile (Teorema 14.4); in particolare ogni insieme della forma ${}^X Y$ lo è.

Definizione 16.1 (AC)**.** Per κ, λ cardinali definiamo l'**esponenziazione cardinale**

$$\kappa^\lambda = |{}^\lambda \kappa|.$$

Quando scriveremo κ^λ assumeremo sempre che l'insieme ${}^\lambda\kappa$ sia bene ordinabile.

Dall'Esercizio 10.24 otteniamo subito che se κ, λ, μ sono cardinali,

$$\begin{aligned} \kappa^\lambda &\leq \nu^\mu && \text{se } \kappa \leq \nu \text{ e } \lambda \leq \mu \\ \left(\kappa^\lambda\right)^\mu &= \kappa^{\lambda\cdot\mu} \\ \kappa^{\lambda+\mu} &= \kappa^\lambda \cdot \kappa^\mu \\ (\kappa\cdot\lambda)^\mu &= \kappa^\mu \cdot \lambda^\mu. \end{aligned}$$

Il Teorema di Cantor 10.23 può essere riformulato come

$$\forall I \left(|I| < 2^{|I|}\right). \tag{16.1}$$

L'**Ipotesi del Continuo** CH è l'enunciato

$$2^{\aleph_0} = \aleph_1,$$

o, equivalentemente,

$$\forall X \subseteq \mathbb{R}\, (|X| \leq \aleph_0 \vee |X| = |\mathbb{R}|)\,.$$

L'**Ipotesi Generalizzata del Continuo** GCH è la generalizzazione di CH a tutti i cardinali infiniti

$$\forall \alpha \in \mathrm{Ord} \left(2^{\aleph_\alpha} = \aleph_{\alpha+1}\right),$$

o, equivalentemente,

$$\forall X \subseteq \mathscr{P}(\aleph_\alpha)\, (|X| \leq \aleph_\alpha \vee |X| = |\mathscr{P}(\aleph_\alpha)|)\,.$$

Tanto CH quanto GCH sono indipendenti da ZFC e da $\mathsf{MK} + \mathsf{AC}$.

L'Ipotesi del Continuo (CH) è riformulata così:

$$\forall \mathcal{A} \subseteq \mathscr{P}(\omega)(\mathrm{card}(\mathcal{A}) \leq \omega \ \vee\ \mathrm{card}(\mathcal{A}) = \mathrm{card}(\mathscr{P}(\omega))).$$

Poiché '$\mathrm{card}(\mathcal{A}) \leq \omega$' significa che $f\colon \mathcal{A} \rightarrowtail \omega$ per qualche f iniettiva, allora $\mathcal{A}$ è bene ordinabile, e quindi è equivalente a '$|\mathcal{A}| \leq \omega$'. L'Ipotesi Generalizzata del Continuo (GCH) diventa

$$\begin{aligned} \forall X\, \forall \mathcal{A} \subseteq \mathscr{P}(X)\, (X \text{ infinito } \Rightarrow \\ \mathrm{card}(\mathcal{A}) \leq \mathrm{card}(X) \ \vee\ \mathrm{card}(\mathcal{A}) = \mathrm{card}(\mathscr{P}(X))). \end{aligned}$$

Così formulato GCH implica l'Assioma di Scelta (Esercizio 16.8).

16..1. *Applicazioni dell'Ipotesi del continuo.*

16.A. Somme e prodotti generalizzati.

Definizione 16.2. (AC) Data una successione $\langle \kappa_i \mid i \in I \rangle$ di cardinali, la **somma generalizzata** dei κ_i è

$$\sum_{i\in I} \kappa_i = |\bigcup_{i\in I} \{i\} \times \kappa_i|,$$

il **prodotto generalizzato** dei κ_i è

$$\prod_{i\in I} \kappa_i = |\bigtimes_{i\in I} \kappa_i|.$$

Osserviamo che la definizione di somma generalizzata di cardinali non richiede l'Assioma di Scelta, se I è bene ordinabile.

Dalla definizione si ottiene subito che

- $\kappa = \sum_{i\in\kappa} 1 = \sum_{i\in\kappa} \kappa_i$, con $\kappa_i = 1$,
- $2^\kappa = \prod_{i\in\kappa} 2 = \prod_{i\in\kappa} \kappa_i$, con $\kappa_i = 2$,
- le operazioni di somma e prodotto generalizzato sono monotone, cioè se $\kappa_i \leq \lambda_i$, allora $\sum_{i\in I} \kappa_i \leq \sum_{i\in I} \lambda_i$.

Proposizione 16.3. *Se I è un insieme infinito e bene ordinabile e $1 \leq \kappa_i$, per ogni $i \in I$,*

$$\sum_{i\in I} \kappa_i = |I| \cdot \sup_{i\in I} \kappa_i.$$

Dimostrazione. Per ogni $\alpha \in \sup_{i\in I} \kappa_i$ scegliamo un $i(\alpha) \in I$ tale che $\alpha \in \kappa_{i(\alpha)}$: la funzione $\sup_{i\in I} \kappa_i \to \bigcup_{i\in I} \{i\} \times \kappa_i$, $\alpha \mapsto (i(\alpha), \alpha)$ è iniettiva e prova che $\sup_{i\in I} \kappa_i \leq \sum_{i\in I} \kappa_i$. Chiaramente

$$|I| = \sum_{i\in I} 1 \leq \sum_{i\in I} \kappa_i$$

e quindi per monotonia e per il Corollario (14.14)

$$|I| \cdot \sup_{i\in I} \kappa_i = \max(|I|, \sup_{i\in I} \kappa_i) \leq \sum_{i\in I} \kappa_i.$$

L'inclusione $\bigcup_{i\in I} \{i\} \times \kappa_i \subseteq I \times \sup_{i\in I} \kappa_i$ prova l'altra disuguaglianza. □

Teorema 16.4. *Se I e Y sono bene ordinabili e $X_i \subseteq Y$ per ogni $i \in I$, allora $\bigcup_{i\in I} X_i$ è bene ordinabile e*

$$|\bigcup_{i\in I} X_i| \leq |I| \cdot \sup_{i\in I} |X_i|.$$

Dimostrazione. Per ogni $x \in \bigcup_{i\in I} X_i$ sia $i(x)$ il minimo $j \in I$ tale che $x \in X_j$. La funzione

$$\bigcup_{i\in I} X_i \to \bigcup_{i\in I} \{i\} \times |X_i| \quad x \mapsto (i(x), f_{i(x)}(x))$$

è iniettiva e quindi $|\bigcup_{i\in I} X_i| \leq \sum_{i\in I}|X_i|$. Il risultato segue immediatamente dalla Proposizione 16.3. □

Teorema 16.5. *Sia κ un cardinale infinito ed $\mathcal{F} = \{f_\alpha \mid \alpha < \lambda\}$ una famiglia di cardinalità $\lambda \leq \kappa$ di funzioni finitarie su un insieme bene ordinabile X di cardinalità κ. Allora*

$$|\mathrm{Cl}_{\mathcal{F}}(Y)| \leq \max\{\omega, \lambda, |Y|\}$$

per ogni $Y \subseteq X$.

Dimostrazione. Posso supporre $X = \kappa$. Per la Proposizione 20.14, $\mathrm{Cl}_{\mathcal{F}}(Y) = \bigcup_n Y_n$, dove $Y_0 = Y$ e $Y_{n+1} = Y_n \cup \{f(\vec{y}) \mid \vec{y} \in Y^{<\omega}\}$. Per il Teorema 16.4 è sufficiente dimostrare che per ogni $n \in \omega$

$$|Y_n| \leq \nu,$$

dove $\nu = \max(\omega, \lambda, |Y|)$. Questo è vero se $n = 0$. Supposto vero per un certo $\bar{n}$, allora $|Y_{\bar{n}}^{<\omega}| \leq \nu$ per il Teorema 14.18, e dato che $Y_{\bar{n}+1}$ è immagine suriettiva di $\mathcal{F} \times Y_{\bar{n}}^{<\omega}$, si ha che $|Y_{\bar{n}+1}| \leq \lambda \cdot \nu = \nu$. □

Esercizio 16.6. Dimostrare che se $|I| \geq 3$ e $2 \leq \kappa_i \leq \lambda_i$ $(i \in I)$, allora la funzione $F\colon \bigcup_{i\in I}\{i\} \times \kappa_i \to \bigtimes_{i\in I}\lambda_i$ che ad (i, α) associa la funzione $F(i,\alpha) \in \bigtimes_{i\in I}\lambda_i$ definita da

$$F(i,\alpha)(j) = \begin{cases} \alpha & \text{se } i = j, \\ 0 & \text{se } i \neq j \text{ e } \alpha > 0, \\ 1 & \text{se } i \neq j \text{ e } \alpha = 0, \end{cases}$$

è iniettiva.

Dalla formula (14.3) (se $|I| = 2$) e dall'Esercizio 16.6 (se $|I| > 2$) ricaviamo che se $I \neq \emptyset$

$$2 \leq \kappa_i \leq \lambda_i \Rightarrow \sum_{i\in I} \kappa_i \leq \prod_{i\in I} \lambda_i.$$

Teorema 16.7 (J. König)**.** *Assumiamo* AC*. Se $\kappa_i < \lambda_i$ per ogni $i \in I$, allora*

$$\sum_{i\in I} \kappa_i < \prod_{i\in I} \lambda_i.$$

Dimostrazione. È sufficiente dimostrare che $\sum_{i\in I} \kappa_i \not\geq \prod_{i\in I} \lambda_i$, cioè che nessuna funzione $F\colon \bigcup_i\{i\} \times \kappa_i \to \bigtimes_{i\in I}\lambda_i$ può essere suriettiva. Fissiamo una F come sopra: per ogni $i \in I$, l'insieme

$$\{F(i,\alpha)(i) \mid \alpha \in \kappa_i\}$$

ha cardinalità $< \lambda_i$, per cui possiamo definire la funzione $f \in \bigtimes_{i\in I}\lambda_i$

$$f(i) = \min\left(\lambda_i \setminus \{F(i,\alpha)(i) \mid \alpha \in \kappa_i\}\right).$$

Verifichiamo che $f \notin \mathrm{ran}(F)$: se, per assurdo, $f = F(i_0, \alpha_0)$, allora per definizione di f,

$$f(i_0) \notin \{F(i_0, \alpha)(i_0) \mid \alpha \in \kappa_{i_0}\},$$

una contraddizione. □

In particolare, se prendiamo $\kappa_i = 1$ e $\lambda_i = 2$ ri-otteniamo la (16.1).

Esercizi

Esercizio 16.8. Dimostrare che AC discende dall'enunciato

$$\forall X\, \forall \mathcal{A} \subseteq \mathscr{P}(X)\, \Big(\mathrm{card}(\mathcal{A}) \leq \mathrm{card}(X) \vee \mathrm{card}(\mathcal{A}) = \mathrm{card}(\mathscr{P}(X))\Big).$$

17. Cardinali regolari e singolari

Definizione 17.1. Una funzione $f\colon \beta \to \alpha$ si dice **cofinale (in α)** se $\mathrm{ran}(f)$ è illimitato in α, cioè

$$\forall \alpha' < \alpha\, \exists \beta' < \beta\, (\alpha' \leq f(\beta'))$$

La **cofinalità** di un ordinale α è il più piccolo β per cui esiste una $f\colon \beta \to \alpha$ cofinale. Questo β lo si denota $\mathrm{cof}(\alpha)$.

Vediamo qualche esempio.

- Dato che $\mathrm{id} \restriction \alpha$ è cofinale, $\mathrm{cof}(\alpha) \leq \alpha$, per ogni α. In particolare $\mathrm{cof}(0) = 0$.
- La cofinalità di un ordinale successore $\gamma + 1$ è 1, come testimoniato dalla funzione $0 \mapsto \gamma$. Viceversa, se λ è limite, $\mathrm{cof}(\lambda)$ è limite.
- $\mathrm{cof}(\omega) = \omega$ e, per il Teorema 22.1, $\mathrm{cof}(\omega_1) = \omega_1$. Invece, $\mathrm{cof}(\aleph_\omega) = \omega$, dato che $n \mapsto \aleph_n$ è cofinale.

Lemma 17.2. *C'è una funzione $f\colon \mathrm{cof}(\alpha) \to \alpha$ cofinale e crescente.*

Dimostrazione. Sia α limite e $g\colon \mathrm{cof}(\alpha) \to \alpha$ cofinale. Definiamo per $\beta < \mathrm{cof}(\alpha)$

$$\begin{aligned} f(0) &= g(0) \\ f(\beta) &= \min\left(\alpha \setminus \sup\{\max(g(\gamma), f(\gamma)) \mid \gamma < \beta\}\right). \end{aligned}$$

Verifichiamo che la f è definita su $\mathrm{cof}(\alpha)$ e cioè che

$$\alpha \setminus \sup\{\max(g(\gamma), f(\gamma)) \mid \gamma < \beta\} \neq \emptyset,$$

per ogni $\beta < \mathrm{cof}(\alpha)$. Sia $\bar\beta \leq \mathrm{cof}(\alpha)$ minimo tale che

$$\alpha = \bigcup\{\max(g(\gamma), f(\gamma)) \mid \gamma < \bar\beta\}.$$

La funzione $f\colon \bar{\beta} \to \alpha$ è strettamente crescente e maggiora $g \restriction \bar{\beta}$, dato che

$$\gamma_1 < \gamma_2 < \bar{\beta} \Rightarrow f(\gamma_2) > \sup\{\max(g(\gamma), f(\gamma)) \mid \gamma < \gamma_2\} \geq f(\gamma_1), g(\gamma_1).$$

Quindi

$$\alpha = \sup\{f(\gamma) \mid \gamma < \bar{\beta}\}$$

e $f\colon \bar{\beta} \to \alpha$ è cofinale e quindi $\bar{\beta} = \mathrm{cof}(\alpha)$. Abbiamo quindi dimostrato che $f\colon \mathrm{cof}(\alpha) \to \alpha$ è cofinale e crescente. □

Lemma 17.3. *Se $f\colon \beta \to \alpha$ e $g\colon \gamma \to \beta$ sono cofinali e crescenti, allora $f \circ g\colon \gamma \to \alpha$ è cofinale e crescente.*

Dimostrazione. La funzione $f \circ g\colon \gamma \to \alpha$ è chiaramente crescente. Se $\alpha' < \alpha$ sia $\beta' < \beta$ tale che $f(\beta') \geq \alpha'$ e sia $\gamma' < \gamma$ tale che $g(\gamma') \geq \beta'$. Allora $f(g(\gamma')) \geq \alpha'$. □

Corollario 17.4. $\mathrm{cof}(\mathrm{cof}(\alpha)) = \mathrm{cof}(\alpha)$.

Definizione 17.5. Un ordinale limite λ si dice **regolare** se $\mathrm{cof}(\lambda) = \lambda$. Altrimenti si dice **singolare**.

Se λ è un cardinale infinito, parleremo di **cardinale regolare** o **singolare**.

Se $f\colon |\lambda| \to \lambda$ è una biezione, allora f è cofinale e quindi un ordinale regolare è sempre un cardinale regolare. Viceversa, gli ordinali limite che non sono cardinali sono ordinali singolari.

Teorema 17.6 (AC)**.** *Ogni cardinale successore infinito κ^+ è regolare.*

Dimostrazione. Sia κ un cardinale $\geq \omega$ e supponiamo, per assurdo, che $\mathrm{cof}(\kappa^+) < \kappa^+$. Sia $f\colon \mathrm{cof}(\kappa^+) \to \kappa^+$ cofinale. Allora

$$\kappa^+ = \bigcup_{i<\mathrm{cof}(\kappa^+)} f(i)$$

e quindi per il Teorema 16.4

$$\kappa^+ = |\kappa^+| \leq \sum_{i<\mathrm{cof}(\kappa^+)} |f(i)| \leq \mathrm{cof}(\kappa) \cdot \sup_{i<\mathrm{cof}(\kappa)} |f(i)| \leq \kappa,$$

assurdo. □

Teorema 17.7 (AC)**.** *Se κ è un cardinale singolare allora esiste una successione crescente $\langle \kappa_i \mid i < \mathrm{cof}(\kappa)\rangle$ di cardinali regolari tale che*

$$\kappa = \sup_{i<\mathrm{cof}(\kappa)} \kappa_i = \sum_{i<\mathrm{cof}(\kappa)} \kappa_i.$$

Dimostrazione. Sia $f\colon \operatorname{cof}(\kappa) \to \kappa$ cofinale e crescente. La funzione

$$g(\alpha) = \min\{\lambda \in \kappa \mid \lambda \text{ è regolare, } \lambda \geq f(\alpha) \text{ e } \forall \beta < \alpha\, (g(\beta) < \lambda)\}$$

è definita per ogni $\alpha < \operatorname{cof}(\kappa)$ dato che i cardinali regolari sono illimitati al di sotto di κ e quindi se $\bar{\alpha} < \operatorname{cof}(\kappa)$ fosse il più piccolo ordinale tale che $g(\bar{\alpha})$ non è definita, allora vorrebbe dire che $\kappa = \sup_{\beta<\bar{\alpha}} g(\beta)$, cioè $g\colon \bar{\alpha} \to \kappa$ sarebbe cofinale, contro il fatto che $\bar{\alpha} < \operatorname{cof}(\kappa)$. Posto $\kappa_i = g(i)$, si ha che

$$\kappa = \sup_{i<\operatorname{cof}(\kappa)} \kappa_i \leq \sum_{i<\operatorname{cof}(\kappa)} \kappa_i \leq \kappa \cdot \operatorname{cof}(\kappa) = \kappa$$

come richiesto. □

Teorema 17.8 (AC)**.** *Se κ è un cardinale infinito*

$$\kappa^{\operatorname{cof}(\kappa)} > \kappa.$$

Dimostrazione. Se κ è regolare l'enunciato diventa $\kappa^\kappa = 2^\kappa > \kappa$, che è vero per (16.1). Suppongo quindi che $\operatorname{cof}(\kappa) < \kappa$. Per il Teorema 17.7 possiamo trovare cardinali κ_i tali che $\kappa = \sup_{i<\operatorname{cof}(\kappa)} \kappa_i$ e quindi per il Teorema di König 16.7

$$\kappa = \sum_{i<\operatorname{cof}(\kappa)} \kappa_i < \prod_{i<\operatorname{cof}(\kappa)} \kappa = \kappa^{\operatorname{cof}(\kappa)}.$$

□

Corollario 17.9 (AC)**.** $\operatorname{cof}(2^\kappa) > \kappa$.

Dimostrazione. Se $\lambda = \operatorname{cof}(2^\kappa) \leq \kappa$, allora $2^\kappa < (2^\kappa)^\lambda = 2^{\kappa\cdot\lambda} = 2^\kappa$, contraddizione. □

In particolare, $\operatorname{cof}(2^{\aleph_0}) > \aleph_0$ e quindi $2^{\aleph_0}$ non può essere $\aleph_\omega$, $\aleph_{\omega+\omega}$ (o, più in generale, $\aleph_\lambda$ con $\lambda < \omega_1$ ordinale limite) né può essere il primo punto fisso della funzione $\aleph$ (vedi pag. 297). Il seguente risultato è noto come **formula di Hausdorff**.

Teorema 17.10 (Hausdorff)**.** *Assumiamo* AC*.*

$$\aleph_{\alpha+1}^{\aleph_\beta} = \max\left(\aleph_{\alpha+1}, \aleph_\alpha^{\aleph_\beta}\right).$$

Dimostrazione. Se $\aleph_{\alpha+1} \leq \aleph_\beta$ allora per la Proposizione 14.15

$$2^{\aleph_\beta} = \aleph_\alpha^{\aleph_\beta} = \aleph_{\alpha+1}^{\aleph_\beta} > \aleph_\beta \geq \aleph_{\alpha+1}$$

e quindi il teorema è dimostrato.

Supponiamo invece che $\aleph_\beta < \aleph_{\alpha+1}$. Se $f\colon \aleph_\beta \to \aleph_{\alpha+1}$, allora per la regolarità di $\aleph_{\alpha+1}$ (Teorema 17.6) c'è un $\gamma < \aleph_{\alpha+1}$ tale che $\operatorname{ran} f \subseteq \gamma$. Quindi ${}^{\aleph_\beta}\aleph_{\alpha+1} = \bigcup_{\gamma<\aleph_{\alpha+1}} {}^{\aleph_\beta}\gamma$ e per il Teorema 16.4

$$\aleph_{\alpha+1}^{\aleph_\beta} = \left|\bigcup_{\gamma<\aleph_{\alpha+1}} {}^{\aleph_\beta}\gamma\right| \leq \aleph_{\alpha+1} \cdot \aleph_\alpha^{\aleph_\beta}.$$

L'altra disuguaglianza è immediata. □

17.A. Insiemi stazionari e club. Estendendo la notazione introdotta a pagina 281, converemo che

Ω denota un cardinale regolare oppure la classe Ord.

Per l'Assioma di Rimpiazzamento, nessuna funzione $f\colon \alpha \to \mathrm{Ord}$ è cofinale in Ord, quindi con licenza di linguaggio diremo che $\Omega \leq \mathrm{Ord}$ è regolare.

Una classe $C \subseteq \Omega$ è **chiusa in** Ω se e solo se per ogni limite $\lambda \in \Omega$

$$\bigcup(C \cap \lambda) = \lambda \Rightarrow \lambda \in C.$$

Il prossimo Esercizio giustifica la scelta dell'aggettivo "chiuso".

Esercizio 17.11. Verificare che C è chiusa in Ω se e solo se $\Omega \setminus C$ è aperta in Ω, secondo la Definizione 24.2.

Esempi di classi chiuse e illimitate in Ord sono la classe degli ordinali limite e la classe dei cardinali singolari.

Teorema 17.12. *Supponiamo che* $\Omega \leq \mathrm{Ord}$ *e che* $\omega < \mathrm{cof}(\Omega)$*. Se* $C, D \subseteq \Omega$ *sono insiemi chiusi e illimitati in* Ω*, allora* $C \cap D$ *è chiuso e illimitato in* Ω*.*

Dimostrazione. Chiaramente $C \cap D$ è chiuso, quindi basta dimostrare che è illimitato in Ω. Fissato un $\alpha < \Omega$ dobbiamo trovare un $\beta \in C \cap D$ con $\alpha < \beta$. Sfruttando il fatto che C e D sono illimitati, costruiamo induttivamente una sequenza crescente di ordinali $\alpha < \gamma_0 < \delta_0 < \gamma_1 < \delta_1 < \dots$ tali che $\gamma_i \in C$ e $\delta_i \in D$. Poiché C e D sono chiusi,

$$\beta = \sup_i \gamma_i = \sup_i \delta_i \in C \cap D$$

come richiesto. □

L'ipotesi che $\mathrm{cof}(\Omega) > \omega$ non può essere eliminata — gli insiemi $\{2n \mid n \in \omega\}$ e $\{2n+1 \mid n \in \omega\}$ sono chiusi e illimitati in ω ma la loro intersezione $\emptyset$ non è illimitata in ω.

Teorema 17.13. *Supponiamo che* $\Omega \leq \mathrm{Ord}$ *e che* $\omega < \mathrm{cof}(\Omega)$*. Se* $\gamma < \mathrm{cof}(\Omega)$ *e* $\langle C_\alpha \mid \alpha < \gamma \rangle$ *è una sequenza di insiemi chiusi e illimitati in* Ω*, allora* $\bigcap_{\alpha<\gamma} C_\alpha$ *è chiuso e illimitato in* Ω*.*

Dimostrazione. Chiaramente $\bigcap_{\alpha<\gamma} C_\alpha$ è un chiuso di Ω, quindi rimane da dimostrare che è un insieme illimitato. Procediamo per induzione su γ. Se $\gamma = 0$ o $\gamma = 1$ non c'è nulla da dimostrare. Il caso di γ ordinale successore segue dal Teorema 17.12, quindi possiamo supporre che γ sia limite. Sostituendo C_α con $\bigcap_{\beta<\alpha} C_\beta$, possiamo supporre che

$$\alpha < \beta < \gamma \Rightarrow C_\beta \subseteq C_\alpha.$$

Fissato un $\nu < \Omega$ costruiamo una successione crescente $\langle \xi_\alpha \mid \alpha < \gamma \rangle$ con $\nu < \xi_0$ e $\xi_\alpha \in C_\alpha$. Allora $\xi = \sup_{\alpha<\gamma} \xi_\alpha \in \Omega$ dato che $\operatorname{cof}(\Omega) > \gamma$, e poiché i C_α sono chiusi e $\{\xi_\beta \mid \beta \geq \alpha\} \subseteq C_\alpha$, allora $\xi \in C_\alpha$ per ogni $\alpha < \gamma$. □

Definizione 17.14. L'**intersezione diagonale** di una sequenza $\langle X_\alpha \mid \alpha < \kappa \rangle$ di sottoinsiemi di Ω è

$$\begin{aligned} \triangle_{\alpha<\kappa} X_\alpha &= \{\beta < \Omega \mid \forall \alpha < \beta \, (\beta \in X_\alpha)\} \\ &= \bigcap_{\alpha<\kappa} (X_\alpha \cup \alpha \dot{+} 1) \end{aligned}$$

Proposizione 17.15. *Se $\Omega > \omega$ è regolare e $C_\alpha \subseteq \Omega$ è chiuso e illimitato per ogni $\alpha < \Omega$, allora $\triangle_{\alpha<\kappa} C_\alpha$ è chiuso e illimitato.*

Dimostrazione. La chiusura è immediata, quindi è sufficiente verificare che $\triangle_{\alpha<\kappa} C_\alpha$ è illimitato. Fissiamo un $\beta_0 < \Omega$. Poiché $\bigcap_{\nu\leq\gamma} C_\nu$ è illimitato in Ω per ogni $\gamma < \Omega$ (Teorema 17.13), si definisce una successione crescente di ordinali

$$\beta_0 < \beta_1 < \beta_2 < \cdots < \beta = \sup_n \beta_n$$

tali che $\beta_{n+1} \in \bigcap_{\nu\leq\beta_n} C_\nu$. Dato che

$$n < m \Rightarrow \beta_m \in C_{\beta n},$$

la chiusura di C_{β_n} implica che $\beta = \sup_{m>n} \beta_m \in C_{\beta_n}$, e quindi $\beta \in \bigcap_n C_{\beta_n} = \bigcap_{\nu<\beta} C_\nu$, cioè $\beta_0 < \beta \in \triangle_{\alpha<\kappa} C_\alpha$ come richiesto. □

Definizione 17.16. $A \subseteq \Omega$ è **stazionario** se $A \cap C \neq \emptyset$ per ogni C chiuso e illimitato in Ω.

Esercizio 17.17. Dimostrare che se $\kappa < \Omega$ è regolare, allora $\textsc{Cof}(\kappa) = \{\alpha < \Omega \mid \operatorname{cof}(\alpha) = \kappa\}$ è stazionario in Ω.

Per il Teorema 17.13, ogni insieme che contenga un chiuso illimitato è stazionario, ma il converso non vale — se $\kappa < \lambda < \Omega$ sono regolari, allora $\textsc{Cof}(\kappa)$ e $\textsc{Cof}(\lambda)$ sono insiemi stazionari disgiunti e quindi non possono contenere un chiuso illimitato.

Teorema 17.18 (Fodor)**.** *Sia $S \subseteq \Omega$ stazionario e sia $F \colon S \to \operatorname{Ord}$ tale che*

$$\forall \alpha \in S \; (\alpha \neq 0 \Rightarrow F(\alpha) < \alpha) \, .$$

Allora F è costante su un insieme stazionario.

Dimostrazione. Supponiamo, per assurdo, che $F^{-1}\{\alpha\}$ non sia stazionario per ogni $\alpha < \Omega$, cioè che

$$\forall \alpha \in \Omega \, \exists C_\alpha \subseteq \Omega \, \Big(C_\alpha \text{ chiuso e illimitato in } \Omega \text{ e } C_\alpha \cap F^{-1}\{\alpha\} = \emptyset \Big) \, .$$

Per la Proposizione 17.15, $\triangle_{\alpha<\Omega} C_\alpha$ è chiuso e illimitato, e poiché anche $(0;\Omega)$ è chiuso e illimitato, per il Teorema 17.13 anche $C = (\triangle_{\alpha<\Omega} C_\alpha) \setminus \{0\}$

lo è. Sia $\alpha \in S \cap C$: allora $F(\alpha) < \alpha$ per definizione di F e $\alpha \in C_{F(\alpha)}$ per definizione di intersezione diagonale, e quindi $\alpha \notin F^{-1}\{\alpha\}$ per definizione dei C_β: contraddizione. □

Un ordinale α è chiuso sotto $f\colon {}^n\Omega \to \Omega$ se $\alpha \in \Omega$ e

$$\forall \beta_1, \dots, \beta_n \in \alpha\, (f(\beta_1, \dots, \beta_n) \in \alpha).$$

La classe degli ordinali chiusi sotto f è denotata con C_f. Questa nozione è strettamente collegata alla nozione introdotta nella Sezione 11.K. In questo caso ammettiamo che il domino di f sia la classe propria Ord, ma richiediamo che gli insiemi chiusi siano a loro volta ordinali.

Teorema 17.19. *Supponiamo Ω sia un cardinale di cofinalità più che numerabile oppure $\Omega = \mathrm{Ord}$.*

(a) *C_f è chiuso e illimitato, per ogni $f\colon {}^n\Omega \to \Omega$.*

(b) *Se $C \subseteq \Omega$ è chiuso e illimitato, allora $C \supseteq C_f$ per qualche $f\colon \Omega \to \Omega$.*

Dimostrazione. (a) Dato $\alpha < \Omega$ dobbiamo trovare un $\gamma \geq \alpha$ chiuso per f. Definiamo

$$\gamma_{i+1} = \sup\{f(\beta_1, \dots, \beta_n) \mid \beta_1, \dots, \beta_n \in \gamma_i\}$$

con $\gamma_0 = \alpha$. Per l'ipotesi su Ω, si ha $|\{f(\beta_1, \dots, \beta_n) \mid \beta_1, \dots, \beta_n \in \gamma_i\}| \leq |\gamma_i|^n < \Omega$, quindi $\gamma = \sup_i \gamma_i < \Omega$ è l'ordinale cercato.

La chiusura di C_f in Ω è immediata.

(b) Sia $C \subseteq \Omega$ un chiuso illimitato sia g la sua funzione enumerante, e sia $f(\alpha) = g(\alpha + 1)$: poiché $\alpha \leq g(\alpha) < f(\alpha)$, se γ è chiuso sotto f, allora γ è limite e $C \cap \gamma$ è illimitato in γ. Quindi $C_f \subseteq C$. □

Corollario 17.20. *Se $\mathcal{F}$ è una famiglia di funzioni finitarie su κ e $|\mathcal{F}| < \mathrm{cof}(\kappa)$, allora*

$$\bigcap_{f \in \mathcal{F}} C_f$$

è chiuso e illimitato in κ.

17.B. Ulteriori risultati di aritmetica cardinale. Come abbiamo visto, la funzione esponenziale

$$\kappa \mapsto 2^\kappa$$

dove κ è un cardinale infinito, deve soddisfare

$$\kappa \leq \lambda \Rightarrow 2^\kappa \leq 2^\lambda, \tag{17.1a}$$

$$\mathrm{cof}(2^\kappa) > \kappa. \tag{17.1b}$$

Un teorema di Easton asserisce che (17.1a) e (17.1b) sono le uniche restrizioni per quanto riguarda i cardinali *regolari*. Per esempio, è possibile che $2^\kappa = \kappa^{++}$ per ogni κ regolare. Oppure è possibile che l'ipotesi generalizzata del continuo

fallisca per la prima volta ad un qualsiasi cardinale regolare, vale a dire: è possibile che $2^\kappa > \kappa^+$ e che $\forall \lambda < \kappa \left(2^\lambda = \lambda^+\right)$, con κ cardinale regolare arbitrario. La situazione per i cardinali *singolari* è drasticamente differente. Silver dimostrò nel 1974 che l'ipotesi generalizzata del continuo non può fallire per la prima volta a un cardinale singolare di *cofinalità più che numerabile*. Più precisamente:

Teorema 17.21. *Se* $\operatorname{cof}(\lambda) > \omega$ *e* $\left\{\alpha < \lambda \mid 2^{\aleph_\alpha} = \aleph_{\alpha+1}\right\}$ *è stazionario in* λ, *allora* $2^{\aleph_\lambda} = \aleph_{\lambda+1}$.

Se $\operatorname{cof}(\lambda) > \omega$ *e* $\left\{\alpha < \lambda \mid 2^{\aleph_\alpha} \leq \aleph_{\alpha+\nu}\right\}$ *è stazionario in* λ, *allora* $2^{\aleph_\lambda} \leq \aleph_{\lambda+\nu}$.

Il caso dei cardinali singolari di cofinalità numerabile è ancora diverso: Magidor dimostrò nel 1978 che l'ipotesi generalizzata del continuo può fallire per la prima volta ad $\aleph_\omega$, cioè che $\forall n < \omega \left(2^{\aleph_n} = \aleph_{n+1}\right)$ e $2^{\aleph_\omega} > \aleph_{\omega+1}$. Tuttavia il valore di $2^{\aleph_\omega}$ non può essere arbitrariamente grande. Infatti nel 1989 Shelah dimostrò che se $\forall n \left(2^{\aleph_n} < \aleph_\omega\right)$, allora

$$2^{\aleph_\omega} < \aleph_{\min(\omega_4, (2^{\aleph_0})^+)}.$$

Esercizi

Esercizio 17.22. Supponiamo che $f_i \colon \kappa_i \to \alpha$ sia cofinale e crescente e che κ_i sia regolare $(i = 0, 1)$. Allora $\kappa_0 = \kappa_1 = \operatorname{cof}(\alpha)$.

Esercizio 17.23. Sia $\mathcal{T}$ una topologia secondo numerabile su un insieme X. Dimostrare che $\textsc{Bor}(X, \mathcal{T}) = \bigcup_{\alpha < \omega_1} \mathcal{S}_\alpha$ e che $|\mathcal{S}_\alpha| \leq 2^{\aleph_0}$. Concludere che $|\textsc{Bor}(X, \mathcal{T})|$, la cardinalità della famiglia dei Boreliani di X, è $\leq 2^{\aleph_0}$. In particolare $|\textsc{Bor}(\mathbb{R})| = 2^{\aleph_0}$.

Note e osservazioni

I risultati di consistenza relativa dell'ipotesi (generalizzata) del continuo e della sua negazione sono stati ottenuti da Gödel nel 1937 e Cohen nel 1963. Per un'esposizione moderna si vedano i libri di Kunen [**Kun83**] e di Jech [**Jec03**]. In particolare, nel secondo libro si trovano tutte le dimostrazioni dei risultati menzionati nella Sezione 17.B.

18. Categorie

Il linguaggio delle categorie è molto utile in varie parti della matematica. In questa sezione introdurremo le nozioni di base che verranno usate nel seguito.

Una categoria è una sequenza di sei oggetti

$$\mathfrak{C} = \left\langle \mathbf{Obj}^{\mathfrak{C}}, \mathbf{Arw}^{\mathfrak{C}}, \mathbf{dom}^{\mathfrak{C}}, \mathbf{cod}^{\mathfrak{C}}, \circ^{\mathfrak{C}}, \mathbf{1} \right\rangle$$

dove

- $\mathbf{Obj}^{\mathfrak{C}}$ e $\mathbf{Arw}^{\mathfrak{C}}$ sono classi non vuote, i cui elementi si dicono, rispettivamente, **oggetti** e **frecce** (o **morfismi**)di $\mathfrak{C}$,
- $\mathbf{dom}^{\mathfrak{C}}$ e $\mathbf{cod}^{\mathfrak{C}}$ sono funzioni (o meglio: relazioni funzionali) da $\mathbf{Arw}^{\mathfrak{C}}$ in $\mathbf{Obj}^{\mathfrak{C}}$,
- $\mathbf{1}^{\mathfrak{C}}$ è una funzione (o meglio: relazione funzionale) da $\mathbf{Obj}^{\mathfrak{C}}$ in $\mathbf{Arw}^{\mathfrak{C}}$
- $\circ^{\mathfrak{C}}$ è un'operazione binaria parziale sulle frecce: $g \circ^{\mathfrak{C}} f$ è definita se e solo se $\mathbf{cod}^{\mathfrak{C}} f = \mathbf{dom}^{\mathfrak{C}} g$, in altre parole, il dominio di $\circ^{\mathfrak{C}}$ è

$$\{(g, f) \in \mathbf{Arw}^{\mathfrak{C}} \times \mathbf{Arw}^{\mathfrak{C}} \mid \mathbf{cod}^{\mathfrak{C}} f = \mathbf{dom}^{\mathfrak{C}} g\}$$

  Il simbolo $\circ^{\mathfrak{C}}$ si dice **operazione di composizione**.

(Quando non c'è pericolo di confusione lasceremo cadere il suffisso $\mathfrak{C}$ e scriveremo **Obj**, **Arw**, **dom**, etc.) Le seguenti proprietà devono essere soddisfatte:

(i) se f e g sono frecce e $g \circ f$ è definita, allora $\mathbf{dom}\, g \circ f = \mathbf{dom}\, f$ e $\mathbf{cod}\, g \circ f = \mathbf{cod}\, g$.

(ii) se $\mathbf{cod}\, f = \mathbf{dom}\, g$ e $\mathbf{cod}\, g = \mathbf{dom}\, h$, allora

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

(Questa è la proprietà associativa della composizione nelle categorie.)

(iii) Per ogni oggetto $a \in \mathbf{Obj}$, la freccia $\mathbf{1}_a$ ha per dominio e codominio a stesso,

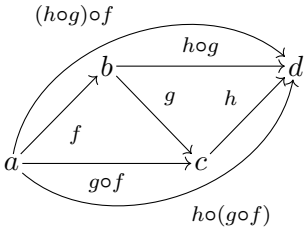
$$\mathbf{dom}\, \mathbf{1}_a = a = \mathbf{cod}\, \mathbf{1}_a;$$

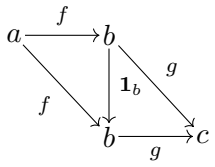
(iv) per ogni $a, b, c \in \mathbf{Obj}$ e ogni f e g tali che $\mathbf{dom}\, f = a$, $\mathbf{cod}\, f = b = \mathbf{dom}\, g$ e $\mathbf{cod}\, g = c$, si ha che

$$f = \mathbf{1}_b \circ f \qquad \text{e} \qquad g = g \circ \mathbf{1}_b.$$

Una freccia da a in b è una $f \in \mathbf{Arw}^{\mathfrak{C}}$ tale che $\mathbf{dom}\, f = a$ e $\mathbf{cod}\, f = b$ e per brevità questo sarà scritto come $f \colon a \to b$ oppure $a \xrightarrow{f} b$ o ancora $a \underset{f}{\to} b$. Le

proprietà (ii) e (iv) possono essere formulate dicendo che i diagrammi





commutano.

Definiamo

$$\hom(a, b) = \{f \in \mathbf{Arw} \mid \mathbf{dom}(f) = a \wedge \mathbf{cod}(f) = b\}.$$

Vediamo ora qualche esempio.

18.A. Esempi di categorie.

18.A.1. *La categoria degli insiemi.* La categoria degli insiemi SETS ha come oggetti gli insiemi e come frecce ha le triple (a, f, b) dove f è una funzione con $\operatorname{dom} f = a$ e $\operatorname{ran} f \subseteq b$. Se poniamo $\mathbf{dom}(a, f, b) = a$, $\mathbf{cod}(a, f, b) = b$, $\circ$ l'usuale composizione di funzioni e $\mathbf{1}_a$ la funzione identità su a, si verifica facilmente che si ottiene una categoria.

La categoria degli ordini parziali PORD ha per oggetti gli insiemi parzialmente ordinati $\langle A, \leq\rangle$ e per per frecce le funzioni crescenti tra ordini parziali. Anche in questo caso una freccia è una tripla (A, f, B) con $f\colon A \to B$.

Analogamente possiamo considerare TOP, la categoria degli spazi topologici, dove i morfismi tra due spazi topologici sono funzioni continue. Oppure le categorie GRPS, RNGS, $\text{VECT}_{\mathbb{k}}$, rispettivamente dei gruppi, degli anelli unitari, degli spazi vettoriali sul campo $\mathbb{k}$, dove la nozione di morfismo è data da una funzione che preserva determinate strutture algebriche.

Negli esempi precedenti la classe degli oggetti era sempre una classe propria e i morfismi erano sempre delle funzioni. Nei prossimi esempi vedremo delle situazioni radicalmente differenti.

18.A.2. *La categoria più semplice.* Consideriamo la categoria più semplice in assoluto, con un unico oggetto $\bullet$ e con un unico morfismo

Questa categoria rappresenta il pre-ordine (non vuoto) più semplice, quello con un solo elemento. In effetti ogni pre-ordine $\langle P, \leq\rangle$ può essere descritto come una categoria ponendo $\mathbf{Obj} = P$ e stabilendo che c'è una (ed una sola) freccia tra p e q se e solo se $p \leq q$.

18.A.3. *Monoidi.* Ogni monoide M può essere considerato come una categoria con un unico oggetto, i cui morfismi sono gli elementi di M, la composizione è l'operazione del monoide ed il morfismo privilegiato è l'identità di M.

Se f è una freccia da a in b diremo che

- f è **mono** ovvero che è un **monomorfismo**, in simboli $f\colon a \rightarrowtail b$, se per ogni oggetto c e ogni coppia di frecce $g\colon c \to a$ e $h\colon c \to a$
$$f \circ g = f \circ h \quad \Rightarrow \quad g = h.$$
- f è **epi** ovvero che è un **epimorfismo**, in simboli $f\colon a \twoheadrightarrow b$, se per ogni oggetto c e ogni coppia di frecce $g\colon b \to c$ e $h\colon b \to c$
$$g \circ f = h \circ f \quad \Rightarrow \quad g = h.$$
- f è **iso** ovvero che è un **isomorfismo**, in simboli $f\colon a \xrightarrow{\sim} b$, se esiste una $g\colon b \to a$ tale che $g \circ f = \mathbf{1}_a$ e $f \circ g = \mathbf{1}_b$.

Osserviamo che la freccia g nella definizione di iso è unica, si dice inversa di f e la si denota con f^{-1}: infatti se g_1 e g_2 sono inverse di f, allora
$$\begin{aligned} g_1 &= \mathbf{1}_a \circ g_1 \\ &= (g_2 \circ f) \circ g_1 \\ &= g_2 \circ (f \circ g_1) \\ &= g_2 \circ \mathbf{1}_b \\ &= g_2. \end{aligned}$$

Esercizio 18.1. Dimostrare che se una freccia iso è anche mono ed epi e che se $f\colon a \to b$ è iso, anche $f^{-1}\colon b \to a$ è iso.

Due oggetti a e b si dicono **isomorfi** se c'è un isomorfismo tra di loro, in simboli $a \cong b$.

Definizione 18.2. Un oggetto a di una categoria $\mathfrak{C}$ si dice

- **iniettivo** se per ogni freccia $f\colon b \to a$ e ogni freccia mono $h\colon b \to c$ c'è un morfismo $g\colon c \to a$ tale che $g \circ h = f$;
- **proiettivo** se per ogni freccia $f\colon a \to b$ e ogni freccia epi $h\colon c \to b$ c'è un morfismo $g\colon a \to c$ tale che $g \circ h = f$.

18.B. Funtori.

Definizione 18.3. Un **funtore covariante F** dalla categoria $\mathfrak{C}$ alla categoria $\mathfrak{D}$
$$\mathbf{F}\colon \mathfrak{C} \to \mathfrak{D}$$
consiste di una mappa $\mathbf{F}\colon \mathbf{Obj}^{\mathfrak{C}} \to \mathbf{Obj}^{\mathfrak{D}}$ ed un'assegnazione (sempre denotata con $\mathbf{F}$) $\mathbf{Arw}^{\mathfrak{C}} \to \mathbf{Arw}^{\mathfrak{D}}$, tale che

(1) $\mathbf{F}(\mathbf{1}^{\mathfrak{C}}_a) = \mathbf{1}^{\mathfrak{D}}_{\mathbf{F}(a)}$,

(2) se $f\colon a \to b$ allora $\mathbf{F}(f)\colon \mathbf{F}(a) \to \mathbf{F}(b)$ e

(3) $\mathbf{F}(g \circ^{\mathfrak{C}} f) = \mathbf{F}(g) \circ^{\mathfrak{D}} \mathbf{F}(f)$.

Un **funtore controvariante F** dalla categoria $\mathfrak{C}$ alla categoria $\mathfrak{D}$ è una $\mathbf{F}$ come sopra che soddisfa (1) e

(2′) se $f\colon a \to b$ allora $\mathbf{F}(f)\colon \mathbf{F}(b) \to \mathbf{F}(a)$ e

(3′) $\mathbf{F}(g \circ^{\mathfrak{C}} f) = \mathbf{F}(f) \circ^{\mathfrak{D}} \mathbf{F}(g)$.

Un funtore trasforma i diagrammi commutativi di $\mathfrak{C}$ in diagrammi commutativi di $\mathfrak{D}$.

Vediamo qualche esempio di funtore.

18.B.1. *Funtore dimenticante.* Consideriamo la mappa che associa ad ogni gruppo il suo insieme sostegno: poiché un omomorfismo tra gruppi è in particolare una funzione sugli insiemi sostegno è facile verificare che questo definisce un funtore covariante $\textsc{Grp} \to \textsc{Set}$ dalla categoria dei gruppi a quella degli insiemi. Un funtore di questo tipo si dice **dimenticante** in quanto dimentica in parte o del tutto la struttura dell'oggetto di partenza. Altri esempi di funtori dimenticanti sono tra la categoria degli anelli nella categoria dei gruppi abeliani, tra la categoria degli spazi topologici e quella degli insiemi, etc.

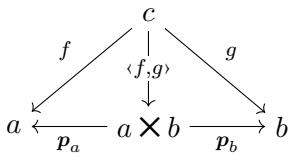
18.B.2. *Insieme potenza.* La costruzione dell'insieme potenza definisce un funtore covariante da $\textsc{Set}$ in sé stessa: ad ogni insieme a associamo $\mathscr{P}(a)$ e ad ogni funzione $f\colon a \to b$ associamo la funzione $\mathscr{P}(a) \to \mathscr{P}(b)$ data da $x \mapsto f[x]$.

18.B.3. *Dualità negli spazi vettoriali.* Ad ogni spazio vettoriale W su un campo $\Bbbk$ associamo il suo duale W^* e ad ogni applicazione lineare $f\colon W \to Z$ associamo l'applicazione duale $f^*\colon Z^* \to W^*$ definita da $f^*(\alpha) = \alpha \circ f$. È immediato verificare che questo definisce un funtore controvariante dalla categoria $\mathfrak{Vect}_{\Bbbk}$ in sé stessa.

18.B.4. *La categoria opposta.* Data una categoria $\mathfrak{C}$, la **categoria opposta** $\mathfrak{C}^{\mathrm{op}}$ ha gli oggetti e le frecce di $\mathfrak{C}$ ma operazioni di **dom** e **cod** scambiate fra di loro e l'operazione di composizione viene eseguita nel verso opposto. Più precisamente: $\mathbf{Obj}^{\mathrm{op}} = \mathbf{Obj}$, $\mathbf{Arw}^{\mathrm{op}} = \mathbf{Arw}$, $\mathbf{dom}(f) = a$ e $\mathbf{cod}(f) = b$ se e solo se $\mathbf{dom}^{\mathrm{op}}(f) = b$ e $\mathbf{cod}(f) = a$ e $f \circ g = h$ se solo se $g \circ^{\mathrm{op}} f = h$. Il funtore identico è controvariante tra $\mathfrak{C}$ e $\mathfrak{C}^{\mathrm{op}}$.

18.C. Prodotti. Se a, b sono oggetti di una categoria $\mathfrak{C}$, un **prodotto** di a e b è un oggetto denotato con $a \times b$ e due frecce $\boldsymbol{p}_a\colon a \times b \to a$ e $\boldsymbol{p}_b\colon a \times b \to b$ tali che per ogni coppia di frecce $f\colon c \to a$ e $g\colon c \to b$ c'è un'unica freccia

$\langle f, g\rangle : c \to a \times b$ che rende il diagramma



commutativo. L'esistenza e unicità della funzione $\langle f, g\rangle$ si dice **proprietà di universalità del prodotto**. Se ogni coppia di oggetti ammette un prodotto diremo che la categoria ha prodotti.

Osservazioni 18.4. (a) Abbiamo scritto *un* prodotto e non *il* prodotto in quanto $a \times b$ è definito a meno di isomorfismi (Esercizio 18.14).

(b) La notazione $a \times b$ non deve trarre in inganno: in molte categorie l'oggetto prodotto è ottenuto mediante un prodotto cartesiano dei due oggetti, ma ciò non è vero in generale (Esercizio 18.15).

Esercizio 18.5. Verificare che le categorie degli insiemi SETS, dei gruppi GRPS, degli spazi topologici TOP ammettono prodotti.

18.D. Limiti. Un **sistema diretto superiormente di oggetti e frecce in una categoria $\mathfrak{C}$**

$$(\langle a_i \mid i \in I\rangle, \langle f_{i,j} \mid i \le j\rangle) \tag{18.1}$$

è dato da un

- insieme diretto superiormente $\langle I, \le\rangle$
- degli oggetti di $\mathfrak{C}$, a_i per $i \in I$,
- delle frecce di $\mathfrak{C}$, $f_{i,j} : a_i \to a_j$, quando $i, j \in I$ e $i \le j$ tali che

$$i \le j \le k \Rightarrow f_{i,k} = f_{j,k} \circ f_{i,j}. \tag{18.2}$$

Il **limite diretto** o **limite induttivo** di (18.1)

$$(a_\infty, \langle f_{i,\infty} \mid i \in I\rangle)$$

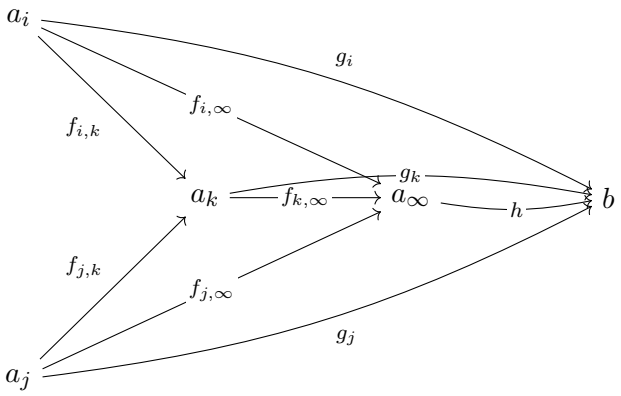
è costituito da:

- un oggetto a_∞ e
- una famiglia di frecce $f_{i,\infty} : a_i \to a_\infty$ $(i \in I)$ che commutano con le $f_{i,j}$, cioè

  $$f_{i,\infty} = f_{j,\infty} \circ f_{i,j} \qquad (\text{ per } i \le j$$

  e tale che per ogni oggetto b e ogni famiglia di frecce g_i $(i \in I)$ che commutano con le $f_{i,j}$, c'è un'unica freccia $h : a_\infty \to b$ che rende commutativo

il diagramma

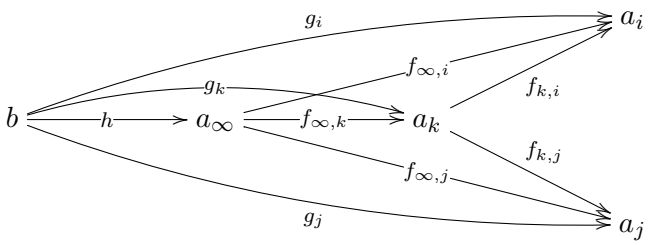


L'esistenza e unicità della freccia h prende il nome di **proprietà universale del limite diretto**. Il limite diretto, se esiste, è definito a meno di isomorfismi: se a_∞ e a'_∞ sono due limiti diretti per lo stesso sistema, siano $h\colon a_\infty \to a'_\infty$ e $h'\colon a'_\infty \to a_\infty$ come da definizione. Se prendiamo $b = a_\infty$ nella definizione di limite diretto, la freccia che rende commutativo il diagramma deve essere $\mathbf{1}_{a_\infty}\colon a_\infty \to a_\infty$. D'altra parte anche $h' \circ h\colon a_\infty \to a_\infty$ è una freccia che commuta, quindi $h' \circ h = \mathbf{1}_{a_\infty}$. Analogamente $h \circ h' = \mathbf{1}_{a'_\infty}$.

La nozione di **limite inverso** o **limite proiettivo** si ottiene "dualizzando" la definizione di limite diretto. Si parte da un ordine diretto inferiormente $\langle I, \leq\rangle$ e un sistema di frecce $f_{i,j}\colon a_i \to a_j$, che commutano, cioè tale che soddisfano (18.2). Un limite inverso è un oggetto a_∞ e un sistema di mappe $f_{\infty,i}\colon a_\infty \to a_i$ $(i \in I)$ che commutano con le $f_{i,j}$, cioè

$$f_{\infty,j} = f_{i,j} \circ f_{\infty,i} \qquad (i \leq j)$$

e tale che per ogni oggetto b e ogni famiglia di frecce g_i $(i \in I)$ che commutano con le $f_{i,j}$, c'è un'unica freccia $h\colon b \to a_\infty$ che rende commutativo il diagramma



Non tutte le categorie ammettono limiti, neppure quando I è finito, ma molte delle categorie familiari sì. In particolare le categorie Set, Grp, POrd, Top ammettono limiti diretti.

18.D.1. *La categoria* Set *degli insiemi.* Fissiamo un sistema diretto

$$(\langle A_i \mid i \in I\rangle, \langle f_{i,j} \mid i \leq j\rangle).$$

Innanzitutto consideriamo un caso particolarmente semplice in cui le frecce sono funzioni di inclusione: in altre parole è data una famiglia A_i $(i \in I)$ di insiemi e la freccia $f_{i,j}\colon A_i \to A_j$ significa che $A_i \subseteq A_j$. Il limite diretto è semplicemente $\bigcup_{i\in I} A_i$.

Se le frecce $f_{i,j}$ sono funzioni iniettive, ma non necessariamente inclusioni, dobbiamo sostituire l'unione con

$$A_\infty = (\bigcup_{i\in I} \{i\} \times A_i)/\!\sim \tag{18.3}$$

vale a dire l'unione disgiunta degli A_i modulo la relazione d'equivalenza

$$(i,x) \sim (j,y) \quad \Leftrightarrow \quad \exists k\,(i \leq k \wedge j \leq k \wedge f_{i,k}(x) = f_{j,k}(y))\,.$$

Le funzioni $f_{i,\infty}\colon A_i \to A_\infty$ sono date da

$$f_{i,\infty}(x) = [(i,x)]_\sim. \tag{18.4}$$

Se B è un altro insieme e $g_i\colon A_i \to B$ commutano con le $f_{i,j}$, definiamo $h\colon A_\infty \to B$

$$[(i,x)]_\sim \mapsto g_i(x). \tag{18.5}$$

Verifichiamo che la definizione non dipende dal rappresentante cioè se $(i,x) \sim (j,y)$ allora $g_i(x) = g_j(y)$. Sia $k \geq i,j$ tale che $f_{i,k}(x) = f_{j,k}(y)$: allora

$$\begin{aligned} g_i(x) &= g_k(f_{i,k}(x)) \\ &= g_k(f_{j,k}(y)) \\ &= g_j(y) \end{aligned}$$

come richiesto.

Esercizio 18.6. Verificare che la funzione in (18.5) è l'unica funzione che verifica la proprietà universale del limite diretto.

Osserviamo che l'ipotesi che le $f_{i,j}$ fossero iniettive non è stata usata. Infatti, la costruzione in (18.3) e (18.4) funziona per *ogni* sistema diretto di insiemi e funzioni.

18.D.2. *La categoria dei gruppi* Grp. Il limite di un sistema diretto di gruppi G_i, $(i \in I)$ e omomorfismi $f_{i,j}$ $(i \leq j)$ è il gruppo che ha G_∞ il cui insieme supporto è dato da (18.3). L'operazione su G_∞ è data da

$$[(i,x)] \cdot [(j,y)] = [(k, f_{i,k}(x) \cdot f_{j,k}(y))]$$

dove $k \geq i,j$ e la moltiplicazione $f_{i,k}(x) \cdot f_{j,k}(y)$ è effettuata in G_k. Verifichiamo che la definizione non dipende dalla scelta dei rappresentanti.

Supponiamo che $(i,x) \sim (i',x')$ e $(j,y) \sim (j',y')$, $k \geq i,j$ e $k' \geq i',j'$: dobbiamo verificare che

$$(k, f_{i,k}(x) \cdot f_{j,k}(y)) \sim (k', f_{i',k'}(x') \cdot f_{j',k'}(y')).$$

Siano $i^* \geq i,i'$ e $j^* \geq j,j'$ tali che $f_{i,i^*}(x) = f_{i',i^*}(x')$ e $f_{j,j^*}(y) = f_{j',j^*}(y')$ e sia $k^* \geq k,k',i^*,j^*$. Allora

$$\begin{aligned} f_{i,k^*}(x) \cdot f_{j,k^*}(y) &= f_{i^*,k^*}(f_{i,i^*}(x)) \cdot f_{j^*,k^*}(f_{j,j^*}(y)) \\ &= f_{i^*,k^*}(f_{i',i^*}(x')) \cdot f_{j^*,k^*}(f_{j',j^*}(y')) \\ &= f_{i',k^*}(x') \cdot f_{j',k^*}(y'), \end{aligned}$$

come dovevasi dimostrare.

L'identità di G_∞ è $[(i, 1_{G_i})]_\sim$, dove 1_{G_i} è l'identità di G_i. I morfismi $f_{i,\infty}\colon G_i \to G_\infty$ sono definiti da (18.4).

Esercizio 18.7. Verificare che G_∞ soddisfa la proprietà universale dei limiti diretti.

Esercizio 18.8. Verificare che se $\langle I, \leq\rangle$ è linearmente ordinato e $f_{i,j}\colon G_i \hookrightarrow G_j$ è la funzione di inclusione, allora $G_\infty = \bigcup_{i\in I} G_i$.

18.D.3. *La categoria degli ordini parziali* POrd. Dato un sistema diretto di ordini $\langle A_i, \preccurlyeq_i\rangle$ $(i \in I)$ e funzioni crescenti $f_{i,j}\colon A_i \to A_j$ (con $i \leq j$) il limite diretto è l'insieme ordinato $\langle A_\infty, \preccurlyeq_\infty\rangle$ dove A_∞ è l'insieme definito in (18.3) e $\preccurlyeq_\infty$ è l'ordinamento

$$[(i,x)]_\sim \preccurlyeq_\infty [(j,y)]_\sim \quad \Leftrightarrow \quad \exists k\, (k \geq i,j \wedge f_{i,k}(x) \preccurlyeq_k f_{j,k}(y))$$

Lasciamo al lettore la verifica che la definizione non dipende dalla scelta dei rappresentanti. Le funzioni $f_{i,\infty}\colon A_i \to A_\infty$ sono come in (18.4): per la commutatività delle $f_{i,j}$, se $x,y \in A_i$ e $x \preccurlyeq_i y$ allora $f_{i,j}(x) \preccurlyeq_j f_{i,j}(y)$ per ogni $i \leq j$ e quindi $f_{i,\infty}(x) \preccurlyeq_\infty f_{i,\infty}(y)$.

Esercizio 18.9. Dimostrare che se gli $\langle A_i, \preccurlyeq_i\rangle$ sono ordini lineari, allora $\langle A_\infty, \preccurlyeq_\infty\rangle$ è lineare. Dimostrare con un contro-esempio che gli $\langle A_i, \preccurlyeq_i\rangle$ possono essere tutti dei buoni ordini, ma $\langle A_\infty, \preccurlyeq_\infty\rangle$ non è necessariamente un buon ordine.

18.D.4. *La categoria degli spazi topologici* Top. Dato un sistema diretto di spazi topologici $\langle X_i, \mathcal{T}_i\rangle$ $(i \in I)$ e funzioni continue $f_{i,j}\colon X_i \to X_j$ $(i \leq j)$ il limite diretto è lo spazio $\langle X_\infty, \mathcal{T}_\infty\rangle$ dove X_∞ è l'insieme limite diretto degli insiemi X_i (18.3) e la topologia è

$$\mathcal{T}_\infty = \{U \subseteq X_\infty \mid \forall i \in I\ f_{i,\infty}^{-1}(U) \in \mathcal{T}_i\}.$$

Verifichiamo che $\mathcal{T}_\infty$ è una topologia su X_∞. Chiaramente $\emptyset, X_\infty \in \mathcal{T}_\infty$. Se $U,Y \in \mathcal{T}_\infty$, allora $f_{i,\infty}^{-1}(U \cap V) = f_{i,\infty}^{-1}(U) \cap f_{i,\infty}^{-1}(V) \in \mathcal{T}_i$ per ogni $i \in I$, cioè $\mathcal{T}_\infty$ è chiusa per intersezioni finite. Se $\{U_j \mid j \in J\} \subseteq \mathcal{T}_\infty$, allora

$f_{i,\infty}^{-1}\left(\bigcup_{j\in J} U_j\right) = \bigcup_{j\in J} f_{i,\infty}^{-1}(U_j) \in \mathcal{T}_i$, per ogni $i \in I$, da cui $\bigcup_{j\in J} U_j \in \mathcal{T}_\infty$. Quindi $\mathcal{T}_\infty$ è una topologia su X_∞.

Le funzioni $f_{i,\infty}\colon X_i \to X_\infty$ sono continue per definizione di $\mathcal{T}_\infty$. Verifichiamo che vale la proprietà di universalità: $\langle X', \mathcal{T}'\rangle$ è uno spazio topologico e $g_i\colon X_i \to X'$ funzioni continue che commutano con le $f_{i,j}$. Poiché la funzione $h\colon X_\infty \to X'$ definita da (18.5) è l'unica funzione che rende sia commutativo il diagramma, è sufficiente dimostrare che è continua: se $U' \subseteq X'$ è aperto,

$$f_{i,\infty}^{-1}(h^{-1}(U')) = g_i^{-1}(U') \in \mathcal{T}_i$$

e quindi $h^{-1}(U') \in \mathcal{T}_\infty$. Quindi $\langle X_\infty, \mathcal{T}_\infty\rangle$ è il limite diretto del sistema.

18.E. Il teorema di Cantor-Lawvere*. Le categorie che utilizzeremo in questo corso sono sono abbastanza vicine alla teoria degli insiemi, nel senso che le frecce tra oggetti sono funzioni che soddisfano opportune proprietà. Per queste categorie è possibile dimostrare una generalizzazione del Teorema di Cantor 10.23.

Teorema 18.10 (Lawvere)**.** *Sia $\mathfrak{C}$ una categoria in cui le frecce sono funzioni, siano a, b oggetti di $\mathfrak{C}$ e supponiamo $F\colon a \to \hom(a,b)$ sia una suriezione tale che*

$$a \to b \qquad x \mapsto F(x)(x)$$

sia un morfismo di $\mathfrak{C}$. Allora b ha la proprietà del punto fisso, cioè per ogni morfismo $f\colon b \to b$ c'è un $x \in b$ tale che $f(x) = x$.

Dimostrazione. Sia $f\colon b \to b$ un morfismo e sia $g\colon a \to b$ la funzione

$$g(x) = f(F(x)(x)). \tag{18.6}$$

Per l'ipotesi su F, la freccia g è un morfismo di $\mathfrak{C}$ e c'è un $\bar{x} \in a$ tale che $F(\bar{x}) = g$. Sia $\bar{y} = g(\bar{x}) \in b$. Allora

$$\begin{aligned} f(\bar{y}) &= f(g(\bar{x})) \\ &= f\big(F(\bar{x})(\bar{x})\big) && \text{(dato che } g = F(\bar{x})\text{)} \\ &= g(\bar{x}) && \text{(per (18.6))} \\ &= \bar{y} \end{aligned}$$

vale a dire: $\bar{y}$ è il punto fisso del morfismo g. □

Come corollario otteniamo il Teorema di Cantor 10.23.

Corollario 18.11. *Se X e Y sono insiemi e Y ha almeno due elementi, non c'è nessuna suriezione $X \twoheadrightarrow Y^X$.*

Ecco un'interessante applicazione topologica

Corollario 18.12. *Supponiamo che X e Y siano spazi topologici e sia $f\colon Y \to Y$ una funzione continua priva di punti fissi. Allora non c'è nessuna suriezione*

$$F\colon X \twoheadrightarrow \mathcal{C}(X,Y) \stackrel{\text{def}}{=} \{f\colon X \to Y \mid f \text{ è continua}\}$$

tale che la mappa $X \to Y$, $x \mapsto F(x)(x)$, sia continua.

Esercizi

Esercizio 18.13. (i) Verificare che nella categoria degli insiemi le frecce mono, epi e iso sono le funzioni iniettive, suriettive e bijettive, rispettivamente.

(ii) Dimostrare che nella categoria degli spazi topologici le frecce mono sono funzioni iniettive; nella categoria degli spazi topologici T_2, una funzione continua $f\colon X \to Y$ è epi se e solo se $\mathrm{ran}(f)$ è denso in Y.

(iii) Considerare il monoide $\langle \mathbb{N}, +, 0\rangle$ come categoria — si veda l'esempio 18.A.3. Dimostrare che tutte le frecce sono mono e epi, ma solo 0 è iso.

Esercizio 18.14. Dimostrare che il prodotto di due oggetti (se esiste) è unico a meno di isomorfismi.

Esercizio 18.15. Consideriamo un insieme parzialmente ordinato $\langle P, \leq\rangle$ come una categoria: gli oggetti sono gli elementi di P e assegniamo una freccia $p \to q$ se e solo se $p \leq q$. Dimostrare che questa categoria ha prodotti se e solo se $\langle P, \leq\rangle$ è un semi-reticolo inferiore e $p \times q = \inf\{p, q\}$.

Note e osservazioni

La teoria delle categorie è stata inventata nel 1942 da Eilenberg e Mac Lane nell'ambito della topologia algebrica. La nostra trattazione è molto ridotta — il lettore interessato può consultare i testi [**ML98**] e [**Gol84**].

Capitolo V

Matematiche elementari da un punto di vista superiore

In questo Capitolo studieremo in dettaglio certi concetti centrali della matematica. Alcune di queste nozioni erano già state introdotte nei Capitoli I–III e l'infusione delle tecniche insiemistiche viste nel Capitolo IV ci permetterà di ottenere nuovi risultati.

19. Funzioni ricorsive

Richiamiamo le definizioni della Sezione 9.

Definizione 19.1. L'insieme delle funzioni primitive ricorsive $\boldsymbol{\mathcal{P}}$ è il più piccolo insieme di funzioni finitarie su $\mathbb{N}$ contenente

- la funzione zero $c_0 \colon \mathbb{N} \to \mathbb{N}$, $c_0(n) = 0$,
- la funzione successore $\mathbf{S} \restriction \mathbb{N} = S \colon \mathbb{N} \to \mathbb{N}$,
- le funzioni di proiezione $I^n_k \colon \mathbb{N}^n \to \mathbb{N}$, dove $I^n_k(x_0, \dots, x_{n-1}) = x_k$,

e chiuso per composizione e ricorsione primitiva.

L'insieme $\boldsymbol{\mathcal{R}}$ delle funzioni ricorsive è il più piccolo insieme di funzioni finitarie su $\mathbb{N}$ contenente $\boldsymbol{\mathcal{P}}$ e chiuso per composizione, ricorsione primitiva e minimalizzazione.

19.A. Funzioni ricorsive e rappresentabilità. Dimostreremo che ogni funzione ricorsiva è rappresentabile nell'aritmetica di Peano (pag. 144), anzi, in sistema di assiomi assai più debole di PA.

Definizione 19.2. L'aritmetica di **Tarski-Mostowski-Robinson** è la teoria Q del linguaggio L_{PA} formato dagli enunciati

$$(\mathsf{Q}1) \qquad \forall x\,(S(x) \neq \overline{0})$$

$$(\mathsf{Q}2) \qquad \forall x, y\,(x \neq y \Rightarrow S(x) \neq S(y))$$

$$(\mathsf{Q}3) \qquad \forall x\,(x + \overline{0} = x)$$

$$(\mathsf{Q}4) \qquad \forall x \forall y\,(x + S(y) = S(x + y))$$

$$(\mathsf{Q}5) \qquad \forall x\,(x \cdot \overline{0} = \overline{0})$$

$$(\mathsf{Q}6) \qquad \forall x\,\forall y\,(x \cdot S(y) = (x \cdot y) + x)$$

$$(\mathsf{Q}7) \qquad \forall x\,\neg(x < \overline{0})$$

$$(\mathsf{Q}8) \qquad \forall x, y\ (x < S(y) \Leftrightarrow (x < y \vee x = y))$$

e dall'assioma di tricotomia

$$(\mathsf{Q}9) \qquad \forall xy\,(x < y \vee x = y \vee y < x)\,.$$

La teoria Q non è in grado di dimostrare la commutatività dell'addizione e della moltiplicazione (Esercizio 19.16).

Al fine di evitare confusioni con il numero naturale zero, useremo il simbolo $\overline{0}$ per la costante di L_{PA}. I **numerali** sono i termini $\overline{n}$ definiti da $\overline{n+1} = S(\overline{n})$.

Per la parte (f) del Teorema 7.15 a pagina 140, l'assioma di tricotomia è un teorema di PA quindi ogni teorema di Q è anche un teorema di PA. Il vantaggio di usare Q è che questa teoria, a differenza di PA, è finitamente assiomatizzabile.

Definizione 19.3. (i) Sia $F\colon \mathbb{N}^k \to \mathbb{N}$ una funzione e $\varphi(x_1, \ldots, x_k, y)$ una L_{PA}-formula. Diremo che $\varphi(x_1, \ldots, x_k, y)$ **rappresenta** F **in** Q se per ogni $a_1, \ldots, a_k \in \mathbb{N}$

$$\mathsf{Q} \models \forall y(\varphi[\![\overline{a_1}/x_1, \ldots \overline{a_k}/x_k]\!] \Leftrightarrow y = \overline{F(a_1, \ldots, a_k)}).$$

Diremo che una funzione $F\colon \mathbb{N}^k \to \mathbb{N}$ **è rappresentabile in** Q se è rappresentata da qualche $\varphi(x_1, \ldots, x_k, y)$.

(ii) Sia $A \subseteq \mathbb{N}^k$ un predicato e $\varphi(x_1, \ldots, x_k)$ una L_{PA}-formula. Diremo che $\varphi(x_1, \ldots, x_k)$ **rappresenta** A **in** Q se per ogni $a_1, \ldots, a_k \in \mathbb{N}$

$$\text{se } (a_1, \ldots, a_k) \in A, \text{ allora } \mathsf{Q} \models \varphi[\![\overline{a_1}/x_1, \ldots \overline{a_k}/x_k]\!]$$
$$\text{se } (a_1, \ldots, a_k) \notin A, \text{ allora } \mathsf{Q} \models \neg\varphi[\![\overline{a_1}/x_1, \ldots \overline{a_k}/x_k]\!].$$

Diremo che un predicato $A \subseteq \mathbb{N}^k$ **è rappresentabile in** Q se è rappresentato da qualche $\varphi(x_1, \ldots, x_k)$.

Osservazione 19.4. La scelta delle variabili per la rappresentazione non è vincolante: se F è rappresentabile e $x_1, \ldots, x_k, y$ sono distinte, allora c'è

una L_{PA}-formula $\varphi(x_1, \dots, x_k, y)$ che rappresenta F. Per vedere ciò fissiamo $\varphi'(x'_1, \dots, x'_k, y')$ che rappresenta F. Sostituendo se necessario φ' con una sua variante (vedi pagina 32), possiamo supporre che $x_1, \dots, x_k, y$ non occorrano vincolate in φ'. Allora $\varphi'[\![x_1/x'_1, \dots, x_k/x'_k, y/y']\!]$ rappresenta F.

Un'osservazione analoga vale per la rappresentabilità dei predicati.

Lemma 19.5. (a) *La formula $x_1 = x_2$ rappresenta il predicato di uguaglianza $\{(a, b) \in \mathbb{N}^2 \mid a = b\}$.*

(b) *La formula $x_1 < x_2$ rappresenta il predicato di ordine $\{(a, b) \in \mathbb{N}^2 \mid a < b\}$.*

Dimostrazione. (a) Chiaramente se $a = b$ allora $\overline{a}$ e $\overline{b}$ sono il medesimo termine, quindi $\mathsf{Q} \models \overline{a} = \overline{b}$. Per l'altra implicazione è sufficiente dimostrare per induzione su $a \in \mathbb{N}$ che

$$\text{se } a < b \text{ allora } \mathsf{Q} \models \overline{a} \neq \overline{b}.$$

Sia $c = b - 1$. Se $a = 0$ allora $\mathsf{Q} \models \overline{0} \neq S(\overline{c}) = \overline{b}$ per ($\mathsf{Q}1$). Se $a > 0$ sia $d = a - 1$: per ipotesi induttiva $\mathsf{Q} \models \overline{d} \neq \overline{c}$ quindi $\mathsf{Q} \models \overline{a} \neq \overline{b}$ per ($\mathsf{Q}2$).

(b) Verifichiamo per induzione su $b \in \mathbb{N}$ che

(19.1a) $$\text{se } a < b \text{ allora } \mathsf{Q} \models \overline{a} < \overline{b}$$

(19.1b) $$\text{se } b \leq a \text{ allora } \mathsf{Q} \models \neg(\overline{a} < \overline{b}).$$

Se $b = 0$ la (19.1a) è banalmente vera e la (19.1b) discende da ($\mathsf{Q}7$). Supponiamo $b = c + 1$. Se $a < b$ allora $a < c$ oppure $a = c$ □

Diremo che il **termine** $t(x_1, \dots, x_k)$ **rappresenta la funzione** $F\colon \mathbb{N}^k \to \mathbb{N}$ se

$$t[\overline{a_1}/x_1, \dots, \overline{a_k}/x_k] = \overline{F(a_1, \dots, a_k)}$$

è un teorema di Q. Equivalentemente: se la formula $t(x_1, \dots, x_k) = y$ rappresenta F.

Esercizio 19.6. I termini $x_1 + x_2$ e $x_1 \cdot x_2$ rappresentano le funzioni somma e prodotto.

Teorema 19.7. *Ogni funzione ricorsiva è rappresentabile in* Q.

Dimostrazione. □

19.B. Ricorsività su altri domini. Finora abbiamo soltanto considerato funzioni e predicati computabili sui numeri naturali, ma data una biezione $u\colon \mathbb{N} \to X$ è possibile trasferire le nozioni di calcolabilità da $\mathbb{N}$ a X. Per esempio, posto $u\colon \mathbb{N} \to \mathbb{Z}$, $u(2n) = n$ and $u(2n + 1) = -n$, la somma e il prodotto in $\mathbb{Z}$ sono elementari ricorsive. Questa idea può essere generalizzata alle strutture numerabili del prim'ordine. Fissiamo un linguaggio

del prim'ordine L con un numero finito di simboli non logici.[1] Data una L-struttura numerabile $\mathcal{M} = (M, \dots)$, una **presentazione ricorsiva** per $\mathcal{M}$ è una biezione $u\colon \mathbb{N} \to M$ tale che per ogni simbolo di funzione n-ario f, la mappa

$$\mathbb{N}^n \to \mathbb{N}, \quad (k_1, \dots, k_n) \mapsto u^{-1}\left(f^{\mathcal{M}}(u(k_1), \dots, u(k_n))\right)$$

è ricorsiva, e per ogni simbolo di predicato n-ario P, l'insieme

$$\{(k_1, \dots, k_n) \in \mathbb{N}^k \mid (u(k_1), \dots, u(k_n)) \in P^{\mathcal{M}}\}$$

è ricorsivo.

19.B.1. *Ricorsività in* V_ω. Ogni $n \in \mathbb{N} \setminus \{0\}$ può essere scritto in un unico modo come

$$n = 2^{x_0} + \cdots + 2^{x_{k(n)}} \tag{19.2}$$

con $0 \leq x_0 < \cdots < x_{k(n)}$. Quindi possiamo definire la funzione

$$u\colon \mathbb{N} \to \mathrm{V}_\omega$$

ponendo $u(0) = \emptyset$ e per $n > 0$

$$u(n) = \left\{u(x_0), \dots, u(x_{k(n)})\right\}$$

dove $x_0, \dots, x_{k(n)}$ sono come in (19.2). Per l'Esercizio 19.17 u è una biezione, $u(n) \in u(m) \Rightarrow n < m$, e

$$E = \{(n, m) \mid u(n) \in u(m)\} \tag{19.3}$$

è elementare ricorsivo.

Ricordiamo che una formula del linguaggio della teoria degli insiemi LST è

- Δ_0 se appartiene alla più piccola collezione di formule contenenti le formule atomiche e chiusa per connettivi e quantificazioni limitate;
- Σ_1 se è della forma $\exists x_1, \dots, x_k\, \varphi$ con φ una formula Δ_0;
- Π_1 se è della forma $\forall x_1, \dots, x_k\, \varphi$ con φ una formula Δ_0.

Un sottoinsieme di V_ω è Δ_0-definibile oppure Σ_1-definibile o Π_1-definibile se è definibile mediante una formula Δ_0 oppure Σ_1 o Π_1. Un sottoinsieme di V_ω che sia tanto Σ_1-definibile quanto Π_1-definibile si dice Δ_1-definibile.

Proposizione 19.8. *Nella struttura* $\langle \mathrm{V}_\omega, \in \rangle$ *ogni elemento è definibile mediante una formula* Δ_0.

[1] È possibile indebolire questa condizione richiedendo che L abbia una quantità numerabile di simboli, e che sia ricorsiva la funzione che associa a ciascun simbolo di predicato/funzione la sua arietà.

Dimostrazione. Dimostriamo per induzione sul rango che ogni $A \in \mathrm{V}_\omega$ è Δ_0-definibile mediante una formula $\varphi(x)$. Se $A = \emptyset$ allora è definibile mediante la formula $\forall y \in x\,(y \neq y)$. Supponiamo $\operatorname{rank} A > 0$, per esempio $A = \{b_1, \dots, b_n\}$. Per ipotesi induttiva ci sono $\varphi_i(y)$ formule Δ_0 che definiscono y_i per $1 \leq i \leq n$. Allora A è definito da $\Big(\exists y_1 \in x \dots \exists y_n \in x \bigwedge_{1\leq i\leq n} \varphi_i(y_i)\Big) \wedge \forall y \in x \bigvee_{1\leq i\leq n} \varphi_i(y)$. □

Proposizione 19.9. *Supponiamo $f\colon A \to \mathrm{V}_\omega$ e che $A \subseteq \mathrm{V}_\omega$ sia Δ_1. Allora $\mathrm{Gr}(f)$ è Σ_1 se e solo se $\mathrm{Gr}(f)$ è Δ_1.*

Dimostrazione. Supponiamo $\varphi(x, y)$ sia una Σ_1 formula che definisce $\mathrm{Gr}(f)$, e sia $\psi(x)$ una Π_1 formula che definisce A. Allora

$$(x, y) \notin \mathrm{Gr}(f) \Leftrightarrow [\neg\psi(x) \vee \exists z\,(\varphi(x, z) \wedge y \neq z]$$

quindi $\mathrm{Gr}(f)$ è Π_1 definibile, e quindi Δ_1 definibile. □

Se $\varphi(x_1, \dots, x_n)$ è una formula di LST, poniamo

$$D_{\varphi(x_1,\dots,x_n)} = \{(k_1, \dots, k_n) \in \mathbb{N}^n \mid \mathrm{V}_\omega \vDash \varphi[u(k_1), \dots, u(k_n)]\}.$$

Lemma 19.10. *Se $\varphi(x_1, \dots, x_n)$ è Δ_0 allora $D_{\varphi(x_1,\dots,x_n)}$ è elementare ricorsiva.*

Dimostrazione. Per l'Esercizio 19.17 l'insieme $E = D_{x\in y}$ in (19.3) è elementare, e se $D_{\varphi(y,x_1,\dots,x_n)}$ è elementare, allora

$$D_{\exists y\in x\,\varphi} = \Big\{(k_1, \dots, k_n) \in \mathbb{N}^n \mid \exists n < k_1\,[(n, m) \in E \wedge (n, k_1, \dots, k_n) \in D_{\varphi(y,x_1,\dots,x_n)}]\Big\}$$

è elementare. Il risultato segue dal fatto che i predicati elementari sono chiusi per combinazioni booleane. □

Proposizione 19.11. *Se $\varphi(x_1, \dots, x_n)$ è una formula Σ_1, allora $D_{\varphi(x_1,\dots,x_n)}$ è ricorsivamente enumerabile.*

Dimostrazione. Supponiamo che $\varphi(x_1, \dots, x_n)$ sia $\exists y\,\varphi(y, x_1, \dots, x_n)$ e $\psi(y, x_1, \dots, x_n)$ una formula Δ_0. Per il Lemma 19.10 l'insieme $D_{\psi(y,x_1,\dots,x_n)}$ è elementare, quindi $D_{\varphi(x_1,\dots,x_n)} = \{\vec{m} \in \mathbb{N}^n \mid \exists k\,(k, \vec{m}) \in D_{\psi(y,x_1,\dots,x_n)}\}$ è ricorsivamente enumerabile. □

Corollario 19.12. *Se $A \subseteq \mathrm{V}_\omega$ è Δ_1-definibile, allora $u^{-1}[A] \subseteq \mathbb{N}$ è ricorsivo.*

Poiché ω è Δ_0-definibile in V_ω, l'insieme $\tilde{\mathbb{N}}u^{-1}[\omega] \subseteq \mathbb{N}$ è ricorsivo e quindi la sua funzione enumerante $u^{-1} \restriction \mathbb{N}\colon \mathbb{N} \to \tilde{\mathbb{N}}$ è ricorsiva, per la Proposizione 9.27.

Teorema 19.13. *Una funzione* $f\colon \mathbb{N}^n \to \mathbb{N}$ *è ricorsiva se e solo se* $\mathrm{Gr}(f) \subseteq \mathrm{V}_\omega$ *è* Δ_1*-definibile.*

Dimostrazione. Sia $\mathcal{F}$ la famiglia delle funzioni finitarie su $\mathbb{N}$ il cui grafo è Δ_1-definibile in V_ω.

L'inclusione $\mathcal{F} \subseteq \boldsymbol{\mathcal{R}}$ vale dato che le funzioni $I^n_k, +, \cdot, \boldsymbol{\chi}_<$ sono in $\mathcal{F}$ e questa famiglia è chiusa per composizione e per minimizzazione: se $f \in \mathcal{F}$ è $n+1$-aria tale che $\forall \vec{x}\, \exists y\, [f(\vec{x}, y) = 0]$, e se $g(\vec{x}) = \boldsymbol{\mu} y\, [f(\vec{x}, y) = 0]$, allora

$$(\vec{x}, y) \in \mathrm{Gr}(g) \Leftrightarrow ((\vec{x}, y), 0) \in \mathrm{Gr}(f) \wedge \forall z \in y\ ((\vec{x}, z), 0) \in \mathrm{Gr}(f))$$

e quindi $g \in \mathcal{F}$.

Viceversa supponiamo $f\colon \mathbb{N}^k \to \mathbb{N}$ sia in $\mathcal{F}$. Allora

$$G \stackrel{\text{def}}{=} \{((n_1, \dots, n_k), m) \mid ((u(n_1), \dots, u(n_k)), u(m)) \in \mathrm{Gr}(f)\}$$

è un sottoinsieme ricorsivo di $\mathbb{N}^n \times \mathbb{N}$ e

$$\mathrm{Gr}(f) = \{((n_1, \dots, n_k), m) \mid ((u^{-1}(n_1), \dots, u^{-1}(n_k)), u^{-1}(m)) \in G\}$$

è ricorsivo. Quindi $f \in \boldsymbol{\mathcal{R}}$ per la Proposizione 9.27. □

19.B.2. *Buoni ordini ricorsivi.* Ricordiamo che se $W \subseteq \mathbb{N}^2$ allora

$$\mathrm{fld}(W) = \{n \in \mathbb{N} \mid \exists m \in \omega\, [(n, m) \in W \vee (m, n) \in W]\}$$

e che W è un buon ordine se è una relazione riflessiva, antisimmetrica, transitiva, connessa su $\mathrm{fld}(W)$ tale che

$$\forall X \subseteq \mathrm{fld}(W)\ [\emptyset \neq X \Rightarrow \exists \bar{n} \in X\, \forall m \in X\ ((m, \bar{n}) \Rightarrow m = \bar{n})]\,.$$

Il tipo d'ordine di $W \subseteq \mathbb{N}^2$ è $\mathrm{ot}(\langle \mathrm{fld}(W), W\rangle)$ ed è solitamente indicato con $\|W\|$. Se $m \in \mathrm{fld}(W)$ allora

$$\begin{aligned}\mathrm{pred}(m, \mathrm{fld}(W); W) &= \{n \in \mathrm{fld}\, W \mid (n, m) \in W \wedge n \neq m\} \\ &= \{n \in \mathrm{fld}\, W \mid (m, n) \notin W\}\end{aligned}$$

e il suo tipo d'ordine è indicato con $\|n\|_W$.

Definizione 19.14. Un **buon ordine ricorsivo** è un insieme ricorsivo $W \subseteq \mathbb{N}^2$ che è un buon ordine. Il tipo d'ordine di un buon ordine ricorsivo è un ordinale ricorsivo **ordinale ricorsivo**.

Se W è un buon ordine ricorsivo e $\bar{n} \in \mathrm{fld}(W)$, allora

$$W \cap \mathrm{pred}(\bar{n}, \mathrm{fld}(W); W)^2 = \{(k, m) \in W \mid (\bar{n}, m) \notin W\}$$

è anche ricorsivo e il suo tipo d'ordine è $\|\bar{n}\|_W$. Per l'Esempio (C) a pagina 190 ω è ricorsivo, così come lo sono i numeri naturali. Poiché c'è una quantità numerabile di sottoinsiemi ricorsivi di $\mathbb{N}^2$, gli ordinali ricorsivi formano un segmento iniziale di ω_1, noto come **ordinale di Church-Kleenee**

$$\omega_1^{\mathrm{CK}} = \{\alpha \mid \alpha \text{ è un ordinale ricorsivo}\}\,.$$

Se W, Z sono buoni ordini ricorsivi, allora $R \subseteq \mathbb{N}^2$ definito da

$$(n,m) \in R \Leftrightarrow [((n)_0, (m)_0) \in W \wedge (n)_0 \neq (m)_0] \vee [((n)_1, (m)_1) \in Z \wedge (n)_0 = (m)_0]$$

è un buon ordine ricorsivo tale che $\|R\| = \|W\| \cdot \|Z\|$. Per l'Esercizio 10.72 a pagina 252 ne segue che

Proposizione 19.15. *ω_1^{CK} è un ordinale numerabile limite più grande di ω, moltiplicativamente (e quindi additivamente) indecomponibile.*

Infatti ω_1^{CK} è esponenzialmente indecomponibile.

Esercizi

Esercizio 19.16. Dimostrare che $\langle \gamma, \dot{+}, \cdot, <, 0\rangle$ soddisfa Q se γ è additivamente indecomponibile.

Concludere che le seguenti formule (o meglio: la loro chiusura universale) non sono conseguenza logica di Q:

$$x + y = y + x$$
$$x \cdot y = y \cdot x$$
$$(x + y) \cdot z = x \cdot z + y \cdot z$$

Esercizio 19.17. Supponiamo che $k, f \colon \mathbb{N} \to \mathbb{N}$ sono definite da $k(0) = f(0) = 0$, e se $n > 0$ allora $f(n) = \langle\!\langle x_0, \ldots, x_{k(n)} \rangle\!\rangle$, dove $n = 2^{x_0} + \cdots + 2^{x_{k(n)}}$ e $0 \leq x_0 < \cdots < x_{k(n)}$. Dimostrare che

(i) k e f sono elementari ricorsive;

(ii) il predicato $\{(n,m) \mid u(n) \in u(m)\}$ è elementare ricorsivo;

(iii) la funzione $u \colon \mathbb{N} \to \mathrm{V}_\omega$ è una biezione;

(iv) $u(n) \in u(m) \Rightarrow n < m$.

Esercizio 19.18. Dimostrare che

(i) se M è un insieme numerabile, transitivo, chiuso per le operazioni $x \mapsto \{x\}$ e $(x,y) \mapsto x \cup y$, allora (M, E) è un grafo aleatorio numerabile, dove $x \mathrel{E} y \Leftrightarrow (x \in y \vee y \in x)$;

(ii) $(\mathbb{N}, F)$ è un grafo aleatorio numerabile, dove $n \mathrel{F} m \Leftrightarrow$ (la n-esima cifra dell'espansione binaria di m è $1 \vee$ la m-esima cifra dell'espansione binaria di n è 1).

Esercizio 19.19. Dimostrare che le seguenti funzioni sono ricorsive:

(i) la funzione di Möbius μ e la funzione $n \mapsto \left|\sum_{k=1}^{n} \mu(k)\right|$ (vedi pagina 10);

(ii)

20. Successioni finite

Se s e t sono funzioni che hanno per dominio un ordinale, diremo che s è un **segmento iniziale** di t se $s \subseteq t$, cioè se $s(\alpha) = t(\alpha)$ per ogni $\alpha \in \mathrm{dom}(s) \subseteq \mathrm{dom}(t)$. Se $s \subset t$ parleremo di segmento iniziale proprio.

Definizione 20.1. Se s e t sono funzioni che hanno per dominio un ordinale e tali che $\mathrm{dom}(s) < \omega$ e $\mathrm{dom}(t) \leq \omega$, la **concatenazione** di s e t è la funzione $s^\frown t$ di domino $\mathrm{dom}(s) \dot{+} \mathrm{dom}(t) \leq \omega$ definita da

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

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

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

L'operazione di concatenazione su $X^{<\omega}$ — l'insieme di tutte le successioni finite di elementi di X definita in (11.8) a pagina 267 — è associativa e $X^{<\omega}$ con questa operazione è un esempio di **semigruppo libero**. Quando ciò non comporta confusione, scriveremo $x_1x_2\ldots x_n$ al posto del più corretto, ma pesante, $\langle x_1, x_2, \ldots, x_n\rangle$, per denotare un elemento di $X^{<\omega}$. Due elementi u e v di $X^{<\omega}$ si dicono **compatibili** se uno è segmento iniziale dell'altro, cioè $u \subseteq v$ oppure $v \subseteq u$. È immediato verificare che

(20.1) $\qquad u^\frown v$ e $u'^\frown v'$ compatibili $\Rightarrow$ u e u' compatibili

e

(20.2) $\qquad u^\frown v$ e $u^\frown v'$ compatibili $\Rightarrow$ v e v' compatibili.

20.A. Espressioni.

Definizione 20.2. L'insieme delle **espressioni** su $\langle S, a\rangle$, dove $a\colon S \to \omega$ e $S \neq \emptyset$

$$\mathrm{Expr} = \mathrm{Expr}(S, a)$$

è il più piccolo $W \subseteq S^{<\omega}$ contenente

$$\{\langle s\rangle \mid s \in S \wedge a(s) = 0\}$$

e chiuso sotto l'operazione

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

Per facilitare la lettura è talvolta comodo utilizzare le parentesi, riscrivendo $s(w_1, \ldots, w_m)$ invece di $\langle s\rangle^\frown w_1{}^\frown \ldots{}^\frown w_m$. Inoltre se $a(s) = 2$ si usa spesso la notazione infissa e si scrive $w_1\, s\, w_2$ invece di $s(w_1, w_2)$.

Esempio 20.3. Se R è un anello e $X_1, X_2, \ldots$ sono indeterminate, sia

$$S = R \cup \{X_i \mid i \in \omega\} \cup \{+, \cdot\}$$

e sia $a\colon S \to \omega$ definita da $a(+) = a(\cdot) = 2$ e $a(s) = 0$ per tutte le altre $s \in S$. Ogni $w \in \mathrm{Expr}(S, a)$ determina un polinomio di $R[X_1, X_2\ldots]$. Naturalmente le espressioni $X_i + X_j$ e $X_j + X_i$ sono distinte.

Più in generale, i termini di un linguaggio del prim'ordine sono espressioni per opportuni S e a.

La Definizione 20.2 può generare un piccolo, ma fastidioso, problema di notazione. Supponiamo che $*, s, t \in S$ con $a(s) = a(t) = 0$ e $a(*) = 2$, e supponiamo che $s = \langle x \rangle$ e $t = \langle y \rangle$. Allora $s * t$ è la stringa $\langle *, \langle x \rangle, \langle y \rangle \rangle$, anche se sarebbe più naturare scriverla come $\langle *, x, y \rangle$. Per questo motivo introduciamo la seguente

Convenzione. Se $a\colon S \to \omega$ e ogni $s \in S$ tale che $a(s) = 0$ è della forma $\langle x \rangle$ per qualche x, allora $\mathrm{Expr}(S, a)$ è il più piccolo insieme W contenente $\{s \mid s \in S \wedge a(s) = 0\}$ e chiuso sotto l'operazione

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

Osserviamo che se $X = \{x \mid \exists s \in S\,(a(s) = 0 \wedge s = \langle x \rangle)\}$, posto $\overline{S} = (S \setminus \{s \in S \mid a(s) = 0\}) \cup X$ e $\overline{a}\colon \overline{S} \to \omega$ definita da $\overline{a}(x) = a(\langle x \rangle)$ e $\overline{a}(s) = a(s)$ per tutti gli altri s, allora $\mathrm{Expr}(S, a)$ computato secondo la nostra convenzione è proprio $\mathrm{Expr}(\overline{S}, \overline{a})$ secondo la Definizione 20.2.

Lemma 20.4. *L'insieme* $\mathrm{Expr}(S, a)$ *delle espressioni su* $\langle S, a \rangle$ *è*

$$\bigcup_n \mathrm{Expr}_n(S, a)$$

dove

$$\begin{aligned} \mathrm{Expr}_0 &= \{\langle s \rangle \mid s \in S \wedge a(s) = 0\} \\ \mathrm{Expr}_{n+1} &= \mathrm{Expr}_n \cup \Big\{ \langle s \rangle {}^\frown w_1 {}^\frown \cdots {}^\frown w_m \mid s \in S \wedge \\ &\qquad w_1, \ldots, w_m \in \mathrm{Expr}_n \wedge a(s) = m \Big\}. \end{aligned}$$

Dimostrazione. Per induzione su n si dimostra che $\mathrm{Expr}_n \subseteq \mathrm{Expr}$ e $\mathrm{Expr}_n \subseteq \mathrm{Expr}_m$, se $n < m$. Quindi è sufficiente dimostrare che se $w_1, \ldots, w_m \in \bigcup_n \mathrm{Expr}_n$ e $a(s) = m$ allora $z = \langle s \rangle {}^\frown w_1 {}^\frown \ldots {}^\frown w_m$ appartiene a $\bigcup_n \mathrm{Expr}_n$: ma se k è sufficientemente grande per cui $w_1, \ldots, w_m \in \mathrm{Expr}_k$, allora $z \in \mathrm{Expr}_{k+1} \subseteq \bigcup_n \mathrm{Expr}_n$. □

Definizione 20.5. L'**altezza** di un'espressione $w \in \mathrm{Expr}(S, a)$ è il più piccolo n tale che $w \in \mathrm{Expr}_n$. La funzione altezza è indicata con

$$\mathrm{ht}\colon \mathrm{Expr}(S, a) \to \omega.$$

Ogni stringa u in $\mathrm{Expr}(S, a)$ può essere scritta come $\langle s \rangle {}^\frown v_1 {}^\frown \ldots {}^\frown v_n$, dove $n = a(s)$ e $v_1, \ldots, v_n \in \mathrm{Expr}(S, a)$. Questa scrittura è unica: infatti il primo elemento s di u determina n e se $u = \langle s \rangle {}^\frown w_1 {}^\frown \ldots {}^\frown w_n$, allora basta osservare che $v_i = w_i$ per $1 \leq i \leq n$, cosa che segue dal seguente Lemma.

Lemma 20.6. *Se* $u_1, \ldots, u_n, v_1, \ldots, v_n \in \mathrm{Expr}(S, a)$ *e* $u_1 {}^\frown \ldots {}^\frown u_n$ *e* $v_1 {}^\frown \ldots {}^\frown v_n$ *sono compatibili, allora* $u_i = v_i$ *per* $1 \leq i \leq n$.

Dimostrazione. Per induzione su $N = \mathrm{lh}(u_1{}^\frown \ldots {}^\frown u_n)$. Sia $s \in S$ il primo elemento della stringa u_1 così che $u_1 = \langle s\rangle {}^\frown w_1{}^\frown \ldots {}^\frown w_k$, dove $k = a(s)$ e $w_1, \ldots, w_k \in \mathrm{Expr}(S, a)$. Allora s è anche il primo elemento della stringa $v_1{}^\frown \ldots {}^\frown v_n$ e quindi $v_1 = \langle s\rangle {}^\frown z_1{}^\frown \ldots {}^\frown z_k$ dove $z_1, \ldots, z_k \in \mathrm{Expr}(S, a)$. Per la (20.1) u_1 e v_1 sono compatibili, quindi $w_1{}^\frown \ldots {}^\frown w_k$ e $z_1{}^\frown \ldots {}^\frown z_k$ sono compatibili. Dato che $\mathrm{lh}(w_1{}^\frown \ldots {}^\frown w_k) < \mathrm{lh}(u_1) \leq N$, per ipotesi induttiva otteniamo $w_i = z_i$ per $1 \leq i \leq k$, e quindi

$$u_1 = \langle s\rangle {}^\frown w_1{}^\frown \ldots {}^\frown w_k = \langle s\rangle {}^\frown z_1{}^\frown \ldots {}^\frown z_k = v_1.$$

Dalla nostra ipotesi e da (20.2) segue che $u_2{}^\frown \ldots {}^\frown u_n$ e $v_2{}^\frown \ldots {}^\frown v_n$ sono compatibili e quindi per ipotesi induttiva $u_i = v_i$ per $2 \leq i \leq n$. □

Corollario 20.7. $\forall w, v \in \mathrm{Expr}(S, a)\,(w \subseteq v \Rightarrow w = v)$.

Questi risultati garantiscono che le espressioni su un insieme S possono essere lette in un unico modo: data una $u \in \mathrm{Expr}(S, a)$ sia $s = u(0)$ e $n = a(s)$: se $\mathrm{lh}(u) = 1$ allora $n = 0$ e se $\mathrm{lh}(u) > 1$ allora esistono e sono unici $u_1, \ldots, u_n \in \mathrm{Expr}(S, a)$ tali che $u = \langle s\rangle {}^\frown u_1{}^\frown \ldots {}^\frown u_n$.

20.B. Occorrenze.

Definizione 20.8. Se $v, w \in S^{<\omega}$ e $w = u_0{}^\frown v{}^\frown u_1$ per qualche u_0, u_1 diremo che v **occorre** in w e scriveremo $v \sqsubseteq w$. Diremo che $s \in S$ occorre in $w \in S^{<\omega}$ se $\langle s\rangle$ occorre in w, cioè se $s \in \mathrm{ran}(w)$.

Se $v, w \in \mathrm{Expr}(S, a)$ e $v \sqsubseteq w$ diremo che v è una **sotto-espressione di** w. Per il Corollario 20.7 se $w = u_0{}^\frown v{}^\frown u_1$ e $u_0 = \emptyset$ allora $u_1 = \emptyset$. Quando $v \sqsubseteq w$ e $v \neq w$ diremo che v è una sotto-espressione propria di w e scriveremo $v \sqsubset w$.

Un'**occorrenza** di $s \in S$ in un'espressione $w \in \mathrm{Expr}(S, a)$ è un $n \in \mathrm{dom}(w)$ tale che $w(n) = s$. Se $s = w(0)$ diremo che s occorre al primo posto di w.

La relazione $\sqsubseteq$ è riflessiva (basta prendere $u_0 = u_1 = \emptyset$) e transitiva su $S^{<\omega}$.

Lemma 20.9. *Se $s \in S$ occorre in $w \in \mathrm{Expr}(S, a)$, allora ogni occorrenza di s in w è un'occorrenza al primo posto di una sotto-espressione v di w, cioè*

$$w(n) = s \Rightarrow \exists v \in \mathrm{Expr}(S, a)\, \exists u_0, u_1 \in S^{<\omega}\, (w = u_0{}^\frown v{}^\frown u_1 \wedge \mathrm{lh}(u_0) = n).$$

Dimostrazione. Procediamo per induzione su $\mathrm{lh}(w)$. Sia n l'occorrenza di s in w. Se $n = 0$, il risultato è dimostrato, quindi possiamo supporre che $n > 0$. Allora $\mathrm{lh}(w) > 1$ e quindi $w = \langle s'\rangle {}^\frown w_1{}^\frown \ldots {}^\frown w_m$ per qualche $s' \in S$ con $a(s') = m > 0$ e $w_1, \ldots, w_m \in \mathrm{Expr}$. Ne segue che l'occorrenza di s si trova in un w_i, vale a dire

$$1 + \mathrm{lh}(w_1) + \cdots + \mathrm{lh}(w_{i-1}) \leq n < 1 + \mathrm{lh}(w_1) + \cdots + \mathrm{lh}(w_i).$$

Allora per ipotesi induttiva, l'occorrenza di s si trova al primo posto di una sotto-espressione v di w_i e poiché $v \sqsubseteq w$ il risultato è dimostrato. □

La definizione di occorrenza può essere opportunamente generalizzata.

Definizione 20.10. Se $v, w \in S^{<\omega}$, un'occorrenza di v in w è un intervallo di naturali

$$\{k, k+1, \ldots, k+n-1\} \subseteq \mathrm{lh}(w)$$

dove $n = \mathrm{lh}(v)$ e tale che $\forall i < n\,(w(k+i) = v(i))$. Se $w = u^\frown w'^\frown z$ diremo che l'occorrenza $\{k, k+1, \ldots, k+n-1\}$ è contenuta in w' se $\mathrm{lh}(u) \leq k$ e $k + n - 1 < \mathrm{lh}(u) + \mathrm{lh}(w')$.

Per esempio le occorrenze di $v = \langle s, s\rangle$ in $w = \langle s, s, s\rangle$ sono $\{0, 1\}$ e $\{1, 2\}$, quindi le occorrenze non sono necessariamente insiemi disgiunti. Il risultato seguente ci garantisce che questo problema non sussiste per le espressioni.

Teorema 20.11. *Supponiamo che $v \sqsubset w$ dove $v, w \in \mathrm{Expr}(S, a)$.*

(a) *Se $w = \langle s\rangle^\frown w_1^\frown \ldots^\frown w_n$, dove $w_1, \ldots, w_n \in \mathrm{Expr}(S, a)$, allora $v \sqsubseteq w_i$ per qualche $1 \leq i \leq n$.*

(b) *Le occorrenze di v in w sono disgiunte. Quindi esistono e sono unici $u_0, \ldots, u_k \in S^{<\omega}$ tali che*

$$w = u_0^\frown v^\frown u_1^\frown \ldots^\frown v^\frown u_k \quad e \quad \forall i \leq k\,(v \not\sqsubseteq u_i)\,.$$

Dimostrazione. (a) Fissiamo u_0, u_1 tali che $w = u_0^\frown v^\frown u_1$. Per il Corollario 20.7 $u_0 \neq \emptyset$. Quindi l'occorrenza $v(0)$ si trova in un qualche w_i e quindi per il Lemma 20.9 si trova al primo posto di una sotto-espressione $\tilde{v} \sqsubseteq w_i$. Poiché v e $\tilde{v}$ sono compatibili, per il Corollario 20.7 $v = \tilde{v}$.

(b) Per induzione su $\mathrm{lh}(w)$. Siano I, J due occorrenze di v in w. Per la parte (a) ci sono $1 \leq i, j \leq n$ tali che l'occorrenza I si trova in w_i e l'occorrenza J si trova in w_j: se $i \neq j$ allora I e J sono disgiunti, se $i = j$ applichiamo l'ipotesi induttiva. □

Introduciamo una nozione ausiliaria: se $w = \langle s\rangle^\frown v_1^\frown \ldots^\frown v_m$ e $v = v_j$ per qualche $1 \leq j \leq m$, scriveremo $v \prec w$. Chiaramente se $v \prec w$ allora $v \sqsubset w$, ma non vale il viceversa. Il prossimo risultato mostra come $\sqsubset$ sia la chiusura transitiva di $\prec$ (si veda la Sezione 13.A.1 per la definizione di chiusura transitiva di una relazione).

Proposizione 20.12. *Per ogni $v, w \in \mathrm{Expr}$*

$$v \sqsubset w \Leftrightarrow \exists k > 0\, \exists z_0, \ldots, z_k \in \mathrm{Expr}\ (v = z_0 \prec z_1 \prec \cdots \prec z_k = w)\,.$$

Dimostrazione. Poiché $\sqsubset$ estende $\prec$, è sufficiente dimostrare un verso della bi-implicazione. Dimostreremo per induzione su n che se $w \in \mathrm{Expr}_n$

$$\forall v \in \mathrm{Expr}\,(v \sqsubset w \Rightarrow \exists k > 0\, \exists z_0, \dots, z_k \in \mathrm{Expr}\,(v = z_0 \prec \cdots \prec z_k = w)).$$

Se $n = 0$ non c'è nulla da dimostrare, quindi possiamo supporre che il risultato valga per un certo n e che $w \in \mathrm{Expr}_{n+1}$ e $v \sqsubset w$. Allora

$$\begin{aligned} w &= \langle s\rangle {}^\frown w_1 {}^\frown \dots {}^\frown w_m \\ &= u_0 {}^\frown v {}^\frown u_1. \end{aligned}$$

Se $u_0 = \emptyset$ allora $v \subseteq w$ e quindi per il Corollario 20.7 $v = w$, contro la nostra assunzione. Quindi la prima occorrenza $v(0)$ in v non è la s iniziale di w e per il Lemma 20.9 risulta essere la prima occorrenza di un'espressione $\tilde{v}$ con $\tilde{v} \sqsubseteq w_i$, per qualche $1 \le i \le m$. Ma allora v e $\tilde{v}$ sono compatibili e ancora per il Corollario 20.7 coincidono e quindi $v \sqsubseteq w_i$. Per ipotesi induttiva ci sono $z_0, \dots, z_k$ tali che $v = z_0 \prec \cdots \prec z_k = w_i$ e poiché $w_i \prec w$, il risultato è dimostrato. □

20.C. Sostituzione. Fissiamo un insieme non vuoto S ed una funzione $a\colon S \to \omega$. Se $w \in S^{<\omega}$ e $s_1, \dots, s_n \in S$ sono distinti, allora

$$w = u_0 {}^\frown \langle s_{i_1}\rangle {}^\frown u_1 {}^\frown \langle s_{i_2}\rangle {}^\frown u_2 {}^\frown \dots {}^\frown \langle s_{i_k}\rangle {}^\frown u_k$$

dove $u_0, \dots, u_k \in S^{<\omega}$ e s_{i_n} non occorre in u_j.

Siano $w, v_1, \dots, v_n \in \mathrm{Expr}(S, a)$ con $v_1, \dots, v_n$ distinti e tali che $v_i \not\sqsubseteq v_j$ per $1 \le i, j \le n$ e $i \ne j$. Allora esistono (e sono unici per il Lemma 20.6) $u_0, \dots, u_k \in S^{<\omega}$ tali che

$$w = u_0 {}^\frown v_{i_1} {}^\frown u_1 {}^\frown v_{i_2} {}^\frown u_2 {}^\frown \dots {}^\frown v_{i_k} {}^\frown u_k$$

con $\{i_1, \dots, i_k\} \subseteq \{1, \dots, n\}$ e $v_i \not\sqsubseteq u_j$ per ogni $1 \le i \le n$ e $j \le k$. Se $z_1, \dots, z_n$ sono espressioni (non necessariamente distinte), l'espressione ottenuta sostituendo $v_1, \dots, v_n$ in w con $z_1, \dots, z_n$ è

$$w[z_1/v_1, \dots, z_n/v_n] = u_0 {}^\frown z_{i_1} {}^\frown u_1 {}^\frown z_{i_2} {}^\frown u_2 {}^\frown \dots {}^\frown z_{i_k} {}^\frown u_k.$$

In particolare, $w[z_1/v_1, \dots, z_n/v_n] = w[z_{j_1}/v_{j_1}, \dots, z_{j_m}/v_{j_m}]$ dove $\{j_1, \dots, j_m\}$ è l'insieme degli indici $1 \le j \le n$ tali che $v_j \sqsubseteq w$.

Esercizio 20.13. Verificare per induzione su $\mathrm{ht}(w)$ che $w[z_1/v_1, \dots, z_n/v_n] \in \mathrm{Expr}(S, a)$.

Osserviamo che la sostituzione deve essere effettuata simultaneamente per tutte le espressioni $v_1, \dots, v_n$ — in generale $w[z_1/v_1, z_2/v_2] \ne (w[z_1/v_1])[z_2/v_2]$.

20.D. Un'applicazione. Se $\mathcal{F}$ è una collezione di funzioni finitarie su X e $Y \subseteq X$, sia

$$S = \mathcal{F} \cup Y$$

e poniamo

$$a(s) = \begin{cases} 0 & \text{se } s \in Y, \\ \mathrm{ar}(s) & \text{se } s \in \mathcal{F}. \end{cases}$$

Usando la notazione del Lemma 20.4 e la Convenzione introdotta a pagina 355, osserviamo che $\mathrm{Expr}_0 = \{s \mid s \in Y \cup C\}$ dove

$$C = \{s \in \mathcal{F} \mid a(s) = 0\}$$

e che se $w \in \mathrm{Expr}_{n+1}$ allora esistono e sono unici $f \in \mathcal{F}$ e $w_1, \dots, w_m \in \mathrm{Expr}_n$ tali che $w = \langle f \rangle {}^\frown w_1 {}^\frown \dots {}^\frown w_m$. Per l'unicità della lettura delle espressioni, possiamo definire una mappa

$$\Phi \colon \mathrm{Expr} \to X$$

ponendo $\Phi \restriction \mathrm{Expr}_0 = \mathrm{id} \restriction \mathrm{Expr}_0$ e

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

Sia $Y_n = \Phi[\mathrm{Expr}_n]$. È facile verificare che

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

e che $Y_0 \subseteq Y_1 \subseteq \dots$. Se $f \in \mathcal{F}$ è n-aria e $x_0, \dots, x_{n-1} \in \bigcup_k Y_k$, fissiamo un m sufficientemente grande tale che $x_0, \dots, x_{n-1} \in Y_m$: allora $f(x_0, \dots, x_{n-1}) \in Y_{m+1} \subseteq \bigcup_k Y_k$. Ne consegue che $\bigcup_k Y_k$ è chiuso sotto $\mathcal{F}$ e quindi $\bigcup_k Y_k \supseteq \mathrm{Cl}_{\mathcal{F}}(Y)$, la chiusura di Y sotto $\mathcal{F}$ definita a pagina 270. Viceversa, è immediato verificare che $\bigcup_k Y_k \subseteq \mathrm{Cl}_{\mathcal{F}}(Y)$. Abbiamo quindi dimostrato che:

Proposizione 20.14. *Se $\mathcal{F}$ è una famiglia di funzioni finitarie su X e $Y \subseteq X$, allora*

$$\mathrm{Cl}_{\mathcal{F}}(Y) = \bigcup_{k \in \omega} Y_k.$$

In altre parole: la chiusura di un insieme $Y \subseteq X$ sotto una famiglia $\mathcal{F}$ di funzioni finitarie su X è l'immagine suriettiva di un insieme di espressioni.

Viceversa, la Definizione 20.2 di $\mathrm{Expr}(S, a)$ può essere riformulata come chiusura sotto un insieme $\mathcal{F}$ di funzioni: dato (S, a) sia $X = S^{<\omega}$ e per ogni $s \in S$ sia

$$f_s \colon X^{a(s)} \to S, \qquad \left\langle w_1, \dots, w_{a(s)} \right\rangle \mapsto \langle s \rangle {}^\frown w_1 {}^\frown \dots {}^\frown w_{a(s)}.$$

Allora $\mathrm{Expr}(S, a) = \mathrm{Cl}_{\mathcal{F}}(\emptyset)$ dove $\mathcal{F} = \{f_s \mid s \in S\}$.

20.E. Alberi.

20.E.1. *Alberi etichettati.* Dato un insieme $\mathcal{F}$ di funzioni finitarie su un qualche insieme X possiamo descrivere tutte le funzioni finitarie su X ottenibili per composizione di funzioni in $\mathcal{F}$: basta considerare $\mathrm{Expr}(S, a)$ l'insieme delle espressioni su $\langle S, a\rangle$ dove $S = \mathcal{F} \cup \{x_n \mid n \in \omega\}$ e $a\colon S \to \omega$ è la funzione arietà su $\mathcal{F}$, con la stipula che $a(x_n) = 0$ per ogni variabile x_n. Per quanto visto nella sezione precedente, possiamo verificare che se x, y, z, u sono variabili e $f, g, h \in \mathcal{F}$ sono, rispettivamente, 1-aria, 2-aria e 3-aria, allora la stringa

$$hfhxzgfuygxfgzyfhfzhyuxz \tag{20.3}$$

è un'espressione di $\langle S, a\rangle$ che descrive una funzione 4-aria su X. Cerchiamo di descrivere questa funzione — o meglio: questa espressione — a partire dalle funzioni che la compongono, cioè dalle espressioni in essa contenute. Cominciamo con l'individuare le espressioni di altezza 1, cioè quelle individuate da una funzione applicata a variabili...

$$hfhxzg\underbrace{fu}\,y\,gx\,f\,\underbrace{gzy}\,f\,h\,\underbrace{fz}\,\underbrace{hyux}\,z$$

...passiamo poi a quelle di altezza 2...

$$hfhxz\,\underbrace{g\boxed{fu}y}\,gx\,\underbrace{f\boxed{gzy}}\,f\,h\,\underbrace{\boxed{fz}\,\boxed{hyux}\,z}$$

...poi a quelle di altezza 3...

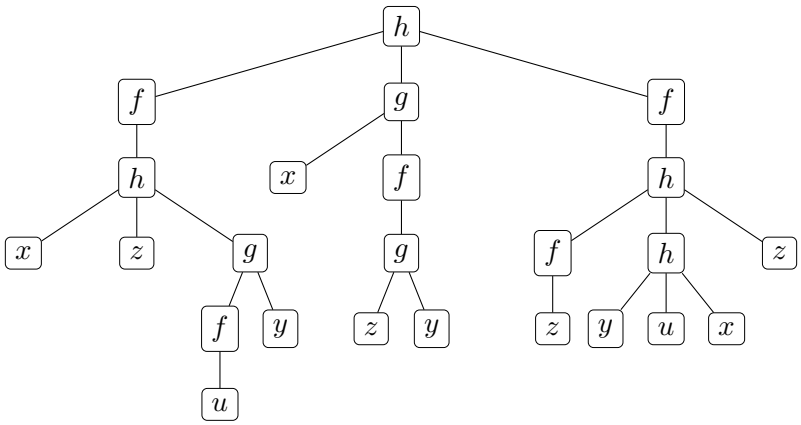
$$hf\,\underbrace{hxz\boxed{g\boxed{fu}y}}\,\underbrace{gx\boxed{f\boxed{gzy}}}\,\underbrace{f\boxed{h\boxed{fz}\,\boxed{hyux}\,z}}$$

...poi a quella di altezza 4...

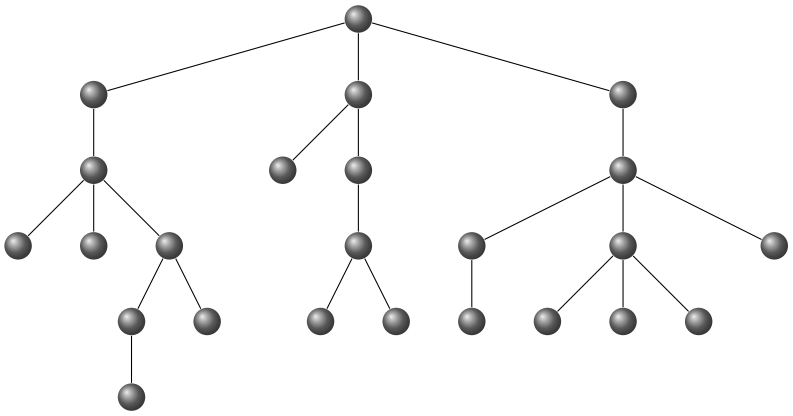
$$h\,\underbrace{f\boxed{hxz\boxed{g\boxed{fu}y}}}\,\boxed{gx\boxed{f\boxed{gzy}}}\,\boxed{f\boxed{h\boxed{fz}\,\boxed{hyux}\,z}}$$

...e a questo punto vediamo che c'è un h seguita da tre espressioni — la prima di altezza 4, le altre due di altezza 3 — e che quindi la stringa (20.3) è un'espressione di altezza 5. Questo algoritmo — che è ben definito grazie al Lemma 20.6 — suggerisce una rappresentazione ad albero della stringa (20.3), ed il diagramma che si ottiene è proprio quello della Figura 2 a pagina 21

con c al posto di u:



Un diagramma di questo tipo si dice albero etichettato. L'idea è di partire da una struttura del tipo



(20.4)

detta albero, e di associare ad ogni ● un elemento di S. Al fine di darne una trattazione formale introduciamo qualche concetto generale.

Definizione 20.15. (i) Un **albero** è un insieme parzialmente ordinato $(T, \lhd)$ tale che $\mathrm{pred}(x) = \{y \in T \mid y \lhd x\}$ è bene ordinato, per ogni $x \in T$.

(ii) Gli elementi di T si dicono **nodi**.

(iii) Un **nodo terminale** è un $x \in T$ privo di successori immediati.

(iv) Se ogni nodo di T ha un numero finito di successori immediati, diremo che T si **ramifica finitamente**.

(v) Un nodo si dice **biforcazione** se ha più di un successore immediato.

(vi) Un **ramo** è una catena massimale.

(vii) La funzione **altezza** è

$$\mathrm{ht}_T \colon T \to \mathrm{Ord} \qquad \mathrm{ht}_T(x) = \mathrm{ot}(\mathrm{pred}(x))$$

e l'ordinale $\mathrm{ht}(T) \stackrel{\mathrm{def}}{=} \mathrm{ran}(\mathrm{ht}_T)$ si dice **l'altezza di** T.

(viii) Il **livello** α-esimo di T è

$$\mathrm{Lev}_\alpha(T) = \{x \in T \mid \mathrm{ht}_T(x) = \alpha\}\,.$$

(ix) Un nodo di $\mathrm{Lev}_0(T)$ si dice **radice** dell'albero.

Esercizio 20.16. Dimostrare che

(i) $(T, \lhd)$ è un albero se e solo se $\lhd$ è irriflessiva, transitiva, ben fondata e $\mathrm{pred}(x, T; \lhd)$ è linearmente ordinato, per ogni $x \in T$,

(ii) se $(T, \lhd)$ è un albero, allora $\mathrm{ht}(T) = \min\{\alpha \mid \mathrm{Lev}_\alpha(T) = \emptyset\}$,

(iii) ogni ramo b di un albero $(T, \lhd)$ è bene ordinato da $\lhd$ e $\mathrm{ot}(b)$ coincide con la sua altezza $\mathrm{ht}(b)$. L'ordinale $\mathrm{ot}(b)$ si dice **lunghezza** del ramo.

Esempi 20.17. (a) Ogni buon ordine è un albero privo di biforcazioni che coincide con il suo unico ramo. Se consideriamo due buoni ordini disgiunti abbiamo un albero con due radici e due rami, ma di nuovo privo di biforcazioni.

(b) Ogni insieme X può essere visto come un albero T di altezza 1, dove $\mathrm{Lev}_0(T) = X$.

(c) Fissato un insieme $X \neq \emptyset$, un **albero su** X è un $T \subseteq X^{<\omega}$ chiuso per segmenti iniziali, cioè tale che se $t \in T$ e $n \in \omega$, allora $t \restriction n \in T$. Se $T \neq \emptyset$ allora la sequenza vuota $\langle\rangle = \emptyset$ appartiene a T ed è l'unica radice dell'albero.

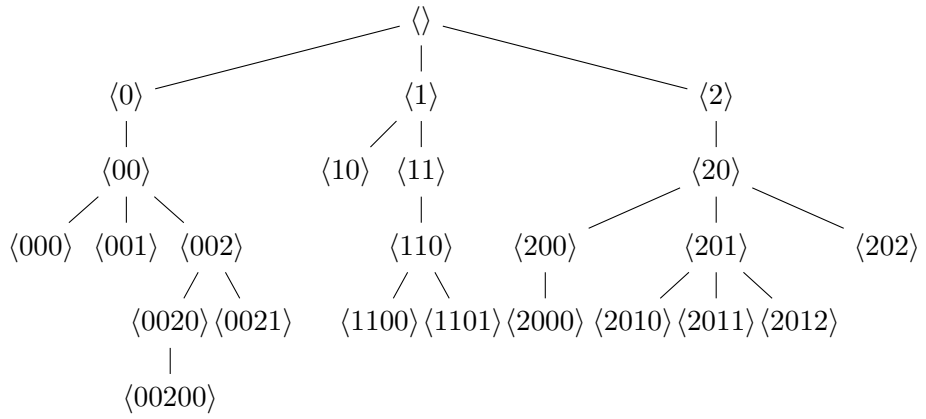
Diremo che un albero T su un ordinale α è **privo di lacune** se

$$s^\frown \langle n\rangle \wedge s^\frown \langle m\rangle \in T \wedge n < m \Rightarrow s^\frown \langle n+1\rangle \in T.$$

Esercizio 20.18. Dimostrare che un albero T su un ordinale α è privo di lacune se e solo se per ogni $t \in T$ l'insieme $\left\{\nu \in \alpha \mid t^\frown \langle\nu\rangle \in T\right\}$ è un ordinale.

Ogni albero finito con un unica radice è isomorfo ad un unico albero privo di lacune su un opportuno $n \in \omega$ (Esercizio 20.28) — per esempio

l'albero del disegno (20.4) è isomorfo all'albero su $3 = \{0, 1, 2\}$



Un **albero etichettato** su un insieme $S \neq \emptyset$ è costituito da un albero T su ω finito e privo di lacune e da una funzione $L\colon T \to S$, detta **etichettatura dell'albero** T.

Un albero etichettato su $\langle S, a\rangle$ dove $a\colon S \to \omega$ è un albero etichettato su S tale che per ogni $t \in T$

$$a(L(t)) = |\{s \mid s \text{ è un successore immediato di } t\}|\,.$$

Per esempio l'albero della Figura 2 a pagina 21 può essere visto come un albero etichettato prendendo l'albero su 3 descritto qui sopra ed etichettandolo così: $L(\langle\rangle) = h$, $L(\langle 0\rangle) = f$, $L(\langle 1\rangle) = g$, $L(\langle 2\rangle) = f$, etc.

20.F. Il Lemma di König. Concludiamo questa sezione con un risultato fondamentale sugli alberi che si ramificano finitamente, noto come **Lemma di König**.

Lemma 20.19. *Sia $(T, \lhd)$ un albero che si ramifica finitamente e che ha un numero finito di radici. Supponiamo che*

(∗) *esiste $<$ un ordine parziale di T che è un ordine totale su ogni $\mathrm{Lev}_n(T)$, per $n \in \omega$*

Allora

$$T \text{ è infinito} \Leftrightarrow T \text{ ha una catena infinita.}$$

Dimostrazione. È sufficiente dimostrare che se T è infinito, allora contiene una catena infinita. È utile introdurre la seguente

Definizione 20.20. Sia $(T, \lhd)$ un albero e $t \in T$. L'insieme

$$T_{[t]} = \{u \in T \mid t \trianglelefteq u\}$$

con l'ordinamento $\lhd$ è un albero e si dice **albero indotto da T sopra t.**

Per ricorsione su n costruiremo $t_n \in \mathrm{Lev}_n(T)$ tali che

(A) $t_n \lhd t_{n+1}$ e

(B) $T_{[t_n]}$ è infinito.

Poiché $T = \bigcup \left\{ T_{[t]} \mid t \in \mathrm{Lev}_0(T) \right\}$ è infinito e $\mathrm{Lev}_0(T)$, l'insieme delle radici di T, è finito, c'è un $t_0 \in \mathrm{Lev}_0(T)$ per cui $T_{[t_0]}$ è infinito. Supponiamo di aver costruito t_i per $i \leq n$ e che (A) e (B) siano soddisfatte: poiché

$$T_{[t_n]} = \{t_n\} \cup \bigcup_{s \in S_n} T_{[s]},$$

dove $S_n = \{s \in T \mid s \text{ è un successore immediato di } t_n\}$, e poiché S_n è finito per ipotesi, allora per (B) c'è un $t_{n+1} \in S_n$ tale che $T_{[t_{n+1}]}$ è infinito. Quindi (A) e (B) sono verificate da t_{n+1}.

La scelta dei t_n non richiede AC. Infatti $\mathrm{Lev}_0(T)$ e gli S_n sono finiti e quindi bene ordinati da $<$, quindi possiamo sempre scegliere t_n come il $<$-minimo nodo che soddisfa le nostre richieste. □

Corollario 20.21. *Assumiamo T sia un albero bene ordinabile di altezza ω, che si ramifica finitamente, e che abbia un numero finito di radici. Allora T ha un ramo infinito.*

Il Teorema 14.18 mostra che ${}^{<\omega}X$ è bene ordinabile se X lo è. Quindi

Corollario 20.22. *Se $T \subseteq X^{<\omega}$ è un albero che si ramifica finitamente su un insieme bene ordinabile X, allora*

$$T \text{ è infinito} \Leftrightarrow T \text{ ha un ramo infinito.}$$

Esercizi

Sia $\varphi\colon S^{<\omega} \to \mathbb{Z}$ la funzione

$$\varphi(\langle s_1 s_2 \dots s_n \rangle) = \varphi(s_1) + \dots + \varphi(s_n).$$

Esercizio 20.23. Sia $u = \langle s_1, \dots, s_n \rangle$ dove $s_1, \dots, s_n \in S^{<\omega}$.

(i) Dimostrare per induzione su k che se $u \in \mathrm{Expr}_k(S, a)$ allora $\varphi(u) = -1$ e $\varphi(\langle s_1, \dots, s_m \rangle) \geq 0$ se $m < n$.

(ii) Dimostrare per induzione su n che se $\varphi(u) = -1$ e $\varphi(\langle s_1, \dots, s_m \rangle) \geq 0$ per ogni $m < n$, allora $u \in \mathrm{Expr}_k(S, a)$.

Esercizio 20.24. Dimostrare che

$$\mathrm{ht}(w) = \max\{\mathrm{ht}(z) \mid z \sqsubset w\} + 1.$$

Esercizio 20.25. Dimostrare che $\mathrm{LTr}(S, a)$ è il più piccolo insieme T contenente $\{\langle s \rangle \mid s \in S \wedge a(s)\}$ tale che $t_1, \dots, t_m \in T \wedge s \in S \wedge a(s) = m \Rightarrow \langle s, t_1, \dots, t_m \rangle \in T$.

Esercizio 20.26. Verificare che $\mathrm{Expr}(S, a)$ e $\mathrm{LTr}(S, a)$ sono in biezione mediante una mappa che preserva le altezze.

Esercizio 20.27. Dimostrare che l'insieme degli alberi etichettati su $\langle S, a\rangle$ è

$$\mathrm{LTr}(S,a) = \bigcup_n \mathrm{LTr}_n(S,a)$$

dove

$$\mathrm{LTr}_0 = \{\langle s\rangle \mid s \in S \wedge a(s) = 0\}$$
$$\mathrm{LTr}_{n+1} = \mathrm{LTr}_n \cup \{\langle s, t_1, \dots, t_m\rangle \mid s \in S \wedge a(s) = m \wedge t_1, \dots, t_m \in \mathrm{LTr}_n\}.$$

La funzione **altezza** $\mathrm{ht}\colon \mathrm{LTr} \to \omega$ è definita da

$$\mathrm{ht}(t) = \min\{n \in \omega \mid t \in \mathrm{LTr}_n\}$$

È facile verificare che c'è una biezione

$$\Phi\colon \mathrm{Expr}(S,a) \to \mathrm{LTr}(S,a)$$

che preserva le altezze e che quindi dimostra che $\mathrm{Expr}_n(S,a)$ è in biezione con $\mathrm{LTr}_n(S,a)$ (Esercizio 20.26). Ne segue che tanto Expr quanto LTr sono formalizzazioni equivalenti del concetto intuitivo di espressione di $\langle S, a\rangle$.

Esercizio 20.28. Dimostrare che ogni albero finito con un unica radice è isomorfo ad un albero privo di lacune su ω.

Esercizio 20.29. Dimostrare che:

(i) c'è una sequenza $s \in 2^{\mathbb{N}}$ che è **universale** nel senso che ogni $u \in 2^{<\mathbb{N}}$ occorre in s, cioè $\forall u \in 2^{<\mathbb{N}}\, \exists n \left(s \restriction n^\frown u \subseteq s\right)$;

(ii) se $s \in 2^{\mathbb{N}}$ è universale, allora $(\mathbb{Z}, E)$ è un grafo aleatorio numerabile, dove $n\ E\ m \Leftrightarrow s(|n - m|) = 1$;

(iii) $\mathrm{Aut}(\mathrm{R}_\omega)$ ha elementi di ordine 2 e elementi di ordine infinito.

21. Spazi Polacchi

21.A. Completamento di spazi metrici. Una funzione $j\colon \langle X_1, d_1\rangle \to \langle X_2, d_2\rangle$ è un'**immersione isometrica** se $d_1(a,b) = d_2(j(a), j(b))$ per ogni $a, b \in X_1$. Un'immersione isometrica è sempre iniettiva; quando è anche surieitiva, si dice un'**isometria** ovvero un **isomorfismo di spazi metrici**. Un **completamento** di uno spazio metrico $\langle X, d\rangle$ è uno spazio metrico completo $\langle \hat{X}, \hat{d}\rangle$ con un'immersione isometrica $j\colon X \to \hat{X}$ tale che $\operatorname{ran} j$ è denso in $\hat{X}$. Un modo per costruire un completamento consiste nel prendere come $\hat{X}$ il quoziente

$$\{(x_n)_n \in X^{\mathbb{N}} \mid (x_n)_n \text{ è una successione di Cauchy in } \langle X, d\rangle\}/\!\sim$$

dove

$$(x_n)_n \sim (y_n)_n \Leftrightarrow \forall \varepsilon > 0\, \exists N\, \forall n, m > N\, d(x_n, y_m) < \varepsilon.$$

Allora

$$\hat{d}([(x_n)_n], [(y_n)_n]) = \lim_{n\to\infty} d(x_n, y_n)$$

è una distanza su $\hat{X}$, la mappa $j\colon X \to \hat{X}$ che manda un punto $x \in X$ nella successione costante $\langle x, x, x, \dots\rangle$, è un'immersione isometrica, e $\operatorname{ran} j$ è denso in $\langle \hat{X}, \hat{d}\rangle$. Se $j_1\colon \langle X, d\rangle \to \langle \hat{X}_1, \hat{d}_1\rangle$ e $j_2\colon \langle X, d\rangle \to \langle \hat{X}_2, \hat{d}_2\rangle$ sono completamenti, allora definiamo $f\colon \hat{X}_1 \to \hat{X}_2$ così: dato $\hat{x} \in \hat{X}_1$ scegliamo

una successione $(x_n)_n$ in X tale che $j_1(x_n) \to \hat{x}$, così che $(j_1(x_n))_n$ è una successione di Cauchy in $\hat{X}_1$, quindi $(x_n)_n$ è una successione di Cauchy in X, quindi $(j_2(x_n))_n$ iè una successione di Cauchy in $\hat{X}_2$, e quindi converge ad un punto $f(\hat{x}) \in \hat{X}_2$. Quindi $f\colon \langle \hat{X}_1, \hat{d}_1\rangle \to \langle \hat{X}_2, \hat{d}_2\rangle$ è un'isometria. Abbiamo quindi dimostrato

Teorema 21.1. *Assumiamo* AC_ω*. Il completamento di uno spazio metrico esiste ed è unico a meno di isomorfismi.*

Identificheremo sempre lo spazio metrico X con la sua copia isomorfa $j[X] \subseteq \hat{X}$. Notiamo che se $\langle X, d\rangle$ contiene un sottoinsieme denso D di taglia κ, allora D è anche denso in $\hat{X}$; in particolare, il completamento di uno spazio metrico separabile è separabile.

Lo spazio metrico $\mathbb{R}$ può essere ottenuto come il completamento di $\mathbb{Q}$ con la metrica euclidea $d(r,s) = |r-s|$.

21.A.1. *Intermezzo: la topologia prodotto.* Siano $(Y_i, \mathcal{T}_i)$ $(i \in I)$ degli spazi topologici e X un insieme. La **topologia su X indotta dalle funzioni** $F_i\colon X \to Y_i$ è la più piccola topologia $\mathcal{T}$ che rende continue le F_i, cioè è la topologia che ha per sottobase $\left\{F_i^{-1}[U] \mid i \in I \wedge U \in \mathcal{T}_i\right\}$.

La **topologia prodotto** o **topologia di Tychonoff** su $\bigtimes_{i\in I} Y_i$ è la topologia indotta dalle funzioni proiezione $p_j\colon \bigtimes_{i\in I} Y_i \to Y_j$; gli aperti di base sono della forma

$$U_{i_1} \times \cdots \times U_{i_n} \times \bigtimes_{j\in I\setminus\{i_1,\dots,i_n\}} Y_j,$$

con $\{i_1, \dots, i_n\} \subseteq I$ e $U_{i_j} \in \mathcal{T}_{i_j}$.

Esercizio 21.2. Dimostrare che

(i) la topologia prodotto su $Y_0 \times Y_1$ ha per base gli insiemi della forma $U \times V$, con U aperto in Y_0 e V aperto in Y_1;

(ii) se gli Y_i sono di Hausdorff, anche $\bigtimes_{i\in I} Y_i$ lo è.

Uno spazio si dice quasi-compatto se da ogni ricoprimento aperto si può estrarre un sotto-ricoprimento finito; uno spazio quasi-compatto e di Hausdorff si dice compatto. Il risultato centrale sulla topologia prodotto è il Teorema di Tychonoff 25.9 che dimostreremo nella Sezione 25.B.1: se assumiamo AC allora il prodotto di spazi quasi-compatti è quasi-compatto.

21.B. Schemi di Cantor. La costruzione dell'insieme di Cantor $E_{1/3}$ della Sezione 10.F.1 può essere generalizzata. Uno **schema di Cantor** in uno spazio metrico completo $\langle X, d\rangle$ è una funzione $\langle (x_s, r_s) \mid s \in {}^{<\omega}2\rangle$ con le seguenti proprietà: per ogni $s \in {}^{<\omega}2$

- $x_s \in X$ e $r_s \in \mathbb{R}_+$,

- $\mathrm{Cl}\,\mathrm{B}(x_{s^\frown\langle i\rangle}; r_{s^\frown\langle i\rangle}) \subseteq \mathrm{B}(x_s; r_s)$, per ogni $i \in 2$,
- $\mathrm{B}(x_{s^\frown\langle 0\rangle}; r_{s^\frown\langle 0\rangle}) \cap \mathrm{B}(x_{s^\frown\langle 1\rangle}; r_{s^\frown\langle 1\rangle}) = \emptyset$,

e tale che $\lim_{n\to\infty} r_{z\restriction n} = 0$ per ogni $z \in {}^\omega 2$. È immediato verificare che

$$s \subset t \Rightarrow \mathrm{B}(x_s; r_s) \supset \mathrm{B}(x_t; r_t). \tag{21.1}$$

Supponiamo invece che $s, t \in 2^{<\mathbb{N}}$ siano inconfrontabili, vale a dire $s \not\subseteq t$ e $s \not\supseteq t$. Sia $\bar n$ tale che $s \restriction \bar n = t \restriction \bar n$, ma $s(\bar n) \neq t(\bar n)$. Allora $\mathrm{B}(x_{s\restriction\bar n+1}; r_{s\restriction\bar n+1}) \cap \mathrm{B}(x_{t\restriction\bar n+1}; r_{t\restriction\bar n+1}) = \emptyset$ e quindi $\mathrm{B}(x_s; r_s) \cap \mathrm{B}(x_t; r_t) = \emptyset$ per (21.1).

Possiamo quindi definire una funzione continua $f\colon {}^\omega 2 \to X$, $\{f(z)\} = \bigcap_n \mathrm{B}(x_{z\restriction n}; r_{z\restriction n})$.

Teorema 21.3. *Sia $\langle X, d\rangle$ uno spazio separabile, metrico completo, privo di punti isolati e non vuoto. Allora c'è una funzione continua e iniettiva $f\colon 2^{\mathbb{N}} \rightarrowtail X$. In particolare: X contiene una copia omeomorfa dell'insieme di Cantor.*

Dimostrazione. Sia $E = \{e_n \mid n \in \omega\}$ denso in X. Costruiamo induttivamente dei numeri reali r_s e dei punti $x_s \in X$ ($s \in 2^{<\mathbb{N}}$), tali che

(i) $0 < r_s \leq 2^{-\mathrm{lh}(s)}$,

(ii) $\mathrm{Cl}(\mathrm{B}(x_{s^\frown\langle i\rangle}; r_{s^\frown\langle i\rangle})) \subseteq \mathrm{B}(x_s, r_s)$, per $i = 0, 1$,

(iii) $\mathrm{Cl}\big(\mathrm{B}(x_{s^\frown\langle 0\rangle}; r_{s^\frown\langle 0\rangle})\big) \cap \mathrm{Cl}\Big(\mathrm{B}(x_{s^\frown\langle 1\rangle}; r_{s^\frown\langle 1\rangle})\Big) = \emptyset$.

Poniamo $x_\emptyset \in X$ e $r_\emptyset = 1$. Dato x_s e r_s è facile verificare che $E \cap \mathrm{B}(x_s, r_s)$ è infinito, quindi possiamo scegliere due punti distinti $x_{s^\frown\langle 0\rangle}$ e $x_{s^\frown\langle 1\rangle}$ in questo insieme. (Prediamo, per esempio e_k ed e_h, dove k e h sono i primi due indici i tali che $e_i \in E \cap \mathrm{B}(x_s, r_s)$.) Prendiamo $r_{s^\frown\langle i\rangle}$ ($i = 0, 1$) sufficientemente piccoli in modo che valgano (i)–(iii).

Per ogni $y \in 2^{\mathbb{N}}$ considero la successione $(x_{y\restriction n})_n$. Poiché $\mathrm{B}(x_{y\restriction n}, r_{y\restriction n}) \supseteq \mathrm{B}(x_{y\restriction n+1}, r_{y\restriction n+1})$ per (ii),

$$\forall k \geq n\, (x_{y\restriction k} \in \mathrm{B}(x_{y\restriction n}, r_{y\restriction n}))\,. \tag{21.2}$$

Quindi la successione $(x_{y\restriction n})_n$ è di Cauchy e sia

$$f(y) = \lim_n x_{y\restriction n}$$

Per (21.2) $f(y) \in \mathrm{Cl}(\mathrm{B}(x_{y\restriction n}, r_{y\restriction n}))$ per ogni n e quindi

$$f(y) \in \bigcap_n \mathrm{Cl}(\mathrm{B}(x_{y\restriction n}, r_{y\restriction n})) = \bigcap_n \mathrm{B}(x_{y\restriction n}, r_{y\restriction n}),$$

dove la seconda uguaglianza segue da (ii). Se $y, z \in 2^{\mathbb{N}}$ sono distinti, sia n tale che $y \restriction n = z \restriction n$ e $y(n) \neq z(n)$. Allora $f(y) \in \mathrm{Cl}(\mathrm{B}(x_{y\restriction n}, r_{y\restriction n}))$ e $f(z) \in \mathrm{Cl}(\mathrm{B}(x_{z\restriction n}, r_{z\restriction n}))$ e quindi $f(y) \neq f(z)$ per (iii). In altre parole, la funzione $f\colon 2^{\mathbb{N}} \to X$ è iniettiva. Resta da dimostrare che è continua. Fissato

un $y \in 2^{\mathbb{N}}$ ed un n, basta trovare un k tale che se $z \restriction k = y \restriction k$, allora $d(x_{z\restriction k}, x_{y\restriction k}) < 2^{-n}$. È facile verificare che $k = n$ funziona. □

21.C. $\mathbb{R}$ ed ω_1. Abbiamo visto due esempi di insiemi più che numerabili: l'insieme dei reali $\mathbb{R}$ ed il primo ordinale più che numerabile ω_1 (pag.287). È naturale chiedersi in che relazione siano questi insiemi: sono equipotenti? c'è qualche iniezione tra di loro? oppure qualche suriezione?

Per la (12.4) e poiché $\mathscr{P}(\omega)$ è equipotente ad $\mathbb{R}$ si ha che

$$\mathbb{R} \twoheadrightarrow \omega_1.$$

Tutte le altre possibilità valgono solo sotto opportune ipotesi. Più precisamente:

- Se $\omega_1 \rightarrowtail \mathbb{R}$ allora è possibile costruire certi sottoinsiemi "patologici" di $\mathbb{R}$ (insiemi che non sono Lebesgue misurabili, che non hanno la proprietà di Baire, etc. — si veda la Sezione 22 per le definizioni di questi concetti).
- Se $\mathbb{R}$ è bene ordinabile allora è equipotente ad un ordinale più che numerabile e quindi $|\omega_1| \leq |\mathbb{R}|$, cioè $\omega_1 \rightarrowtail \mathbb{R}$.
- Se $\mathbb{R} \rightarrowtail \omega_1$, allora $\mathbb{R}$ è bene ordinabile ed essendo ω_1 il primo ordinale più che numerabile, ne segue che ω_1 è equipotente ad $\mathbb{R}$.
- Se $f\colon \omega_1 \twoheadrightarrow \mathbb{R}$ allora $\mathbb{R}$ è bene ordinabile (Esercizio 12.28) e $g\colon \mathbb{R} \to \omega_1$

  $$g(x) = \min\{\alpha \mid f(\alpha) = x\}$$

  è iniettiva e quindi ω_1 è equipotente ad $\mathbb{R}$.

L'affermazione '$\mathbb{R}$ è bene ordinabile' è conseguenza dell'assioma della scelta AC, ma non è discende dagli assiomi di MK o di ZF e un discorso analogo vale per l'affermazione '$\omega_1 \rightarrowtail \mathbb{R}$'. L'affermazione che $\mathbb{R}$ e ω_1 sono equipotenti è nota come **ipotesi del continuo** e verrà esaminata nella Sezione 16.

Esercizi

Esercizio 21.4. Dimostrare che

(i) $\langle {}^{\omega}2, <_{\text{lex}}\rangle$ è omeomorfo allo spazio di Cantor;

(ii) $\langle {}^{\omega}\omega, <_{\text{lex}}\rangle$ è isomorfo (e quindi omeomorfo) a $\langle [0;1), <\rangle$. In particolare$\langle {}^{\omega}\omega, <_{\text{lex}}\rangle$ non è omeomorfo allo spazio di Baire.

Esercizio 21.5. Fissiamo un ordinale $0 < \xi < \omega_1$ e sia $<$ l'ordinamento lessicografico su ${}^{<\omega}\xi$, cioè

$$s < t \Leftrightarrow \exists u \in {}^{<\omega}\xi\,(u \neq \emptyset \wedge s^\frown u = t) \vee \exists u, v, w \in {}^{<\omega}\xi\,\exists \alpha, \beta \in \xi\,(s = u^\frown \langle \alpha \rangle {}^\frown v \wedge t = u^\frown \langle \beta \rangle {}^\frown w \wedge \alpha < \beta).$$

Sia $I = {}^{<\omega}\xi \setminus \left\{ s^\frown \langle 0\rangle \mid s \in {}^{<\omega}\xi \right\}$ l'insieme delle sequenze che non terminano con uno 0. Per $s \in {}^{<\omega}\xi$ definiamo s^- l'unico elemento di I tale che $s = s^-{}^\frown 0^{(n)}$ per qualche $n < \omega$, dove

$$0^{(n)} = \underbrace{\langle 0, \ldots, 0\rangle}_{n}.$$

(i) Dimostrare che se $s = s^-{}^\frown 0^{(n)}$ e $t = t^-{}^\frown 0^{(m)}$ allora

$$s < t \Leftrightarrow s^- < t^- \vee (s^- = t^- \wedge n < m).$$

(ii) Dimostrare che $\langle I, <\rangle$ è isomorfo a $\mathbb{Q} \cap [0;1)$.

(iii) Concludere che $\left\langle {}^{<\omega}\xi, < \right\rangle$ è isomorfo a $(\mathbb{Q} \cap [0;1)) \times \omega$ con l'ordinamento prodotto.

(iv) Descrivere esplicitamente un isomorfismo tra $\langle {}^{<\omega}2, <\rangle$ e $\langle {}^{<\omega}3, <\rangle$.

Esercizio 21.6. Define the operation of addition and multiplication, and the order relation on $\hat{\mathbb{Q}}$, the completion of $\mathbb{Q}$ with the Euclidean distance, and show that the resulting structure is isomorphic (as ordered field) and homeomorphic (as a topological space) to the real line $\mathbb{R}$ defined in Section **??** by means of Dedekind sections.

Esercizio 21.7. Dimostrare la seguente estensione del Teorema 21.3:

> *Sia C un chiuso di uno spazio metrico completo e separabile e sia $P \cup S$ la sua decomposizione in una parte perfetta P ed una parte sparsa S (Teorema 10.39). Allora $P = \emptyset$ oppure c'è un'iniezione continua $2^{\mathbb{N}} \rightarrowtail P$.*
>
> *Quindi, in uno spazio metrico completo e separabile, i chiusi sono numerabili o sono equipotenti ad $\mathbb{R}$.*

Nel prossimo esercizio costruiremo una suriezione continua da $2^{\mathbb{N}}$ (e quindi da $E_{1/3}$) su $[0;1]$.

Esercizio 21.8. Dimostrare che la funzione $\Psi\colon 2^{\mathbb{N}} \to [0;1]$

$$\Psi(x) = \sum_{n=0}^{\infty} \frac{x(n)}{2^{n+1}}$$

- è ben definita (vale a dire: la serie converge),
- è suriettiva,
- $x \leq_{\text{lex}} y \Rightarrow \Psi(x) \leq \Psi(y)$,
- se $x <_{\text{lex}} y$ e $\Psi(x) = \Psi(y)$, allora $x = s^\frown \langle 0, 1, 1, \ldots\rangle$ e $y = s^\frown \langle 1, 0, 0, \ldots\rangle$.

Concludere che Ψ è continua.

Esercizio 21.9. Dimostrare che esistono suriezioni continue $[0;1] \twoheadrightarrow [0;1]^n$ ($n \in \mathbb{N}$) e $[0;1] \twoheadrightarrow [0;1]^{\mathbb{N}}$. (Nel caso $n = 2$ la funzione si dice **curva di Peano**.)

Esercizio 21.10. Dimostrare che se la funzione

$$X \to \mathbb{R}^{\mathbb{N}} \qquad x \mapsto \langle d(x, q_n) \mid n \in \mathbb{N}\rangle$$

definita nella Sezione 10.G.3 è un omeomorfismo di X sulla sua immagine e che se d è una metrica completa su X, allora l'immagine è un chiuso di $\mathbb{R}^{\mathbb{N}}$. Concludere che, a meno di omeomorfismi, tutti gli spazi separabili, metrici completi sono dei chiusi di $\mathbb{R}^{\mathbb{N}}$.

Esercizio 21.11. Dimostrare che $\mathbb{R} \twoheadrightarrow \mathscr{P}_{\omega_1}(\mathbb{R})$ e $\mathbb{R} \rightarrowtail \mathscr{P}_{\omega_1}(\mathbb{R})$ dove $\mathscr{P}_{\omega_1}(\mathbb{R})$ è l'insieme dei sottoinsiemi numerabili di $\mathbb{R}$ secondo la Definizione 14.16 di pagina 309. Concludere che se $\mathbb{R}$ è bene ordinabile, allora $|\mathbb{R}| = |\mathscr{P}_{\omega_1}(\mathbb{R})|$.

Esercizio 21.12. Assumere che $\mathbb{R}$ è bene ordinabile e concludere che l'insieme delle funzioni monotone da $\mathbb{R}$ in sé stesso è equipotente ad $\mathbb{R}$.

Note e osservazioni

L'Esercizio 21.5 è tratto da [**Boo88**].

22. Forme deboli dell'Assioma di Scelta

Richiamiamo dalla Sezione 14.A.1 che $\mathsf{AC}_\omega(X)$ è l'enunciato

> per ogni successione $(A_n)_n$ di sottoinsiemi non vuoti di X c'è una successione $(a_n)_n$ di elementi di X tali che $\forall n\ (a_n \in A_n)$.

Se $\alpha_n < \omega_1$, allora $\sup\{\alpha_n \mid n < \omega\} = \bigcup_n \alpha_n < \omega_1$ per il Teorema 14.2 e analizzando la dimostrazione si vede che è sufficiente assumere $\mathsf{AC}_\omega(\mathbb{R})$: per ogni n scegliamo[2] un $R_n \subseteq \omega \times \omega$ tale che $\langle \mathrm{fld}(R_n), R_n\rangle$ è un buon ordine di tipo α_n. Da R_n possiamo ricostruire la funzione $f_n \colon \alpha_n \rightarrowtail \omega$ e la dimostrazione procede come prima. Abbiamo quindi dimostrato:

Teorema 22.1. $\mathsf{AC}_\omega(\mathbb{R})$ *implica che ogni successione* $\langle \alpha_n \mid n < \omega\rangle$ *in* ω_1 *è superiormente limitata in* ω_1*, cioè* ω_1 *è regolare.*

Esercizio 22.2. Sia κ un cardinale infinito e siano X_α tali che $|X_\alpha| \leq \kappa$ per ogni $\alpha < \kappa$. Dimostrare che AC implica che $|\bigcup_{\alpha<\kappa} X_\alpha| \leq \kappa$.

Un'altra forma debole dell'Assioma di Scelta è data dall'**Assioma delle Scelte Dipendenti**. Per ogni insieme $X \neq \emptyset$, $\mathsf{DC}(X)$ asserisce che:

> Se R è una relazione su X tale che $\forall x \exists y\,(x\ R\ y)$, allora per ogni $x_0 \in X$ c'è una $f \in {}^\omega X$ tale che $f(0) = x_0$ e $\forall n\,(f(n)\ R\ f(n+1))$.

Come per l'Assioma delle Scelte numerabili, $\mathsf{DC}(X)$ è dimostrabile quando X è bene ordinabile.

Esercizio 22.3. Dimostrare che $X \twoheadrightarrow Y \wedge \mathsf{DC}(X) \Rightarrow \mathsf{DC}(Y)$.

Proposizione 22.4. $\mathsf{AC} \Rightarrow \mathsf{DC} \Rightarrow \mathsf{AC}_\omega$.

Dimostrazione. Cominciamo col dimostrare che DC è conseguenza di AC. Sia X un insieme e $R \subseteq X \times X$ tale che $\forall x \exists y\,(x\ R\ y)$. Fissiamo un $x_0 \in X$ e una funzione di scelta $C \colon \mathscr{P}(X) \setminus \{\emptyset\} \to X$. Per ricorsione definiamo la funzione $f \colon \omega \to X$ ponendo $f(0) = x_0$ e

$$f(n+1) = C\left(\{y \in X \mid f(n)\ R\ y\}\right).$$

È immediato verificare che la funzione f soddisfa DC.

[2] $R_n \in \mathscr{P}(\omega \times \omega) \approx \mathbb{R}$, per cui $\mathsf{AC}_\omega(\mathbb{R})$ è sufficiente.

Per verificare che $\mathsf{DC} \Rightarrow \mathsf{AC}_\omega$ fissiamo una famiglia $\{A_n \mid n \in \omega\}$ di insiemi non vuoti. Sia $X = \bigcup_n (A_n \times \{n\})$ e sia $R \subseteq X \times X$ la relazione

$$(a, n)\ R\ (b, m) \quad \Leftrightarrow \quad m = n + 1.$$

Fissiamo un elemento $a_0 \in A_0$: per DC c'è una funzione $f\colon \omega \to X$ tale che $f(0) = (a_0, 0)$ e $f(n)\ R\ f(n+1)$ per tutti gli n. La funzione

$$g(n) = \text{la prima componente della coppia ordinata } f(n)$$

è la funzione cercata. □

È stato dimostrato che le implicazioni nella Proposizione 22.4 non possono essere rovesciate.

Esercizio 22.5. Assumiamo DC. Dimostrare che una relazione irriflessiva R su un insieme X è ben-fondata se e solo se non esistono sequenze $\langle x_n \mid n < \omega \rangle$ tali che $x_{n+1}\ R\ x_n$, per tutti gli n.

22.A. La misura di Lebesgue. Una famiglia di insiemi $\mathcal{S} \subseteq \mathscr{P}(X)$ è una **σ-algebra** se è una sub-algebra di Boole di $\mathscr{P}(X)$ e se è numerabilmente completa, cioè $\bigcup \mathcal{A} \in \mathcal{S}$ per ogni $\mathcal{A} \subseteq \mathcal{S}$ numerabile. La σ-algebra generata da $\mathcal{A}$ è

$$\bigcap \{\mathcal{S} \subseteq \mathscr{P}(X) \mid \mathcal{S} \text{ è una } \sigma\text{-algebra e } \mathcal{A} \subseteq \mathcal{S}\}$$

(È facile verificare che questa è proprio una σ-algebra.) Questa è una definizione *dall'alto*, ma se si assume $\mathsf{AC}_\omega(\mathbb{R})$, è possibile dare una descrizione alternativa *dal basso*:

$$\begin{aligned} \mathcal{S}_0 &= \mathcal{A} \cup \breve{\mathcal{A}} \cup \{\emptyset, X\} \\ \mathcal{S}_{\alpha+1} &= \{\bigcup_{n\in\omega} A_n \mid A_n \in \mathcal{S}_\alpha \cup \breve{\mathcal{S}}_\alpha\} \\ \mathcal{S}_\lambda &= \bigcup_{\alpha<\lambda} \mathcal{S}_\alpha \qquad\qquad (\lambda \text{ limite}), \end{aligned}$$

dove $\breve{\mathcal{B}} \stackrel{\text{def}}{=} \{X \setminus B \mid B \in \mathcal{B}\}$, per ogni $\mathcal{B} \subseteq \mathscr{P}(X)$. È facile verificare per induzione su α che

- $\beta < \alpha \Rightarrow \mathcal{S}_\beta \cup \breve{\mathcal{S}}_\beta \subseteq \mathcal{S}_\alpha$ e
- $\mathcal{S}_\alpha$ è contenuto nella σ-algebra generata da $\mathcal{A}$.

Per costruzione $\mathcal{S}_{\omega_1}$ è non vuoto, contiene $\mathcal{A}$ ed è chiuso per complementi: se $A \in \mathcal{S}_{\omega_1}$ allora $A \in \mathcal{S}_\alpha$, quindi $X \setminus A \in \breve{\mathcal{S}}_\alpha \subseteq \mathcal{S}_{\alpha+1}$. Inoltre, data una successione di insiemi $A_n \in \mathcal{S}_{\omega_1}$, $(n \in \omega)$, scegliamo degli ordinali $\alpha_n \in \omega_1$ tali che $A_n \in \mathcal{S}_{\alpha_n}$: per il Teorema 22.1 esiste $\alpha < \omega_1$ tale che $\{A_n \mid n \in \omega\} \subseteq \mathcal{S}_\alpha$ e quindi $\bigcup_n A_n \in \mathcal{S}_{\alpha+1}$. Quindi $\mathcal{S}_{\omega_1}$ è una σ-algebra ed è la σ-algebra generata da $\mathcal{A}$.

Se X è un insieme dotato di una topologia $\mathcal{T}$, la σ-algebra generata da $\mathcal{T}$ è la σ-algebra dei **Boreliani**

$$\textsc{Bor}(X, \mathcal{T}).$$

Quando la topologia $\mathcal{T}$ è chiara dal contesto scriveremo semplicemente $\textsc{Bor}(X)$.

Uno **spazio di misura** è una tripla $\langle X, \mathcal{S}, \mu\rangle$ tale che

- $\mathcal{S}$ è una σ-algebra su X
- $\mu\colon \mathcal{S} \to [0; +\infty]$ soddisfa
  (a) $\mu(\emptyset) = 0$,
  (b) se $A_n \in \mathcal{S}$ sono a due a due disgiunti, allora

$$\mu\Big(\bigcup_n A_n\Big) = \sum_{n=0}^{\infty} \mu(A_n). \tag{22.1}$$

La serie (22.1) è a termini positivi, quindi la sua somma è ben definita. Gli insiemi in $\mathcal{S}$ si dicono **$\mathcal{S}$-misurabili**, o misurabili secondo $\mathcal{S}$, mentre la funzione μ si dice **misura**. La proprietà (22.1) si dice **σ-additività**.

Esercizio 22.6. Dimostrare che per ogni misura μ,

$$A \subseteq B \Rightarrow \mu(A) \leq \mu(B)$$
$$\mu(A \cup B) = \mu(A) + \mu(B) - \mu(A \cap B)$$

Osserviamo che la nozione di spazio di misura è ridondante, dato che dalla misura μ possiamo ricavare la σ-algebra $\mathcal{S} = \mathrm{dom}(\mu)$ e da questa si ricava l'insieme $X = \bigcup \mathcal{S}$. Tuttavia spesso non si distingue tra una misura μ ed una sua restrizione ad una sotto-σ-algebra, per cui la nozione di spazio di misura risulta molto comoda. Uno spazio di misura $\langle X, \mathcal{S}, \mu\rangle$ si dice:

spazio di misura completo se

$$\forall A \in \mathcal{S} \forall B \subseteq A\, (\mu(A) = 0 \Rightarrow B \in \mathcal{S} \wedge \mu(B) = 0)\,;$$

spazio di probabilità se $\mu(X) = 1$;

spazio di misura finito se $\mu(X) < \infty$;

spazio di misura σ-finito se esistono $X_n \in \mathcal{S}$ tali che $X = \bigcup_n X_n$ e $\mu(X_n) < \infty$.

La misura μ si dirà, rispettivamente, **misura completa**, **misura di probabilità**, **misura finita**, **misura σ-finita**. Una **misura esterna** su X è una funzione

$$F\colon \mathscr{P}(X) \to [0; +\infty]$$

che soddisfa

(1) $F(\emptyset) = 0$,

(2) $A \subseteq B \Rightarrow F(A) \leq F(B)$,

(3) $F(\bigcup_n X_n) \leq \sum_{n=0}^{\infty} F(X_n)$, per ogni successione $X_n \in \mathcal{S}$, $(n \in \omega)$.

La proprietà (3) si dice **σ-sub-additività**. A dispetto del nome, una misura esterna non è necessariamente una misura. Tuttavia ogni misura esterna induce una misura.

Teorema 22.7 (Carathéodory)**.** *Se F è una misura esterna su X, allora*

$$\mathcal{S} = \{A \subseteq X \mid \forall B \subseteq X\, (F(B \cap A) + F(B \setminus A) \leq F(B))\}$$

è una σ-algebra, $\mu = F \restriction \mathcal{S}$ è una misura e lo spazio $\langle X, \mathcal{S}, \mu\rangle$ è completo.

Per una dimostrazione si veda un qualsiasi testo di teoria della misura, per esempio [**Fre04a**, Theorem 113C].

Diamo ora un cenno su come si definisce la misura di Lebesgue su $\mathbb{R}$. Definiamo $F\colon \mathscr{P}(\mathbb{R}) \to [0;\infty]$

$$F(A) = \inf\{\sum_n (b_n - a_n) \mid A \subseteq \bigcup_{n<\omega} [a_n; b_n)\},$$

dove tacitamente assumiamo che quando si considera l'intervallo semiaperto $[a;b)$ si ha che $b \geq a$. È facile verificare che F verifica le proprietà (1) e (2) della definizione di misura esterna. Per dimostrare la sub-additività, fissiamo un $\varepsilon > 0$ e facciamo vedere che $F(\bigcup_n X_n) \leq \sum_{n=0}^{\infty} F(X_n) + \varepsilon$. Per ogni n scegliamo una famiglia di intervalli semiaperti che ricopre X_n e che approssima $F(X_n)$ a meno di $\varepsilon/2^{n+1}$, cioè

$$X_n \subseteq \bigcup_{i\in\omega} [a_i^{(n)}; b_i^{(n)}) \qquad \text{e} \qquad \sum_{i=0}^{\infty} (b_i^{(n)} - a_i^{(n)}) < F(X_n) + \varepsilon/2^{n+1}. \tag{22.2}$$

Per far questo dobbiamo effettuare ω scelte elementi di $(\mathbb{R}^2)^\omega$ e dato che quest'insieme è equipotente ad $\mathbb{R}$ (Sezione 10.G.1) è sufficiente usare $\mathsf{AC}_\omega(\mathbb{R})$. Scelti gli $[a_i^{(n)}; b_i^{(n)})$ possiamo concludere osservando che $\bigcup_n X_n \subseteq \bigcup_n \bigcup_i [a_i^{(n)}; b_i^{(n)})$ e

$$\sum_{n=0}^{\infty} \sum_{i=0}^{\infty} (b_i^{(n)} - a_i^{(n)}) \leq \sum_{n=0}^{\infty} (F(X_n) + \varepsilon/2^{n+1}) = \sum_{n=0}^{\infty} F(X_n) + \varepsilon.$$

Quindi F è una misura esterna su $\mathbb{R}$. La misura indotta da questa F si dice **misura di Lebesgue** su $\mathbb{R}$ e la si indica con λ, e la σ-algebra data dal teorema di Carathéodory è la famiglia degli **insiemi Lebesgue misurabili** e la si denota con $\textsc{Meas}(\mathbb{R}, \lambda)$ o semplicemente $\textsc{Meas}(\lambda)$. Questa σ-algebra è più grande di $\textsc{Bor}(\mathbb{R})$, la σ-algebra dei Boreliani di $\mathbb{R}$.

La costruzione della misura di Lebesgue può essere ripetuta per $\mathbb{R}^n$, usando invece degli intervalli $[a;b)$ gli insiemi

$$[\boldsymbol{a}; \boldsymbol{b}) \stackrel{\text{def}}{=} \{\boldsymbol{c} \in \mathbb{R}^n \mid a_i \leq c_i < b_i\}$$

dove usiamo la convenzione di denotare la n-upla $(x_1, \dots, x_n) \in \mathbb{R}^n$ con $\boldsymbol{x}$. Analogamente, al posto della lunghezza $(b-a)$ si considera il volume $\prod_{i=1}^n (b_i - a_i)$. La misura e la σ-algebra corrispondenti si denotano con λ^n e $\textsc{Meas}(\mathbb{R}^n, \lambda^n)$ o $\textsc{Meas}(\lambda^n)$.

La misura λ^n gode della seguente proprietà: per ogni $A \subseteq \mathbb{R}^n$ Lebesgue misurabile,

$$\begin{aligned} \lambda^n(A) &= \sup\{\lambda^n(K) \mid K \subseteq A \wedge K \text{ compatto}\} \\ &= \inf\{\lambda^n(U) \mid U \supseteq A \wedge U \text{ aperto}\} \end{aligned} \tag{22.3}$$

Un sotto-insieme di uno spazio topologico si dice $\mathbf{G}_\delta$ se è intersezione numerabile di aperti e $\mathbf{F}_\sigma$ se è unione numerabile di chiusi. Un insieme che sia unione numerabile di compatti si dice $\mathbf{K}_\sigma$.

$$\begin{aligned} \forall A \subseteq \mathbb{R}^n \big[& A \in \textsc{Meas}(\lambda^n) \Leftrightarrow \\ & \exists F \in \mathbf{K}_\sigma \exists G \in \mathbf{G}_\delta \, (F \subseteq A \subseteq G \ \wedge \lambda^n(F) = \lambda^n(G))\big]. \end{aligned} \tag{22.4}$$

Un'altra importante caratteristica della misura di Lebesgue è che è invariante per isometrie, cioè se $\sigma \colon \mathbb{R}^n \to \mathbb{R}^n$ è un'isometria e $A \in \textsc{Meas}(\lambda^n)$, allora $\sigma[A] \in \textsc{Meas}(\lambda^n)$ e $\lambda^n(\sigma[A]) = \lambda^n(A)$.

La misura di Lebesgue sugli intervalli coincide con la lunghezza, cioè se I è un intervallo (aperto, chiuso, semiaperto) di estremi $a < b$, allora $\lambda(I) = b - a$. Ricordiamo che l'insieme $E_{1/3}$ di Cantor (vedi pagina 237) è ottenuto rimuovendo dall'intervallo $[0;1]$ una famiglia numerabile di aperti. La misura del suo complementare in $[0;1]$ è

$$\sum_{n=1}^{\infty} \frac{1}{3^n} = 1$$

quindi $\lambda(E_{1/3}) = 0$. Quindi l'insieme $E_{1/3}$ di Cantor è un esempio di insieme chiuso, più che numerabile, privo di interno e di misura 0.

Argomentando come per la misura di Lebesgue, si dimostra che la funzione $F \colon \mathscr{P}(2^{\mathbb{N}}) \to [0;1]$

$$F(A) = \inf\{\sum_{s \in \mathcal{A}} 2^{-\operatorname{lh}(s)} \mid \mathcal{A} \subseteq 2^{<\mathbb{N}} \wedge \bigcup \mathcal{A} \supseteq A\}$$

è una misura esterna e quindi risulta definita uno spazio di misura $\left\langle 2^{\mathbb{N}}, \textsc{Meas}, \mu \right\rangle$. Per verificare la sub-additività di F, in analogia con quanto fatto in (22.2), dati $X_n \subseteq 2^{\mathbb{N}}$ si scelgono $\mathcal{A}_n \subseteq 2^{<\mathbb{N}}$ tali che $F(X_n) \leq \sum_{s \in \mathcal{A}_n} 2^{-\operatorname{lh}(s)} + \varepsilon/2^{n+1}$ e poiché $\mathcal{A}_n$ è un elemento di $\mathscr{P}(2^{<\mathbb{N}})$ che è equipotente ad $\mathbb{R}$, tale scelta è lecita per $\mathsf{AC}_\omega(\mathbb{R})$. È facile verificare che è di probabilità e che $\mu(\boldsymbol{N}_s) = 2^{-\operatorname{lh}(s)}$.

Osservazione 22.8. La misura μ si dice **misura di Cantor** o anche **misura di Lebesgue sull'insieme di Cantor**. La scelta di chiamare μ misura di Lebesgue può apparire per lo meno bizzarra, visto che $2^{\mathbb{N}}$ viene spesso

identificato con $E_{1/3}$ e $\mu(2^{\mathbb{N}}) = 1$, mentre $\lambda(E_{1/3}) = 0$. Tuttavia $2^{\mathbb{N}}$ è anche identificabile con (cioè omeomorfo a) un sotto-insieme di $[0;2]$ che ha λ-misura uguale ad 1 (Esercizio 22.21). Un sottoinsieme di $\mathbb{R}$ omeomorfo a $2^{\mathbb{N}}$ può essere ottenuto generalizzando la costruzione di $E_{1/3}$ in più direzioni. Per esempio possiamo rimpiazzare l'intervallo $[0;1]$ con un generico intervallo chiuso J e scegliere un coefficiente $r_n \in (0;1)$ da utilizzare al passo n della costruzione, cioè definiamo

$$\text{Cantor}(J;(r_m)_m) = \bigcap_n \text{Cantor}^{(n)}(J;(r_m)_m) \tag{22.5}$$

dove $\text{Cantor}^{(0)}(J;(r_m)_m) = J$, $\text{Cantor}^{(n)}(J;(r_m)_m)$ è unione di 2^n intervalli chiusi disgiunti e $\text{Cantor}^{(n+1)}(J;(r_m)_m)$ è ottenuto rimpiazzando ciascuno intervallo I di $\text{Cantor}^{(n)}(J;(r_m)_m)$ con $I_{(0;r_n)}$ e $I_{(1;r_n)}$, definiti in (10.11). Gli insiemi $\text{Cantor}(J;(r_m)_m)$ si dicono **insiemi di Cantor generalizzati**. Quando la successione $(r_n)_n$ è costantemente uguale a r scriveremo $\text{Cantor}(J,r)$. Quindi $E_{1/3}^{(n)} = \text{Cantor}^{(n)}([0;1],1/3)$ e

$$E_{1/3} = \text{Cantor}([0;1],1/3).$$

22.B. La categoria di Baire. Sia $\langle P,\leq\rangle$ un insieme pre-ordinato e consideriamo la topologia $\mathcal{T}$ su P generata dagli insiemi

$$\boldsymbol{N}(p) \stackrel{\text{def}}{=} \{q \in P \mid q \leq p\} \qquad (p \in P).$$

$\boldsymbol{N}(p)$ è un intorno di base del punto p. Questa topologia, che non deve essere confusa con la topologia degli intervalli (si veda pagina **??**), in generale non è neppure T_0. Un insieme $D \subseteq P$ è denso in questa topologia se

$$\forall p \in P \exists q \in D\,(q \leq p)\,.$$

Per evitare confusioni con l'altra nozione di densità, se vale la proprietà introdotta qui sopra diremo che D è **denso nel senso del *forcing***.[3] Vediamo un paio di esempi.

22.B.1. Se X è uno spazio topologico sia P l'insieme degli aperti non-vuoti di X con l'ordinamento

$$p \leq q \quad \Leftrightarrow \quad p \subseteq q.$$

Se $U \subseteq X$ è un aperto denso, allora

$$\{p \in P \mid p \subseteq U\}$$

è un insieme denso (nel senso del *forcing*) in P. Se X è metrico, anche l'insieme

$$\{p \in P \mid \text{diam}(p) \leq 2^{-n}\}$$

è denso.

[3] Il nome *forcing* si riferisce ad un'importante tecnica usata in teoria degli insiemi.

22.B.2. Sia $P = \{p \mid p \text{ è una funzione, } p \subseteq \omega \times \omega, |p| < \omega\}$ con l'ordinamento

$$p \leq q \quad \Leftrightarrow \quad p \supseteq q.$$

A prima vista l'ordinamento di P sembra contro-intuitivo, ma se identifichiamo ogni $p \in P$ con l'aperto $\boldsymbol{N}(p) = \{x \in {}^{\omega}\omega \mid p \subset x\}$ dello spazio di Baire ${}^{\omega}\omega$, vediamo che $p \leq q$ se e solo se $\boldsymbol{N}(p) \subseteq \boldsymbol{N}(q)$, come nell'esempio precedente.

Esercizio 22.9. Verificare che per ogni $n \in \omega$ gli insiemi

$$A_n = \{p \mid n \in \mathrm{dom}(p)\} \qquad \text{e} \qquad B_n = \{p \mid n \in \mathrm{ran}(p)\}$$

sono densi in P.

Il seguente semplice risultato risulta spesso utile.

Teorema 22.10. *Assumiamo* DC*. Sia $\langle P, \leq\rangle$ un insieme pre-ordinato e siano $D_n \subseteq P$ ($n \in \omega$) degli insiemi densi nel senso del* forcing*. Allora per ogni $\bar{p} \in P$ c'è una successione $\bar{p} \geq p_0 \geq p_1 \geq \ldots$ di elementi di P tale che $\forall n \in \omega\, (p_n \in D_n)$.*

Dimostrazione. Fissiamo $\bar{p} \in P$ e consideriamo la relazione R su $\bigcup_{n\in\omega}\{n\}\times D_n$,

$$(n, q)\ R\ (m, r) \quad \Leftrightarrow \quad m = n + 1 \wedge q \geq r.$$

Per densità troviamo un $p_0 \in D_0$ tale che $\bar{p} \geq p_0$ e applicando DC si ottenere una successione

$$(0, p_0)\ R\ (1, p_1)\ R\ (2, p_2)\ R \ldots$$

e quindi la successione $\bar{p} \geq p_0 \geq p_1 \geq \ldots$ è come richiesto. □

Osservazione 22.11. Nella dimostrazione precedente DC è stata applicata all'insieme $\omega \times P$. Quindi per l'Esercizio 22.3, se P è numerabile (cioè finito o in biezione con ω), il risultato vale senza ipotesi aggiuntive.

Il prossimo risultato, noto come **Teorema di Categoria di Baire**, asserisce che in molti spazi topologici, l'intersezione numerabile di aperti densi è non vuota. Ricordiamo che uno spazio topologico X si dice localmente compatto se è T_2 e ogni punto ha un intorno la cui chiusura è compatta. Ne segue che se $x \in U$ esiste $V \subseteq U$ intorno compatto di x.

Teorema 22.12. *Assumiamo* DC*. Sia $X \neq \emptyset$ uno spazio localmente compatto, oppure metrico completo. Se gli U_n sono aperti densi e se U è un aperto non vuoto, allora*

$$\bigcap_{n\in\omega} U_n \cap U \neq \emptyset.$$

Dimostrazione. Supponiamo che X sia metrico completo. Sia

$$P = \{p \subseteq X \mid p \text{ è una palla aperta}\}$$

con l'ordinamento $p \leq q \Leftrightarrow p \subseteq q$. Sia

$$D_n = \{p \mid \operatorname{diam}(p) \leq 2^{-n} \wedge \operatorname{Cl}(p) \subseteq U_n\}.$$

Come osservato nell'Esempio 22.B.1, l'insieme D_n è denso in P. Sia $\bar{p} \in P$ tale che $\bar{p} \subseteq U$. Possiamo quindi trovare una successione $(p_n)_n$ come nel Teorema 22.10. Sia $x_n \in X$ il centro di p_n. Per costruzione, $x_i, x_j \in p_N$ e quindi $d(x_i, x_j) < 2^{-N}$, per ogni $i, j \geq N$ e quindi $(x_n)_n$ è una successione di Cauchy rispetto alla metrica completa d. Quindi c'è un $\bar{x} \in X$ che è limite della successione $(x_n)_n$. Per ogni $n \in \mathbb{N}$, $d(\bar{x}, x_n) \leq 2^{-n}$ e quindi $\bar{x} \in \operatorname{Cl}(p_n) \subseteq U_n$. In altre parole: $\bar{x} \in \bigcap_n U_n$. Dato che $\bar{x} \in p_0 \subseteq U$, abbiamo provato che $\bigcap_{n\in\omega} U_n \cap U \neq \emptyset$, come richiesto.

Supponiamo ora X localmente compatto: il pre-ordine è

$$P = \{p \subseteq X \mid p \neq \emptyset \text{ è un aperto con chiusura compatta}\}$$

con l'ordinamento $p \leq q \Leftrightarrow \operatorname{Cl}(p) = \operatorname{Cl}(q)$ e sia

$$D_n = \{p \in P \mid p \subseteq U_n\}.$$

Sia $\bar{p} \in P$ tale che $\bar{p} \subseteq U$. Fissata la successione $(p_n)_n$ come dal Teorema 22.10, osserviamo che

$$\{\operatorname{Cl}(p_n) \mid n \in \omega\}$$

è una famiglia decrescente di compatti non vuoti e quindi, per la proprietà dell'intersezione finita, $\bigcap_n \operatorname{Cl}(p_n)$ contiene un elemento $\bar{x}$. Quindi $\bar{x} \in \bigcap_n U_n$ e dato che $\bar{x} \in p_0 \subseteq \bar{p} \subseteq U$, il teorema è dimostrato. □

Osservazioni 22.13. (a) Se X è *separabile* metrico completo, oppure *secondo numerabile* localmente compatto, allora l'ordine P può essere preso numerabile e quindi, per l'Osservazione 22.11, il ricorso a DC può essere evitato. (Nel caso degli spazi metrici si prendono palle aperte centrate nei punti dell'insieme numerabile e di raggio razionale; nel caso degli spazi localmente compatti si prendono gli aperti di base con chiusura compatta.) In particolare, il Teorema 22.12 per $\mathbb{R}^n$ o per uno spazio di Banach separabile è dimostrabile senza scelta.

(b) Il Teorema 22.12 per X metrico completo arbitrario implica DC.

(c) Se X soddisfa le ipotesi del Teorema 22.12 e non ha punti isolati, allora $X \setminus \{x\}$ è un aperto denso di X e quindi X non è numerabile.

Un sotto-insieme M di uno spazio topologico X si dice **magro** o di **prima categoria** se esistono chiusi C_n con interno vuoto tali che $M \subseteq \bigcup_n C_n$. Quindi il teorema di Categoria di Baire dice che in uno spazio localmente compatto, oppure metrico completo, nessun aperto non vuoto è magro.

Il Teorema di Categoria di Baire viene spesso usato per dimostrare risultati di *esistenza*: se vogliamo dimostrare l'esistenza di un $x \in X$ che soddisfa la proprietà P (e se X è metrico completo oppure localmente compatto) è sufficiente dimostrare che $\{x \in X \mid P(x)\}$ è non magro e quindi non vuoto. (In molti casi si dimostra che questo insieme è comagro e quindi non magro.) Per esempio l'insieme

$$\mathscr{D} = \{\mathscr{C}([0;1]) \mid \exists x \in [0;1] \ f \text{ è differenziabile in } x\}$$

è magro e quindi $\mathscr{C}([0;1]) \setminus \mathscr{D}$ è comagro [**Fol99**, pag.??]. In particolare, la generica funzione continua su $[0;1]$ non è differenziabile in alcun punto. Vediamo ora un'applicazione alle algebre di Boole del Teorema 22.10.

Teorema 22.14. *Due algebre di Boole numerabili e prive di atomi sono isomorfe.*

Per dimostrare questo risultato introduciamo la seguente

Definizione 22.15. Siano A e B due algebre di Boole. Un **isomorfismo parziale** di A in B è un isomorfismo $p\colon A' \to B'$ dove A' e B' sono subalgebre finite di A e B, rispettivamente.

Lemma 22.16. *Siano A e B algebre di Boole e sia $p\colon A' \to B'$ un isomorfismo parziale di A in B. Supponiamo B sia priva di atomi. Allora $\forall x \in A \setminus A' \exists y \in B \setminus B'$ tale che p si estende ad un isomorfismo parziale $q\colon A'' \to B''$, dove A'' e B'' sono le algebre di Boole generate da $A' \cup \{x\}$ e $B' \cup \{y\}$.*

Dimostrazione. Per il Corollario 8.35

$$A'' = \{(u \curlywedge x) \curlyvee (v \curlywedge x^*) \mid u, v \in A'\},$$

quindi gli atomi di A'' sono gli elementi non nulli di

$$\{a \curlywedge x \mid a \in \mathrm{At}(A')\} \cup \{a \curlywedge x^* \mid a \in \mathrm{At}(A')\}.$$

Se $a \curlywedge x \neq \mathbf{0}_A$, allora ci sono due possibilità:

(1) $\mathbf{0}_A < (a \curlywedge x) < a$ e quindi anche $\mathbf{0}_A < (a \curlywedge x^*) < a$, oppure

(2) $a \curlywedge x = a$, cioè $a \leq x$, da cui $a < x < 1_A$, visto che $x \notin A'$.

Analogamente, se $a \curlywedge x \neq \mathbf{0}_A$ allora vale 1 oppure

(3) $a < x^* < 1_A$.

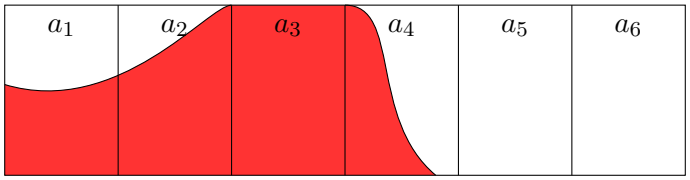
Gli atomi di A' sono classificati in tre famiglie disgiunte:

$$\mathcal{A}_1 = \{a \in \mathrm{At}(A') \mid \mathbf{0}_A < (a \curlywedge x) < a\}$$
$$\mathcal{A}_2 = \{a \in \mathrm{At}(A') \mid a < x\}$$
$$\mathcal{A}_3 = \{a \in \mathrm{At}(A') \mid a \curlywedge x = \mathbf{0}_A\}$$

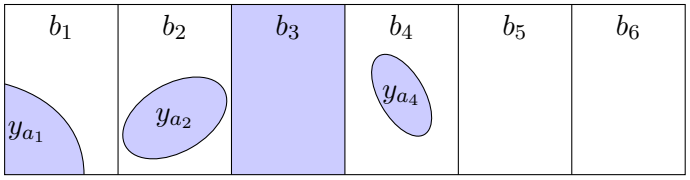
e quindi gli atomi di A'' sono gli elementi di

$$\{a \curlywedge x \mid a \in \mathcal{A}_1\} \cup \{a \curlywedge x^* \mid a \in \mathcal{A}_1\} \cup \mathcal{A}_2 \cup \mathcal{A}_3.$$

Se identifichiamo A con una sub-algebra di un qualche $\mathscr{P}(Z)$ (Teorema di Stone 23.26), la sub-algebra A' risulta essere una sub-algebra atomica di Z e i suoi atomi $\mathrm{At}(A') = \{a_1, \dots, a_n\}$ formano una partizione di Z (Esercizio 8.77). Gli insiemi $\mathcal{A}_1$, $\mathcal{A}_2$ e $\mathcal{A}_3$ sono le collezioni degli $a_i \in \mathrm{At}(A')$ tali che $\emptyset \neq a_i \cap x \subset x$, $a_i \subset x$ e $a_i \cap x = \emptyset$, rispettivamente. Per esempio, nel disegno qui sotto $n = 6$, $\mathcal{A}_1 = \{a_1, a_2, a_4\}$, $\mathcal{A}_2 = \{a_3\}$, $\mathcal{A}_3 = \{a_5, a_6\}$ e la regione rossa denota l'insieme x:



Analogamente, B è (identificabile con) una sub-algebra di un qualche $\mathscr{P}(W)$ e posto $b_i = p(a_i)$ si ha che $\mathrm{At}(B') = \{b_1, \dots, b_n\}$ formano una partizione di W. Poiché B non ha atomi, per ogni $a \in \mathcal{A}_1$ possiamo trovare un $y_a \in B$ tale che $\emptyset \subset y_a \subset a$. Sia $y = (\bigcup_{a \in \mathcal{A}_1} y_a) \cup (\bigcup_{a \in \mathcal{A}_2} p(a))$ denotato dall'area blu nel disegno qui sotto:



Per costruzione l'insieme y interseca i b_k come x interseca gli a_k, cioè

$$\begin{gathered} \emptyset \subset a_k \cap x \subset x \Leftrightarrow \emptyset \subset b_k \cap y \subset y \\ a_k \subset x \Leftrightarrow b_k \subset y \\ a_k \cap x = \emptyset \Leftrightarrow b_k \cap y \end{gathered}$$

e la funzione $p \cup \{(x, y)\}$ si estende in modo unico ad un isomorfismo tra A'' e B''.

Vediamo ora i dettagli. Per $a \in \mathcal{A}_1$ scegliamo[4] un y_a tale che $\mathbf{0}_B < y_a < p(a)$, per $a \in \mathcal{A}_2$ poniamo $y_a = p(a)$ e per $a \in \mathcal{A}_3$ poniamo $y_a = \mathbf{0}_B$. Sia

$$y = \bigvee_{a \in \mathrm{At}(A')} y_a$$

[4]L'assioma di scelta non serve qui, visto che $\mathcal{A}_1$ è finito.

e sia B'' l'algebra generata da $B' \cup \{y\}$. (L'operazione di sup è legittima in quanto $\mathrm{At}(A')$ è finito.) Dato che $\forall a \in \mathrm{At}(A')\,(p(a) \curlywedge y = y_a)$, si ha che

$$a \in \mathcal{A}_1 \Rightarrow \mathbf{0}_B < (p(a) \curlywedge y) < p(a)$$
$$a \in \mathcal{A}_3 \Rightarrow p(a) \curlywedge y = \mathbf{0}_B.$$

Supponiamo $a \in \mathcal{A}_2$: allora

$$a < x = x \curlywedge 1_A = x \curlywedge \bigvee_{a' \in \mathrm{At}(A')} a' = \bigvee_{a' \in \mathrm{At}(A')} (x \curlywedge a')$$

e quindi deve esistere un $a' \in \mathrm{At}(A') \setminus \{a\}$ tale che $a' \curlywedge x \neq \mathbf{0}_A$. Da ciò segue che $p(a) = y_a < (y_a \curlyvee y_{a'}) \leq y$. Per l'arbitrarietà di $a \in \mathcal{A}_2$ si ha

$$a \in \mathcal{A}_2 \Rightarrow p(a) < y.$$

Argomentando come sopra, gli atomi di B'' sono gli elementi di $\{y_a \mid a \in \mathcal{A}_1\} \cup \{p(a) \mid a \in \mathcal{A}_2 \cup \mathcal{A}_3\}$. La corrispondenza

$$a \curlywedge x \mapsto p(a) \curlywedge y \qquad (a \in \mathcal{A}_1)$$
$$a \mapsto p(a) \qquad (a \in \mathcal{A}_2 \cup \mathcal{A}_3)$$

è una biezione tra $\mathrm{At}(A'') \to \mathrm{At}(B'')$ che si estende in modo naturale ad un isomorfismo $A'' \to B''$. □

Siamo ora in grado di dimostrare il Teorema 22.14.

Dimostrazione. Siano $A = \{a_n \mid n \in \omega\}$ e $B = \{b_n \mid n \in \omega\}$ due algebre di Boole come nell'enunciato del teorema. Un isomorfismo parziale di A in B è un isomorfismo $p\colon A' \to B'$ dove A' e B' sono subalgebre finite di A e B, rispettivamente.

Il Lemma ci assicura che ogni isomorfismo parziale da A in B può essere esteso in modo da contenere nel dominio un qualsiasi $x \in A$. Poiché l'inverso di un isomorfismo parziale da A in B è un isomorfismo parziale da B in A, quindi il Lemma dimostra che ogni isomorfismo parziale può essere esteso in modo da contenere nell'immagine un qualsiasi $y \in B$. Sia

$$P = \{p \mid p \text{ è un isomorfismo parziale di } A \text{ in } B\}$$

ordinato mediante il converso dell'inclusione, cioè $p \leq q \Leftrightarrow q \subseteq p$. Il Lemma 22.16 ci assicura che gli insiemi $D_{2n} = \{p \in P \mid a_n \in \mathrm{dom}(p)\}$ sono densi e dato che l'inverso di un isomorfismo parziale di A in B è un isomorfismo parziale di B in A, abbiamo che anche gli $D_{2n+1} = \{p \in P \mid b_n \in \mathrm{ran}(p)\}$ sono densi. Possiamo quindi trovare una successione $p_0 \geq p_1 \geq p_2 \geq \ldots$ tale che $p_i \in D_i$. Per costruzione la funzione

$$f \stackrel{\mathrm{def}}{=} \bigcup_n p_n\colon A \to B$$

è una biezione tra A e B. È quindi sufficiente dimostrare che f è un omomorfismo. Se $x, y \in A$, fissiamo indici $m, n, h, k \in \omega$ tali che $x = a_m$, $y = a_n$, $x^* = a_h$ e $x \curlywedge y = a_k$. Allora $x, y, x^*, x \curlywedge y \in \mathrm{dom}(p_{2N})$ dove $N = \max\{n, m, h, k\}$ e poiché p_{2N} è un isomorfismo parziale, $p_{2N}(x^*) = p_{2N}(x)^*$ e $p_{2N}(x \curlywedge y) = p_{2N}(x) \curlywedge p_{2N}(y)$. Dal momento che f estende p_{2N} si ha che $f(x^*) = f(x)^*$ e $f(x \curlywedge y) = f(x) \wedge f(y)$. Essendo x e y arbitrari in A, otteniamo che f è un morfismo. □

Corollario 22.17. *Le algebre di Boole* $\mathrm{Prop}(L)$*, dove* L *è un insieme numerabile e l'algebra degli intervalli di* $\mathbb{Q}$ *sono isomorfe.*

22.C. σ-ideali. Un ideale I su un insieme X è un **σ-ideale** se è chiuso per unioni numerabili, vale a dire se $A_n \in I$, allora

$$\bigcup_n A_n \in I.$$

Per il Teorema 14.2 la famiglia dei sottoinsiemi numerabili di X

$$\{A \subseteq X \mid |A| \leq \aleph_0\} \tag{22.6}$$

è un σ-ideale. È un ideale proprio se e solo se X non è numerabile. Conviene introdurre la seguente notazione: per ogni cardinale κ (finito o infinito) e ogni insieme X definiamo

$$[X]^{\kappa} = \{A \subseteq X \mid |A| = \kappa\} \tag{22.7}$$

$$[X]^{<\kappa} = \{A \subseteq X \mid |A| < \kappa\} \tag{22.8}$$

$$[X]^{\leq\kappa} = \{A \subseteq X \mid |A| \leq \kappa\} \tag{22.9}$$

sono, rispettivamente, la famiglia dei sottoinsiemi di X di cardinalità κ, minore di κ, al più κ. Osserviamo che la formula (22.7) è la generalizzazione ad un insieme X arbitrario della Definizione 14.16. Il σ-ideale (22.6) è

$$[X]^{\leq\aleph_0},$$

mentre l'ideale dei sottoinsiemi finiti è

$$[X]^{<\aleph_0}.$$

Se μ è una misura completa sull'insieme X,

$$\textsc{Null}(\mu) \stackrel{\text{def}}{=} \{A \subseteq X \mid \mu(A) = 0\}$$

è il σ-ideale dei sottoinsiemi di μ-misura 0; se X è uno spazio localmente compatto, oppure metrico completo,

$$\textsc{Mgr}(X) \stackrel{\text{def}}{=} \{A \subseteq X \mid A \text{ è magro in } X\}$$

è il σ-ideale dei sottoinsiemi magri di X. Chiaramente ogni sottoinsieme numerabile di $\mathbb{R}$ è di misura (di Lebesgue) nulla e di prima categoria, cioè

$$[\mathbb{R}]^{\leq\omega} \subseteq \textsc{Null}(\lambda) \cap \textsc{Mgr}(\mathbb{R}).$$

I σ-ideali su $\mathbb{R}$ sono nozioni di "trascurabilità": in molte dimostrazioni è sufficiente argomentare che una certa proprietà φ vale per tutti i numeri reali *eccetto che per una quantità trascurabile di eccezioni*, vale a dire

$$\{x \in \mathbb{R} \mid \neg\varphi(x)\}$$

è in un qualche σ-ideale proprio, quale $[\mathbb{R}]^{\leq\omega}$, $\textsc{Null}(\lambda)$, o $\textsc{Mgr}(\mathbb{R})$. Osserviamo che gli ideali $\textsc{Null}(\lambda)$ e $\textsc{Mgr}(\mathbb{R})$ sono distinti, anzi ortogonali: infatti c'è un sottoinsieme $\mathbb{R}$ di misura 0 il cui complemento è magro (Esercizio 22.27).

22.D. Teoremi equivalenti a forme deboli dell'Assioma di Scelta.

Esercizi

Un insieme si dice **Dedekind-infinito** o, più brevemente, **D-infinito**, se è in biezione con un suo sottoinsieme proprio. Altrimenti si dice **Dedekind-finito**, ovvero **D-finito**.

Esercizio 22.18. Dimostrare che per ogni insieme X le seguenti condizioni sono equivalenti:

(i) X è D-infinito,

(ii) X e $X \setminus \{x\}$ sono equipotenti, per ogni $x \in X$,

(iii) c'è una funzione $f\colon \omega \rightarrowtail X$.

Concludere che da AC_ω segue che un insieme è D-finito se e solo se è finito.

Esercizio 22.19. Supponiamo che esista un $A \subseteq \mathbb{R}$ infinito ma D-finito. (Naturalmente non possiamo assumere AC_ω.) Dimostrare che A può essere preso contenuto in $(0;1)$ e tale che $0 = \inf A$. Verificare che la funzione caratteristica $\boldsymbol{\chi}_A$ è discontinua in 0, ma è sequenzialmente continua in 0.

Esercizio 22.20. (i) Dimostrare che $\mathsf{DC}(X)$ è equivalente al seguente enunciato, apparentemente più debole, in cui non si fissa il primo elemento della successione f:

> Se R è una relazione su X è tale che $\forall x \exists y\, (x\ R\ y)$, allora c'è una $f \in {}^{\omega}X$ tale che $\forall n\, (f(n)\ R\ f(n+1))$.

(ii) Dimostrare che DC implica la sua versione per classi proprie:

> Per ogni classe $X \neq \emptyset$ (propria o meno), per ogni $x_0 \in X$ e ogni relazione R su X tale che $\forall x \exists y\, (x\ R\ y)$, c'è una $f \in {}^{\omega}X$ tale che $f(0) = x_0$ e $\forall n\, (f(n)\ R\ f(n+1))$.

Esercizio 22.21. Dimostrare che:

(i) Per ogni $a < b$ e ogni successione $(r_n)_n$ di reali in $(0;1)$, gli insiemi $2^{\mathbb{N}}$ e $\mathrm{Cantor}([a;b], (r_n)_n)$ sono omeomorfi, vale a dire, tutti gli insiemi di Cantor generalizzati (vedi (22.5)) sono tra loro omeomorfi.

(ii) $\lambda\,(\mathrm{Cantor}([a;b], r)) = 0$,

(iii) Per ogni $0 \leq s < b - a$ c'è una successione $(r_n)_n$ tale che

$$\lambda\,(\mathrm{Cantor}([a;b], (r_n)_n)) = 0.$$

Esercizio 22.22. Se $\emptyset \neq A_n \subseteq \mathbb{R}$ poniamo $B_n = A_0 \times \cdots \times B_n \subseteq \mathbb{R}^n$. Dimostrare che se c'è una successione strettamente crescente di naturali $(n_i)_i$ ed una successione di reali $(b_i)_i$ tali che $b_i \in B_{n_i}$, allora c'è una successione di reali $(a_n)_n$ tale che $a_n \in A_n$, per ogni n. Concludere che $\mathsf{AC}_\omega(\mathbb{R})$ è equivalente all'enunciato (apparentemente più debole):

> Se $\emptyset \neq A_n \subseteq \mathbb{R}$, allora c'è una successione strettamente crescente di naturali $(n_i)_i$ e una una successione di reali $(b_i)_i$ tale che $b_i \in A_{n_i}$.

Esercizio 22.23. Sia $\emptyset \neq A_n \subseteq (2^{-n-1}; 2^{-n})$ e sia $f\colon \mathbb{R} \to \mathbb{R}$ la funzione caratteristica di $\bigcup_n A_n$,

$$f(x) = \sum_{i=0}^{\infty} \boldsymbol{\chi}_{A_n}(x).$$

Dimostrare che f è discontinua in 0 e che se $x_i \to 0$ è tale che $f(x_i) \not\to 0$, allora c'è una successione crescente $(n_i)_i$ ed una successione di reali $(b_i)_i$ tali che $b_i \in A_{n_i}$.

Usare l'Esercizio 22.22 per concludere che (14.1) implica $\mathsf{AC}_\omega(\mathbb{R})$.

Esercizio 22.24. Verificare che il Teorema 22.12 per $X = \mathbb{R}$ vale senza ipotesi addizionali.

Esercizio 22.25. Assumere $\mathsf{AC}_\omega(\mathbb{R})$ e verificare che $\textsc{Null}(\lambda)$ e $\textsc{Mgr}(\mathbb{R})$ sono σ-ideali su $\mathbb{R}$.

Esercizio 22.26. Dimostrare che se vale AC_ω, allora uno spazio secondo numerabile è separabile.

Esercizio 22.27. Dimostrare che per ogni $\varepsilon > 0$ ci sono aperti densi $U_n^\varepsilon \subseteq \mathbb{R}$ tali che $\lambda(U_n^\varepsilon) \leq \varepsilon$.

Concludere che c'è un $F \subseteq \mathbb{R}$ che è $F = \bigcup_n C_n$, C_n è chiuso e privo di interno, $\mathbb{R} \setminus F$ ha misura di Lebesgue nulla.

Esercizio 22.28. Dimostrare che se $A, B \subseteq \mathbb{R}$ sono bene-ordinati sotto l'usuale ordinamento di $\mathbb{R}$, allora $A + B = \{a + b \mid a \in A, b \in B\}$ è bene ordinato.

(Suggerimento: Per assurdo, considerare una successione strettamente decrescente $a_n + b_n$ e usare l'Esercizio 13.27.)

Esercizio 22.29. Dimostrare che se A è un'algebra di Boole numerabile e B è un'algebra di Boole priva di atomi, allora ogni isomorfismo parziale $p\colon A' \to B'$ si estende ad un monomorfismo $f\colon A \to B$.

Esercizio 22.30. Dimostrare che un'algebra di Boole numerabile priva di atomi B è **ultraomogenea** cioè ogni isomorfismo parziale $p\colon B' \to B''$ con $B, B'' \subseteq B$ si estende ad un automorfismo $f\colon B \to B$.

Il prossimo esercizio richiede qualche nozione di analisi funzionale. Uno **spazio di Fréchet** è uno spazio vettoriale su $\mathbb{R}$ dotato di una metrica completa d tale che le operazioni di somma $F \times F \to F$ e di prodotto per scalare $\mathbb{R} \times F \to F$ sono continue. In particolare ogni spazio di Banach è uno spazio di Fréchet (ma non viceversa).

Esercizio 22.31. Sia F uno spazio di Fréchet di dimensione infinita. Dimostrare che ogni suo sotto-spazio di dimensione finita è un chiuso privo di interno. Concludere che la dimensione di F è maggiore di $\aleph_0$.

Note e osservazioni

Gli assiomi delle scelte numerabili AC_ω e delle scelte dipendenti DC, sono usati comunemente in matematica, per esempio per verificare che una funzione è continua (Esercizio **??**), o per costruire la misura di Lebesgue (si veda pag. 373), o per dimostrare il Teorema di Baire 22.12. Il libro [**Oxt80**] è un'ottima introduzione alle tecniche di misura e categoria. Per una trattazione enciclopedica della teoria della misura il riferimento d'obbligo è Measure Theory, il trattato in cinque volumi [**Fre04a, Fre03, Fre04b, Fre06, Fre08**]. Inoltre, se non assumiamo questi principi, varie patologie possono manifestarsi: sottoinsiemi di $\mathbb{R}$ infiniti ma Dedekind-finiti, funzioni discontinue in un punto $\bar{x}$, ma sequenzialmente continue in $\bar{x}$, ecc. (si veda gli Esercizi 22.18 e 22.19). Per una panoramica dei vari "disastri" che possono capitare se non si assume AC_ω oppure DC rimandiamo a [**Her06**]. Viceversa i vari "disastri" in analisi (insiemi non Lebesgue misurabili, decomposizioni paradossali della sfera — si veda la Sezione 25.C) costruiti mediante AC, l'assioma di scelta vero e proprio, non sono ottenibili da DC, come afferma un celebre risultato di Solovay del 1965 (vedi [**Jec03**, pag.??]). Rimandiamo il lettore interessato al libro [**Sch97**], una vera enciclopedia per quanto riguarda gli aspetti fondazionali dell'analisi matematica. Per un'introduzione all'analisi funzionale si veda il libro [**Rud91**].

23. Algebre di Boole

Richiamiamo alcuni concetti introdotti nella Sezione 8.

Un reticolo è un ordine parziale M in cui $\sup\{x,y\} = x \curlyvee y$ e $\inf\{x,y\} = x \curlywedge y$ esistono per ogni $x, y \in M$. Se $\sup X = \bigvee X$ e $\inf X = \bigwedge X$ esistono per ogni $X \subseteq M$ parleremo di reticolo completo. Un'algebra di Boole è un reticolo distributivo complementato; il complemento di un elemento x è denotato da x^*. Equivalentemente, un'algebra di Boole è una struttura $(B, \curlywedge, \curlyvee, {}^*, \mathbf{0}, \mathbf{1})$ che soddisfa certe equazioni (Definizione 8.28). Un'algebra di Boole è completa se è completa come reticolo.

Attenzione. In questa sezione riserveremo il simbolo $\perp$ per la relazione di incompatibilità (definita a pagina 390), quindi, al fine di evitare fraintendimenti, il minimo e il massimo di un ordine parziale P saranno indicati con $\mathbf{0}$ e $\mathbf{1}$, o con $\mathbf{0}_P$ e $\mathbf{1}_P$ se vogliamo sottolineare la dipendenza dall'ordine P.

23.A. Operatori di chiusura. Un **operatore di chiusura** su un insieme X è una funzione

$$c\colon \mathscr{P}(X) \to \mathscr{P}(X)$$

che soddisfa

$$S \subseteq c(S),$$
$$S \subseteq T \Rightarrow c(S) \subseteq c(T),$$
$$c(c(S)) = c(S),$$

per ogni $S, T \subseteq X$. L'insieme $c(S)$ si dice c-chiusura di S e un insieme che coincide con la sua c-chiusura si dice c-chiuso.

Esercizio 23.1. Dato un operatore di chiusura c, la famiglia dei c-chiusi

$$\mathcal{C}_c = \{S \subseteq X \mid c(S) = S\}$$

contiene X ed è chiusa per intersezioni arbitrarie.

Viceversa, ogni famiglia $\mathcal{C} \subseteq \mathscr{P}(X)$ chiusa per intersezioni arbitrarie e contenente X definisce un operatore di chiusura c tale che $\mathcal{C} = \mathcal{C}_c$.

Quindi un operatore di chiusura c è completamente determinato dalla famiglia $\mathcal{C}_c$ degli insiemi c-chiusi, e $\mathcal{C}_c$ è un reticolo completo (Esempio 8.25(g)).

Chiaramente $\mathrm{Cl}_{\mathcal{F}}$ è un operatore di chiusura, per ogni famiglia $\mathcal{F}$ di funzioni finitarie. Il seguente risultato caratterizza gli operatori di chiusura di questa forma.

Proposizione 23.2. *Sia $c\colon \mathscr{P}(X) \to \mathscr{P}(X)$ un operatore di chiusura e sia $\mathcal{C} = \mathrm{ran}(c)$. Le seguenti affermazioni sono equivalenti.*

(a) *$c = \mathrm{Cl}_{\mathcal{F}}$ per qualche famiglia $\mathcal{F}$ di funzioni finitarie su X;*

(b) *Se* $\mathcal{S} \subseteq \mathcal{C}$ *è* ***diretto superiormente per inclusione****, cioè*

$$\forall S_1, S_2 \in \mathcal{S}\, \exists S \in \mathcal{S}\, (S_1 \cup S_2 \subseteq S),$$

allora $\bigcup \mathcal{S} \in \mathcal{C}$*;*

(c) *Se* $\mathcal{S} \subseteq \mathscr{P}(X)$ *è diretto superiormente per inclusione, allora* $c(\bigcup \mathcal{S}) \subseteq \bigcup_{S\in\mathcal{S}} c(S)$*;*

(d) $\forall S \subseteq X\ (c(S) = \bigcup \{c(F) \mid F \subseteq S \wedge F \textit{ finito}\})$.

Dimostrazione. (d)⇒(a) Sia $\mathcal{C} = \mathcal{C}_c$ e sia $\mathcal{F}$ l'insieme di tutte le funzioni finitarie per cui ogni sottoinsieme in $\mathcal{C}$ è chiuso, cioè

$$\mathcal{F} = \{f \mid \exists n \in \omega\, (f\colon X^n \to X \wedge \forall S \in \mathcal{C}\ (f[S^n] \subseteq S))\}\,.$$

Osserviamo che se $f \in \mathcal{F}$ è 0-aria, allora il suo valore appartiene a $\bigcap \mathcal{C}$; viceversa, se $x \in \bigcap \mathcal{C}$, allora la funzione 0-aria di valore x è in $\mathcal{F}$.

Sia $\mathcal{K}$ la famiglia degli insiemi $\mathrm{Cl}_{\mathcal{F}}$-chiusi. È sufficiente verificare che $\mathcal{C} = \mathcal{K}$. Per costruzione $\mathcal{C} \subseteq \mathcal{K}$, quindi è sufficiente dimostrare che se $S \in \mathcal{K}$, allora $c(S) \subseteq S$. Supponiamo $x \in c(S)$ e cerchiamo di provare che $x \in S$. Per ipotesi, $x \in c(F)$ dove F è un sottoinsieme finito di S, quindi possiamo fissare una sua enumerazione $\langle x_1, \dots, x_n\rangle$. Sia $f\colon X^n \to X$

$$f(y_1, \dots, y_n) = \begin{cases} x & \text{se } (x_1, \dots, x_n) = (y_1, \dots, y_n), \\ y_1 & \text{altrimenti.} \end{cases}$$

Fatto 23.2.1. $f \in \mathcal{F}$

Dimostrazione. Sia $T \in \mathcal{C}$ e $y_1, \dots, y_n \in T$: dobbiamo verificare che $f(y_1, \dots, y_n) \in T$. Se $(x_1, \dots, x_n) = (y_1, \dots, y_n)$ allora $\{x_1, \dots, x_n\} \subseteq T$ quindi $x = f(y_1, \dots, y_n) \in c(F) \subseteq c(T) = T$; se invece $(x_1, \dots, x_n) \neq (y_1, \dots, y_n)$ allora $f(y_1, \dots, y_n) = y_1 \in T$. □

Poiché $S \in \mathcal{K}$ risulta essere chiuso per f, allora $f(x_1, \dots, x_n) = x \in S$ come richiesto.

Le altre implicazioni sono lasciate come esercizio. □

23.B. Ideali e filtri.

Definizione 23.3. Un **ideale di un reticolo** M è un segmento iniziale $\emptyset \neq I \subseteq M$ chiuso sotto $\curlyvee$. Se $I \neq M$ diremo che I è **proprio**. Per ogni $a \in M$ l'insieme

$$\downarrow a = \{x \in M \mid x \leq a\}$$

è l'**ideale principale** generato da a. Un **ideale primo** è un ideale proprio I tale che

$$\forall x, y\, (x \curlywedge y \in I \Rightarrow x \in I \vee y \in I).$$

Un **ideale massimale** è un ideale proprio che non è contenuto in nessun altro ideale proprio.

La concetto duale di 'ideale' è quello di 'filtro': un **filtro di un reticolo** M è un segmento finale $\emptyset \neq F \subseteq M$ chiuso per $\curlywedge$. Le nozioni di ideale proprio, principale, primo, massimale possono essere dualizzate nel modo ovvio: un filtro F di un reticolo M è **proprio** se $F \neq M$, **principale** se $F = {\uparrow}a$ per qualche $a \in M$, **primo** se $a \curlyvee b \in F$ implica che $a \in F$ o $b \in F$, **massimale** se è proprio e non è contenuto in nessun altro filtro proprio. Se M ha minimo $\mathbf{0}$, allora un filtro $F \subseteq M$ è proprio se e solo se $0 \notin F$; dualmente se M ha massimo $\mathbf{1}$, allora un ideale $I \subseteq M$ è proprio se e solo se $\mathbf{1} notin I$.

Teorema 23.4. *Sia M un reticolo bene ordinabile. Se M ha minimo, allora ogni filtro proprio può essere esteso ad un filtro massimale. Dualmente, se M ha massimo, allora ogni ideale proprio può essere esteso ad un ideale massimale.*

In particolare, AC *implica che ogni filtro proprio in reticolo con minimo può essere esteso ad un filtro massimale, e ogni ideale proprio in reticolo con massimo può essere esteso ad un ideale massimale.*

Dimostrazione. Supponiamo F sia un filtro proprio di un reticolo bene-ordinabile M dotato di minimo $\mathbf{0}$. Enumeriamo $M \setminus F$ come $\{x_\alpha \mid \alpha < \kappa\}$ e costruiamo $\langle F_\alpha \mid \alpha \leq \kappa \rangle$ ponendo $F_0 = F$, $F_\lambda = \bigcup_{\alpha<\lambda} F_\alpha$ se λ è limite, e

$$F_{\alpha+1} = \begin{cases} {\uparrow}\{x_\alpha \curlywedge y \mid y \in F_\alpha\} & \text{se questo è un filtro proprio,} \\ F_\alpha & \text{altrimenti.} \end{cases}$$

Osserviamo che gli F_α sono filtri e che $\alpha < \beta \Rightarrow F_\alpha \subseteq F_\beta$. Inoltre gli F_α sono filtri propri. Infatti se $\alpha \leq \kappa$ fosse il minimo ordinale tale che $F_\alpha = M$, allora α è limite e quindi $\mathbf{0} \in F_\beta$ per qualche $\beta < \alpha$, e quindi $F_\beta = M$, contro la minimalità di α. La dimostrazione è conclusa se dimostriamo che F_κ è massimale. Se, per assurdo, $G \supseteq F_\kappa$ fosse un filtro proprio, fissiamo $x_\alpha \in G \setminus F_\kappa$: ma allora $x_\alpha \in F_{\alpha+1} \subseteq F_\kappa$, contraddizione. □

Una **base per filtro** di un reticolo limitato M è un $X \subseteq M$ chiuso sotto $\curlywedge$ e tale che $\mathbf{0} \notin X$; una **sottobase per filtro** è un $X \subseteq M$ tale che $X^{\curlywedge}$ è una base per filtro.[5] Se X è una base per filtro, allora ${\uparrow}X$ è un filtro proprio e si dice filtro generato da X.

Definizione 23.5. Un reticolo M è **κ-completo** se $\bigvee X$ e $\bigwedge X$ esistono, per ogni $X \subseteq M$ di taglia $< \kappa$. Un reticolo è **completo** se è κ-completo per ogni cardinale κ.

[5] L'insieme $X^{\curlywedge}$ è stato definito nella Sezione 8.E a pagina 171.

Un **ideale κ-completo** I di un reticolo κ-completo M è un ideale tale che $\bigvee X \in I$ per ogni $X \subseteq I$ di taglia $\leq \kappa$. Il duale di un ideale κ-completo è un filtro κ-completo.

Un reticolo completo M è **completamente distributivo** se per ogni coppia di insiemi non vuoti di indici I e J, vale

$$\bigwedge_{i\in I}\bigvee_{j\in J} a_{i,j} = \bigvee_{f\in {}^I J}\bigwedge_{i\in I} a_{i,f(i)}$$

e ogni scelta di elementi $a_{i,j} \in M$. (Quando $I = J = 2$ si ottiene l'usuale nozione di reticolo distributivo.)

Se non assumiamo la completezza di M, l'equazione qui sopra deve essere intesa nel senso che quando entrambi i membri sono definiti, allora coincidono, e si ottiene la nozione di reticolo **relativamente assolutamente distributivo**. Sorprendentemente, questa è una nozione esprimibile al prim'ordine nel linguaggio dei reticoli — si veda [**Bal84**] e [**Hod93**, pag. 81].

Un **filtro F su un insieme non vuoto** X è un filtro dell'algebra di Boole $\mathscr{P}(X)$, cioè una famiglia non vuota $F \subseteq \mathscr{P}(X)$ tale che

$$A, B \in F \Rightarrow A \cap B \in F$$
$$A \in F \wedge A \subseteq B \subseteq X \Rightarrow B \in F.$$

La famiglia $\check{S} = \{X \setminus A \mid A \in S\}$, con $S \subseteq \mathscr{P}(X)$ si dice **duale di** S e la mappa $S \mapsto \check{S}$ trasforma ideali (propri/principali/primi/massimali) in filtri (propri/principali/primi/massimali) e viceversa. La parte (b) della Proposizione 8.40 può essere riformulata così: se F è un filtro proprio di un'algebra di Boole B,

$$F \text{ è primo} \Leftrightarrow F \text{ è massimale} \Leftrightarrow \forall x\,(x \notin F \Leftrightarrow x^* \in F)\,. \tag{23.1}$$

Osservazione 23.6. L'equivalenza tra la nozione di *ideale primo* e *ideale massimale* (e dualmente: *filtro primo* e *ultrafiltro*) per le algebre di Boole (Proposizione 8.40(b)), non si generalizza al caso dei reticoli. In un reticolo distributivo, ogni ideale massimale è primo, ma non viceversa, e in un reticolo modulare non è detto che un ideale massimale sia primo (Esercizio 23.47).

Definizione 23.7. Sia B un'algebra di Boole. Una **misura finitamente additiva a valori in** $\{0,1\}$ è una funzione $\mu\colon B \to \{0,1\}$ tale che

- $\mu(\mathbf{0}_B) = 0$ e
- $\mu(a \curlyvee b) = \mu(a) + \mu(b)$ se $a \curlywedge b = \mathbf{0}_B$ (additività).

Se B è κ-completa e se l'ipotesi di additività è rafforzata a

- $\mu(\bigvee_{n\in\omega} a_n) = \sum_{n=0}^{\infty} \mu(a_n)$ se $a_n \curlywedge a_m = \mathbf{0}_B$ per n, m distinti (σ-additività)

diremo che μ è una misura σ-additiva.

Esercizio 23.8. Sia B un'algebra di Boole. Dimostrare che:

(i) Se I è un ideale massimale di B, allora $\mu_I\colon B \to \{0,1\}$

$$\mu_I(a) = \begin{cases} 0 & \text{se } a \in I, \\ 1 & \text{altrimenti,} \end{cases}$$

è una misura su B. Viceversa, ogni misura su B è della forma μ_I per qualche ideale massimale I.

(ii) Se B e I sono ω_1-completi, allora μ_I è una misura σ-additiva.

Esercizio 23.9. Se F è un filtro su $X \neq \emptyset$ e $\emptyset \neq Y \in F$, allora

$$F \restriction Y = \{Z \subseteq Y \mid Z \in F\}$$

è un filtro su Y.

23.C. Esempi.

23.C.1. *Insiemi finiti e cofiniti.* Se X è un insieme,

$$\{Y \subseteq X \mid |Y| < \aleph_0 \vee |X \setminus Y| < \aleph_0\}$$

è una sub-algebra di $\mathscr{P}(X)$. Chiaramente, se X è finito, coincide con $\mathscr{P}(X)$.

Più in generale, se $\lambda \leq \kappa$ sono cardinali infiniti,

$$\{Y \subseteq \kappa \mid |Y| < \lambda \vee |\kappa \setminus Y| < \lambda\}$$

è una sub-algebra di $\mathscr{P}(\kappa)$.

23.C.2. *L'ideale degli insiemi finiti.* Se $\lambda \leq \kappa$ sono cardinali infiniti,

$$\{X \subseteq \kappa \mid |X| < \lambda\}$$

è un ideale proprio non principale. Quando $\kappa = \lambda = \omega$ otteniamo Fin, l'ideale dei sottoinsiemi finiti di $\mathbb{N}$. Il duale di Fin, il filtro degli insiemi co-finiti, si dice **filtro di Fréchet**.

23.C.3. *Il filtro degli intorni di un punto.* Se X è uno spazio topologico, la famiglia degli intorni di un punto $\bar{x} \in X$ è un filtro proprio. Se X è T_2, è un ultrafiltro se e solo se è principale se e solo se $\bar{x}$ è un punto isolato di X.

23.C.4. *Inclusione a meno di insiemi finiti.* La relazione $\subseteq^*$ su $\mathscr{P}(\mathbb{N})$

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

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

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

$A \subset^* B$ 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 $P = \mathscr{P}(\mathbb{N})/=^*$ è un reticolo limitato; infatti è un'algebra di Boole, dato che $P = \mathscr{P}(\mathbb{N})/\operatorname{Fin}$ e Fin è un ideale.

Se $[A] < [B]$, cioè $A \subset^* B$, allora $B \setminus A$ è un insieme infinito $\{k_0 < k_1 < \ldots\}$ e quindi $[A] < [C] < [B]$ dove $C = A \cup \{k_{2i} \mid i \in \mathbb{N}\}$. Ne segue che $\langle P, \leq \rangle$ è

denso in sé stesso. Se consideriamo il sottoinsieme $P \setminus \{[\emptyset], [\mathbb{N}]\}$, otteniamo un ordine denso in sé stesso, privo di elementi massimali o minimali. Dal seguente enunciato si ottiene che ogni sottoinsieme di P ha un maggiorante e un minorante, ma non ha necessariamente un massimo o un minimo (Esercizio 23.52)

Proposizione 23.10. *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 $\mathscr{P}(\mathbb{N})/=^*$ ha un maggiorante.

Dimostrazione. Aggiungendo un numero all'insieme, se serve, possiamo supporre che $A_0 \neq \emptyset$. Poiché

$$A_n \cup A_{n-1} \cup \dots \cup A_0 = A_n \cup (A_{n-1} \setminus A_n) \cup (A_{n-2} \setminus A_{n-1}) \cup \dots \cup (A_0 \setminus A_1)$$

si ha che

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

è infinito in quanto differenza tra un insieme infinito $A_{n+1} \setminus A_n$ ed un'unione finita di insiemi finiti:

$$A_{n-1} \setminus A_n, \quad A_{n-2} \setminus A_{n-1}, \quad \dots, \quad A_0 \setminus A_1.$$

Definiamo induttivamente $k_0 \in A_0$ e $k_{n+1} \in B_{n+1}$ in modo 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. □

23.C.5. *Dominazione di funzioni.* Se $f, g \in \mathbb{N}^\mathbb{N}$ poniamo

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

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

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

L'ordinamento $\leq$ sul quoziente $\mathbb{N}^\mathbb{N}/=^*$ è un reticolo, ha un minimo, ma non ha massimo. Le operazioni di reticolo sono $[f] \curlywedge [g] = [\min(f, g)]$ e

$[f] \curlyvee [g] = [\max(f,g)]$, dove

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

È un reticolo distributivo (Esercizio 23.50) e ogni famiglia numerabile di elementi di $\mathbb{N}^\mathbb{N}$ ha un maggiorante e un minorante, ma non ha necessariamente un estremo superiore o un estremo inferiore, quindi non è un reticolo completo (Esercizio 23.51).

23.D. Completamento di algebre di Boole. Dimostriamo ora che ogni algebra di Boole B ha un completamento, cioè c'è un'algebra di Boole completa $\hat{B}$ con un'immersione $\hat{\imath}\colon B \to \hat{B}$ tale che $\hat{B}$ è, in un certo senso, minimale. Infatti dimostreremo che per un'ampia classe di ordini P, c'è un algebra di Boole completa in cui P si immerge. Come nel caso del completamento di Dedekind degli ordini lineari densi, utilizzeremo un'opportuna topologia.

Innanzi tutto, qualche definizione. Un elemento b di un'algebra di Boole B è **positivo** se $b \neq \mathbf{0}_B$, e se $X \subseteq B$ sia

$$X^+ = X \setminus \{\mathbf{0}\}$$

l'insieme degli elementi positivi di X. Dato un insieme pre-ordinato $(P, \leq)$, due elementi p, q sono **incompatibili**, in simboli $p \perp q$ se

$$\neg\exists r \in P\ (r \leq p \wedge r \leq q)\,,$$

altrimenti si dicono **compatibili**, in simboli $p \parallel q$.

Definizione 23.11. La **topologia inferiore** su un insieme pre-ordinato $(P, \leq)$ è la topologia su P generata dagli insiemi

$$\downarrow p = \{q \in P \mid q \leq p\}$$

con $p \in P$.

Un sottoinsieme $X \subseteq P$ si dirà chiuso/aperto/denso/... se è chiuso/aperto/denso/... rispetto alla topologia inferiore su P.

Quindi $\downarrow p$ è il più piccolo aperto contenente p, da cui

$$\begin{aligned} p \leq q &\Leftrightarrow \downarrow p \subseteq \downarrow q \\ p \perp q &\Leftrightarrow \downarrow p \cap \downarrow q = \emptyset. \end{aligned}$$

Esercizio 23.12. Sia $(P, \leq)$ un insieme pre-ordinato, e sia $\mathcal{T}$ la topologia inferiore su P. Dimostrare che:

(i) $\mathcal{T}$ è T_0 sse $\leq$ è antisimmetrica, i.e., $(P, \leq)$ è un ordine parziale;

(ii) $\mathcal{T}$ è T_1 sse è T_2 sse gli elementi di P sono a due a due incompatibli;

(iii) la chiusura di $X \subseteq P$ è $\uparrow X$;

(iv) $D \subseteq P$ è topolgicamente denso se e solo se $\forall p \in P\, \exists q \in D\, (q \leq p)$;

(v) se $(Q, \preceq)$ è un altro insieme pre-ordinato, una funzione $P \to Q$ è crescente sse è continua rispetto alle topologie inferiori.

Definizione 23.13. Un'immersione $f\colon P \to Q$ di ordini è **un'immersione densa** se $\operatorname{ran} f$ è densa in Q.

Quando un insieme pre-ordinato ha un minimo, come avviene per le algebre di Boole, allora tutti i suoi elementi sono compatibili, e ogni sottoinsieme contenente il minimo è denso. Analogamente, ogni immersione $f\colon P \to Q$ tra insiemi ordinati, che assuma il minimo di Q risulta densa. Al fine di evitare banalità, stipuliamo la seguente:

Convenzione. Quando si considerano algebre di Boole B, la relazione di incompatibilità è da intendersi come la relazione $\perp$ dell'ordine parziale su B^+, quindi poniamo

$$\forall b, c \in B\ (b \perp c \Leftrightarrow b \curlywedge c = \mathbf{0})\,.$$

Analogamente, quando scriviamo "X è denso in B" si intende che "X^+ è denso in B^+", quindi se B' è un'algebra di Boole, allora "$f\colon B' \to B$ è un'immersione densa" significa che "$(\operatorname{ran} f)^+$ è denso in B^+".

Osservazione 23.14. La relazione di compatibilità $\parallel$ è definibile mediante una formula positiva, quindi è preservata dai morfismi; in particolare, se $j\colon P \to Q$ è un'immersione di insiemi pre-ordinati, allora j manda elementi compatibili in elementi compatibili.

L'analogo risultato per $\perp$ non è necessariamente vero: è possibile che $j\colon P \to Q$ sia un'immersione di insiemi (pre-)ordinati e che p, p' siano incompatibili in P, e tuttavia $j(p), j(p')$ siano compatibili in Q. Per dimostrare il risultato per $\perp$ dobbiamo supporre che j sia un'immersione densa, o che P e Q siano algebre di Boole e che j sia un'immersione di algebre di Boole (Esercizio 23.61).

L'inclusione (e più in generale l'ordinamento in un'algebra di Boole) gode della seguente proprietà: se $X \subseteq Y$, allora c'è un insieme non vuoto $Z \subset Y$ che è disgiunto da X (prendere per esempio $Z = Y \setminus X$). Questa proprietà è sufficientemente importante da meritare un'apposita definizione.

Definizione 23.15. Un pre-ordine $(P, \leq)$ è **separativo** se e solo se

$$\forall p, q \in P\, [p \not\leq q \Rightarrow \exists r \leq p\ (r \perp q)]$$

se e solo se

$$\forall p, q \in P\, [{\downarrow}p \not\subseteq {\downarrow}q \Rightarrow \exists r \leq p\ ({\downarrow}r \cap {\downarrow}q = \emptyset)]\,.$$

Esercizio 23.16. Sia P un insieme pre-ordinato e sia B un'algebra di Boole. Se c'è un'immersione $P \to B^+$, allora P è un ordine separativo.

Dato un pre-ordine $(P, \leq)$ possiamo definire la relazione di equivalenza

$$p \sim q \Leftrightarrow \left[\forall r \leq p\ (r \not\perp q) \wedge \forall r \leq q\ (r \not\perp p)\right]$$

e dotare $P/\!\sim$ dell'ordinamento $\lesssim$ definito da

$$[p] \lesssim [q] \Leftrightarrow p \leq q.$$

Quindi ogni pre-ordine P si surietta su di un ordine separativo $(P/\!\sim, \lesssim)$, detto il **quoziente separativo** di P (Esercizio 23.59).

Ricordiamo (Sezione 8.I.6) che un aperto U di uno spazio topologico X è regolare se $\operatorname{Int}\operatorname{Cl}(U) = U$, e che $\mathbf{RO}(X)$, la famiglia degli aperti regolari di X, è un' algebra di Boole completa. Dato che $U \subseteq \operatorname{Int}\operatorname{Cl}(U)$ per ogni aperto U, allora $\downarrow p \subseteq \operatorname{Int}\operatorname{Cl}(\downarrow p)$. Osserviamo che

$$\begin{aligned}\operatorname{Int}\operatorname{Cl}(\downarrow p) &= \{q \in P \mid \downarrow q \subseteq \operatorname{Cl}(\downarrow p)\}\\ &= \{q \in P \mid \forall r \leq q \downarrow r \cap \downarrow p \neq \emptyset\}\\ &= \{q \in P \mid \forall r \leq q\,(r \not\perp p)\}\,.\end{aligned}$$

Proposizione 23.17. *P è separativo se e solo se $\forall p \in P\ (\downarrow p \in \mathbf{RO}(P))$.*

Dimostrazione. Supponiamo P sia separativo. Se $q \in \operatorname{Int}\operatorname{Cl}(\downarrow p)$ allora $\forall r \leq q\,(r \not\perp p)$ e quindi $q \in \downarrow p$ dato che P è separativo. D'altra parte se $\downarrow p = \operatorname{Int}\operatorname{Cl}(\downarrow p)$ per ogni $p \in P$, allora $q \not\leq p$ implica che $\exists r \leq q\,(r \perp p)$, cioè P è separativo. □

Passiamo ora alle algebre di Boole complete.

Lemma 23.18. *Supponiamo che B sia un'algebra di Boole completa e che $D \subseteq B^+$ sia denso. Siano*

$$\begin{aligned}&F\colon B \to \operatorname{Down}(D) && F(b) = \{d \in D \mid d \leq b\}\\ &G\colon \operatorname{Down}(D) \to B && G(X) = \sup X.\end{aligned}$$

Allora

(a) *F è iniettiva, $F(\mathbf{0}) = \emptyset$, $F(\mathbf{1}) = D$, e $F(b_1 \curlywedge b_2) = F(b_1) \cap F(b_2)$,*

(b) *G è suriettiva, $G(\emptyset) = \mathbf{0}$, $G(D) = \mathbf{1}$, e $G(X_1 \cup X_2) = G(X_1) \curlyvee G(X_2)$,*

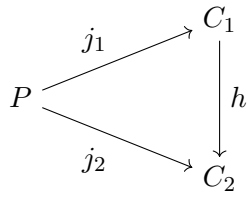
(c) *$G \circ F$ è l'identità su B.*

Dimostrazione. È immediato verificare che $F(\mathbf{0}) = \emptyset$, $F(\mathbf{1}) = D$, $G(\emptyset) = \mathbf{0}$, che $F(b_1 \curlywedge b_2) = F(b_1) \cap F(b_2)$ e che $G(X_1 \cup X_2) = G(X_1) \curlyvee G(X_2)$.

Chiaramente $b \geq \sup_B \{d \in D \mid d \leq b\} = G(F(b))$. Se $b > G(F(b))$ allora scegliamo un $d \in D$ tale che $d \leq b \curlywedge (G(F(b))^* \neq \mathbf{0}$, quindi $d \in F(b)$, da cui $d \leq G(F(b))$: una contraddizione. Questo prova (c), quindi F è iniettiva e G è suriettiva, e $\mathbf{1} = G(F(\mathbf{1})) = \sup D$. □

Notare che F e G non sono omomorfismi.

Lemma 23.19. *Siano C_1, C_2 algebre di Boole complete, sia P un insieme ordinato, e siano $j_i \colon P \to C_i$ delle immersioni dense ($i = 1, 2$). Allora c'è un unico isomorfismo $h \colon C_1 \to C_2$ che rende commutativo il diagramma*



Dimostrazione. Per il Lemma 23.18 ogni $a \in C_1$ è della forma $a = \sup_{C_1} j_1[X_a]$, dove $X_a = \{p \in P \mid j_1(p) \leq a\}$, e ogni $b \in C_2$ è della forma $b = \sup_{C_2} j_2[Y_b]$, dove $Y_b = \{p \in P \mid j_2(p) \leq b\}$. Definiamo $h \colon C_1 \to C_2$ come

$$h(a) = \sup_{C_2} j_2[X_a].$$

Allora h è una biezione che preserva l'ordine, e quindi è un isomorfismo di algebre di Boole, ed è l'unica funzione h' tale che $j_2 = h' \circ j_1$. □

Definizione 23.20. Il **completamento booleano** di un insieme pre-ordinato P è un'algebra di Boole completa B con un'immersione densa $i \colon P \to B^+$. Il completamento booleano di un'algebra di Boole B è il completamento booleano di B^+.

Per il Lemma 23.19 il completamento booleano è ben definito a meno di isomorfismi, e per l'Esercizio 23.16 possiamo restringerci agli ordini separabili. Mostriamo ora l'esistenza del completamento booleano per un ordine separativo.

Fissiamo un ordine separativo P e dotiamolo della topologia inferiore. Per la Proposizione 23.17 la mappa $i \colon P \to \mathbf{RO}(P)^+$, $i(p) = {\downarrow}p$ è ben definita, ed è un'immersione. Inoltre, poiché gli insiemi ${\downarrow}p$ formano una base per la topologia, si tratta di un'immersione densa.

Abbiamo quindi dimostrato il

Teorema 23.21. *Se P è un ordine separativo, allora $(\mathbf{RO}(P), i)$ è il completamento booleano di P, dove $i \colon P \to \mathbf{RO}(P)^+$ è la funzione $p \mapsto {\downarrow}p$.*

Corollario 23.22. *Ogni algebra di Boole si immerge densamente in un'algebra di Boole completa.*

Il **completamento di Dedekind-MacNeille** di un insieme ordinato $(P, <)$ è

$$\mathbf{DM}(P) = \left\{ A^{\mathrm{UL}} \mid A \subseteq P \right\}$$

ordinato per inclusione, dove X^{U} e X^{L} sono gli insiemi degli estremi superiori e inferiori di X (si veda pagina 153). L'Esercizio 23.63 mostra che

$$j\colon P \to \mathbf{DM}(P), \quad j(x) = {\downarrow}x,$$

è un'immersione che preserva gli estremi superiori ed inferiori, quando questi esistono in P, e che $j[P]$ è denso in $\mathbf{DM}(P)$. (Se M è un reticolo, allora $D \subseteq M$ è denso se $x = \bigvee\{d \in D \mid d \leq x\} = \bigwedge\{d \in D \mid x \leq d\}$, per ogni $x \in M$.) L'Esercizio 23.64 mostra come la costruzione del completamento di Dedekind-MacNeille generalizzi tanto la costruzione del completamento booleano di un ordine separativo quanto la costruzione del completamento di Dedekind di un ordine lineare denso (Sezione 8.A).

23.E. Ultrafiltri e il Teorema di Stone. Dal Teorema 23.4 si ottiene

Corollario 23.23. *Sia B un'algebra di Boole e supponiamo che sia bene ordinabile. Allora ogni filtro proprio di B può essere esteso ad un ultrafiltro.*

In particolare, AC *implica che ogni filtro proprio in un'algebra di Boole può essere esteso ad un ultrafiltro.*

Molte delle applicazioni dell'Assioma di Scelta in matematica sono in realtà conseguenza del Corollario 23.23, per cui è conveniente isolare il seguente enunciato, noto come **Principio dell'ideale primo per algebre di Boole**.

Definizione 23.24. BPI è l'enunciato:

> Se I è un ideale proprio di un'algebra di Boole B, allora c'è un ideale primo $J \supseteq I$.

Osservazioni 23.25. (a) AC $\Rightarrow$ BPI per il Corollario 23.23, ma l'implicazione inversa non vale [**HL71**].

(b) BPI è equivalente all'enunciato apparentemente più debole: in ogni algebra di Boole c'è un ideale primo.

L'insieme degli ultrafiltri di un'algebra di Boole B è indicato con

$$\mathrm{St}(B).$$

Teorema 23.26. *Supponiamo B sia un'algebra di Boole bene ordinabile, oppure si assuma* BPI*. La funzione*

$$\mathcal{U}\colon B \to \mathscr{P}(\mathrm{St}(B)), \qquad \mathcal{U}(b) = \{U \in \mathrm{St}(B) \mid b \in U\}, \tag{23.2}$$

è un omomorfismo iniettivo.

Dimostrazione. $\mathcal{U}(\mathbf{0}_B) = \emptyset$ e $\mathcal{U}(\mathbf{1}_B) = \mathrm{St}(B)$, poiché nessun ultrafiltro contiene $\mathbf{0}_B$ e tutti contengono $\mathbf{1}_B$. Supponiamo $U \in \mathcal{U}(b) \cup \mathcal{U}(c)$: allora $b \in U$ o $c \in U$ e poiché $b, c \leq b \curlyvee c$ otteniamo in ogni caso $b \curlyvee c \in U$, cioè

$U \in \mathcal{U}(b \curlyvee c)$. Viceversa, se $U \in \mathcal{U}(b \curlyvee c)$, cioè $b \curlyvee c \in U$, allora $b \in U$ o $c \in U$ dato che U è primo, quindi $U \in \mathcal{U}(b) \cup \mathcal{U}(c)$. Ne segue che

$$\forall b, c \in B \, (\mathcal{U}(b \curlyvee c) = \mathcal{U}(b) \cup \mathcal{U}(c)) \, .$$

Nessun ultrafiltro può contenere b e b^*, quindi $\mathcal{U}(b) \cap \mathcal{U}(b^*) = \emptyset$. Viceversa se $U \notin \mathcal{U}(b)$, allora $b^* \in U$ per la 23.1 e quindi $D \in \mathcal{U}(b^*)$. Cioè

$$\forall b \in B \, (\mathcal{U}(b^*) = \mathrm{St}(B) \setminus \mathcal{U}(b)) \, .$$

Per ogni $b \neq \mathbf{0}_B$, l'insieme $\{c \in B \mid b \leq c\}$ è un filtro che quindi può essere esteso ad un ultrafiltro, quindi

$$\forall b \in B \setminus \{\mathbf{0}_B\} \, (\mathcal{U}(b) \neq \emptyset) \, .$$

Ne segue che $\ker \mathcal{U} = \{\mathbf{0}_B\}$, cioè $\mathcal{U}$ è un omomorfismo iniettivo. □

Come corollario otteniamo il seguente risultato noto come **Teorema di Rappresentazione per le algebre di Boole**:

Teorema 23.27. *Sia B un'algebra di Boole bene ordinabile, oppure si assuma* BPI. *Allora B è isomorfa ad un'algebra di insiemi.*

23.F. Dualità di Stone.

Lemma 23.28. *Se X è compatto e $\mathcal{B}$ è un'algebra di insiemi che è una base per X, allora $\mathcal{B} = \mathbf{CLOP}(X)$.*

Dimostrazione. Dato che $\mathcal{B}$ è chiuso per complementi, ogni insieme di $\mathcal{B}$ è chiuso-aperto, quindi $\mathcal{B} \subseteq \mathbf{CLOP}(X)$. Vice versa, se $C \in \mathbf{CLOP}(X)$, allora C è compatto, quindi ogni ricoprimento $C = \bigcup_{i \in I} U_i$ con $U_i \in \mathcal{B}$ ammette un sottoricoprimento finito $C = U_{i_1} \cup \cdots \cup U_{i_n}$. Poiché $\mathcal{B}$ è chiuso per unioni finite, $C \in \mathcal{B}$. □

Uno spazio topologico è **zero dimensionale** se ha una base di insiemi chiusi-aperti.

Se dotiamo l'insieme $\mathrm{St}(B)$ della topologia generata dagli insiemi $\mathcal{U}(b)$ di (23.2), lo spazio risultante si dice **spazio di Stone di** B, da cui la notazione.

Teorema 23.29. *Supponiamo che B sia bene ordinabile, oppure assumiamo* BPI. *Allora $\mathrm{St}(B)$ è compatto, di Hausdorff, zero dimensionale, e B è isomorfa a* $\mathbf{CLOP}\,(\mathrm{St}(B))$.

Dimostrazione. Dato che $\mathcal{U}(b^*) = \mathrm{St}(B) \setminus \mathcal{U}(b)$, allora

(23.3) $\{\mathcal{U}(b) \mid b \in B\}$ è una base di insiemi chiusi-aperti.

Se $U, D \in \mathrm{St}(B)$ sono distinti, sia $b \in U \setminus D$: allora $b^* \in D \setminus U$ e $\mathcal{U}(b)$ e $\mathcal{U}(b^*)$ sono intorni disgiunti di U e D. Questo mostra che $\mathrm{St}(B)$ è zero-dimensionale e T_2.

Per la compattezza basta dimostrare che ogni ricoprimento aperto della forma $\mathrm{St}(B) = \bigcup_{i\in I} \mathcal{U}(b_i)$ ammette un sottoricoprimento finito. Per assurdo, supponiamo che $\mathrm{St}(B) = \bigcup_{i\in J} \mathcal{U}(b_i)$ per ogni $J \subseteq I$ finito, così che

$$\begin{aligned}\mathcal{U}(\bigwedge_{i\in J} b_i^*) &= \bigcap_{i\in J} \mathcal{U}\left(\mathcal{U}(b_i^*)\right)\\ &= \mathrm{St}(B) \setminus \bigcup_{i\in J} \mathcal{U}(b_i)\\ &\neq \emptyset\\ &= \mathcal{U}(\mathbf{0}_B).\end{aligned}$$

Poiché $\mathcal{U}$ è un omomorfismo iniettivo, ne segue che $\bigwedge_{i\in J} b_i^* \neq \mathbf{0}_B$ per ogni $J \subseteq I$ finito, quindi $\{b_i^* \mid i \in I\}$ genera un filtro che può essere esteso ad un ultrafiltro U. Per ipotesi $U \in \mathcal{U}(b_{i_0})$ per qualche $i_0 \in I$, e $b_{i_0}^* \in U$ per costruzione: contraddizione.

Infine, $B \cong \mathbf{CLOP}\left(\mathrm{St}(B)\right)$ segue da (23.3), dal Lemma 23.28 e dal Teorema 23.26. □

Teorema 23.30. *Sia X compatto, di Hausdorff, e zero dimensionale. Allora X è omeomorfo a* $\mathrm{St}(\mathbf{CLOP}(X))$.

Dimostrazione. Sia $U \in \mathrm{St}(\mathbf{CLOP}(X))$. Allora U è una famiglia di chiusi-aperti non vuoti di X, e per la definizione di filtro, $C_1 \cap \cdots \cap C_n \neq \emptyset$ per ogni $C_1, \ldots, C_n \in U$. Per compattezza, $K = \bigcap U \neq \emptyset$. Se $x, y \in K$ fossero distinti, scegliamo $D \in \mathbf{CLOP}(X)$ tale che $x \in D$ e $y \notin D$. Un sottoinsieme finito di $\mathcal{F} = \{C \cap D \mid C \in U\}$ ha intersezione non vuota, dato che x appartiene a tale intersezione, quindi $\mathcal{F}$ genera un filtro proprio che può essere esteso ad un ultrafiltro U'. Allora $U' \subseteq U$ e per la massimalità degli ultrafiltri $U' = U$, quindi $K = \bigcap U' \subseteq D$ da cui $y \in D$: contraddizione. Quindi $\bigcap U$ è un singoletto, per ogni $U \in \mathrm{St}(\mathbf{CLOP}(X))$.

Sia

$$h\colon \mathrm{St}(\mathbf{CLOP}(X)) \to X, \qquad h(U) = \text{l'unico elemento di } \bigcap U.$$

Dimostreremo che h è un omeomorfismo.

Innanzi tutto notiamo che per ogni $U \in \mathrm{St}(\mathbf{CLOP}(X))$ e ogni $C \in \mathbf{CLOP}(X)$

$$h(U) \in C \Leftrightarrow C \in U \tag{23.4}$$

Infatti se $h(U) \in C$ e $C \notin U$ allora $X \setminus C \in U$ quindi $h(U) \in X \setminus C$, una contraddizione. Vice versa, se $C \in U$ e $h(U) \notin C$ allora $h(U) \in X \setminus C$ quindi $X \setminus C \in U$, di nuovo una contraddizione.

Supponiamo $U, U' \in \mathrm{St}(\mathbf{CLOP}(X))$ siano distinti. allora c'è $C \in \mathbf{CLOP}(X)$ tale che $C \in U$ e $C \notin U'$, quindi $h(U) \in C$ e $h(U') \notin C$ per (23.4). Questo prova che h è iniettiva.

Fissiamo $x \in X$ e sia $\mathcal{F} = \{C \in \mathbf{CLOP}(X) \mid x \in C\}$. Allora $\mathcal{F}$ genera un filtro proprio che può essere esteso ad un ultrafiltro U. Per (23.4) è facile vedere che $h(U) = x$. Questo mostra che h è suriettiva.

Per $C \in \mathbf{CLOP}(X)$

$$\begin{aligned} h^{-1}(C) &= \{U \mid h(U) \in C\} \\ &= \{U \in \mathrm{St}(\mathbf{CLOP}(X)) \mid C \in U\} && \text{per (23.4)} \\ &= \mathcal{U}(C) && \text{dove } \mathcal{U} \text{ è come in (23.2)} \end{aligned}$$

quindi la controimmagine di un insieme chiuso-aperto di X è chiuso-aperto in $\mathrm{St}(\mathbf{CLOP}(X))$. Dato che stiamo lavorando con spazi compatti, questo mostra che h è un omeomorfismo. □

Esercizio 23.31. Sia Boole la categoria delle algebre di Boole e sia ZdCmp la categoria degli spazi compatti di Hausdorff zero-dimensionali. Dimostrare che $\mathrm{St}\colon \textsc{Boole} \to \textsc{ZdCmp}$,

$$f\colon B \to C \quad \rightsquigarrow \quad f_{\mathrm{St}}\colon \mathrm{St}(C) \to \mathrm{St}(B)$$

$f_{\mathrm{St}}(U) = f^{-1}[U]$, e $\mathbf{CLOP}\colon \textsc{ZdCmp} \to \textsc{Boole}$,

$$f\colon X \to Y \quad \rightsquigarrow \quad f_{\mathbf{CLOP}}\colon \mathbf{CLOP}(Y) \to \mathbf{CLOP}(X)$$

$f_{\mathbf{CLOP}}(C) = f^{-1}[C]$, sono funtori controvarianti, e che sono l'inverso l'uno dell'altro.

Ne segue che lo studio delle algebre di Boole è equivalente allo studio degli spazi compatti di Hausdorff zero dimensionali, quindi tecniche/risultati/problemi in un'area possono essere riformulati nell'altra area: se B è un'algebra di Boole e X è il suo spazio di Stone,

- B è completa se e solo se X è **estremamente sconnesso**, cioè la chiusura di ogni aperto è un chiuso-aperto (Esercizio 23.65),
- B è numerabile se e solo se X è separabile (Esercizio 23.66)
- un atomo di B corrisponde tad un punto isolato di X; in particolare B è priva di atomi se e solo se X non ha punti isolati (Esercizio 23.67).

Il Teorema 22.14 mostra che due algebre numerabili prive di atomi sono isomorfe, quindi due spazi di Hausdorff compatti, separabili e senza punti isolati sono omeomorfi. In particolare

Teorema 23.32. *Lo spazio di Cantor è, a meno di omeomorfismo, l'unico spazio compatto, separabile, zero dimensionale senza punti isolati.*

23.G. Ultraprodotti. Vediamo ora una costruzione che generalizza la nozione di prodotto cartesiano generalizzato. Data una successione di insiemi non vuoti $\langle A_i \mid i \in I\rangle$ e un filtro F sull'insieme $I \neq \emptyset$ definiamo la relazione d'equivalenza $\sim_F$ su $\bigtimes_{i\in I} A_i$

$$f \sim_F g \Leftrightarrow \{i \in I \mid f(i) = g(i)\} \in F.$$

La relazione $\sim_F$ è chiaramente riflessiva e simmetrica; la proprietà transitiva discende dal fatto che F è chiuso per intersezioni e soprainsiemi e da $\{i \in I \mid f(i) = h(i)\} \supseteq \{i \in I \mid f(i) = g(i)\} \cap \{i \in I \mid g(i) = h(i)\}$. Il **prodotto ridotto degli** A_i **modulo** F è l'insieme quoziente

$$\prod_F A_i \stackrel{\text{def}}{=} \bigtimes_{i\in I} A_i/\sim_F.$$

Se $F = \mathscr{P}(I)$ è il filtro improprio, $\prod_F A_i$ è un singoletto; se $F = \{I\}$ è il filtro banale, $\prod_F A_i$ è identificabile con $\bigtimes_{i\in I} A_i$; se F è proprio e $\{i_0\} \in F$ per qualche $i_0 \in I$, allora $\prod_F A_i \to A_{i_0}$, $[f] \mapsto f(i_0)$, è una biezione. Quando F è un ultrafiltro il prodotto ridotto si dice **ultraprodotto**. Se gli insiemi A_i sono lo stesso insieme A parleremo di **potenza ridotta** e scriveremo A^I/F; se F è un ultrafiltro parleremo di **ultrapotenza**.

Osservazione 23.33. La costruzione delle potenze ridotte è simile alla costruzione degli spazi $L^p(X, \mu)$ in analisi, dove si parte da un un insieme X dotato di una misura μ e si quozienta l'insieme

$$\{f \mid f\colon X \to \mathbb{R} \text{ è } \mu\text{-misurabile e } \textstyle\int_X |f(x)|^p \,\mathrm{d}x < +\infty\}$$

ponendo

$$f \sim g \Leftrightarrow \{x \in X \mid f(x) = g(x)\} \in F,$$

dove $F = \{Y \subseteq X \mid \mu(X \setminus Y) = 0\}$ è il filtro degli insiemi il cui complementare è trascurabile. (Nel caso in cui μ sia una misura di probabilità $F = \{Y \subseteq X \mid \mu(Y) = 1\}$.) La somma, il prodotto e l'ordinamento su $L^p(X, \mu)$ sono così definiti: $[f] + [g] = [f + g]$ e $[f] \cdot [g] = [f \cdot g]$, dove $(f + g)(x) = f(x) + g(x)$ e $(f \cdot g)(x) = f(x) \cdot g(x)$, e $[f] < [g]$ se e solo se $\{x \in X \mid f(x) < g(x)\} \in F$.

Nel caso in cui la misura si concentri su un punto $\bar{x} \in X$, cioè $F = \{Y \subseteq X \mid \bar{x} \in Y\}$ è un ultrafiltro principale, $L^p(X, \mu)$ è isomorfo ad $\mathbb{R}$.

Se gli A_i sono dotati di qualche struttura (algebrica o di ordine) il prodotto ridotto eredita questa struttura. Vediamo due esempi specifici quando F è un filtro proprio, non banale, non principale su $I = \omega$.

23.G.1. *Ultrapotenza di* $\langle \mathbb{N}, <\rangle$. Fissiamo un filtro F su $\mathbb{N}$ e consideriamo la potenza ridotta $\mathbb{N}^{\mathbb{N}}/F$ con l'ordinamento

$$[f] \leq [g] \Leftrightarrow \{n \in \mathbb{N} \mid f(n) \leq g(n)\} \in F$$

Se $\{n \mid f(n) = f'(n)\}, \{n \mid g(n) = g'(n)\}, \{n \in \mathbb{N} \mid f(n) \leq g(n)\} \in F$ allora

$$\{n \in \mathbb{N} \mid f'(n) \leq g'(n)\} \supseteq$$
$$\{n \mid f(n) = f'(n)\} \cap \{n \mid g(n) = g'(n)\} \cap \{n \in \mathbb{N} \mid f(n) \leq g(n)\} \in F$$

quindi la definizione di ordinamento non dipende dal rappresentante. In modo analogo si verifica che $\leq$ è riflessiva, antisimmetrica e transitiva su $\mathbb{N}^{\mathbb{N}}/F$, cioè $\left\langle \mathbb{N}^{\mathbb{N}}/F, \leq \right\rangle$ è un insieme ordinato.

Per ipotesi F contiene il filtro di Fréchet (Sezione 23.C.2), quindi se $f, g \in \mathbb{N}^{\mathbb{N}}$ coincidono da un certo punto in poi, allora $f \sim_F g$. Se F è proprio il filtro di Fréchet, l'ordinamento è quello della dominazione quasi ovunque descritto nella Sezione 23.C.5, che non è un ordine lineare.

Supponiamo adesso F sia un ultrafiltro. Per ogni coppia di $f, g \in \mathbb{N}^{\mathbb{N}}$ gli insiemi

$$\{n \mid f(n) < g(n)\}, \quad \{n \mid f(n) = g(n)\}, \quad \{n \mid f(n) > g(n)\}$$

formano una partizione dei naturali, quindi una ed una sola delle seguenti condizioni vale:

$$[f] < [g], \quad [f] = [g], \quad [f] > [g].$$

In altre parole: $\leq$ è un ordine lineare su $\mathbb{N}^{\mathbb{N}}/F$.

Se inoltre F non è principale, allora $\leq$ non è un buon ordine su $\mathbb{N}^{\mathbb{N}}/F$: se

$$f_k(n) = \begin{cases} n - k & \text{se } n \geq k, \\ 0 & \text{altrimenti,} \end{cases}$$

allora $[f_0] > [f_1] > [f_2] > \dots$ forma una catena discendente.

23.G.2. *Ultraprodotto di campi.* Se gli $\mathcal{A}_n = \Bbbk_n$ sono campi, definiamo le operazioni di somma e prodotto su $\prod_F \Bbbk_n$ ponendo

$$[f] + [g] = [f + g] \qquad \text{e} \qquad [f] \cdot [g] = [f \cdot g]$$

dove le successioni $f + g$ e $f \cdot g$ sono definite da

$$(f + g)(n) = f(n) +_n g(n) \qquad \text{e} \qquad (f \cdot g)(n) = f(n) \cdot_n g(n),$$

e le operazioni $+_n$ e $\cdot_n$ a secondo membro denotano l'addizione e la moltiplicazione nel campo $\Bbbk_n$. Con queste operazioni si ottiene un anello commutativo unitario — l'elemento neutro per la somma e per il prodotto sono le classi di equivalenza delle successioni $n \mapsto 0_{\Bbbk_n}$ e $n \mapsto 1_{\Bbbk_n}$, rispettivamente, e verranno indicate con $\mathbf{0}$ e $\mathbf{1}$.

Supponiamo che $[f] \neq \mathbf{0} \neq [g]$ma che $[f] \cdot [g] = \mathbf{0}$. Questo significa che

$$\{n \mid f(n) = 0_{\Bbbk_n}\} \notin F \quad \text{e} \quad \{n \mid g(n) = 0_{\Bbbk_n}\} \notin F$$

ma

$$\{n \mid f(n) \cdot g(n) = 0_{\Bbbk_n}\} = \{n \mid f(n) = 0_{\Bbbk_n}\} \cup \{n \mid g(n) = 0_{\Bbbk_n}\} \in F$$

e cioè F non è primo.

Viceversa, se F è primo, cioè è un ultrafiltro, allora $\prod_F \Bbbk_n$ è un campo. Infatti se $[f] \neq \mathbf{0}$, allora $A \stackrel{\text{def}}{=} \{n \mid f(n) \neq 0_{\Bbbk_n}\} \in F$ e quindi possiamo definire

$$f'(n) = \begin{cases} f(n) & \text{se } n \in A, \\ 1_{\Bbbk_n} & \text{altrimenti,} \end{cases}$$

così che $[f] = [f']$ e $\forall n\ (f'(n) \neq 0_{\Bbbk_n})$. Se $g(n)$ è l'elemento di $\Bbbk_n$ tale che $f'(n) \cdot g(n) = 1_{\Bbbk_n}$, allora $\forall n\ (f'(n) \cdot g(n) = 1_{\Bbbk_n})$ cioè $[f] \cdot [g] = \mathbf{1}$.

Se F è l'ultrafiltro generato da un $n_0 \in \mathbb{N}$, la mappa $\prod_F \Bbbk_n \to \Bbbk_{n_0}$, $[f] \mapsto f(n_0)$ è un isomorfismo di campi. Se invece F non è principale, l'ultraprodotto non è necessariamente isomorfo ad uno dei fattori. Per esempio supponiamo che i campi $\Bbbk_n$ abbiano tutti caratteristica finita e che la caratteristica tenda all'infinito, cioè $\lim_{n\to\infty} \mathrm{char}(\Bbbk_n) = \infty$. Fissiamo un $m > 0$ e sia $[f]$ un elemento non nullo dell'ultraprodotto — per quanto visto sopra possiamo supporre che $f(n) \neq 0_{\Bbbk_n}$, per ogni $n \in \mathbb{N}$. L'elemento

$$m[f] \stackrel{\text{def}}{=} \underbrace{[f] + \cdots + [f]}_{m}$$

è la classe di equivalenza della funzione $mf \in \mathbb{X}_n \Bbbk_n$ definita da

$$n \mapsto mf(n) \stackrel{\text{def}}{=} \underbrace{f(n) + \cdots + f(n)}_{m}$$

Sia M tale che $\forall n \geq M\,(\mathrm{char}(\Bbbk_n) > m)$ e quindi $\forall n \geq M\,(m \cdot f(n) \neq 0_{\Bbbk_n})$. La successione

$$g(n) = \begin{cases} mf(n) & \text{se } n \geq M \\ 1_{\Bbbk_n} & \text{altrimenti} \end{cases}$$

è equivalente a mf visto che F è non principale e quindi $\mathbb{N} \setminus M \in F$. Ne segue che $m[f]$ è non nullo. Essendo m ed $[f]$ arbitrari, abbiamo verificato che $\prod_F \Bbbk_n$ ha caratteristica 0.

23.H. Il calcolo proposizionale. In questa Sezione rivediamo in modo algebrico le nozioni introdotte nella Sezione 3.C.1.

23.H.1. *Proposizioni.* Fissato un insieme non vuoto L i cui elementi vengono detti **lettere proposizionali**, l'insieme $\mathrm{Prop}(L)$ delle **proposizioni** su L è l'insieme delle espressioni su $\langle S, a\rangle$ dove

$$S = \{\boldsymbol{\neg}, \boldsymbol{\vee}, \boldsymbol{\wedge}, \boldsymbol{\Rightarrow}, \boldsymbol{\Leftrightarrow}\} \cup L,$$

e $\boldsymbol{\neg}, \boldsymbol{\vee}, \boldsymbol{\wedge}, \boldsymbol{\Rightarrow}, \boldsymbol{\Leftrightarrow}$ sono oggetti distinti[6] e

- $a(\boldsymbol{\neg}) = 1$, $a(\square) = 2$, per ogni $\square \in \{\boldsymbol{\vee}, \boldsymbol{\wedge}, \boldsymbol{\Rightarrow}, \boldsymbol{\Leftrightarrow}\}$

[6] Usiamo i simboli $\boldsymbol{\neg}, \boldsymbol{\vee}, \ldots$ in neretto per distinguerli dai connettivi $\neg, \vee, \ldots$ del linguaggio matematico informale.

- $a(A) = 0$, per ogni $A \in L$.

L'insieme $\mathrm{Prop}(L)$ si dice anche **calcolo proposizionale** sull'insieme L.

Dal Corollario 20.7 otteniamo:

Proposizione 23.34. *Sia* $\boldsymbol{p} \in \mathrm{Prop}(L)$. *Allora:*

- *se* $\mathrm{lh}(\boldsymbol{p}) = 1$, *allora* $\boldsymbol{p} = \langle A \rangle$, *per una ed una sola* $A \in L$,
- *se* $\mathrm{lh}(\boldsymbol{p}) > 1$ *e la stringa* $\boldsymbol{p}$ *comincia con* $\boldsymbol{\neg}$, *allora esiste ed è unica* $\boldsymbol{q} \in \mathrm{Prop}(L)$ *tale che* $\boldsymbol{p} = \langle \boldsymbol{\neg} \rangle^\frown \boldsymbol{q}$,
- *se* $\mathrm{lh}(\boldsymbol{p}) > 1$ *e la stringa* $\boldsymbol{p}$ *comincia con un simbolo* $\square$ *di connettivo binario, allora esistono e sono uniche* $\boldsymbol{q}, \boldsymbol{r} \in \mathrm{Prop}(L)$ *tali che* $\boldsymbol{p} = \langle \square \rangle^\frown \boldsymbol{q}^\frown \boldsymbol{r}$.

Per semplicità notazionale scriveremo $\boldsymbol{\neg p}$ e $\boldsymbol{p} \,\square\, \boldsymbol{r}$ invece di $\langle \boldsymbol{\neg} \rangle^\frown \boldsymbol{p}$ e $\langle \square \rangle^\frown \boldsymbol{p}^\frown \boldsymbol{r}$. Inoltre useremo la convenzione che il connettivo $\boldsymbol{\neg}$ lega più strettamente degli altri connettivi binari e quindi potremo risparmiarci l'uso di qualche parentesi.

Seguendo lo schema della Sezione 3, una proposizione può essere descritta mediante un albero etichettato (Sezione 20.E).

Una **valutazione in un'algebra di Boole** B o B-valutazione è una funzione $v\colon \mathrm{Prop}(L) \to B$ tale che

$$\begin{aligned} v(\boldsymbol{\neg p}) &= v(\boldsymbol{p})^* \\ v(\boldsymbol{p} \boldsymbol{\wedge} \boldsymbol{q}) &= v(\boldsymbol{p}) \curlywedge v(\boldsymbol{q}) \\ v(\boldsymbol{p} \boldsymbol{\vee} \boldsymbol{q}) &= v(\boldsymbol{p}) \curlyvee v(\boldsymbol{q}) \\ v(\boldsymbol{p} \boldsymbol{\Rightarrow} \boldsymbol{q}) &= v(\boldsymbol{p})^* \curlyvee v(\boldsymbol{q}) \\ v(\boldsymbol{p} \boldsymbol{\Leftrightarrow} \boldsymbol{q}) &= (v(\boldsymbol{p})^* \curlyvee v(\boldsymbol{q})) \curlywedge (v(\boldsymbol{p}) \curlyvee v(\boldsymbol{q})^*). \end{aligned}$$

Lemma 23.35. *Ogni funzione* $F\colon L \to B$ *può essere estesa ad un'unica* B*-valutazione.*

Dimostrazione. Sia $\mathrm{Prop}_n = \{\boldsymbol{p} \in \mathrm{Prop}(L) \mid \mathrm{ht}(\boldsymbol{p}) \leq n\}$. Definiamo induttivamente $F_n\colon \mathrm{Prop}_n \to B$ ponendo $F_0(\langle A \rangle) = F(A)$ e

$$F_{n+1}(\boldsymbol{p}) = \begin{cases} F_n(\boldsymbol{p}) & \text{se } \boldsymbol{p} \in \mathrm{Prop}_n, \\ F_n(\boldsymbol{q})^* & \text{se } \boldsymbol{p} = \boldsymbol{\neg q}, \\ F_n(\boldsymbol{q}) \curlyvee F_n(\boldsymbol{r}) & \text{se } \boldsymbol{p} = \boldsymbol{q} \boldsymbol{\vee} \boldsymbol{r}, \\ F_n(\boldsymbol{q}) \curlywedge F_n(\boldsymbol{r}) & \text{se } \boldsymbol{p} = \boldsymbol{q} \boldsymbol{\wedge} \boldsymbol{r}, \\ F_n(\boldsymbol{q})^* \curlyvee F_n(\boldsymbol{r}) & \text{se } \boldsymbol{p} = \boldsymbol{q} \boldsymbol{\Rightarrow} \boldsymbol{r}, \\ (F_n(\boldsymbol{q}) + F_n(\boldsymbol{r}))^* & \text{se } \boldsymbol{p} = \boldsymbol{q} \boldsymbol{\Leftrightarrow} \boldsymbol{r}, \end{cases}$$

dove $+$ è l'operazione di somma in B definita nella Sezione (8.H). Poiché $F_0 \subseteq F_1 \subseteq \ldots$, la funzione $v \stackrel{\text{def}}{=} \bigcup_n F_n\colon \mathrm{Prop} \to B$ è una funzione ed è la B-valutazione cercata. □

Esercizio 23.36. Dimostrare che se v è una B-valutazione, $v(\boldsymbol{p} \boldsymbol{\Rightarrow} \boldsymbol{q}) = \mathbf{1}_B$ se e solo se $v(\boldsymbol{p}) \leq v(\boldsymbol{q})$.

In particolare, ogni funzione

$$v\colon L \to \{0,1\}$$

che associa ad ogni lettera un valore di verità: vero (1) o falso (0), può essere estesa in modo canonico ad una valutazione (che indicheremo ancora con v)

$$v\colon \operatorname{Prop}(L) \to \{0,1\}.$$

Definizione 23.37. Una $v \in {}^L2$ **soddisfa** $\Gamma \subseteq \operatorname{Prop}(L)$ ovvero v è un **modello** di Γ se

$$\forall \boldsymbol{p} \in \Gamma\, (v(\boldsymbol{p}) = 1)\,.$$

Quando Γ è un singoletto $\{\boldsymbol{p}\}$ diremo che v è un modello di $\boldsymbol{p}$.

Se $\Gamma \subseteq \operatorname{Prop}(L)$, diremo che $\boldsymbol{p}$ è **conseguenza tautologica** di Γ, in simboli

$$\Gamma \models \boldsymbol{p},$$

se e solo se ogni modello di Γ è un modello di $\boldsymbol{p}$. Quando Γ è il singoletto $\{\boldsymbol{q}\}$ scriveremo $\boldsymbol{q} \models \boldsymbol{p}$ invece di $\Gamma \models \boldsymbol{p}$.

Una $\boldsymbol{p}$ che è soddisfatta da ogni v si dice **tautologia proposizionale**; una $\boldsymbol{p}$ che non ha nessun modello (cioè che non è soddisfatta da alcuna v) si dice **contraddizione proposizionale**.

Se $\boldsymbol{p} \models \boldsymbol{q}$ e $\boldsymbol{q} \models \boldsymbol{p}$, allora diremo che $\boldsymbol{p}$ e $\boldsymbol{q}$ sono **tautologicamente equivalenti**, in simboli

$$\boldsymbol{p} \equiv \boldsymbol{q}.$$

Equivalentemente, $\boldsymbol{p} \equiv \boldsymbol{q}$ se e solo se $v(\boldsymbol{p}) = v(\boldsymbol{q})$, per ogni valutazione v. La $\equiv$ è una relazione di equivalenza su $\operatorname{Prop}(L)$. Le tautologie proposizionali sono tutte $\equiv$-equivalenti e formano una classe d'equivalenza che si indica con $\top$. Analogamente le contraddizioni proposizionali formano una classe d'equivalenza che si indica con $\bot$. Se $[\boldsymbol{p}], [\boldsymbol{q}] \in \operatorname{Prop}(L)/{\equiv}$ poniamo

$$[\boldsymbol{p}] \curlyvee [\boldsymbol{q}] = [\boldsymbol{p} \boldsymbol{\vee} \boldsymbol{q}]$$
$$[\boldsymbol{p}] \curlywedge [\boldsymbol{q}] = [\boldsymbol{p} \boldsymbol{\wedge} \boldsymbol{q}]$$
$$[\boldsymbol{p}]^* = [\boldsymbol{\neg p}].$$

Esercizio 23.38. Dimostrare che:

(i) con queste operazioni $\operatorname{Prop}(L)/{\equiv}$ è un'algebra di Boole, con $\bot$ minimo e $\top$ massimo,

(ii) se $\boldsymbol{p} \in \operatorname{Prop}(L)$ e v, w sono valutazioni tali che $v(A) = w(A)$ per ogni lettera A che compare in $\boldsymbol{p}$, allora $v(\boldsymbol{p}) = w(\boldsymbol{p})$,

(iii) le seguenti affermazioni sono equivalenti

(a) $[\boldsymbol{p}] \leq [\boldsymbol{q}]$
(b) $\boldsymbol{p} \Rightarrow \boldsymbol{q}$ è una tautologia proposizionale,
(c) $v(\boldsymbol{p}) \leq v(\boldsymbol{q})$, per ogni valutazione v.

Teorema 23.39. *Sia* $B = \mathrm{Prop}(L)/\equiv$.

(a) *Se* L *è finito,* $L = \{A_0, \ldots, A_{n-1}\}$*, allora* B *è atomica e gli atomi sono le classi d'equivalenza delle proposizioni della forma*

$$\boldsymbol{q}^s = A_0^{s(0)} \boldsymbol{\wedge} \ldots \boldsymbol{\wedge} A_{n-1}^{s(n-1)}$$

dove $s \in {}^n2$ *e*

$$A_k^i = \begin{cases} A_k & \text{se } i = 1, \\ \boldsymbol{\neg} A_k & \text{se } i = 0. \end{cases}$$

Quindi $|\mathrm{At}(B)| = 2^n$ *e* $|B| = 2^{2^n}$.

(b) *Se* L *è infinito, allora* B *è priva di atomi.*

Dimostrazione. (a) Osserviamo che $v(\boldsymbol{q}^s) = \top$ se e solo se $v(A_k) = s(k)$. In altre parole, $\boldsymbol{q}^s$ è soddisfatta da un'unica valutazione che indichiamo con v_s. Questo implica che $\boldsymbol{q}^s \not\equiv \boldsymbol{q}^t$ quando $s \neq t$. Se $[\boldsymbol{p}] < [\boldsymbol{q}^s]$ allora per l'Esercizio 23.38 $v(\boldsymbol{p}) \leq v(\boldsymbol{q}^s)$ per ogni v e

$$0 = w(\boldsymbol{p}) < w(\boldsymbol{q}^s) = \top$$

per una qualche w. Ma $w(\boldsymbol{q}^s) = \top$ se e solo se $w = v_s$, quindi $v(\boldsymbol{p}) = 0$ per ogni valutazione, cioè $\boldsymbol{p}$ è una contraddizione proposizionale, ovvero $[\boldsymbol{p}] = \bot$. Segue che i $[\boldsymbol{q}^s]$ sono atomi. Infine mostriamo che se $[\boldsymbol{p}] > \bot$, allora $[\boldsymbol{p}] \geq [\boldsymbol{q}^s]$ per qualche s: sia w una valutazione tale che $w(\boldsymbol{p}) = \top$ e sia $s \in {}^n2$ tale che $w = v_s$, vale a dire $s(k) = w(A_k)$ per $k = 0, \ldots, n-1$. Se $v = w$, allora $\top = w(\boldsymbol{q}^s) \leq w(\boldsymbol{p}) = \top$. Se $v \neq w$, allora $0 = v(\boldsymbol{q}^s) \leq v(\boldsymbol{p})$. Quindi $[\boldsymbol{q}^s] \leq [\boldsymbol{p}]$.

(b) Sia $\boldsymbol{p} \in \mathrm{Prop}(L) \setminus \bot$ e sia A una lettera che non occorre in $\boldsymbol{p}$. Dimostriamo che $\bot < [A \boldsymbol{\wedge} \boldsymbol{p}] < [\boldsymbol{p}]$. Chiaramente $w(A \boldsymbol{\wedge} \boldsymbol{p}) \leq w(\boldsymbol{p})$ per ogni valutazione w e poiché $\boldsymbol{p}$ non è una contraddizione proposizionale, c'è una valutazione v tale che $v(\boldsymbol{p}) = \top$. Siano v_0 e v_1 le valutazioni

$$v_i(B) = \begin{cases} v(B) & \text{se } B \neq A, \\ i & \text{se } B = A. \end{cases}$$

Per l'Esercizio 23.38 v_0 e v_1 testimoniano, rispettivamente, che $[A \boldsymbol{\wedge} \boldsymbol{p}] < [\boldsymbol{p}]$ e $\bot < [A \boldsymbol{\wedge} \boldsymbol{p}]$.

Per l'arbitrarietà di $\boldsymbol{p}$ e A, questo prova che B è priva di atomi. □

Definizione 23.40. Un insieme Γ di proposizioni si dice **soddisfacibile** se esiste una valutazione v tale che $\forall \boldsymbol{p} \in \Gamma\, (v(\boldsymbol{p}) = \top)$. Si dice **finitamente soddisfacibile** se ogni sottoinsieme finito di Γ è soddisfacibile.

Chiaramente se Γ è soddisfacibile è anche finitamente soddisfacibile e, banalmente, se L è finito vale anche l'implicazione inversa per il Teorema 23.39. Nella prossima sezione dimostreremo che l'implicazione vale per tutti gli L (Teorema 23.42).

Una **tavola di verità** n-aria per L è semplicemente una funzione

$$T\colon {}^n2 \to 2.$$

Ogni proposizione $\boldsymbol{p}$ contenente n lettere proposizionali $A_1, \dots, A_n$ definisce una tavola di verità n-aria: ad ognuna delle 2^n valutazioni v di $A_1, \dots, A_n$ associamo il valore $v(\boldsymbol{p})$. Utilizzando le costruzione della **forma normale disgiuntiva** e **congiuntiva** (Esercizio 3.36 della Sezione 3.C.1) si dimostra la seguente:

Proposizione 23.41. *Ogni tavola di verità n-aria è la tavola di verità di una proposizione $\boldsymbol{p}$ contenente le lettere $A_1, \dots, A_n$. Inoltre possiamo supporre che $\boldsymbol{p}$ contenga soltanto i connettivi $\neg$ e $\wedge$, oppure soltanto i connettivi $\neg$ e $\vee$.*

23.H.2. *Il teorema di compattezza per il calcolo proposizionale.* Il seguente risultato è noto come **Teorema di Compattezza per il calcolo proposizionale**.

Teorema 23.42. *Supponiamo che l'insieme L sia bene ordinabile e sia $\Gamma \subseteq \mathrm{Prop}(L)$ un insieme finitamente soddisfacibile. Allora Γ è soddisfacibile.*

Dimostrazione. L'ipotesi su Γ equivale a dire che $\bot \neq [\boldsymbol{p}_1 \wedge \dots \wedge \boldsymbol{p}_n]$ per ogni $\boldsymbol{p}_1 \dots, \boldsymbol{p}_n \in \Gamma$, cioè che il filtro generato da $\{[\boldsymbol{p}] \mid \boldsymbol{p} \in \Gamma\}$ è proprio. Sia D un ultrafiltro che estende questo filtro e sia $v\colon L \to 2$

$$v(A) = 1 \qquad \text{se e solo se} \qquad [A] \in D.$$

È facile verificare che

$$v(\boldsymbol{p}) = 1 \qquad \text{se e solo se} \qquad [\boldsymbol{p}] \in D. \tag{23.5}$$

Quindi $\boldsymbol{p} \in \Gamma$ implica che $[\boldsymbol{p}] \in F \subseteq D$, da cui $v(\boldsymbol{p}) = 1$. Abbiamo quindi dimostrato che Γ è soddisfacibile. □

Esercizio 23.43. Completare i dettagli della dimostrazione precedente dimostrando, per induzione sulla lunghezza di $\boldsymbol{p}$, che vale (23.5).

Corollario 23.44. *Se $\Gamma \vDash \boldsymbol{p}$ allora $\Delta \vDash \boldsymbol{p}$ per qualche $\Delta \subseteq \Gamma$ finito.*

Dimostrazione. Supponiamo, per assurdo, che $\Delta \nvDash \boldsymbol{p}$, per ogni $\Delta \subseteq \Gamma$ finito e sia v_Δ una valutazione che soddisfa Δ ma tale che $v_\Delta(\boldsymbol{p}) = 0$. Allora v_Δ soddisfa $\Delta \cup \{\neg \boldsymbol{p}\}$. Ne segue che

$$\forall \Delta \subseteq \Gamma\, (\Delta \text{ finito } \Rightarrow \Delta \cup \{\neg \boldsymbol{p}\} \text{ è soddisfacibile})$$

e quindi per il Teorema di Compattezza $\Gamma \cup \{\neg \boldsymbol{p}\}$ è soddisfacibile. Sia v una valutazione che soddisfa Γ e $\neg \boldsymbol{p}$. Ma, per ipotesi, ogni valutazione che soddisfa Γ deve soddisfare anche $\boldsymbol{p}$: contraddizione. □

Vediamo un'interessante applicazione del Teorema di Compattezza del calcolo proposizionale.

Teorema 23.45. *Ogni ordine parziale stretto $\prec$ su un insieme X può essere esteso ad un ordine totale stretto $\lhd$ su X, vale a dire $\langle X, \lhd \rangle$ è lineare e*

$$\forall x, y \in X \, (x \prec y \Rightarrow x \lhd y) \, .$$

Dimostrazione. Sia $\langle X, \prec \rangle$ un ordine parziale stretto: per la Proposizione 8.7 possiamo supporre che X sia infinito. Sia $L = X \times X$ e consideriamo il calcolo proposizionale $\mathrm{Prop}(L)$ in cui le lettere proposizionali sono le coppie ordinate (x, y), con $x, y \in X$. Sia $\Gamma \subseteq \mathrm{Prop}(L)$ l'insieme

$$\{\neg(x,x) \mid x \in X\} \cup \{(x,y) \vee (y,x) \mid x, y \in X, x \neq y\}$$
$$\cup \{((x,y) \wedge (y,z)) \Rightarrow (x,z) \mid x, y, z \in X\}.$$

L'idea è che una lettera proposizionale (x, y) asserisce che x precede y in un ordine stretto su X. L'insieme Γ è costituito da tre insiemi: il primo insieme equivale alla proprietà irriflessiva, il secondo alla connessione, il terzo alla transitività. Per ogni $v \colon L \to 2$ definiamo una relazione binaria $\lhd = \lhd_v$ su X

$$x \lhd y \quad \Leftrightarrow \quad v(A) = 1, \text{ dove } A = (x, y) \in L$$

e, viceversa, ogni relazione binaria $\lhd$ definisce una valutazione $v = v_{\lhd}$. Allora v soddisfa Γ se e solo se $\lhd$ è un ordine lineare stretto su X. Inoltre se v soddisfa $\Gamma \cup \Delta$, dove

$$\Delta = \{(x, y) \mid x \prec y\},$$

allora l'ordinamento indotto $\lhd$ estende $\prec$. Quindi, per il Teorema di Compattezza, è sufficiente dimostrare che $\Gamma \cup \Delta$ è finitamente soddisfacibile.

Sia $\Gamma_0 \cup \Delta_0$ finito, con $\Gamma_0 \subseteq \Gamma$ e $\Delta_0 \subseteq \Delta$. Sia X_0 l'insieme degli $x \in X$ che occorrono in una qualche lettera proposizionale di $\Gamma_0 \cup \Delta_0$. Allora X_0 è finito e per la Proposizione 8.7 c'è un ordine totale stretto $\lhd$ su X_0 che estende $\prec$ su X_0. Sia $v \colon L \to 2$ una valutazione tale che

$$\forall x, y \in X_0 \, (v(x, y) = 1 \Leftrightarrow x \lhd y) \, .$$

Verifichiamo che $v(\boldsymbol{p}) = 1$ per ogni $p \in \Gamma_0 \cup \Delta_0$. Se $\boldsymbol{p} = \neg(x, y) \in \Gamma_0$, allora $x \in X_0$ e la tesi discende dal fatto che $x \lhd x$ non vale. Se $\boldsymbol{p} = (x, y) \vee (y, x) \in \Gamma_0$ allora $x \neq y$ e quindi $x \lhd y$ oppure $y \lhd x$, cioè $v(x, y) = 1$ oppure $v(y, x) = 1$. Se $\boldsymbol{p} = ((x, y) \wedge (y, z)) \Rightarrow (x, z) \in \Gamma_0$ e, per assurdo, $v(\boldsymbol{p}) = 0$, allora $v(x, y) = v(y, z) = 1$ e $v(x, z) = 0$, cioè $x \lhd y$ e $y \lhd z$ ma $\neg(x \lhd z)$: contraddizione. Se $\boldsymbol{p} \in \Delta_0$ allora $\boldsymbol{p} = (x, y)$ e $x \prec y$, quindi $x \lhd y$, da cui $v(\boldsymbol{p}) = 1$. Quindi v soddisfa $\Gamma_0 \cup \Delta_0$.

Per l'arbitrarietà di $\Gamma_0 \cup \Delta_0$ si ha che $\Gamma \cup \Delta$ è finitamente soddisfacibile, come richiesto. □

Esercizi

Esercizio 23.46. Completare la dimostrazione della Proposizione 23.2.

Esercizio 23.47. Dimostrare che:

(i) in un reticolo distributivo un ideale massimale è primo;

(ii) il reticolo $\mathcal{M}_3$ della Figura 1 a pagina 156 ha tre ideali massimali, nessuno dei quali è primo;

(iii) nel reticolo $\mathcal{O}$ degli aperti di $\mathbb{R}$, per ogni $r \in \mathbb{R}$ la famiglia $\{U \in \mathcal{O} \mid r \in U\}$ è un filtro primo, ma non massimale.

Esercizio 23.48. Dimostrare che:

(i) Se $\emptyset \neq \mathcal{I}$ è una famiglia di ideali di un reticolo M, allora $\bigcap \mathcal{I}$ è un ideale di M. Analogamente per $\mathcal{F}$ famiglia non vuota di filtri su M.

(ii) Il filtro D generato da $X \subseteq B$ è

$$D = \bigcap \{F \mid F \supseteq X \text{ e } F \text{ è un filtro}\}$$

è il più piccolo filtro contenente X.

(iii) Se F è il filtro generato dalla sottobase X allora F è proprio se e solo se $\mathbf{0} \notin X^{\curlywedge}$.

(iv) Se $f\colon B \to C$ è un omomorfismo suriettivo di algebre di Boole, allora $\ker(f)$ è massimale se e solo se C è l'algebra minimale $\{\mathbf{0}, \mathbf{1}\}$.

Esercizio 23.49. La famiglia degli aperti di uno spazio topologico è un reticolo distributivo. Il suo duale è il reticolo dei chiusi.

Esercizio 23.50. Dimostrare che il reticolo $\left\langle \mathbb{N}^{\mathbb{N}}/=^*, \leq^* \right\rangle$ è distributivo.

Esercizio 23.51. 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 23.52. 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 23.C.4. Dimostrare che c'è un $C \subseteq \mathbb{N}$ tale che

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

Esercizio 23.53. Dimostrare che se F è un filtro proprio e generato da a, allora$F$ è un ultrafiltro se e solo se a è un atomo.

Esercizio 23.54. Dimostrare che se D è un ultrafiltro su un insieme X e $\{X_0, \ldots, X_k\}$ è una partizione di X, allora c'è un unico $i < k$ tale che $X_i \in D$.

Esercizio 23.55. Dimostrare che ogni ultrafiltro non principale su $\mathbb{N}$ estende il filtro di Fréchet.

Esercizio 23.56. Sia B un'algebra di Boole e sia $b \in B \setminus \{\bot\}$ un elemento al di sotto del quale non ci sono atomi.

(1) Costruire una funzione $\left\langle b_s \mid s \in 2^{<\mathbb{N}} \right\rangle$ tale che
   (i) $b_\emptyset = b$,
   (ii) $\bot < b_{s^\frown\langle i\rangle} < b_s$ e
   (iii) $b_{s^\frown\langle 0\rangle} \curlywedge b_{s^\frown\langle 1\rangle} = \bot$.

(2) Dimostrare che $2^{\mathbb{N}}$ si inietta in $\{F \mid F \text{ è un filtro di } B \text{ e } b \in F\}$.

(3) Concludere che se B è numerabile e priva di atomi, allora l'insieme degli ultrafiltri di B è equipotente ad $\mathbb{R}$.

Esercizio 23.57. Siano $(A_n, \lhd_n)$ dei buoni ordini non vuoti e sia U un ultrafiltro non principale su ω. Supponiamo che $n \leq |A_{k_n}|$ per una qualche successione crescente $k_0 < k_1 < \dots$ tale che $\{k_i \mid i \in \omega\} \in U$. Allora ${}^{\omega}2 \precsim \prod_U A_n$, cioè l'ultraprodotto ha taglia maggiore o uguale a $\mathbb{R}$.

[Suggerimento: considerare dapprima il caso in cui $2^n \leq |A_n|$.]

Esercizio 23.58. Dimostrare l'Osservazione 23.25(b).

Esercizio 23.59. Sia $(P, \leq)$ un pre-ordine non vuoto.

(i) Dimostrare che $\sim$ è davvero una relazione di equivalenza, che $\lesssim$ è un ordine parziale, che $(P/{\sim}, \lesssim)$ è separativo, e che la mappa

$$(P, \leq, \perp) \to (P/{\sim}, \lesssim, \perp^*), \qquad p \mapsto [p]$$

è un morfismo di strutture, dove $\perp^*$ è la relazione di incompatibilità per $\lesssim$.

(ii) Un **nodo al di sotto di** p è un $q \leq p$ che è confrontabile con ogni elemento minore di p, cioè

$$\forall r \leq p \; (q \leq r \vee r \leq q) \, .$$

Dimostrare che se q è un nodo sotto p allora $q \sim p$. Concludere che se gli elementi di P sono tutti tra loro confrontabili, oppure se P ha un minimo, allora il quoziente separabile ha solo un elemento.

Esercizio 23.60. Dimostrare che se D è un sottoinsieme denso di un'algebra di Boole completa B, allora

$$\forall X \subseteq B \, \exists Y \subseteq D \, [\bigvee Y = \bigvee X].$$

Esercizio 23.61. Sia $j \colon P \to Q$ una mappa tra ordini e supponiamo che j sia un'immersione densa, oppure che P e Q siano algebre di Boole e j un'immersione di algebre di Boole. Dimostrare che j è un'immersione di strutture $(P, \leq_P, \perp_P) \to (Q, \leq_Q, \perp_Q)$.

Esercizio 23.62. Supponiamo che M sia un reticolo completo e separativo. Dimostrare che

(i) M è complementato,

(ii) M è un'algebra di Boole completa.

Esercizio 23.63. Siano $A, B \subseteq P$, un insieme ordinato. Dimostrare che:

(i) $A^{\mathrm{U}} \supseteq B \Leftrightarrow A \subseteq B^{\mathrm{L}}$;

(ii) $A \subseteq A^{\mathrm{UL}}$ and $A \subseteq A^{\mathrm{LU}}$;

(iii) se $A \subseteq B$ allora $B^{\mathrm{L}} \subseteq A^{\mathrm{L}}$ e $B^{\mathrm{U}} \subseteq A^{\mathrm{U}}$;

(iv) $A^{\mathrm{U}} = A^{\mathrm{ULU}}$ e $A^{\mathrm{L}} = A^{\mathrm{LUL}}$;

(v) la funzione $\mathscr{P}(P) \to \mathscr{P}(P)$, $A \mapsto A^{\mathrm{UL}}$ è un operatore di chiusura, quindi $\mathbf{DM}(P)$ è un reticolo completo;

(vi) $\downarrow x \in \mathbf{DM}(P)$, per ogni $x \in P$;

(vii) se A ha un estremo superiore in P, diciamo a, allora $A^{\mathrm{UL}} = \downarrow a$. Similmente, se a è l'estremo inferiore in P di A, allora $A^{\mathrm{LU}} = \uparrow a$;

(viii) la funzione $j \colon P \to \mathbf{DM}(P)$, $j(x) = \downarrow x$, è un'immersione di ordini che preserva gli estremi superiori ed inferiori, quando esistono in P;

(ix) $j[P]$ è denso in $\mathbf{DM}(P)$;

(x) se L è un reticolo completo e $i \colon P \to L$ è un'immersione tale che $i[P]$ è denso in L, allora $L \cong \mathbf{DM}(P)$.

Esercizio 23.64. Sia P un insieme ordinato. Dimostrare che:

(i) se P è separativo, allora anche $\mathbf{DM}(P)$ è separativo, quindi $\mathbf{DM}(P) \cong \mathbf{RO}(P)$;

(ii) se P è un ordine lineare denso, allora $\mathbf{DM}(P) \cong \mathbf{D}(P)$.

Esercizio 23.65. Dimostrare che un'algebra di Boole B è completa se e solo se $\mathrm{St}(B)$ è estremamente sconnesso, cioè la chiusura di ogni aperto è un chiuso-aperto.

Esercizio 23.66. Dimostrare che un'algebra di Boole è numerabile se e solo se il suo spazio di Stone è separabile.

Esercizio 23.67. Dimostrare che un'algebra di Boole è priva di atomi se e solo se il suo spazio di Stone non ha punti isolati.

Esercizio 23.68. Siano $\boldsymbol{p} \in \mathrm{Prop}\{A_1, \ldots, A_n\}$ e $\boldsymbol{q}_1, \ldots, \boldsymbol{q}_n \in \mathrm{Prop}(L)$. Dimostrare che $\boldsymbol{p}$ è una tautologia/contraddizione se e solo se $\boldsymbol{p}[\boldsymbol{q}_1/A_1, \ldots, \boldsymbol{q}_n/A_n]$ è una tautologia/contraddizione.

Note e osservazioni

Il Teorema 23.26 è stato dimostrato nel 1936 da Stone. La costruzione di $\mathbf{DM}(P)$ e la sua versione specifica, il completamento booleano, è stata introdotta da MacNeille nel 1937.

24. Gli ordinali e la topologia*

Richiamiamo dalla Sezione 10.I.1 la costruzione di X', il derivato di uno spazio topologico X, e della successione $X^{(\alpha)}$. Per l'assioma del rimpiazzamento c'è un primo $\bar{\alpha}$ tale che $X^{(\bar{\alpha})} = X^{(\bar{\alpha}+1)}$, e quindi $X^{(\bar{\alpha})} = X^{(\beta)}$ per ogni $\beta > \bar{\alpha}$. Tale $\bar{\alpha}$ è il rango di Cantor-Bendixson X ed è denotato con $\|X\|_{\mathrm{CB}}$.

L'**altezza** di X

$$\mathrm{ht}(X) = \sup\left\{o(x) \mid x \in X \setminus X^{(\bar{\alpha})}\right\}.$$

Allora $\mathrm{ht}(X) = \|X\|_{\mathrm{CB}}$ se $\|X\|_{\mathrm{CB}}$ è limite, e $\mathrm{ht}(X) \dot{+} 1 = \|X\|_{\mathrm{CB}}$ altrimenti.

Corollario 24.1. *Se X è compatto e numerabile, allora $\|X\|_{\mathrm{CB}}$ è un ordinale successore.*

Dimostrazione. Per il Teorema di Cantor-Bendixson possiamo decomporre X nella sua parte perfetta P e la sua parte sparsa S. Per quanto osservato poco sopra, $P = K^{(\bar{\alpha})} = \emptyset$, dove $\bar{\alpha} = \|K\|_{\mathrm{CB}}$. Se $\bar{\alpha}$ fosse limite allora $K^{(\bar{\alpha})} = \bigcap_{\beta<\bar{\alpha}} K^{(\beta)}$ sarebbe intersezione vuota di una famiglia decrescente di compatti non vuoti, contro la proprietà dell'intersezione finita. □

Quindi in un compatto metrico numerabile K l'ordinale $\gamma \stackrel{\mathrm{def}}{=} \mathrm{ht}(K)$ è il predecessore di $\|K\|_{\mathrm{CB}}$, così che $K^{(\gamma)} \neq \emptyset$, ma $K^{(\gamma\dot{+}1)} = \emptyset$. L'insieme $K^{(\gamma)}$ non può essere infinito, altrimenti $\{\{x\} \mid x \in K^{(\gamma)}\}$ sarebbe un ricoprimento aperto privo di sotto-ricoprimenti finiti — la sua taglia n verrà indicata con $\mathrm{wd}(K)$. L'ordinale $\mathrm{ht}(K)$ può assumere valori arbitrariamente grandi, come vedremo nella prossima sezione, quindi possiamo caratterizzare il primo ordinale più che numerabile come

$$\omega_1 = \sup\{\mathrm{ht}(K) \mid K \text{ compatto metrico numerabile}\}.$$

Il Teorema 24.9 più sotto mostra come $\mathrm{ht}(K)$ e $\mathrm{wd}(K)$ caratterizzino i compatti metrici numerabili a meno di omeomorfismo.

24.A. La topologia degli ordinali. Ogni ordinale può essere visto come spazio topologico, e dato che α è un sottospazio di β quando $\alpha < \beta$, è naturale considerare la topologia su un ordinale come indotta dalla topologia degli intervalli su $\langle \mathrm{Ord}, \leq \rangle$. Il problema è che non ha senso parlare di topologia su una classe propria quale è Ord. Tuttavia possiamo dare la seguente

Definizione 24.2. Sia $\Omega \leq \mathrm{Ord}$. Una classe $A \subseteq \Omega$ si dice aperta in Ω se per ogni $\alpha \in A$ c'è un intervallo di base I tale che $\alpha \in I \subseteq A$. Se $\Omega \setminus A$ è aperta in Ω, diremo che A è chiusa in Ω.

Esercizio 24.3. Sia $\Omega \leq \mathrm{Ord}$. Dimostrare che:

(i) Gli intervalli di base di Ω sono della forma $[\alpha; \beta)$ con $\alpha < \beta \leq \Omega$.

(ii) La topologia su Ω è totalmente sconnessa.

(iii) α è aperto in Ω, per ogni $\alpha < \Omega$.

(iv) Se $\lambda \in A \subseteq \Omega$ con A aperto e λ limite, allora $\lambda \in [\alpha \dot{+} 1; \lambda] \subseteq A$ per qualche α.

(v) $C \subseteq \Omega$ è chiuso se e solo se

$$\forall \lambda \in \alpha \, (\lambda \text{ limite e } \lambda = \bigcup (C \cap \lambda) \Rightarrow \lambda \in C) \, .$$

A quali condizioni deve soddisfare $f \colon \alpha \to \beta$ affinché sia una funzione continua? Chiaramente la continuità non è mai un problema agli ordinali successori, in quanto sono punti isolati. Supponiamo quindi $\gamma < \alpha$ sia limite. Se $f(\gamma)$ è un successore, allora per la continuità di f, c'è un intervallo $[\beta; \gamma]$ che è mandato da f nel singoletto $\{f(\gamma)\}$; in altre parole: f è definitivamente costante al di sotto di γ. Se $f(\gamma)$ è limite, allora per ogni $\delta < f(\gamma)$ c'è un $\beta < \gamma$ tale che l'intervallo $[\beta; \gamma]$ è mandato da f nell'intervallo $[\delta; f(\gamma)]$.

Esercizio 24.4. (i) Dimostrare che se f è una funzione crescente dove $f \colon \alpha \to \beta$ oppure $f \colon \mathrm{Ord} \to \mathrm{Ord}$, allora f è continua (nel senso della topologia) se e solo se è continua nel senso della formula (13.3) a pagina 296, cioè

$$\forall \lambda (\lambda \text{ limite} \Rightarrow f(\lambda) = \sup_{\beta < \lambda} f(\beta)).$$

(ii) Dimostrare che se ξ e λ sono ordinali limite, $f \colon \xi \to \lambda$ è crescente e continua e $\bigcup \mathrm{ran}(f) = \lambda$, allora $\mathrm{ran}(f)$ è un chiuso di λ.

Vale anche il converso della parte (ii) dell'Esercizio 24.4 (Esercizio 24.20).

Teorema 24.5. *Se $\alpha < \omega_1$, allora α è immergibile in $\mathbb{R}$, cioè c'è una funzione $f \colon \alpha \to \mathbb{R}$ che preserva l'ordine e tale che* $\mathrm{ran}(f)$ *è un chiuso di* $\mathbb{R}$.

La dimostrazione è differita alla Sezione **??** (Esercizio 10.78).

Esercizio 24.6. Se $f\colon \alpha \rightarrowtail \mathbb{R}$ è un'immersione, allora f è un omeomorfismo tra α e $\operatorname{ran}(f) \subseteq \mathbb{R}$.

Quindi gli spazi $\alpha \dotplus 1$ (con $\alpha < \omega_1$) sono esempi di spazi compatti, numerabili e completamente metrizzabili, cioè ammettono una metrica completa compatibile con la topologia ordinale. Benché siano tutti distinguibili come ordini, non sono tutti distinguibili come spazi topologici.

Esercizio 24.7. Se $\lambda \geq \omega$ è limite, allora $\lambda \dotplus n$ e $\lambda \dotplus m$ sono omeomorfi per ogni $0 < n, m < \omega$.

Enunciamo ora tre risultati che saranno dimostrati nella prossima sezione. Il primo risultato classifica, a meno di omeomorfismi, tutti gli ordinali numerabili.

Teorema 24.8. *Un ordinale numerabile è omeomorfo ad uno ed uno solo degli ordinali della forma*

$$\begin{aligned}
&(24.1a) && n && (n < \omega),\\
&(24.1b) && \omega^{\cdot\gamma} \cdot n \dotplus \omega^{\cdot\delta} \cdot m && (0 < \delta < \gamma < \omega_1, 0 \leq n < \omega, 0 < m < \omega),\\
&(24.1c) && \omega^{\cdot\gamma} \cdot n \dotplus 1 && (0 < \gamma < \omega_1, 0 < n < \omega).
\end{aligned}$$

e $n_1, \ldots, n_k, n_{k+1} > 0$*,*

Il secondo risultato classifica, a meno di omeomorfismi, tutti i compatti metrici numerabili.

Teorema 24.9. *Se K è un compatto metrico numerabile infinito e $\operatorname{ht}(K) = \gamma$ e $\operatorname{wd}(K) = n$, allora K è omeomorfo a $\omega^{\cdot\gamma} \cdot n \dotplus 1$. In particolare, due spazi compatti metrici numerabili K_1 e K_2 sono omeomorfi se e solo se $\operatorname{ht}(K_1) = \operatorname{ht}(K_2)$ e $\operatorname{wd}(K_1) = \operatorname{wd}(K_2)$.*

Mettendo insieme i Teoremi 24.8 e 24.9 otteniamo che gli spazi compatti metrici numerabili sono, a meno di omeomorfismi, i numeri naturali, oppure gli ordinali della forma $\omega^{\cdot\gamma} \cdot n \dotplus 1$, con $0 < n < \omega$ e $\gamma < \omega_1$.

Corollario 24.10. *Uno spazio metrico localmente compatto numerabile X è omeomorfo ad un ordinale numerabile della forma*

(a) $\omega^{\cdot \operatorname{ht}(X)} \cdot n \dotplus 1$*, per qualche $0 < n < \omega$, se X è compatto,*

(b) $\omega^{\cdot \operatorname{ht}(X)} \cdot n \dotplus \omega^{\cdot\delta} \cdot m$*, per qualche $\delta < \operatorname{ht}(X)$, $0 < n < \omega$ e $0 \leq m < \omega$ se X non è compatto.*

Osservazione 24.11. L'ipotesi di metrizzabilità nell'enunciato del Teorema 24.9 e del Corollario 24.10 può essere eliminata, assumendo AC. Infatti uno spazio compatto numerabile è uno spazio primo numerabile [**Eng89**,

Esercizio 3.1.F(a), pag. 135] e per la numerabilità dello spazio questo implica che è secondo numerabile. Ma ogni spazio normale secondo numerabile è metrizzabile [**Eng89**, ??].

24.B. Caratterizzazione dei compatti numerabili. L'ordine di isolamento è un invariante topologico, nel senso che se $o^X(x) = \alpha$ e $f\colon X \to Y$ è un omeomorfismo, allora $o^Y(f(x)) = \alpha$, e f è un omeomorfismo di $X^{(\alpha)}$ su $Y^{(\alpha)}$. Se $Y \subseteq X$ e $y \in Y$ allora $o^Y(y) \leq o^X(y)$ — la disuguaglianza può essere stretta dato che y potrebbe risultare isolato in Y e non in X, ma se Y è aperto vale l'uguaglianza. In particolare, se H è un chiuso-aperto di un compatto numerabile metrico K, allora $o^H(x) = o^K(x)$ per tutti gli $x \in H$. Osserviamo che se $U \subseteq X$ è aperto e contiene un punto di ordine α, allora contiene punti di ogni ordine $\beta < \alpha$. Definiamo $o(\alpha)$, l'ordine di isolamento di un ordinale α, come $o^{\alpha\dot{+}1}(\alpha)$. Poiché un ordinale è un aperto di ogni ordinale più grande, $o(\alpha) = o^\beta(\alpha)$ per ogni $\beta > \alpha$. In analogia a quanto fatto per gli spazi topologici (che per statuto sono insiemi, e non classi proprie) per ogni $X \subseteq \mathrm{Ord}$ possiamo definire

$$X' = X \setminus \{\alpha \in X \mid \exists \beta < \alpha\, ((\beta; \alpha] \cap X = \{\alpha\})\}$$

e le sue iterazioni come in (**??**). In particolare

$$\mathrm{Ord}^{(\alpha)} = \{\beta \mid o(\beta) \geq \alpha\}\,.$$

Poiché lo spazio $Y = \gamma$ è un aperto di Ord, si ha che $Y^{(\alpha)} = Y \cap \mathrm{Ord}^{(\alpha)}$ per ogni α, quindi per analizzare le classi derivate $Y^{(\alpha)}$ è sufficiente studiare le classi $\mathrm{Ord}^{(\alpha)}$.

Lemma 24.12. *Se $\alpha > 0$, allora*

$$\mathrm{Ord}^{(\alpha)} = \{\omega^{\cdot\alpha} \cdot \nu \mid 0 < \nu\}. \tag{24.2}$$

Dimostrazione. I punti non isolati di Ord sono gli ordinali limite che, per l'Esercizio 10.70, sono della forma $\omega \cdot \nu$. Quindi la (24.2) vale per $\alpha = 1$. Analogamente, se vale per α, allora i punti non isolati di $\mathrm{Ord}^{(\alpha)}$ sono della forma $\omega^{\cdot\alpha} \cdot \nu$ con ν limite, che quindi può essere scritto come $\omega \cdot \xi$. Ne consegue che $\mathrm{Ord}^{(\alpha\dot{+}1)} = \{\omega^{\cdot\alpha\dot{+}1} \cdot \xi \mid 0 < \xi\}$, cioè la formula (24.2) vale per $\alpha \dot{+} 1$. Supponiamo infine che α sia limite e che (24.2) valga per ogni $\alpha^* < \alpha$. Sia $\lambda \in \mathrm{Ord}^{(\alpha)} = \bigcap_{\alpha^*<\alpha} \mathrm{Ord}^{(\alpha^*)}$: è un ordinale limite e la sua forma normale di Cantor (Esercizio 15.15) è

$$\lambda = \omega^{\cdot\xi_0} \cdot n_0 \dot{+} \cdots \dot{+} \omega^{\cdot\xi_k} \cdot n_k \tag{24.3}$$

dove $\xi_0 > \cdots > \xi_k > 0$ e $n_0, \ldots, n_k > 0$.

Poiché λ è della forma $\omega^{\cdot\alpha'} \cdot \nu^*$, per ogni $\alpha^* < \alpha$, si verifica facilmente (vedi l'Esercizio 24.13 qui sotto) che $\xi_k \geq \alpha^*$. Quindi λ è della forma $\omega^{\cdot\alpha} \cdot \nu$, con $\nu > 0$. Viceversa, se $\lambda = \omega^{\cdot\alpha} \cdot \nu$ e $\alpha^* < \alpha$, allora $\lambda = \omega^{\cdot\alpha^*} \cdot (\omega^{\cdot\eta} \cdot \nu)$, dove

η è tale che $\alpha^* \dot{+} \eta = \alpha$, e quindi $\lambda \in \mathrm{Ord}^{(\alpha^*)}$. Poiché α^* è arbitrario si ha che $\lambda \in \bigcap_{\alpha^*<\alpha} \mathrm{Ord}^{(\alpha^*)} = \mathrm{Ord}^{(\alpha)}$. Quindi la formula (24.2) vale anche per α limite. □

Esercizio 24.13. Un ordinale limite $\lambda > 0$ è della forma $\omega^{\cdot\alpha} \cdot \nu$, con $\nu > 0$ se e solo se $\alpha \leq \xi_k$, dove ξ_k è il coefficiente della forma normale di Cantor di λ come in (24.3).

Quindi per $\alpha \neq 0$,

$$o(\alpha) = \gamma \Leftrightarrow \alpha = \omega^{\cdot\gamma} \cdot (\nu \dot{+} 1).$$

Un ordinale è topologicamente incomprimibile se non è omeomorfo ad un ordinale più piccolo.

Lemma 24.14. *Se $\xi, n > 0$ allora $\omega^{\cdot\xi} \cdot n$ è incomprimibile.*

Dimostrazione. Supponiamo, per assurdo, che $\omega^{\cdot\xi} \cdot n$ sia omeomorfo ad un ordinale λ più piccolo. Per la Proposizione **??** λ è limite e possiamo supporre che la sua forma normale di Cantor sia data dalla (24.3). Se $\xi_0 < \xi$ si ottiene una contraddizione dal fatto che

$$\left\{\omega^{\cdot\xi_0} \cdot m \mid m \in \omega\right\} \subseteq \omega^{\cdot\xi} \cdot n$$

mostra che ci sono infiniti punti in $\omega^{\cdot\xi} \cdot n$ di ordine ξ_0, mentre in λ ce ne sono una quantità finita. Quindi $\xi = \xi_0$ e $n_0 < n$. Ma $\omega^{\cdot\xi} \cdot n$ e λ non possono essere omeomorfi dato che $\omega^{\cdot\xi} \cdot n$ contiene almeno n_0 punti di ordine ξ, mentre λ non ne contiene altrettanti. □

Esercizio 24.15. Dimostrare che $\omega^{\cdot\gamma_0} \cdot n_0 \dot{+} \omega^{\cdot\delta_0} \cdot m_0$ è omeomorfo a $\omega^{\cdot\gamma_1} \cdot n_1 \dot{+} \omega^{\cdot\delta_1} \cdot m_1$, con $\gamma_i > \delta_i$ e $n_i, m_i > 0$ per $i = 0, 1$ se e solo se $\gamma_0 = \gamma_1$, $\delta_0 = \delta_1$, $n_0 = n_1$ e $m_0 = m_1$.

Quindi gli ordinali della forma (24.1a) e (24.1b) sono a due a due non omeomorfi.

Per l'Esercizio 24.7 gli ordinali incomprimibili infiniti sono della forma λ oppure $\lambda \dot{+} 1$ con λ limite. Fissiamo un ordinale della forma $\lambda \dot{+} 1$ con λ limite e consideriamo la sua espansione in forma normale di Cantor (Esercizio 15.15)

$$\lambda \dot{+} 1 = \omega^{\cdot\xi_0} \cdot n_0 \dot{+} \cdots \dot{+} \omega^{\cdot\xi_k} \cdot n_k \dot{+} 1 \tag{24.4}$$

con $\xi_0 > \cdots > \xi_k > 0$ e $n_0, \ldots, n_k > 0$. Siano $\gamma_0 = \omega^{\cdot\xi_0} \cdot n_0$ e $\gamma_{i+1} = \gamma_i \dot{+} \omega^{\cdot\xi_{i+1}} \cdot n_{i+1}$ così che $\gamma_0 < \cdots < \gamma_k$. Gli insiemi

$$D_0^* = [0; \gamma_0],\ D_1^* = [\gamma_0 \dot{+} 1; \gamma_1],\ \ldots,\ D_k^* = [\gamma_{k-1} \dot{+} 1; \gamma_k]$$

sono chiusi-aperti, formano una partizione di $\lambda \dot{+} 1$, e $\mathrm{ot}(D_i^*) = \omega^{\cdot\xi_i} \cdot n_i \dot{+} 1$ per $i \leq k$. Abbiamo bisogno di un semplice risultato di topologia.

Esercizio 24.16. (i) Sia $X = \bigcup_{i<\nu} D_i$ uno spazio topologico e supponiamo che $\{D_i \mid i < \nu\}$ sia una partizione dello spazio in chiusi-aperti non vuoti. Supponiamo inoltre che α_i sia un ordinale successore e che $f_i \colon D_i \to \alpha_i$ sia un omeomorfismo, per ogni $i < \nu$. Allora X è omeomorfo a $\dot\sum_{i<\nu}\alpha_i$, l'ordinale definito a pagina 324.

(ii) Sia X uno spazio topologico, $\bar x \in X$ un punto non isolato e sia $X = V_0 \supset V_1 \supset \dots$ una base di intorni chiusi-aperti di $\bar x$. Supponiamo f_i ed α_i siano come nella parte (i), dove $D_i = V_i \setminus V_{i+1}$ e $i < \omega$. Allora X è omeomorfo a $(\dot\sum_{i<\omega}\alpha_i) \dotplus 1$.

Applicando la parte (i) dell'Esercizio 24.16 allo spazio $X = \lambda \dotplus 1$ e agli insiemi $D_i = D^*_{k-i}$ (per $i \le k$) si ottiene che $\lambda \dotplus 1$ è omeomorfo a

$$(\omega^{\cdot\xi_k} \cdot n_k \dotplus 1) \dotplus (\omega^{\cdot\xi_{k-1}} \cdot n_{k-1} \dotplus 1) \dotplus \dots \dotplus (\omega^{\cdot\xi_0} \cdot n_0 \dotplus 1)$$

e poiché $\omega^{\cdot\xi_0}$ è additivamente indecomponibile (Esercizio 10.71) e $\omega^{\cdot\xi_i}\cdot n_i \dotplus 1 < \omega^{\cdot\xi_0}$ per ogni $0 < i \le k$, questo ordinale è $\omega^{\cdot\xi_0} \cdot n_0 \dotplus 1$.

Abbiamo quindi dimostrato che:

(24.5) Se $\lambda \dotplus 1$ è come in (24.4) e λ è limite,

allora $\lambda \dotplus 1$ è omeomorfo a $\omega^{\cdot\xi_0} \cdot n_0 \dotplus 1$.

Argomentando come nella dimostrazione del Lemma 24.14 si verifica che $\omega^{\cdot\gamma} \cdot n \dotplus 1$ è omeomorfo a $\omega^{\cdot\delta} \cdot m \dotplus 1$ se e solo se $\gamma = \delta$ e $n = m$, cioè

(24.6) $\alpha \dotplus 1 \ge \omega$ è incomprimibile se e solo se $\alpha \dotplus 1 = \omega^{\cdot\gamma} \cdot n \dotplus 1$, per qualche $\gamma > 0$ e $n > 0$.

Quindi gli ordinali successori incomprimibili sono tutti e soli quelli della forma (24.1a) o (24.1c).

Dimostriamo ora che un ordinale limite è omeomorfo ad un ordinale della forma $\omega^{\cdot\gamma} \cdot n$, oppure della forma $\omega^{\cdot\gamma} \cdot n \dotplus \omega^{\cdot\delta} \cdot m$. Supponiamo λ sia limite come in (24.3). Se $k = 0$ allora $\lambda = \omega^{\cdot\xi_0} \cdot n_0$, quindi possiamo supporre $k > 0$. Per (24.5) $\alpha = \omega^{\cdot\xi_0} \cdot n_0 \dotplus \dots \dotplus \omega^{\cdot\xi_{k-1}} \cdot n_{k-1} \dotplus 1$ è omeomorfo ad $\alpha^* = \omega^{\cdot\xi_0}\cdot n_0 \dotplus 1$ e poiché questi sono chiusi-aperti negli spazi $\alpha \dotplus \omega^{\cdot\xi_k}\cdot n_k = \lambda$ e $\alpha^* \dotplus \omega^{\cdot\xi_k} \cdot n_k = \omega^{\cdot\xi_0} \cdot n_0 \dotplus \omega^{\cdot\xi_k} \cdot n_k$, rispettivamente, si deduce che λ è omeomorfo a $\omega^{\cdot\xi_0} \cdot n_0 \dotplus \omega^{\cdot\xi_k} \cdot n_k$. Abbiamo quindi dimostrato che:

(24.7)

Se λ è limite come in (24.3), allora

$$\lambda \text{ è omeomorfo a } \begin{cases} \omega^{\cdot\xi_0} \cdot n_0 \dotplus \omega^{\cdot\xi_k} \cdot n_k & \text{se } k > 0, \\ \omega^{\cdot\xi_0} \cdot n_0 & \text{se } k = 0. \end{cases}$$

Dimostrazione del Teorema 24.8. Fissiamo $\alpha < \omega_1$. Un ordinale finito può essere omeomorfo soltanto a sé stesso, quindi possiamo supporre che $\alpha \ge \omega$. Se α è limite, allora per (24.7) α è omeomorfo and un unico

(Esercizio 24.15) ordinale della forma $\omega^{\cdot\gamma}\cdot n$ oppure della forma $\omega^{\cdot\gamma}\cdot n \dot{+} \omega^{\cdot\delta}\cdot m$, con $\gamma > \delta$. Se α è successore, allora è omeomorfo a $\lambda \dot{+} 1$ con λ limite per l'Esercizio 24.7, quindi è omeomorfo ad uno ed un solo ordinale della forma $\omega^{\cdot\xi}\cdot n \dot{+} 1$ (24.5).

Infine, per le Proposizioni 10.40 e **??** nessun ordinale $\omega^{\cdot\gamma_0}\cdot n_0 \dot{+} 1$ è omeomorfo ad un ordinale della forma $\omega^{\cdot\gamma_1}\cdot n_1$ o della forma $\omega^{\cdot\gamma_1}\cdot n_1 \dot{+} 1 \dot{+} \omega^{\cdot\delta_1}\cdot n_1$ con $\gamma_1 > \delta_1$. □

Dimostrazione del Teorema 24.9. Dimostriamo per induzione su $\gamma = \mathrm{ht}(K)$ che K è omeomorfo a $\omega^{\cdot\gamma}\cdot n \dot{+} 1$, dove $n = \mathrm{wd}(K)$.

Innanzitutto osserviamo che è sufficiente dimostrare il risultato quando $n = 1$. Infatti se $x_1, \dots, x_n$ sono i punti di ordine γ, fissiamo $H_1, \dots, H_n$ intorni chiusi-aperti di $x_1, \dots, x_n$. Rimpiazzando H_1 con $K \setminus (H_2 \cup \dots \cup H_n)$ se necessario, possiamo supporre che $H_1, \dots, H_n$ formino una partizione di$K$. Poiché $\mathrm{ht}(H_i) = \gamma$ e $\mathrm{wd}(H_i) = 1$ allora H_i è omeomorfo a $\omega^{\cdot\gamma} \dot{+} 1$ e poiché K è la somma degli spazi H_i, per la parte (i) dell'Esercizio 24.16 K è omeomorfo a $(\omega^{\cdot\gamma} \dot{+} 1)\cdot n = \omega^{\cdot\gamma}\cdot n \dot{+} 1$.

Quindi possiamo supporre che $\mathrm{wd}(K) = 1$ e che $\bar{x} \in X$ sia l'unico punto tale che $o(\bar{x}) = \gamma > 0$.

Se $\gamma = \delta \dot{+} 1$ allora $\bar{x}$ è l'unico punto di accumulazione di $\{x_n \mid n < \omega\}$, l'insieme dei punti di ordine δ. Per il Corollario 10.43, fissiamo $K = V_0 \supset V_1 \supset V_2 \supset \dots$ base di intorni chiusi-aperti di $\bar{x}$ tali che $x_n \in V_n$ e $x_{n+1} \notin V_n$. Allora i $D_i = V_i \setminus V_{i+1}$ sono chiusi-aperti disgiunti che formano una partizione di $K \setminus \{\bar{x}\}$ e tali che $\mathrm{ht}(D_i) = \delta$ e $\mathrm{wd}(D_i) = 1$. Se $\delta = 0$ è immediato verificare che i D_i sono singoletti e che K è omeomorfo a $\omega \dot{+} 1$. Supponiamo quindi $\delta > 0$. Per ipotesi induttiva ci sono omeomorfismi $f_i \colon D_i \to \omega^{\cdot\delta} \dot{+} 1$, quindi per la parte (ii) dell'Esercizio 24.16, K è omeomorfo a $\omega^{\cdot\delta+1} \dot{+} 1 = \omega^{\cdot\gamma} \dot{+} 1$.

Supponiamo infine che γ sia limite. Per il Corollario 10.43 possiamo fissare una base di intorni chiusi-aperti $X = V_0 \supset V_1 \supset V_2 \supset \dots$ del punto $\bar{x}$. Se, per assurdo, $D_i \stackrel{\mathrm{def}}{=} V_i \setminus V_{i+1}$ avesse altezza γ, allora dovrebbe contenere un punto y tale che $o^{D_i}(y) = o^X(y)$ e quindi per ipotesi $y = \bar{x}$, contraddicendo il fatto che $\bar{x} \notin D_i$. Per ipotesi induttiva

(24.8) per ogni $i < \omega$ c'è un omeomorfismo $f_i \colon D_i \to \omega^{\cdot\gamma_i}\cdot m_i \dot{+} 1$

per qualche γ_i e n_i. Per la parte (ii) dell'Esercizio 24.16 c'è un omeomorfismo $f \colon X \to \alpha \dot{+} 1$ dove

$$\alpha \dot{+} 1 \stackrel{\mathrm{def}}{=} \big(\dot{\sum}_{i<\omega} \omega^{\cdot\gamma_i}\cdot m_i \dot{+} 1\big) \dot{+} 1 \leq \omega^{\cdot\gamma} \dot{+} 1.$$

Supponiamo per assurdo che $\alpha \dot{+} 1 < \omega^{\cdot\gamma} \dot{+} 1$ e sia $\delta < \gamma$ tale che $\alpha \dot{+} 1 < \omega^{\cdot\delta}$. Fissiamo un $y \in X^{(\delta)}$ e per il Corollario 10.43 sia D un chiuso-aperto di X tale che $D \cap X^{(\delta)} = \{y\}$. Poiché D è un compatto che contiene esattamente

un punto di ordine δ e nessun punto di ordine superiore, cioè $\mathrm{ht}(D) = \delta$ e $\mathrm{wd}(D) = 1$, per ipotesi induttiva D è omeomorfo a $\omega^{\cdot\delta} \dot{+} 1$. L'insieme $f[X \setminus D]$ è un sottoinsieme chiuso-aperto di $\alpha \dot{+} 1$ che è isomorfo come ordine (e quindi omeomorfo come spazio topologico) ad un ordinale $\eta \dot{+} 1 \leq \alpha \dot{+} 1$. Per la parte (i) dell'Esercizio 24.16 lo spazio X è omeomorfo a $\eta \dot{+} 1 \dot{+} \omega^{\cdot\delta} \dot{+} 1 = \omega^{\cdot\delta} \dot{+} 1$. In particolare $\omega^{\cdot\delta} \dot{+} 1$ è omeomorfo a $\alpha \dot{+} 1$, contro (24.6). □

Osservazione 24.17. La dimostrazione qui sopra del Teorema 24.9 usa l'Assioma della Scelta quando scegliamo gli omeomorfismi f_i nella (24.8). Per vedere che questo uso di AC non è necessario si può modificare la dimostrazione in modo opportuno, oppure usare un profondo risultato di teoria degli insiemi (il teorema di assolutezza di Shoenfield) per dimostrare che il ricorso alla scelta è eliminabile.

Dimostrazione del Corollario 24.10. Sia X uno spazio metrico, localmente compatto e numerabile. Il caso in cui X è compatto è stato risolto nel Teorema 24.9, quindi possiamo supporre che X non sia compatto. Sia $\hat{X}$ la **compattificazione di Alexandroff** di X, cioè lo spazio $X \cup \{\infty\}$ dove $\infty \notin X$ e gli aperti di $\hat{X}$ sono quelli di X e gli insiemi della forma $\{\infty\} \cup X \setminus K$ con $K \subseteq X$ compatto. Poiché X è aperto in $\hat{X}$, l'ordine $o(x)$ di un punto $x \in X$ è il medesimo, calcolato in X o in $\hat{X}$, quindi $\mathrm{ht}(X) \leq \mathrm{ht}(\hat{X})$. Infatti $\mathrm{ht}(\hat{X}) = \mathrm{ht}(X) \dot{+} 1$ se e solo se $o(\infty) = \mathrm{ht}(X) = \sup_{x \in X} o(x)$. Lo spazio $\hat{X}$ è metrico, compatto e numerabile, quindi c'è un omeomorfismo da $\hat{X}$ su $\omega^{\cdot\gamma} \cdot n$, dove $\gamma = \mathrm{ht}(\hat{X})$ e $n = \mathrm{wd}(\hat{X})$. Per costruzione ∞ non è isolato in $\hat{X}$ quindi $f(\infty)$ è limite. Se $f(\infty) = \omega^{\cdot\gamma} \cdot n$, allora X è omeomorfo ad $\omega^{\cdot\gamma} \cdot n$. Se invece $f(\infty) = \lambda < \omega^{\cdot\gamma} \cdot n$, allora X è omeomorfo a $(\omega^{\cdot\gamma} \cdot n \dot{+} 1) \setminus \{\lambda\}$, che è partizionato nei due chiusi-aperti

$$D_0 = (\omega^{\cdot\gamma} \cdot n \dot{+} 1) \setminus (\lambda \dot{+} 1) \quad \text{e} \quad D_1 = \lambda.$$

Dato che $\omega^{\cdot\gamma}$ è additivamente indecomponibile, $\mathrm{ot}(D_0) = \omega^{\cdot\gamma} \cdot n \dot{+} 1$, quindi per l'Esercizio 24.16 X è omeomorfo a $\omega^{\cdot\gamma} \cdot n \dot{+} 1 \dot{+} \lambda = \omega^{\cdot\gamma} \cdot n \dot{+} \lambda$. Se $\omega^{\cdot\xi_0} \cdot n_0 \dot{+} \cdots \dot{+} \omega^{\cdot\xi_k} \cdot n_k$ è la forma normale di Cantor di λ, per (24.7) si ha che $\omega^{\cdot\gamma} \cdot n \dot{+} \omega^{\cdot\xi_0} \cdot n_0 \dot{+} \cdots \dot{+} \omega^{\cdot\xi_k} \cdot n_k$ è omeomorfo a $\omega^{\cdot\gamma} \cdot n \dot{+} \omega^{\cdot\xi_k} \cdot n_k$. □

Esercizi

Esercizio 24.18. Dimostrare che ogni funzione $f \colon \omega \to \omega$ è continua.

Esercizio 24.19. Dimostrare che la relazione funzionale $\mathrm{Ord} \to \mathrm{Ord}$, $\alpha \mapsto \alpha \dot{+} 1$, è discontinua su tutti gli ordinali limite.

Esercizio 24.20. 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.

Esercizio 24.21. Dimostrare che gli ordinali della forma (24.1a), (24.1b) e (24.1c) nell'enunciato del Teorema (24.8) sono incomprimibili.

Note e osservazioni

I Teoremi 24.8, 24.9 e 24.10 che caratterizzano gli spazi localmente compatti numerabili mediante ordinali sono dovuti a ??. Queste caratterizzazioni sono molto utili nello studio degli spazi di Banach $\mathscr{C}(K)$ con K compatto numerabile [**Ros03**].

25. Applicazioni dell'Assioma di Scelta*

L'Assioma di Scelta, introdotto nella Sezione 14, ha molte conseguenze in matematica. Qui sotto riportiamo alcune delle applicazioni più significative.

25.A. Teoremi la cui dimostrazione dipende dall'Assioma di Scelta.

In questa Sezione assumeremo AC

25.A.1. *Algebra.*

Lemma 25.1 (Krull)**.** *In un anello commutativo unitario, ogni ideale proprio può essere esteso ad un ideale massimale.*

Dimostrazione. Se I è un ideale proprio di un commutativo unitario R, sia

$$\mathcal{J} = \{J \subseteq R \mid I \subseteq J \wedge J \text{ ideale proprio di } R\}\,.$$

Se $\mathcal{C} \subseteq \mathcal{J}$ è una catena, allora $\bigcup \mathcal{C}$ è un ideale di R contenente I. Inoltre $\bigcup \mathcal{C}$ è proprio: se, per assurdo, $1_R \in \bigcup \mathcal{C}$ allora $1_R \in J \in \mathcal{C}$ contrariamente al fatto che ogni $J \in \mathcal{C} \subseteq \mathcal{J}$ è proprio. Quindi $\bigcup \mathcal{C} \in \mathcal{J}$. Le ipotesi del Lemma di Zorn sono verificate, quindi possiamo concludere che esiste $J \in \mathcal{J}$ massimale. □

Poiché un'algebra di Boole è un anello commutativo unitario (Sezione 8.H), il Lemma di Krull 25.1 implica BPI (Definizione 23.24), ma, come vedremo nella Sezione 25.D, il Lemma di Krull è equivalente ad AC, quindi per l'Osservazione 23.25(a) l'implicazione inversa non vale.

L'ipotesi che l'anello sia unitario non può essere rimossa (Esercizio 25.21).

Teorema 25.2. *Sia V uno spazio vettoriale su un campo $\Bbbk$.*

(a) *V ha una base, e due basi di V sono in biezione.*

(b) *V è iniettivo nella categoria degli spazi vettoriali, cioè ogni applicazione lineare $f\colon U \to V$ da U sottospazio vettoriale di uno spazio vettoriale W su $\Bbbk$ può essere estesa ad un'applicazione lineare $\bar{f}\colon W \to V$.*

(c) *V è proiettivo nella categoria degli spazi vettoriali, cioè per ogni applicazione lineare $f\colon V \to U$ e $g\colon W \to U$ c'è un'applicazione lineare $\bar f\colon V \to W$ tale che $f = g \circ \bar f$.*

Dimostrazione. □

Un campo $\Bbbk$ si dice algebricamente chiuso se ogni polinomio a coefficienti in $\Bbbk$ ha una soluzione in $\Bbbk$. Un campo algebricamente chiuso $\overline{\Bbbk}$ si dice **chiusura algebrica** di un campo $\Bbbk$ se $\overline{\Bbbk} \supseteq \Bbbk$ e non esistono campi algebricamente chiusi $\Bbbk'$ tali che $\Bbbk \subset \Bbbk' \subset \overline{\Bbbk}$. Una **base di trascendenza** per un campo $\Bbbk$ è un insieme $B \subseteq \mathbb{C}$ algebricamente indipendente.

Teorema 25.3. (a) *Per ogni campo $\Bbbk$, la chiusura algebrica esiste ed è unica a meno di isomorfismi.*

(b) *Se $\Bbbk_0$ e $\Bbbk_1$ sono campi algebricamente chiusi di caratteristica $p \in \mathrm{Pr} \cup \{0\}$, e se B_i è una base di trascendenza per $\Bbbk_i$, allora ogni biezione $f\colon B_0 \to B_1$ può essere estesa ad un isomorfismo $\bar f\colon \Bbbk_0 \to \Bbbk_1$.*

Teorema 25.4 (Neilsen-Schreier)**.** *Ogni sottogruppo di un gruppo libero è libero.*

Teorema 25.5. (a) *Ogni gruppo abeliano libero è proiettivo.*

(b) *Ogni gruppo abeliano divisibile è iniettivo.*

25.B. Reticoli e algebre di Boole. Argomentando come nella dimostrazione del Lemma di Krull si dimostra:

Proposizione 25.6. *In un reticolo dotato di massimo, ogni ideale proprio può essere esteso ad un ideale massimale. Dualmente, in un reticolo dotato di minimo, ogni filtro proprio può essere esteso ad un ultrafiltro.*

Poiché nei reticoli gli ideali massimali non sono necessariamente primi non possiamo dedurre che ogni ideale proprio può essere esteso ad un ideale primo; anzi non è neppure detto che esistano ideali primi (Osservazione 23.6 ed Esercizio 23.47). Poiché in un ideale distributivo gli ideali massimali sono primi otteniamo che

Proposizione 25.7. *In un reticolo distributivo dotato di massimo, ogni ideale proprio può essere esteso ad un ideale massimale. Dualmente, in un reticolo dotato di minimo, ogni filtro proprio può essere esteso ad un filtro primo.*

Il seguente risultato è noto come Teorema di Estensione di Sikorski.

Teorema 25.8 (Sikorski)**.** *Ogni algebra di Boole completa C è iniettiva nella categoria delle algebre di Boole, cioè per ogni algebra di Boole B e ogni subalgebra A di B, ogni morfismo $A \to C$ può essere esteso ad un morfismo $B \to C$.*

25.B.1. *Topologia.* Ricordiamo che la **topologia prodotto** è generata dagli aperti di base

$$\begin{aligned}\boldsymbol{N}(U_{i_0},\dots,U_{i_n}) &= \{f \in \bigtimes_{i\in I} X_i \mid f(i_k) \in U_{i_k},\ k=0,\dots,n\}\\ &= \bigtimes_{j\in\{i_0,\dots,i_n\}} U_j \times \bigtimes_{i\in I\setminus\{i_0,\dots,i_n\}} X_i\end{aligned}$$

dove $\{i_0,\dots,i_n\} \subseteq I$ e U_{i_k} è aperto in X_{i_k}.

Teorema 25.9 (Tychonoff)**.** *Il prodotto di spazi compatti è compatto.*

25.B.2. *Analisi.*

Teorema 25.10 (Ascoli-Arzelà)**.** *Siano X uno spazio* T_2 *localmente compatto e Y uno spazio metrico, e dotiamo $\mathscr{C}(X,Y)$ l'insieme delle funzioni continue da X in Y della* topologia compatta-aperta*, cioè generata dagli insiemi $\{f \mid f[K] \subseteq U\}$ con $K \subseteq X$ compatto e $U \subseteq Y$ aperto. Un insieme $F \subseteq \mathscr{C}(X,Y)$ è compatto se e solo se*

- *$\{f(x) \mid f \in F\}$ è compatto in Y,*
- *F è un chiuso di Y^X con la* topologia prodotto*,*
- *F è equicontinuo, cioè*

$$\forall x \in X\, \exists \varepsilon > 0\, \exists U \text{ aperto } e\ x \in U\, \forall f \in F\, \forall y \in U\, [d(f(x),f(y)) < \varepsilon].$$

Teorema 25.11 (Hahn-Banach)**.** *Siano X uno spazio vettoriale su $\mathbb{R}$, $X_0 \subseteq X$ un sottospazio e $\lambda_0 \colon X_0 \to \mathbb{R}$ un'applicazione lineare. Supponiamo $p \colon X \to \mathbb{R}$ sia un'applicazione sub-lineare, cioè*

$$p(x+y) \le p(x) + p(y)$$

tale che $\forall x \in X_0\, (\lambda_0(x) \le p(x))$. Allora c'è un'estensione lineare $\lambda \colon X \to \mathbb{R}$ di λ_0 tale che $\forall x \in X\, (\lambda(x) \le p(x))$.

Il duale E^* di uno spazio di Banach E è l'insieme delle funzioni lineari $f \colon E \to \mathbb{R}$ che sono limitate, cioè tali che $\exists M\, \forall x \in E\, (|f(x)| \le M\, \|x\|)$. Lo spazio vettoriale E^* è uno spazio di Banach con la norma $\|f\| = \sup_{x\neq 0} |f(x)| \,/\, \|x\|$. Ogni $x \in E$ definisce una funzione lineare continua $x^{**} \colon E^* \to \mathbb{R}$ mediante $x^{**}(f) = f(x)$. La topologia debole* su E^* è la topologia più debole che rende tutte queste mappe continue.

Teorema 25.12 (Alaoglu)**.** *Sia E uno spazio di Banach. Allora $B = \{f \in E^* \mid \|f\| \le 1\}$ è compatto nella topologia debole*.*

25.C. Insiemi patologici. AC ha anche alcune conseguenze indesiderabili sul continuo.

In questa sezione assumiamo che $\mathbb{R}$ sia bene ordinabile

Naturalmente, un buon ordine su $\mathbb{R}$ induce un buon ordine su $\mathbb{R}^n$ per ogni $n \in \omega$.

Teorema 25.13. *Per ogni $n \geq 1$ c'è una base dello spazio vettoriale $\mathbb{R}^n$ su $\mathbb{Q}$. Ogni base di $\mathbb{R}^n$ su $\mathbb{Q}$ ha cardinalità $2^{\aleph_0}$.*

Una base di $\mathbb{R}$ come spazio vettoriale su $\mathbb{Q}$ si dice **base di Hamel**.

Esercizio 25.14. Sia $f\colon \mathbb{R} \to \mathbb{R}$ una funzione che soddisfa l'equazione funzionale $f(x+y) = f(x) + f(y)$, e sia $a = f(1)$. Dimostrare che

(i) $f\colon \langle \mathbb{R}, + \rangle \to \langle \mathbb{R}, + \rangle$ è un omomorfismo e $\forall q \in \mathbb{Q}\ (f(q) = aq)$;

(ii) se f è continua, allora $\forall x \in \mathbb{R}\ (f(x) = ax)$.

Data una base di Hamel H, è possibile definire un omomorfismo discontinuo da $\langle \mathbb{R}, + \rangle$ in sé stesso: ogni funzione $g\colon H \to \mathbb{R}$ può essere estesa ad una funzione $\mathbb{Q}$-lineare $f\colon \mathbb{R} \to \mathbb{R}$, quindi se g non è monotona, l'omomorfismo risultante f è discontinuo.

Teorema 25.15. (a) *C'è una base di trascendenza per $\mathbb{C}$.*

(b) *C'è una base di trascendenza per $\mathbb{R}$, cioè un insieme $B \subseteq \mathbb{R}$ algebricamente indipendente e massimale.*

Il prossimo risultato richiede delle nozioni di teoria della misura che verranno introdotte nella Sezione 22.A.

Teorema 25.16 (Vitali)**.** *Esiste un sottoinsieme di $\mathbb{R}$ non Lebesgue misurabile.*

Dall'esistenza di un sottoinsieme non Lebesgue-misurabile di un qualche $\mathbb{R}^k$ segue l'esistenza di sottoinsiemi non Lebesgue-misurabili di $\mathbb{R}^n$, per ogni $n \geq 1$.

Osservazione 25.17. L'esistenza di un omomorfismo discontinuo $\langle \mathbb{R}, + \rangle \to \langle \mathbb{R}, + \rangle$ implica l'esistenza di insiemi non Lebesgue-misurabili [**Her06**, Teorema 5.5, p. 119] e l'esistenza di un automorfismo di $\langle \mathbb{C}, +, \cdot \rangle$ diverso dall'identità e dal coniugio, implica l'esistenza di un omomorfismo discontinuo $\langle \mathbb{R}, + \rangle \to \langle \mathbb{R}, + \rangle$ (Esercizio 25.24).

Teorema 25.18 (Bernstein)**.** *C'è un $B \subseteq \mathbb{R}$ tale che né B né $\mathbb{R} \setminus B$ contengono un insieme perfetto non vuoto.*

Il risultato seguente, noto come **Paradosso di Banach-Tarski** è probabilmente la più contro-intuitiva conseguenza dell'Assioma di Scelta.

Teorema 25.19 (Banach-Tarski)**.** *Sia*

$$B = \{(x, y, z) \in \mathbb{R}^3 \mid x^2 + y^2 + z^2 \leq 1\}$$

la palla unitaria dello spazio euclideo. Esiste una partizione

$$\{X_1, \ldots, X_n, Y_1, \ldots, Y_m\}$$

di B ed esistono $\sigma_1, \ldots, \sigma_n, \tau_1, \ldots, \tau_m$ isometrie di $\mathbb{R}^3$ tali che

$$\{\sigma_1[X_1], \ldots, \sigma_n[X_n]\} \quad e \quad \{\tau_1[Y_1], \ldots, \tau_m[Y_m]\}$$

sono partizioni di B.

In altre parole: è possibile suddividere B in un numero finito di pezzi che opportunamente traslati e ruotati formano due copie di B.

25.D. Teoremi equivalenti a qualche forma di Assioma di Scelta. Numerosi teoremi risultano essere equivalenti a qualche forma di assioma di scelta. Per esempio i seguenti enunciati sono equivalenti ad AC:

- AC(1) Il Lemma di Krull 25.1 [**Hod79**].
- AC(2) Ogni spazio vettoriale ha una base [**Bla84**].
- AC(3) Ogni spazio vettoriale è iniettivo.
- AC(4) Ogni spazio vettoriale è proiettivo.
- AC(5) Ogni gruppo abeliano libero è proiettivo [**Bla79**]
- AC(6) Ogni gruppo abeliano divisibile è iniettivo [**Bla79**].
- AC(7) Il Teorema di Tychonoff per spazi T_1 (Esercizio 25.23).
- AC(8) Il reticolo dei chiusi di uno spazio topologico ammette un filtro massimale. Dualmente: il reticolo degli aperti di uno spazio topologico ammette un ideale massimale.

Invece i seguenti enunciati sono equivalenti a BPI:

- BPI(1) In un anello commutativo unitario, ogni ideale non banale può essere esteso ad un ideale primo.
- BPI(2) Il Teorema 23.26 di Stone per le algebre di Boole (Esercizio 25.22).
- BPI(3) I Teoremi di Compattezza 31.1 e di Esistenza di Modelli 35.3 per i linguaggi del prim'ordine.
- BPI(4) Il Teorema di Tychonoff per spazi T_2 (Esercizio **??**).
- BPI(5) Il reticolo dei chiusi di uno spazio topologico ammette un ideale massimale. Dualmente: il reticolo degli aperti di uno spazio topologico ammette un filtro massimale.
- BPI(6) Il Teorema di Alaoglu 25.12 [**Joh84**].
- BPI(7) Il Teorema di Ascoli-Arzelà 25.10 [**Her97**].
- BPI(8) L'equivalenza delle due definizioni di radicale di un ideale di un anello commutativo (vedi la Sezione 5.C.2) [**Rav77**].

Osservazione 25.20. La AC(8) e la BPI(5) mettono in luce una sottile differenza tra il reticolo degli aperti e quello dei chiusi. Per il Teorema 23.4,

l'esistenza di filtri massimali nel reticolo dei chiusi $\mathsf{AC}(8)$ è equivalente all'esistenza di filtri massimali nei reticoli completi, e in quelli distributivi.

BPI implica il Teorema 25.3. Il Teorema di Hahn-Banach 25.11 discende da (ma è strettamente più debole di) BPI, ed è equivalente a:

> Se F è un filtro proprio di un'algebra di Boole B, allora c'è una misura finitamente additiva $m\colon B \to [0;1]$ tale che $m(x) = 1$ per ogni $x \in F$.

Inoltre il Teorema di Hahn-Banach 25.11 implica il Teorema di Banach-Tarski 25.19 [**FW91, Paw91**], quindi implica l'esistenza di insiemi non Lebesgue misurabili.

Esercizi

Esercizio 25.21. Dimostrare che $(\mathbb{Q}, +)$ non ha sottogruppi propri massimali. Concludere che l'anello $(\mathbb{Q}, +, *)$ dove $a * b = 0$ per ogni $a, b \in \mathbb{Q}$ non ha ideali massimali.

Esercizio 25.22. Dimostrare che il Teorema 23.26 di Rappresentazione di Stone per le algebre di Boole implica BPI.

Nel prossimo esercizio dimostreremo che la seguente versione del Teorema di Tychonoff implica AC:

(T) Se $\langle (Y_i, \mathcal{T}_i) \mid i \in I\rangle$ è una una famiglia di spazi compatti e T_1, e se l'*insieme* $\bigtimes_{i\in I} Y_i$ è non-vuoto, allora lo spazio prodotto $\prod_{i\in I}(Y_i, \mathcal{T}_i)$ è compatto.

(L'ipotesi che $\emptyset \neq \bigtimes_{i\in I} Y_i$ è necessaria, in quanto l'affermazione che il prodotto di insiemi non vuoti è non vuoto è già equivalente ad AC — Esercizio 11.17(iv).)

Esercizio 25.23. Sia $\langle X_i \mid i \in I\rangle$ una famiglia di insiemi non vuoti, sia $z \notin \bigcup_{i\in I} X_i$, sia $Y_i = X_i \cup \{z\}$, e sia $\mathcal{T}_i$ la famiglia dei sottoinsiemi cofiniti di Y_i con l'aggiunta di $\emptyset$ e $\{z\}$. Dimostrare che:

(i) $(Y_i, \mathcal{T}_i)$ è compatto T_1,

(ii) (T) $\Rightarrow \bigtimes_{i\in I} X_i \neq \emptyset$.

Esercizio 25.24. Dimostrare che

(i) un automorfismo continuo del campo complesso è l'identità o il coniugio $z \mapsto \bar{z}$;

(ii) se $f\colon \mathbb{C} \to \mathbb{C}$ è un automorfismo discontinuo del campo complesso, allora $\Re \circ f \restriction \mathbb{R}\colon \langle \mathbb{R}, +\rangle \to \langle \mathbb{R}, +\rangle$ è un omomorfismo discontinuo di gruppi.

Esercizio 25.25. Supporre che $\mathbb{R}$ sia bene ordinabile e dimostrare che $\langle \mathbb{R}, +\rangle$ è isomorfo a $\langle \mathbb{R}^n, +\rangle$ per ogni $n \geq 1$. In particolare $\mathbb{R}$ e $\mathbb{C}$ sono isomorfi come gruppi.

Note ed osservazioni

L'assioma di scelta ha uno *status* particolare in matematica in quanto ha molte conseguenze utili e interessanti e alcune altre contro-intuitive e bizzarre. Dato che le prime sono di gran lunga più numerose delle seconde, AC viene considerato dalla maggioranza dei matematici un principio insiemisticamente valido. Inoltre nel 1937 Gödel ha dimostrato che se mai una contraddizione in matematica fosse ottenibile mediante l'assioma di scelta, allora si potrebbe ottenere una contraddizione anche senza usare AC. In altre parole: non possiamo refutare AC a partire dagli assiomi di MK o di ZF, a meno che queste teorie non siano contraddittorie, nel qual caso ogni affermazione sarebbe dimostrabile. Nel 1963 Cohen dimostrò un risultato analogo per la negazione di AC, e quindi non possiamo dimostrare AC a partire dagli assiomi di MK o di ZF, a meno che queste teorie non siano contraddittorie. Per una panoramica dei vari "disastri" che possono capitare in matematica se si assume o se non si assume AC rimandiamo a [**Her06**]. La monografia [**Wag93**] contiene un'esposizione dettagliata del paradosso di Banach-Tarski (Teorema 25.19).

26. Il Teorema di Ramsey*

Gli ultrafiltri su ω hanno importanti applicazioni in vari settori della matematica, per esempio la topologia generale, l'analisi funzionale, ecc. In questa sezione vedremo alcune applicazioni alla combinatorica.

Richiamiamo alcuni concetti visti nella Sezione 5.H. Un grafo $\langle V, E\rangle$ è costituito da un insieme non vuoto di vertici V e da un insieme $E \subseteq [V]^2$ degli spigoli; se $E = [V]^2$ diremo che è il grafo completo su V. Una colorazione (degli spigoli) è una funzione c di dominio E: se $\mathrm{ran}(c) \subseteq k$ parleremo di k-colorazione. Equivalentemente, una k-colorazione è una partizione degli spigoli in al più k parti.

Se c è una k-colorazione di $\langle V, E\rangle$, diremo che $H \subseteq V$ è **monocromatico** ovvero **omogeneo** per c se $c \restriction E \cap [H]^2$ è costante, vale a dire

$$\exists i \in k \forall x, y \in H\, (\{x, y\} \in E \Rightarrow c(\{x, y\}) = i)\,.$$

Equivalentemente, se $[V]^2 = C_0 \cup \cdots \cup C_{k-1}$, allora $[H]^2 \subseteq C_i$, per qualche i.

Teorema 26.1 (Teorema di Ramsey nel caso infinito)**.** *Supponiamo V sia un insieme numerabile e supponiamo*

$$[V]^r = C_0 \cup \cdots \cup C_{k-1}$$

dove $k, r \in \omega \setminus \{0\}$ e $C_i \subseteq [V]^r$, allora esiste un $H \subseteq V$ infinito tale che $[H]^r \subseteq C_i$, per qualche $i < k$.

Dimostrazione. Cominciamo con due semplici osservazioni. Innanzi tutto possiamo supporre che i C_i siano a due a due disgiunti. La seconda osservazione è che basta dimostrare il Teorema per $k = 2$. Infatti il caso $k = 1$ è banale e per $k > 2$ si procede per induzione: supponiamo vero il risultato

per $k \geq 2$ e dimostriamolo per $k+1$. Per il Teorema nel caso $k = 2$, esiste $H \subseteq V$ infinito tale che $[H]^r \subseteq C_0$ oppure $[H]^r \subseteq C_1 \cup \cdots \cup C_k$. Se vale la prima possibilità abbiamo dimostrato il teorema, quindi possiamo supporre

$$[H]^r \subseteq (C_1 \cap [H]^r) \cup \cdots \cup (C_k \cap [H]^r)\,.$$

Per ipotesi induttiva c'è un $H' \subseteq H$ infinito tale che $[H]^r \subseteq C_i$ per qualche $1 \leq i \leq k$, come richiesto.

Dimostriamo quindi il teorema per $k = 2$. La dimostrazione procede per induzione su $r \geq 1$.

Supponiamo $r = 1$: l'insieme $[V]^1$ è identificabile con V per cui il risultato diventa:

$$\text{Se } V = C_0 \cup C_1, \text{ allora almeno uno tra } C_0 \text{ e } C_1 \text{ è infinito,}$$

e questo discende immediatamente dalla Proposizione 10.22.

Assumiamo il risultato vero per r e dimostriamolo per $r+1$. Per semplicità notazionale possiamo supporre che $V = \omega$. Sia

$$f\colon [\omega]^{r+1} \to 2$$

la colorazione associata alla partizione $\{C_0, C_1\}$, vale a dire

$$f(\bar{x}) = i \;\Leftrightarrow\; \bar{x} \in C_i.$$

Se C_i è finito, allora

$$H = \{n \in \omega \mid \neg\exists \bar{x} \in [\omega]^r\,(n \in \bar{x} \wedge \bar{x} \in C_i)\}$$

è infinito e $[H]^r \subseteq C_{1-i}$, quindi possiamo supporre che C_0 e C_1 siano entrambi infiniti. Costruiremo un insieme $K \subseteq \omega$ tale che

$$\forall \bar{x}, \bar{y} \in [K]^{r+1}\,(x_0 = y_0 \wedge \cdots \wedge x_{r-1} = y_{r-1} \Rightarrow f(\bar{x}) = f(\bar{y})) \tag{26.1}$$

vale a dire: il valore di $f(\bar{x})$ dipende solo dai primi r elementi di $\bar{x}$. Possiamo quindi definire una funzione $g\colon [K]^r \to 2$ ponendo

$$g(\bar{x}) = f(\bar{x} \cup \{n\})$$

per qualche (equivalentemente: per ogni) $n \in K$ con $n > \max(\bar{x})$. Per ipotesi induttiva c'è un $H \subseteq K$ infinito ed omogeneo per g. Fissiamo $\bar{x}, \bar{y} \in [H]^{r+1}$. Poiché K soddisfa (26.1) e $H \subseteq K$, se $\bar{x}, \bar{y} \in [H]^{r+1}$ allora

$$\begin{aligned} f(\bar{x}) &= g(\{x_0, \ldots, x_{r-1}\}) \\ &= g(\{y_0, \ldots, y_{r-1}\}) \\ &= f(\bar{y}), \end{aligned}$$

cioè H è l'insieme omogeneo cercato. Quindi è sufficiente dimostrare l'esistenza di un insieme K che soddisfa (26.1).

Fissiamo un ultrafiltro non principale U su ω. Per ogni $\bar{x} \in [\omega]^r$ sia

$$D_i(\bar{x}) = \{n \in \omega \mid n > \max \bar{x} \,\wedge\, f(\bar{x} \cup \{n\}) = i\}.$$

Poiché

$$D_0(\bar{x}) \cup D_1(\bar{x}) = \omega \setminus (\max \bar{x} + 1) \in U$$

sia

$$i(\bar{x}) = \text{l'unico } i \in 2 \text{ tale che } D_i(\bar{x}) \in U.$$

Costruiamo induttivamente una successione di naturali y_n come segue:

- poiché $r = \{0, 1, \ldots, r-1\} \in [\omega]^r$, allora
$$Y_0 = D_{i(r)}(r)$$
è ben definito; sia
$$y_0 = \min Y_0.$$
Osserviamo che $y_0 > r$.
- Supponiamo di aver definito $y_0, \ldots, y_n$. L'insieme
$$\mathcal{X}_n = [r \cup \{y_0, \ldots, y_n\}]^r$$
è finito (ha esattamente $\binom{r+n+1}{r}$ elementi) e poiché U è chiuso per intersezioni finite,
$$Y_{n+1} = \bigcap_{\bar{x} \in \mathcal{X}_n} D_{i(\bar{x})}(\bar{x}) \in U.$$
Dato che $\emptyset \notin U$, ne segue che $Y_{n+1} \neq \emptyset$. Sia
$$y_{n+1} = \min Y_{n+1}.$$

È facile verificare che $r \leq y_0 < y_1 < \ldots$ e che $Y_0 \supset Y_1 \supset \ldots$. Sia

$$K = \{y_n \mid n \in \omega\}.$$

Fissiamo un $\bar{x} \in [K]^r$ e sia $y_n = \max \bar{x}$, per cui $\bar{x} \in \mathcal{X}_n$. Se $n < m, h$, allora $y_m, y_h \in Y_{n+1} \subseteq D_{i(\bar{x})}(\bar{x})$ per cui $f(\bar{x} \cup \{y_m\}) = f(\bar{x} \cup \{y_h\})$. Quindi K soddisfa (26.1). □

Corollario 26.2. *Se $<$ e $\prec$ sono due ordini totali su un insieme infinito X, allora c'è un sottoinsieme infinito $H \subseteq X$ su cui $<$ coincide con $\prec$ oppure con l'ordinamento inverso $\succ$, vale a dire*

$$\forall x, y \in H\, (x < y \Leftrightarrow x \prec y) \vee \forall x, y \in H\, (x < y \Leftrightarrow y \prec x)\,.$$

La notazione

$$\alpha \to (\beta)^n_k$$

significa che per ogni colorazione $f\colon [\alpha]^n \to k$ c'è un $H \subseteq \alpha$ di tipo d'ordine β che è omogeneo per f, cioè $f \restriction [H]^n$ è costante. Quindi il Teorema di Ramsey 26.1 può essere scritto in questa notazione come $\omega \to (\omega)^n_k$. L'ordinale ω non può essere rimpiazzato da ω_1 (Esercizio 26.5). Infatti c'è una colorazione $f\colon [\omega_1]^2 \to \omega_1$ tale che $\operatorname{ran}(f \restriction [X]^2) = \omega_1$ per *ogni* $X \subseteq \omega_1$. In altre parole: c'è un'operazione binaria commutativa $*$ su ω_1 tale che

applicando $*$ agli elementi di un qualsiasi sottoinsieme più che numerabile di ω_1, si ottiene ω_1.

È possibile considerare tipi d'ordine invece di ordinali. Per esempio l'Esercizio 10.60 mostra come $\mathbb{Q} \to (\mathbb{Q})^1_k$, cioè se si partiziona $\mathbb{Q}$ in un numero finito di pezzi, allora almeno uno di questi contiene un sottoinsieme isomorfo a $\mathbb{Q}$. Viceversa $\mathbb{Q} \to (\mathbb{Q})^2_2$ non vale, cioè c'è una colorazione $f\colon [\mathbb{Q}]^2 \to 2$ tale che $f \restriction [X]^2$ assume due valori, per ogni sottoinsieme X isomorfo a $\mathbb{Q}$ (Esercizio 26.4). Tuttavia, in un certo senso questo è il caso peggiore, dato che se $f\colon [\mathbb{Q}]^2 \to k$, allora c'è un $X \subseteq \mathbb{Q}$ isomorfo a $\mathbb{Q}$ tale che $|f \restriction [X]^2| \leq 2$, per ogni k. Infatti per ogni $n \in \omega$ c'è un $t_n \in \omega$ minimo tale che per ogni k-colorazione $f\colon [\mathbb{Q}]^n \to k$ c'è un $X \subseteq \mathbb{Q}$ isomorfo a $\mathbb{Q}$ tale che $|\mathrm{ran}(f \restriction [X]^n)| \leq t_n$.

Esercizi

Esercizio 26.3. Due elementi x, y di un insieme ordinato $\langle X, \leq\rangle$ si dicono **incomparabili** se

$$x \not\leq y \quad \wedge \quad y \not\leq x.$$

Un sottoinsieme di X costituito da elementi a due a due incomparabili si dice **indipendente**.

Dimostrare che per ogni successione $\langle x_n \mid n \in \omega\rangle$ di elementi distinti di X ammette una sottosuccessione $\langle x_{n_k} \mid k \in \omega\rangle$ strettamente crescente, oppure strettamente decrescente, oppure tale che $\{x_{n_k} \mid k \in \omega\}$ è un insieme indipendente di $\langle X, \leq\rangle$.

In particolare AC_ω implica che ogni insieme ordinato infinito contiene una catena infinita, oppure insieme indipendente infinito.

Esercizio 26.4. Dimostrare che c'è una $f\colon [\mathbb{Q}]^2 \to 2$ tale che $\forall X \subseteq \mathbb{Q}\ \big(X \cong \mathbb{Q} \Rightarrow |f \restriction [X]^2| = 2\big)$.

Esercizio 26.5. Dimostrare che $2^{\aleph_0} \not\to (\omega)^2_2$.

Capitolo VI

Strutture e linguaggi

27. Strutture

In questa sezione svilupperemo in dettaglio le nozioni di linguaggio del prim'ordine e di struttura che erano state introdotte informalmente nella Sezione 3 del Capitolo I.

Un **tipo di similarità** o **segnatura** è una 4-upla $\tau = \langle I, J, K, \mathrm{ar}\rangle$, con I, J, K insiemi disgiunti e $\mathrm{ar}\colon I \cup J \to \omega \setminus \{0\}$. Una segnatura τ si dice

- **relazionale** se $J = K = \emptyset$,
- **funzionale** se $I = K = \emptyset$,
- **bene ordinabile** se I, J, K sono bene ordinabili,
- **finita** se I, J e K sono insiemi finiti.

La **cardinalità** $\mathrm{card}(\tau)$ **della segnatura** τ è $\mathrm{card}(I)+\mathrm{card}(J)+\mathrm{card}(K)$, cioè $|I| + |J| + |K|$ quando τ è bene ordinabile.

Una **τ-struttura** è una 4-upla

$$\mathcal{A} = \langle A, \langle R_i^{\mathcal{A}} \mid i \in I\rangle, \langle f_j^{\mathcal{A}} \mid j \in J\rangle, \langle c_k^{\mathcal{A}} \mid k \in K\rangle\rangle$$

tale che

- A è un insieme non-vuoto detto l'**universo** di $\mathcal{A}$, denotato con $\|\mathcal{A}\|$,
- $R_i^{\mathcal{A}} \subseteq A^{\mathrm{ar}(i)}$, per ogni $i \in I$,
- $f_j^{\mathcal{A}}\colon A^{\mathrm{ar}(j)} \to A$, per ogni $j \in J$,
- $c_k^{\mathcal{A}} \in A$, per ogni $k \in K$.

Le relazioni $R_i^{\mathcal{A}}$, le funzioni $f_j^{\mathcal{A}}$ e gli elementi $c_k^{\mathcal{A}}$ si dicono, rispettivamente, **relazioni**, **funzioni** e **costanti** di $\mathcal{A}$. Una τ-struttura si dice relazionale

(funzionale) se τ è relazionale (rispettivamente: funzionale). La classe delle τ-strutture si indica con

$$\mathrm{Str}(\tau).$$

Due segnature $\tau = \langle I, J, K, \mathrm{ar}\rangle$ e $\tau' = \langle I', J', K', \mathrm{ar}'\rangle$ sono **isomorfe** se esiste una biezione $\varphi\colon I \cup J \cup K \to I' \cup J' \cup K'$ tale che $\varphi[I] = I'$, $\varphi[J] = J'$, $\varphi[K] = K$ e per ogni $x \in I \cup J$

$$\mathrm{ar}'(\varphi(x)) = \mathrm{ar}(x).$$

È evidente che ogni τ-struttura può essere vista come una τ'-struttura e viceversa, cioè φ induce una classe-funzione biettiva

$$\Phi\colon \mathrm{Str}(\tau) \to \mathrm{Str}(\tau').$$

Con abuso di notazione, scriveremo

$$\tau \subseteq \tau'$$

per dire che $I \subseteq I'$, $J \subseteq J'$, $K \subseteq K'$ e $\mathrm{ar} = \mathrm{ar}' \restriction I \cup J$.

Notazione. Per semplicità di notazione se π è una funzione di dominio A, scriveremo $\vec{a} \in A$ e $\pi(\vec{a})$ invece di $(a_1, \dots, a_n) \in A^{<\omega}$ e $(\pi(a_1), \dots, \pi(a_n))$.

Come nella Sezione 3.F.2, un **morfismo** da $\mathcal{A}$ in $\mathcal{B}$, dove $\mathcal{A}, \mathcal{B} \in \mathrm{Str}(\tau)$, è una funzione $\pi\colon \|\mathcal{A}\| \to \|\mathcal{B}\|$ tale che

(A) $\forall \vec{a} \in A^{\mathrm{ar}(i)} \left(\vec{a} \in R_i^{\mathcal{A}} \Rightarrow \pi(\vec{a}) \in R_i^{\mathcal{B}}\right)$, per ogni $i \in I$,

(B) $\forall \vec{a} \in A^{\mathrm{ar}(j)} (\pi(f_j^{\mathcal{A}}(\vec{a})) = f_j^{\mathcal{B}}(\pi(\vec{a})))$, per ogni $j \in J$,

(C) $\pi(c_k^{\mathcal{A}}) = c_k^{\mathcal{B}}$, per ogni $k \in K$.

Quindi $\mathrm{Str}(\tau)$ è una classe propria ed è una categoria, prendendo come frecce tra le strutture i morfismi.

Se la (A) viene rafforzata da

(A′) $\forall \vec{a} \in A^{\mathrm{ar}(i)} \left(\vec{a} \in R_i^{\mathcal{A}} \Leftrightarrow \pi(\vec{a}) \in R_i^{\mathcal{B}}\right)$, per ogni $i \in I$,

parleremo di **morfismo completo** o **pieno**. Un'**immersione** di $\mathcal{A}$ in $\mathcal{B}$ è un morfismo completo iniettivo di $\mathcal{A}$ in $\mathcal{B}$; un **isomorfismo** è un morfismo biettivo tale che l'inversa è anche un morfismo; equivalentemente: è un morfismo completo e biettivo. Due τ-strutture sono isomorfe $\mathcal{A} \cong \mathcal{B}$ se c'è un isomorfismo tra di loro; un **automorfismo** è un isomorfismo di una struttura in sè stessa e $\mathrm{Aut}(\mathcal{A})$ è il gruppo degli automorfismi di $\mathcal{A}$; se $\mathrm{Aut}(\mathcal{A})$ è il gruppo banale, cioè l'identità è l'unico automorfismo, diremo che $\mathcal{A}$ è **rigida**. Diremo che $\mathcal{A}$ **si immerge in** $\mathcal{B}$, in simboli

$$\mathcal{A} \dot{\subseteq} \mathcal{B}.$$

se c'è un'immersione di $\mathcal{A}$ in $\mathcal{B}$. Nel caso in cui l'universo di $\mathcal{A}$ sia contenuto nell'universo di $\mathcal{B}$ e le relazioni, funzioni, costanti di $\mathcal{A}$ coincidano con le

restrizioni di quelli di $\mathcal{B}$, cioè se $\|\mathcal{A}\| \subseteq \|\mathcal{B}\|$ e la funzione identica $\mathcal{A} \hookrightarrow \mathcal{B}$ è un'immersione, allora diremo che $\mathcal{A}$ è una **sotto-struttura** di $\mathcal{B}$

$$\mathcal{A} \subseteq \mathcal{B}.$$

Se $\mathcal{A} \subseteq \mathcal{B}$ e $\|\mathcal{A}\| \neq \|\mathcal{B}\|$ diremo che $\mathcal{A}$ è una **sotto-struttura propria** di $\mathcal{B}$, in simboli

$$\mathcal{A} \subset \mathcal{B}.$$

L'espressione $\mathcal{A} \subsetneq \mathcal{B}$ significa che $\mathcal{A}$ è (isomorfo a) una sotto-struttura di $\mathcal{B}$; analogamente $\mathcal{A} \subset \mathcal{B}$ significa che $\mathcal{A}$ è (isomorfo a) una sotto-struttura *propria* di $\mathcal{B}$. La **cardinalità** di $\mathcal{A}$

$$\mathrm{card}(\mathcal{A})$$

è la cardinalità dell'universo $A = \|\mathcal{A}\|$.

Se $\mathcal{A}'$ è una τ'-struttura e $\tau \subseteq \tau'$, la **contrazione di $\mathcal{A}'$ a τ** è la τ-struttura

$$\mathcal{A}' \restriction \tau = \langle \|\mathcal{A}'\|, \langle R_i^{\mathcal{A}'} \mid i \in I\rangle, \langle f_j^{\mathcal{A}'} \mid j \in J\rangle, \langle c_k^{\mathcal{A}'} \mid k \in K\rangle\rangle.$$

Chiaramente la mappa $\mathrm{Str}(\tau') \to \mathrm{Str}(\tau)$ è un funtore dimenticante. Viceversa, se $\mathcal{A}$ è una τ-struttura e $\mathcal{A}'$ è una τ'-struttura la cui contrazione a τ è $\mathcal{A}$, allora diremo che $\mathcal{A}'$ è un'**espansione di $\mathcal{A}$ a τ'**. Ogni τ-struttura ammette una τ'-espansione, ma, in generale, ad una stessa τ-struttura corrispondono più τ'-espansioni. In altre parole il funtore contrazione $\mathrm{Str}(\tau') \twoheadrightarrow \mathrm{Str}(\tau)$ è suriettivo, ma non iniettivo.

Definizione 27.1. Sia $\tau = \langle I, J, K, \mathrm{ar}\rangle$ una segnatura e sia

$$\mathcal{A} = \langle A, \langle R_i^{\mathcal{A}} \mid i \in I\rangle, \langle f_j^{\mathcal{A}} \mid j \in J\rangle, \langle c_k^{\mathcal{A}} \mid k \in K\rangle\rangle$$

una τ-struttura. L'**espansione canonica di $\mathcal{A}$ mediante gli elementi di $B \subseteq A$** è l'espansione $\mathcal{A}'$ di $\mathcal{A}$ in cui ogni elemento $b \in B$ è una costante. Formalmente si pone

$$\tau' = \langle I, J, K \cup \{\mathring{b} \mid b \in B\}, \mathrm{ar}\rangle$$

dove i $\mathring{b}$ sono oggetti distinti e tali che $\mathring{b} \notin I \cup J \cup K$ — per esempio possiamo porre $\mathring{b} = (b, I \cup J \cup K)$ — e $\mathcal{A}'$ è la struttura che ha per universo $A = \|\mathcal{A}\|$, e tale che $R_i^{\mathcal{A}'} = R_i^{\mathcal{A}}$, $f_j^{\mathcal{A}'} = f_j^{\mathcal{A}}$, $c_k^{\mathcal{A}'} = c_k^{\mathcal{A}}$ per ogni $i \in I$, $j \in J$, $k \in K$ e

$$\mathring{b}^{\mathcal{A}'} = b,$$

per ogni $b \in B$. La struttura $\mathcal{A}'$ viene usualmente indicata così;

$$\langle \mathcal{A}, b\rangle_{b\in B} = \langle A, \langle R_i^{\mathcal{A}} \mid i \in I\rangle, \langle f_j^{\mathcal{A}} \mid j \in J\rangle, \langle c_k^{\mathcal{A}} \mid k \in K\rangle \cup \langle b \mid b \in B\rangle\rangle.$$

Analogamente, se R_x è una relazione su $\|\mathcal{A}\|$ e f_y è una funzione finitaria su $\|\mathcal{A}\|$, dove $x \in X$ e $y \in Y$, **l'espansione canonica di $\mathcal{A}$ mediante le**

relazioni R_x e le funzioni f_y è la struttura

$$\mathcal{A}^* = \langle A, \langle R_i^{\mathcal{A}} \mid i \in I\rangle \cup \langle R_x \mid x^* \in X^*\rangle, \\ \langle f_j^{\mathcal{A}} \mid j \in J\rangle \cup \langle f_y \mid y^* \in Y^*\rangle, \langle c_k^{\mathcal{A}} \mid k \in K\rangle\rangle.$$

che ha segnatura $\tau^* = \langle I \cup X^*, J \cup Y^*, K, \mathrm{ar}^*\rangle$ dove

- X^* e Y^* sono insiemi equipotenti a X e Y rispettivamente mediante le corrispondenze $x \leftrightarrow x^*$ e $y \leftrightarrow y^*$,
- X^* e Y^* sono disgiunti tra loro e da $I \cup J \cup K$,
- $R_x^{\mathcal{A}^*} = R_x$ e $f_y^{\mathcal{A}^*} = f_y$ e $\mathrm{ar}^*(x^*)$ e $\mathrm{ar}^*(y^*)$ sono le arietà di R_x e di f_y, rispettivamente,
- $\mathrm{ar}^* \restriction I \cup J = \mathrm{ar}$.

Indicheremo $\mathcal{A}^*$ con $\langle \mathcal{A}, R_x, f_y\rangle_{x\in X, y\in Y}$.

Vediamo ora tre metodi per costruire nuove strutture a partire da vecchie: sottostrutture, limiti diretti, ultraprodotti.

27.A. Sottostrutture. Se $\mathcal{B} \subseteq \mathcal{A}$, allora $B = \|\mathcal{B}\|$ è un sottoinsieme dell'universo di $\mathcal{A}$. Il viceversa non è vero: cioè se $B \subseteq \|\mathcal{A}\|$, non è detto che B sia l'universo di una $\mathcal{B}$ sotto-struttura di $\mathcal{A}$. Quando ciò accade la struttura $\mathcal{B}$ è unica e quindi, con abuso di linguaggio, diremo che B è una sotto-struttura di $\mathcal{A}$.

Esercizio 27.2. (i) Sia $\mathcal{A}$ una τ-struttura priva di funzioni, cioè $J = \emptyset$. Dimostrare che se $\emptyset \neq B \subseteq \|\mathcal{A}\|$ e $B \supseteq \{c_k^{\mathcal{A}} \mid k \in K\}$, allora B è l'universo di una sotto-struttura di $\mathcal{A}$.

(ii) Dimostrare che se $\emptyset \neq X \subseteq \|\mathcal{A}\|$ e

$$S = \bigcap\{\|\mathcal{B}\| \mid X \subseteq \|\mathcal{B}\| \wedge \mathcal{B} \subseteq \mathcal{A}\},$$

allora S è l'universo di una sotto-struttura $\mathcal{S} \subseteq \mathcal{A}$, la **sotto-struttura generata da** X. Dimostrare che S è la chiusura di $X \cup \{c_k^{\mathcal{A}} \mid k \in K\}$ sotto le funzioni $\{f_j^{\mathcal{A}} \mid j \in J\}$ e quindi se τ è bene ordinabile

$$|S| \leq \max(|J|, |K|, |X|, \aleph_0)$$

per il Teorema 16.5 a pagina 328.

Se $\mathcal{A}$ coincide con la sottostruttura generata da un suo sottoinsieme finito, diremo che è **finitamente generata**. La famiglia delle sottostrutture di $\mathcal{A}$ è un reticolo completo, mentre la famiglia delle sottostrutture finitamente generate è un semireticolo superiore completo, ma non è un reticolo — si veda l'Esempio 14.21 a pagina 313 e l'Esempio 8.25(e) a pagina 166.

27.B. Limiti diretti. La categoria $\mathrm{Str}(L)$ delle L-strutture ammette limiti diretti — la verifica è una generalizzazione del fatto che GRP, la categoria dei gruppi (Sezione 18.D.2) e PORD, la categoria degli ordini (Sezione 18.D.3) ammettono limiti diretti.

Un **sistema diretto di τ-strutture e morfismi** è una coppia

$$\left(\langle \mathcal{A}_x \mid x \in X\rangle, \langle \pi_{x,y} \mid x, y \in X \wedge x \leq y\rangle\right)$$

dove $\langle X, \leq\rangle$ è un insieme diretto superiormente tale che

- ogni $\mathcal{A}_x$ è una τ-struttura,
- $\pi_{x,y} \colon \mathcal{A}_x \to \mathcal{A}_y$ è un morfismo,
- $\pi_{x,x} = \mathrm{id} \restriction \mathcal{A}_x$,
- $\pi_{x,z} = \pi_{y,z} \circ \pi_{x,y}$ se $x \leq y \leq z$.

Poiché $\left(\langle \|\mathcal{A}_x\| \mid x \in X\rangle, \langle \pi_{x,y} \mid x, y \in X \wedge x \leq y\rangle\right)$ è un sistema diretto di insiemi e funzioni, possiamo calcolarne il limite diretto

$$\left(A_\infty, \langle \pi_{x,y} \mid x, y \in X \wedge x \leq y\rangle\right)$$

definito in (18.3) a pagina 342. L'insieme A_∞ è l'universo di una τ-struttura $\mathcal{A}_\infty$ definita come segue.

- Se $\mathrm{ar}(i) = n$ definiamo $R_i^{\mathcal{A}_\infty} \subseteq A_\infty^n$

$$([(x_1, a_1)]_\sim, \ldots, [(x_n, a_n)]_\sim) \in R_i^{\mathcal{A}_\infty} \quad \Leftrightarrow \quad \exists y \geq x_1, \ldots, x_n \left((\pi_{x_1,y}(a_1), \ldots, \pi_{x_n,y}(a_n)) \in R_i^{\mathcal{A}_y}\right).$$

- Se $\mathrm{ar}(j) = n$ definiamo $f_j^{\mathcal{A}_\infty} \colon A_\infty^n \to A_\infty$

$$f_j^{\mathcal{A}_\infty}([(x_1, a_1)], \ldots, [(x_n, a_n)]) = [f_j^{\mathcal{A}_y}(\pi_{x_1,y}(a_1), \ldots, \pi_{x_n,y}(a_n))]$$

  per qualche/ogni $y \geq x_1, \ldots, x_n$.
- Se $k \in K$ definiamo $c_k^{\mathcal{A}_\infty} \in A_\infty$ come

$$c_k^{\mathcal{A}_\infty} = [(x, c_k^{\mathcal{A}_x})]$$

  per un qualche/ogni $x \in X$.

La verifica che le definizioni di $R_i^{\mathcal{A}_\infty}$, $f_j^{\mathcal{A}_\infty}$ e $c_k^{\mathcal{A}_\infty}$ non dipendono dalla scelta dei rappresentanti e che $\pi_{x,\infty} \colon \mathcal{A}_x \to \mathcal{A}_\infty$ sono dei morfismi che commutano con le $\pi_{x,y}$ è analoga a quanto visto nel caso degli ordini (Sezione 18.D.3) e nel caso dei gruppi (Sezione 18.D.2). Diremo che

$$\left(\mathcal{A}_\infty, \langle \pi_{x,\infty} \mid x \in X\rangle\right)$$

è il limite diretto di $\left(\langle \mathcal{A}_x \mid x \in X\rangle, \langle \pi_{x,y} \mid x, y \in X \wedge x \leq y\rangle\right)$. Spesso indicheremo la struttura $\mathcal{A}_\infty$ con $\lim_{x \in X} \mathcal{A}_x$.

L'unione $\bigcup_{n\in\omega} \mathcal{A}_n$ di una catena crescente di strutture $\mathcal{A}_0 \subseteq \mathcal{A}_1 \subseteq \dots$ è un caso particolare di limite diretto (Esercizio 27.5 parte (iii)).

27.C. Ultraprodotti.

27.C.1. *Prodotti.* Innanzi tutto verifichiamo che la categoria $\mathrm{Str}(\tau)$ ammette prodotti, anzi prodotti con un numero arbitrario di fattori. La costruzione del prodotto di strutture è una generalizzazione del prodotto di ordini (Sezione 12.A) e del prodotto diretto di gruppi. Sia X un insieme non vuoto, che chiamiamo insieme degli indici.[1] Il **prodotto diretto** o **prodotto** di una famiglia di τ-strutture $\langle \mathcal{A}_x \mid x \in X\rangle$ è la τ-struttura $\mathcal{A} = \prod_x \mathcal{A}_x$ di universo $\bigtimes_{x\in X} \|\mathcal{A}_x\|$ e tale che:

- se $\mathrm{ar}(i) = n$

$$(g_1, \dots, g_n) \in R_i^{\mathcal{A}} \Leftrightarrow \forall x \in X \left((g_1(x), \dots, g_n(x)) \in R_i^{\mathcal{A}_x}\right).$$

- se $\mathrm{ar}(j) = n$ definiamo $f_j^{\mathcal{A}} \colon A^n \to A$

$$f_j^{\mathcal{A}}(g_1, \dots, g_n) = \langle f_j^{\mathcal{A}_x}(g_1(x), \dots, g_n(x)) \mid x \in X\rangle,$$

- se $k \in K$ definiamo $c_k^{\mathcal{A}} \in A$ come

$$c_k^{\mathcal{A}} = \langle c_k^{\mathcal{A}_x} \mid x \in X\rangle.$$

Osservazione 27.3. Se $K = \emptyset$, cioè τ non contiene costanti, si assume AC per verificare che $\bigtimes_{x\in X} \|\mathcal{A}_x\| \neq \emptyset$, e che quindi si ha una τ-struttura.

Quando X è composto da due elementi, cioè $\langle \mathcal{A}_x \mid x \in X\rangle$ consiste di sole due strutture, diciamo $\mathcal{A}_0$ e $\mathcal{A}_1$, indicheremo il prodotto con

$$\mathcal{A}_0 \times \mathcal{A}_1.$$

Le mappe

$$\pi_m \colon \bigtimes_{x\in X} \|\mathcal{A}_x\| \to \|\mathcal{A}_m\|, \quad f \mapsto f(m) \qquad (m \in X)$$

sono dei morfismi di strutture e soddisfano alla proprietà di universalità dei prodotti.

27.C.2. *Prodotti ridotti.* Se F è un filtro su X, abbiamo definito nella Sezione 23.G la relazione d'equivalenza $g \sim_F h \Leftrightarrow \{x \in X \mid g(x) = h(x)\} \in F$ su $\bigtimes_{x\in X} \|\mathcal{A}_x\|$ e abbiamo indicato con $\prod_F \|\mathcal{A}_x\|$ il quoziente $\bigtimes_{x\in X} \|\mathcal{A}_x\| /{\sim_F}$. Il **prodotto ridotto modulo** F **di** $\langle \mathcal{A}_x \mid x \in X\rangle$ è la τ-struttura

$$\prod_F \mathcal{A}_x$$

di universo $\prod_F \|\mathcal{A}_x\|$ costruita in modo analogo a quanto visto nella Sezione 23.G.1 per gli ordini e nella Sezione 23.G.2 per i campi:

[1] La scelta della lettera X per denotare l'insieme degli indici può apparire singolare, ma le altre lettere che solitamente si usano I, J, K sono già impegnate per altri scopi.

- se $\mathrm{ar}(i) = n$ e $[g_1], \dots, [g_n] \in A_F$, allora

$$([g_1], \dots, [g_n]) \in R_i^{\prod_F \mathcal{A}_x} \Leftrightarrow \{x \in X \mid (g_1(x), \dots, g_n(x)) \in R_i^{\mathcal{A}_x}\} \in F$$

- se $\mathrm{ar}(j) = n$ e $[g_1], \dots, [g_n] \in A_F$, allora

$$f_j^{\prod_F \mathcal{A}_x}([g_1], \dots, [g_n]) = [\langle f_j^{\mathcal{A}_x}(g_1(x), \dots, g_n(x)) \mid x \in X\rangle]$$

- $c_k^{\prod_F \mathcal{A}_x} = [\langle c_k^{\mathcal{A}_x} \mid x \in X\rangle]$.

Esercizio 27.4. Verificare che:

(i) se $Y \in F$ e $\pi_y \colon \mathcal{A}_y \to \mathcal{B}_y$ è un isomorfismo per ogni $y \in Y$, allora $\prod_F \mathcal{A}_x \cong \prod_F \mathcal{B}_x$;

(ii) se $Y \in F$ e $F \restriction Y$ è il filtro indotto da F su Y (Esercizio 23.57), allora $\prod_F \mathcal{A}_x$ è isomorfo al prodotto ridotto $\prod_{F\restriction Y} \mathcal{A}_y$ di $\langle \mathcal{A}_y \mid y \in Y\rangle$ modulo $F \restriction Y$. In particolare, se $\{x_0\} \in F$ per qualche $x_0 \in N$, allora $\prod_F \mathcal{A}_x \cong \mathcal{A}_{x_0}$.

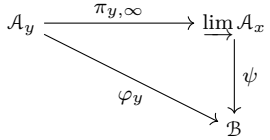
Se $\mathcal{A}_x = \mathcal{A}$ per ogni $x \in X$, diremo che

$$\prod_F \mathcal{A}_x = \mathcal{A}^N/F$$

è una **potenza ridotta**. Se F è un ultrafiltro su N diremo che $\prod_F \mathcal{A}_x$ è un **ultraprodotto**, e se $\mathcal{A}_x = \mathcal{A}$ per ogni $x \in N$, parleremo di **ultrapotenza**.

Esercizi

Esercizio 27.5. (i) Verificare che nella definizione di limite diretto le $\pi_{x,\infty}$ sono davvero dei morfismi e che vale la seguente proprietà di universalità: per ogni $\mathcal{B} \in \mathrm{Str}(\tau)$ e per ogni famiglia di morfismi $\varphi_x \colon \mathcal{A}_x \to \mathcal{B}$ tali che $x \leq y \Rightarrow \varphi_y \circ \pi_{x,y} = \varphi_x$ esiste un unico morfismo $\psi \colon \varinjlim \mathcal{A}_x \rightarrowtail \mathcal{B}$ che rende il diagramma



commutativo.

(ii) Verificare che se le φ_y sono immersioni anche ψ è un'immersione.

(iii) Se $\langle X, \leq\rangle$ è un ordine lineare e $\pi_{x,y} \colon \mathcal{A}_x \to \mathcal{A}_y$ è la mappa di inclusione, dimostrare che $\|\mathcal{A}_\infty\|$ è identificabile con $\bigcup_{x\in X} \|\mathcal{A}_x\|$ e con questa identificazione le mappe $\pi_{y,\infty}$ sono funzioni di inclusione. In questo caso il limite diretto è detto **unione di una catena di strutture**.

Esercizio 27.6. Per ogni τ-struttura $\mathcal{A}$ sia

$$\mathrm{FG}(\mathcal{A}) = \{\mathcal{B} \mid \mathcal{B} \subseteq \mathcal{A} \text{ e } \mathcal{B} \text{ è finitamente generata}\}.$$

Per $\mathcal{B} \subseteq \mathcal{C}$ sotto-strutture finitamente generate di $\mathcal{A}$ sia $\pi_{\mathcal{B},\mathcal{C}} \colon \mathcal{B} \hookrightarrow \mathcal{C}$ la mappa di inclusione. Dimostrare che $\langle \mathrm{FG}(\mathcal{A}), \subseteq \rangle$ è diretto superiormente e che $\mathrm{FG}(\mathcal{A})$ con le funzioni $\pi_{\mathcal{B},\mathcal{C}}$ forma un sistema diretto superiormente di τ-strutture e morfismi e che

$$\mathcal{A} \;\cong\; \varinjlim \langle \mathcal{B} \mid \mathcal{B} \in \mathrm{FG}(\mathcal{A}) \rangle \,.$$

Note e osservazioni

28. Linguaggi del prim'ordine

Lo scopo di questa sezione è di dare una trattazione rigorosa nella teoria degli insiemi delle nozioni viste nel Capitolo I. Per ogni segnatura τ costruiremo un linguaggio L e a partire da esso costruiremo i suoi termini $\boldsymbol{\varphi}$ e le sue formule $\boldsymbol{\varphi}$. (Tanto i linguaggi quanto i termini e le formule saranno insiemi.) Le formule di L sono la codifica insiemistica delle usuali espressioni matematiche riguardanti le τ-strutture e quindi avremo bisogno di una controparte insiemistica dei vari simboli logici

$$\neg, \vee, \wedge, \Rightarrow, \Leftrightarrow, \exists, \forall.$$

Al fine di evitare confusioni, in questo capitolo distingueremo tipograficamente tra i simboli del linguaggio oggetto (che sono insiemi) e quelli del linguaggio informale in cui vengono esposti i risultati.

28.A. Simboli. Un **linguaggio del prim'ordine** L è costituito da

- una ω-successione di oggetti che chiamiamo **variabili**

$$\boldsymbol{v}_0, \boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n, \ldots$$

- due oggetti distinti che chiamiamo **connettivi**: $\boldsymbol{\neg}$ e $\boldsymbol{\vee}$,
- un oggetto che chiamiamo **simbolo di uguaglianza** $\equiv$,
- tre famiglie disgiunte di oggetti

$$\{\boldsymbol{R}_i \mid i \in I\}, \quad \{\boldsymbol{f}_j \mid j \in J\}, \quad \{\boldsymbol{c}_k \mid k \in K\}$$

  che chiamiamo, rispettivamente, **simboli di relazione**, **simboli di funzione** o **di operazione**, **simboli di costante**,

- una funzione $\mathrm{ar} \colon \{\boldsymbol{R}_i \mid i \in I\} \cup \{\boldsymbol{f}_j \mid j \in J\} \to \omega \setminus \{0\}$, detta **arietà**.

Spesso i simboli di relazione sono detti **predicati**. La natura di questi oggetti è irrilevante. Noi stipuliamo che

il simbolo...	è un'abbreviazione di...
$\boldsymbol{\neg}$	0
$\boldsymbol{\vee}$	1
$\boldsymbol{\equiv}$	2
$\boldsymbol{v}_n$	$\langle n\rangle$
$\boldsymbol{R}_i$	$\langle(0,i)\rangle$
$\boldsymbol{f}_j$	$\langle(1,j)\rangle$
$\boldsymbol{c}_k$	$\langle(2,k)\rangle$.

Definizione 28.1. Un linguaggio del prim'ordine L è una coppia $(\mathcal{S}, \mathrm{ar})$ che soddisfa le seguenti proprietà

- esistono insiemi I, J e K tali che

$$\mathcal{S} = \mathrm{Rel}_L \cup \mathrm{Func}_L \cup \mathrm{Const}_L \cup \{\boldsymbol{\neg}, \boldsymbol{\vee}, \boldsymbol{\equiv}\} \cup \textsc{Vbl}$$

  dove

$$\textsc{Vbl} = \{\boldsymbol{v}_n \mid n \in \omega\}$$

  e $\mathrm{Rel}_L = {}^1(\{0\} \times I)$, $\mathrm{Func}_L = {}^1(\{1\} \times J)$ e $\mathrm{Const}_L = {}^1(\{2\} \times K)$.
- $\mathrm{ar}\colon (\{0\} \times I) \cup (\{1\} \times J) \to \omega \setminus \{0\}$.

I **simboli non logici di** L sono gli elementi di $\mathrm{Rel}_L \cup \mathrm{Func}_L \cup \mathrm{Const}_L$. Quando diciamo che un linguaggio L contiene un simbolo non logico s intendiamo dire che $s \in \mathcal{S}$. Ogni segnatura τ genera un linguaggio L_τ e, viceversa, ogni linguaggio L genera una segnatura τ_L. Due linguaggi sono **isomorfi** se e solo se sono isomorfe le loro segnature. Diremo che L è un **sotto-linguaggio** di L' ovvero che L' è un'**estensione** di L se e solo se $\tau_L \subseteq \tau_{L'}$.

Osservazione 28.2. Visto che un linguaggio è completamente identificato dalla sua segnatura, nella pratica le due nozioni sono spesso confuse, per lo meno a livello di notazioni. Anche la funzione di arietà è spesso soppressa, quando la si evince dal contesto — per esempio scriveremo $L_{\textsc{gruppi}} = \{\cdot, {}^{-1}, 1\}$ per indicare il linguaggio dei gruppi. Questo abuso di linguaggio verrà perpetrato ogni qual volta la notazione insiemistica ci permetta asserire in modo conciso fatti relativi ai linguaggi, la cui definizione precisa richiederebbe una notazione barocca. Quindi scriveremo $L \subseteq L'$ per dire che L' è un'estensione di L, oppure $L \cap L'$ per indicare il linguaggio i cui simboli non logici sono quelli che occorrono tanto in L quanto in L', e così via.

Un linguaggio è **bene ordinabile** se la sua segnatura è bene ordinabile. La **cardinalità** di L è

$$\mathrm{card}(L) = \aleph_0 + \mathrm{card}(\tau_L).$$

Un **linguaggio finito** è un linguaggio la cui segnatura è finita. Una L-struttura è, per definizione, una τ_L-struttura e poniamo per definizione

$$\mathrm{Str}(L) = \mathrm{Str}(\tau_L).$$

Nel Capitolo I e in particolare nella Sezione 5 abbiamo visto molti esempi di linguaggi finiti, e quindi bene ordinabili. Invece l'esempio degli spazi vettoriali su $\mathbb{R}$ descritto a pagina 84 definisce una segnatura (e quindi un linguaggio) più che numerabile che non è ben ordinabile se non si assume AC. Un esempio importante di linguaggio infinito ben ordinabile è il linguaggio numerabile universale L_∞ che ha $\aleph_0$ ha simboli di costante $\boldsymbol{c}_n$ ($n \in \omega$) e $\aleph_0$ simboli di relazione $\boldsymbol{R}_{n,m}$ e di funzione $\boldsymbol{f}_{n,m}$ di ogni arietà, cioè $\mathrm{ar}(\boldsymbol{R}_{n,m}) = \mathrm{ar}(\boldsymbol{f}_{n,m}) = m$ per ogni $n \geq 0$ e $m > 0$. Ogni linguaggio numerabile L è (isomorfo ad) un sottolinguaggio di L_∞, quindi ogni L-struttura è la contrazione di una L_∞-struttura.

28.B. Termini e formule. Le definizioni e i risultati di questa sezione non sono altro che una rivisitazione dei concetti esposti nella Sezione 20.

28.B.1. *Termini.* L'insieme $\mathrm{Term} = \mathrm{Term}(L)$ dei termini di L è l'insieme

$$\mathrm{Expr}(\textsc{Vbl} \cup \mathrm{Func} \cup \mathrm{Const}, a)$$

delle espressioni sull'insieme di simboli $\textsc{Vbl} \cup \mathrm{Func} \cup \mathrm{Const}$, dove

- $a(s) = 0$, se $s \in \textsc{Vbl} \cup \mathrm{Const}$ e
- $a(s) = \mathrm{ar}(s)$, se $s \in \mathrm{Func}$.

Poiché vogliamo che le costanti e le variabili siano termini, adotteremo la Convenzione sulle espressioni introdotta a pagina 355. L'**altezza di un termine $\boldsymbol{t}$** è la sua altezza $\mathrm{ht}(\boldsymbol{t})$ vista come espressione.

Le lettere $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}, \boldsymbol{w}$ variano su $\textsc{Vbl}$, mentre le lettere $\boldsymbol{t}, \boldsymbol{u}, \boldsymbol{s}$ variano su Term. Il Corollario 20.7 garantisce che un termine che non sia una variabile o una costante è della forma $\boldsymbol{f}_j(\boldsymbol{t}_1, \dots, \boldsymbol{t}_m)$ per un'unica m-upla $\boldsymbol{t}_1, \dots, \boldsymbol{t}_m$ di termini. L'insieme $\textsc{Vbl}(\boldsymbol{t})$ delle **variabili di un termine $\boldsymbol{t}$** è definito per ricorsione su $\mathrm{ht}(\boldsymbol{t})$:

$$\begin{aligned} \textsc{Vbl}(\boldsymbol{c}_k) &= \emptyset \\ \textsc{Vbl}(\boldsymbol{v}_n) &= \{\boldsymbol{v}_n\} \\ \textsc{Vbl}(\boldsymbol{f}_j(\boldsymbol{t}_1, \dots, \boldsymbol{t}_m)) &= \textsc{Vbl}(\boldsymbol{t}_1) \cup \cdots \cup \textsc{Vbl}(\boldsymbol{t}_m). \end{aligned}$$

L'insieme dei **termini chiusi**

$$\mathrm{ClTerm} = \{\boldsymbol{t} \in \mathrm{Term} \mid \textsc{Vbl}(\boldsymbol{t}) = \emptyset\}$$

è la collezione dei termini costruiti a partire dalle costanti.

28.B.2. *Formule.*

Definizione 28.3. Una **formula atomica** di L è una sequenza della forma

$$\langle \boldsymbol{R}_i \rangle^\frown \boldsymbol{t}_1{}^\frown \ldots {}^\frown \boldsymbol{t}_m$$

dove $\boldsymbol{R}_i$ è m-ario e $\boldsymbol{t}_1, \ldots, \boldsymbol{t}_m$ sono termini, oppure è della forma

$$\langle \equiv \rangle^\frown \boldsymbol{t}_1{}^\frown \boldsymbol{t}_2$$

con $\boldsymbol{t}_1$ e $\boldsymbol{t}_2$ termini. Scriveremo AtFml = AtFml(L) per indicare l'insieme delle formule atomiche di L.

L'insieme Fml = Fml(L) delle **formule** di L è il più piccolo insieme di stringhe contenente AtFml e chiuso sotto le seguenti operazioni:

- $\boldsymbol{\varphi} \mapsto \langle \boldsymbol{\neg} \rangle^\frown \boldsymbol{\varphi}$,
- $(\boldsymbol{\varphi}, \boldsymbol{\psi}) \mapsto \langle \boldsymbol{\vee} \rangle^\frown \boldsymbol{\varphi}^\frown \boldsymbol{\psi}$, e
- $\boldsymbol{\varphi} \mapsto \langle \boldsymbol{v}_n \rangle^\frown \boldsymbol{\varphi}$ $(n \in \omega)$.

In altre parole Fml = Expr(S, a) dove

$$S = \{\boldsymbol{\neg}, \boldsymbol{\vee}\} \cup \{\boldsymbol{v}_n \mid n \in \omega\} \cup \text{AtFml}$$

e $a \colon S \to \omega$ soddisfa:

- $a(\boldsymbol{\varphi}) = 0$, per ogni $\boldsymbol{\varphi} \in$ AtFml,
- $a(\boldsymbol{\neg}) = 1$ e $a(\boldsymbol{\vee}) = 2$,
- $a(\boldsymbol{v}_n) = 1$, per ogni $n \in \omega$.

Le lettere $\boldsymbol{\varphi}, \boldsymbol{\psi}, \boldsymbol{\chi}, \ldots$ variano su Fml.

È immediato verificare che gli insiemi $\{\boldsymbol{\neg}, \boldsymbol{\vee}\}$, $\{\boldsymbol{v}_n \mid n \in \omega\}$ e AtFml sono disgiunti e quindi la funzione a della Definizione 28.3 è ben definita. Poiché vogliamo che AtFml $\subseteq$ Fml, adotteremo la Convenzione sulle espressioni introdotta a pagina 355. Al fine di alleggerire la notazione, utilizzeremo le seguenti convenzioni:

la scrittura…	equivale a dire…
$(\boldsymbol{t}_1 \equiv \boldsymbol{t}_2)$	$\langle \equiv \rangle^\frown \boldsymbol{t}_1{}^\frown \boldsymbol{t}_2$
$(\boldsymbol{t}_1 \not\equiv \boldsymbol{t}_2)$	$\langle \boldsymbol{\neg}, \equiv \rangle^\frown \boldsymbol{t}_1{}^\frown \boldsymbol{t}_2$
$\boldsymbol{R}_i(\boldsymbol{t}_1, \ldots, \boldsymbol{t}_n)$	$\langle \boldsymbol{R}_i \rangle^\frown \boldsymbol{t}_1{}^\frown \ldots {}^\frown \boldsymbol{t}_n$
$\boldsymbol{\neg\varphi}$	$\langle \boldsymbol{\neg} \rangle^\frown \boldsymbol{\varphi}$
$(\boldsymbol{\varphi} \boldsymbol{\vee} \boldsymbol{\psi})$	$\langle \boldsymbol{\vee} \rangle^\frown \boldsymbol{\varphi}^\frown \boldsymbol{\psi}$
$\boldsymbol{\exists v}_n \boldsymbol{\varphi}$	$\langle \boldsymbol{v}_n \rangle^\frown \boldsymbol{\varphi}$

Quindi scriveremo

$$\boldsymbol{\exists x}\, (\boldsymbol{x} \not\equiv \boldsymbol{y} \boldsymbol{\vee} \boldsymbol{R}_i(\boldsymbol{y}, \boldsymbol{x}))$$

invece di

$$\langle \boldsymbol{x}, \boldsymbol{\vee}, \boldsymbol{\neg}, \langle \equiv, \boldsymbol{x}, \boldsymbol{y} \rangle, \langle \boldsymbol{R}_i, \boldsymbol{y}, \boldsymbol{x} \rangle \rangle.$$

I connettivi $\bigwedge$, $\Rightarrow$ e $\Leftrightarrow$, e il quantificatore $\forall$ sono introdotti tramite le definizioni:

la scrittura...	è un'abbreviazione di...
$\boldsymbol{\varphi \wedge \psi}$	$\boldsymbol{\neg(\neg\varphi \vee \neg\psi)}$
$\boldsymbol{\varphi \Rightarrow \psi}$	$\boldsymbol{(\neg\varphi \vee \psi)}$
$\boldsymbol{\varphi \Leftrightarrow \psi}$	$\boldsymbol{\neg(\neg(\neg\varphi \vee \psi) \vee (\neg(\varphi \vee \neg\psi)))}$
$\boldsymbol{\forall x \varphi}$	$\boldsymbol{\neg\exists x \neg\varphi}$

Quindi $\boldsymbol{\neg\exists x \neg\,(x \not\equiv y \vee R_i(y, x))}$ può essere scritta come

$$\boldsymbol{\forall x\,(x \equiv y \Rightarrow R_i(y, x))}\,.$$

Per evitare un eccessivo uso di parentesi, adotteremo la convenzione già introdotta a pagina 23 per cui $\boldsymbol{\neg}$ lega più fortemente di $\boldsymbol{\vee}$ e di $\boldsymbol{\wedge}$, e questi legano più fortemente di $\boldsymbol{\Rightarrow}$ e di $\boldsymbol{\Leftrightarrow}$.

Chiaramente nella definizione dell'insieme delle formule si può partire da un insieme di simboli S differente — per esempio potremmo prendere

$$S = \{\boldsymbol{\neg}, \boldsymbol{\vee}, \boldsymbol{\wedge}, \boldsymbol{\Rightarrow}, \boldsymbol{\Leftrightarrow}\} \cup \{\boldsymbol{\exists v}_n \mid n \in \omega\} \cup \{\boldsymbol{\forall v}_n \mid n \in \omega\} \cup \mathrm{AtFml}$$

dove gli oggetti $\boldsymbol{\exists v}_n$ e $\boldsymbol{\forall v}_n$ sono tutti distinti e la funzione $a\colon S \to \omega$ è definita da $a(\boldsymbol{\neg}) = a(\boldsymbol{\exists v}_n) = a(\boldsymbol{\forall v}_n) = 1$ e $a(\boldsymbol{\vee}) = a(\boldsymbol{\wedge}) = a(\boldsymbol{\Rightarrow}) = a(\boldsymbol{\Leftrightarrow}) = 2$. In questo modo potremmo utilizzare ufficialmente tutti i connettivi e entrambi i quantificatori. Il vantaggio del nostro approccio è che quando dobbiamo argomentare per induzione sulla complessità delle formule, ci sono meno casi da verificare.

L'**altezza di una formula** $\mathrm{ht}(\boldsymbol{\varphi})$ è la sua altezza vista come espressione. In particolare l'altezza della formula $\boldsymbol{\forall x\,(x \equiv y \Rightarrow R_i(y, x))}$ è 6, mentre la lunghezza di questa formula — intesa come sequenza finita — è 7

$$\langle \boldsymbol{\neg}, \boldsymbol{x}, \boldsymbol{\neg}, \boldsymbol{\vee}, \boldsymbol{\neg}, \langle \boldsymbol{\equiv}, \boldsymbol{x}, \boldsymbol{y}\rangle, \langle \boldsymbol{R}_i, \boldsymbol{x}, \boldsymbol{y}\rangle\rangle.$$

Tuttavia è più naturale vedere questa formula come una sequenza di lunghezza 11:

$$\langle \boldsymbol{\neg}, \boldsymbol{x}, \boldsymbol{\neg}, \boldsymbol{\vee}, \boldsymbol{\neg}, \boldsymbol{\equiv}, \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{R}_i, \boldsymbol{x}, \boldsymbol{y}\rangle.$$

Per questo motivo introduciamo la seguente

Definizione 28.4. La **forma estesa** di una formula,

$$\boldsymbol{\varphi} = u_0{}^\frown \boldsymbol{\psi}_1{}^\frown u_1{}^\frown \boldsymbol{\psi}_2{}^\frown u_2{}^\frown \ldots {}^\frown u_{n-1}{}^\frown \boldsymbol{\psi}_n{}^\frown u_n$$

dove $u_i \in (\{\boldsymbol{\neg}, \boldsymbol{\vee}\} \cup \mathrm{Vbl})^{<\omega}$ e $\boldsymbol{\psi}_i \in \mathrm{AtFml}$ è la sequenza

$$\boldsymbol{\varphi}^{\mathrm{e}} = u_0{}^\frown v_1{}^\frown u_1{}^\frown v_2{}^\frown u_2{}^\frown \ldots {}^\frown u_{n-1}{}^\frown v_n{}^\frown u_n,$$

dove $\boldsymbol{\psi}_i = \langle v_i\rangle$. La **lunghezza** $\ell(\boldsymbol{\varphi})$ **di una formula** è la lunghezza della sua forma estesa, cioè $\ell(\boldsymbol{\varphi}) = \mathrm{lh}(\boldsymbol{\varphi}^{\mathrm{e}})$.

Osservazione 28.5. La forma estesa di una formula è un elemento di

$$(\{\neg, \vee\} \cup \mathrm{Vbl} \cup \mathrm{Rel}_L \cup \mathrm{Func}_L \cup \mathrm{Const}_L)^{<\omega},$$

ma non è un'espressione.

I termini e le formule di un linguaggio sono particolari tipi di espressioni e in questo caso il concetto di sotto-espressione (pag. 356) diventa rispettivamente la nozione di **sotto-termine** e di **sotto-formula**. Scriveremo $\mathrm{Sub}(\boldsymbol{\varphi})$ per l'insieme delle sotto-formule proprie di $\boldsymbol{\varphi}$.

28.C. Occorrenze. Un'**occorrenza** di una variabile $\boldsymbol{x}$ in una formula $\boldsymbol{\varphi}$ è un'occorrenza (nel senso della Sezione 20.B) di $\boldsymbol{x}$ nella sua forma estesa e l'insieme delle **occorrenze di $\boldsymbol{x}$ in $\boldsymbol{\varphi}$** è un sottoinsieme di $\ell(\boldsymbol{\varphi})$ ed è indicato con $\textsc{Occ}(\boldsymbol{x}; \boldsymbol{\varphi})$. Chiaramente $\textsc{Occ}(\boldsymbol{x}; \boldsymbol{\varphi}) = \emptyset$ se e solo se $\boldsymbol{x}$ non compare in $\boldsymbol{\varphi}^{\mathrm{e}}$ la forma estesa di $\boldsymbol{\varphi}$. Diremo che una variabile $\boldsymbol{x}$ **occorre** in $\boldsymbol{\varphi}$ se e solo se $\textsc{Occ}(\boldsymbol{x}; \boldsymbol{\varphi}) \neq \emptyset$. L'insieme

$$\mathrm{FO}(\boldsymbol{x}; \boldsymbol{\varphi}) \subseteq \textsc{Occ}(\boldsymbol{x}; \boldsymbol{\varphi})$$

delle **occorrenze libere** di $\boldsymbol{x}$ in $\boldsymbol{\varphi}$ è definito induttivamente come segue:

- se $\boldsymbol{\varphi} \in \mathrm{AtFml}$, allora $\mathrm{FO}(\boldsymbol{x}; \boldsymbol{\varphi}) = \textsc{Occ}(\boldsymbol{x}; \boldsymbol{\varphi})$
- se $\boldsymbol{\varphi} = \boldsymbol{\psi} \vee \boldsymbol{\chi}$, allora

  $$\mathrm{FO}(\boldsymbol{x}; \boldsymbol{\varphi}) = \{1 + n \mid n \in \mathrm{FO}(\boldsymbol{x}; \boldsymbol{\psi})\} \cup \{1 + \ell(\boldsymbol{\psi}) + n \mid n \in \mathrm{FO}(\boldsymbol{x}; \boldsymbol{\chi})\}$$

- se $\boldsymbol{\varphi} = \neg\boldsymbol{\psi}$, allora

  $$\mathrm{FO}(\boldsymbol{x}; \boldsymbol{\varphi}) = \{1 + n \mid n \in \mathrm{FO}(\boldsymbol{x}; \boldsymbol{\psi})\}$$

- se $\boldsymbol{\varphi} = \exists \boldsymbol{y}\, \boldsymbol{\psi}$ e $\boldsymbol{y} \neq \boldsymbol{x}$, allora

  $$\mathrm{FO}(\boldsymbol{x}; \boldsymbol{\varphi}) = \{1 + n \mid n \in \mathrm{FO}(\boldsymbol{x}; \boldsymbol{\psi})\}$$

- se $\boldsymbol{\varphi} = \exists \boldsymbol{x}\, \boldsymbol{\psi}$, allora $\mathrm{FO}(\boldsymbol{x}; \boldsymbol{\varphi}) = \emptyset$.

L'insieme

$$\textsc{Occ}(\boldsymbol{x}; \boldsymbol{\varphi}) \setminus \mathrm{FO}(\boldsymbol{x}; \boldsymbol{\varphi})$$

è l'**insieme delle occorrenze vincolate di $\boldsymbol{x}$ in $\boldsymbol{\varphi}$**. Una variabile $\boldsymbol{x}$ **occorre libera in $\boldsymbol{\varphi}$** se $\mathrm{FO}(\boldsymbol{x}; \boldsymbol{\varphi}) \neq \emptyset$ e **occorre vincolata in $\boldsymbol{\varphi}$** se $\textsc{Occ}(\boldsymbol{x}; \boldsymbol{\varphi}) \setminus \mathrm{FO}(\boldsymbol{x}; \boldsymbol{\varphi}) \neq \emptyset$, quindi una variabile può occorrere libera e vincolata nella medesima formula. L'insieme delle variabili che occorrono libere in $\boldsymbol{\varphi}$ è indicato con

$$\textsc{Fv}(\boldsymbol{\varphi}) \stackrel{\mathrm{def}}{=} \{\boldsymbol{x} \in \textsc{Vbl} \mid \mathrm{FO}(\boldsymbol{x}; \boldsymbol{\varphi}) \neq \emptyset\}.$$

Se $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ sono distinte, la notazione

$$\boldsymbol{\varphi}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)$$

significa che $\mathrm{Fv}(\boldsymbol{\varphi}) \subseteq \{\boldsymbol{x}_1, \dots, \boldsymbol{x}_n\}$. Un **enunciato** è una formula priva di variabili libere e l'insieme degli L-enunciati si indica con

$$\mathrm{Sent}(L).$$

Useremo le lettere $\boldsymbol{\sigma}, \boldsymbol{\tau}, \dots$ variamente decorate per denotare un enunciato.

28.D. Sostituzione. Nella Sezione 3.C.3 del Capitolo I abbiamo definito l'operazione di sostituzione per le espressioni:

$$w, z_1, \dots, z_k, v_1, \dots, v_k \in \mathrm{Expr}(S, a) \wedge \bigwedge_{1 \le i < j \le n} v_i \neq v_j \Rightarrow w[z_1/v_1, \dots, z_k/v_k] \in \mathrm{Expr}(S, a).$$

L'operazione di sostituzione è anche definita quando $w, z_1, \dots, z_k \in S^{<\omega}$ e $v_1, \dots, v_k \in S$ sono distinti e in questo caso $w[z_1/v_1, \dots, z_k/v_k]$ appartiene a $S^{<\omega}$. In particolare,

$$\boldsymbol{t}, \boldsymbol{u}_1, \dots, \boldsymbol{u}_n, \boldsymbol{s}_1, \dots, \boldsymbol{s}_n \in \mathrm{Term} \wedge \bigwedge_{1 \le i < j \le n} \boldsymbol{s}_i \neq \boldsymbol{s}_j \Rightarrow \boldsymbol{t}[\boldsymbol{u}_1/\boldsymbol{s}_1, \dots, \boldsymbol{u}_n/\boldsymbol{s}_n] \in \mathrm{Term}$$

e

$$\boldsymbol{\varphi}, \boldsymbol{\psi}_1, \dots, \boldsymbol{\psi}_n, \boldsymbol{\chi}_1, \dots, \boldsymbol{\chi}_n \in \mathrm{Fml} \wedge \bigwedge_{1 \le i < j \le n} \boldsymbol{\chi}_i \neq \boldsymbol{\chi}_j \Rightarrow \boldsymbol{\varphi}[\boldsymbol{\psi}_1/\boldsymbol{\chi}_1, \dots, \boldsymbol{\psi}_n/\boldsymbol{\chi}_n] \in \mathrm{Fml}\,.$$

Vogliamo ora definire $\boldsymbol{\varphi}[\![\boldsymbol{t}_1/\boldsymbol{s}_1, \dots, \boldsymbol{t}_n/\boldsymbol{s}_n]\!]$, dove $\boldsymbol{\varphi} \in \mathrm{Fml}$ e $\boldsymbol{t}_1, \dots, \boldsymbol{t}_n, \boldsymbol{s}_1, \dots, \boldsymbol{s}_n \in \mathrm{Term}$ e $\boldsymbol{s}_1, \dots, \boldsymbol{s}_n$ sono distinti. Poiché $\boldsymbol{t}_1, \dots, \boldsymbol{t}_n, \boldsymbol{s}_1, \dots, \boldsymbol{s}_n$ non sono sottoespressioni di $\boldsymbol{\varphi}$, dobbiamo considerare la forma estesa $\boldsymbol{\varphi}^{\mathrm{e}}$ della formula. Tuttavia non è detto che $\boldsymbol{\varphi}^{\mathrm{e}}[\boldsymbol{t}_1/\boldsymbol{s}_1, \dots, \boldsymbol{t}_n/\boldsymbol{s}_n]$ sia la forma estesa di una qualche formula: per si incorre in problemi se qualcuna delle $\boldsymbol{s}_i$ è una variabile che ha occorrenze vincolate in $\boldsymbol{\varphi}$. Cominciamo col dare una definizione rigorosa della nozione di variante di una formula, vista nella Sezione 3.C.3.

Ricordiamo che $\langle \boldsymbol{v}_n \mid n \in \omega \rangle$ è la lista ufficiale delle variabili dei linguaggi del prim'ordine introdotta a pagina 434. Se $\boldsymbol{t} \in \mathrm{Term}$ e $\boldsymbol{\varphi} \in \mathrm{Fml}$ siano $\boldsymbol{i}(\boldsymbol{t})$ il più piccolo k tale che ogni variabile che occorre in $\boldsymbol{t}$ ha indice $< k$ e $\boldsymbol{i}(\boldsymbol{\varphi})$ il più piccolo k tale che ogni variabile che occorre libera in $\boldsymbol{\varphi}$ ha indice $< k$, cioè

$$\boldsymbol{i}(\boldsymbol{t}) = \max\{n \mid \textsc{Vbl}(\boldsymbol{t})\} + 1.$$
$$\boldsymbol{i}(\boldsymbol{\varphi}) = \max\{n \mid \boldsymbol{v}_n \in \mathrm{Fv}(\boldsymbol{\varphi})\} + 1.$$

Quando $n \ge \boldsymbol{i}(\boldsymbol{\varphi})$, la formula $\boldsymbol{\varphi}_{(n)}$ è ottenuta sostituendo in $\boldsymbol{\varphi}$ le variabili quantificate con variabili di indice $\ge n$. Formalmente è definita induttivamente così:

- se $\boldsymbol{\varphi}$ è atomica, allora $\boldsymbol{\varphi}_{(n)} = \boldsymbol{\varphi}$,
- se $\boldsymbol{\varphi} = \neg\boldsymbol{\psi}$, allora $\boldsymbol{\varphi}_{(n)} = \neg\boldsymbol{\psi}_{(n)}$,
- se $\boldsymbol{\varphi} = \boldsymbol{\psi} \odot \boldsymbol{\chi}$, con $\odot \in \{\wedge, \vee, \Rightarrow, \Leftrightarrow\}$ allora $\boldsymbol{\varphi}_{(n)} = \boldsymbol{\psi}_{(n)} \odot \boldsymbol{\chi}_{(n)}$,
- se $\boldsymbol{\varphi} = \exists \boldsymbol{v}_k \boldsymbol{\psi}$ con $k < n$, allora $\boldsymbol{\varphi}_{(n)} = \exists \boldsymbol{v}_k \boldsymbol{\chi}$, dove $\boldsymbol{\chi}$ è la formula la cui forma estesa è $\boldsymbol{\chi}^{\mathrm{e}} = \boldsymbol{\psi}_{(n)}[\boldsymbol{v}_i/\boldsymbol{v}_k]$ e $i = \boldsymbol{i}(\boldsymbol{\psi}_{(n)})$.

Diremo $\boldsymbol{\varphi}$ è una **variante** di $\boldsymbol{\psi}$ se $\boldsymbol{\varphi}_{(n)} = \boldsymbol{\psi}_{(n)}$ per qualche $n \geq \boldsymbol{i}(\boldsymbol{\varphi}), \boldsymbol{i}(\boldsymbol{\psi})$.

Esercizio 28.6. Verificare che

(i) $\boldsymbol{\varphi}_{(n)} \in \mathrm{Fml}$ e $\mathrm{Fv}(\boldsymbol{\varphi}_{(n)}) = \mathrm{Fv}(\boldsymbol{\varphi})$;

(ii) $\boldsymbol{\varphi}$ è una variante di $\boldsymbol{\psi}$ se $\boldsymbol{\varphi}_{(n)} = \boldsymbol{\psi}_{(n)}$ per ogni $n \geq \boldsymbol{i}(\boldsymbol{\varphi}), \boldsymbol{i}(\boldsymbol{\psi})$.

Definizione 28.7. Se $\boldsymbol{\varphi} \in \mathrm{Fml}$ e $\boldsymbol{t}_1, \dots, \boldsymbol{t}_n, \boldsymbol{s}_1, \dots, \boldsymbol{s}_n \in \mathrm{Term}$ e $\boldsymbol{s}_1, \dots, \boldsymbol{s}_n$ sono distinti, allora

$$\boldsymbol{\varphi}[\![\boldsymbol{t}_1/\boldsymbol{s}_1, \dots, \boldsymbol{t}_n/\boldsymbol{s}_n]\!] = \boldsymbol{\varphi}^{\mathrm{e}}_{(m)}[\boldsymbol{t}_1/\boldsymbol{s}_1, \dots, \boldsymbol{t}_n/\boldsymbol{s}_n]$$

dove $m \geq \max\{\boldsymbol{i}(\boldsymbol{\varphi}), \boldsymbol{i}(\boldsymbol{t}_1), \dots, \boldsymbol{i}(\boldsymbol{t}_n), \boldsymbol{i}(\boldsymbol{s}_1), \dots, \boldsymbol{i}(\boldsymbol{s}_n)\}$.

28.E. Linguaggi ricorsivi.

Esercizi

29. La relazione di soddisfazione

In questa sezione vedremo come definire rigorosamente la nozione "la formula $\boldsymbol{\varphi}$ è vera nella struttura $\mathcal{A}$".

29.A. Interpretazione di termini in strutture.

Definizione 29.1. Un'**assegnazione in una struttura** $\mathcal{A}$ è una funzione

$$g\colon \textsc{Vbl} \to \|\mathcal{A}\|\,.$$

A partire da un'assegnazione g, per ogni $a \in \|\mathcal{A}\|$ possiamo definire l'assegnazione $g_{\boldsymbol{x}\mapsto a}$

$$g_{\boldsymbol{x}\mapsto a}(\boldsymbol{v}_n) = \begin{cases} a & \text{se } \boldsymbol{x} = \boldsymbol{v}_n, \\ g(\boldsymbol{v}_n) & \text{altrimenti.} \end{cases}$$

Notare che

$$\boldsymbol{x} \neq \boldsymbol{y} \Rightarrow (g_{\boldsymbol{x}\mapsto a})_{\boldsymbol{y}\mapsto b} = (g_{\boldsymbol{y}\mapsto b})_{\boldsymbol{x}\mapsto a} \tag{29.1}$$

per ogni assegnazione $g\colon \textsc{Vbl} \to \|\mathcal{A}\|$ e ogni $a, b \in \|\mathcal{A}\|$.

L'**interpretazione di $\boldsymbol{t}$ in $\mathcal{A}$ mediante** g è definita ricorsivamente come

$$\boldsymbol{t}^{\mathcal{A}}[g] = \begin{cases} \boldsymbol{c}^{\mathcal{A}} & \text{se } \boldsymbol{t} = \boldsymbol{c}, \\ g(\boldsymbol{x}) & \text{se } \boldsymbol{t} = \boldsymbol{x}, \\ \boldsymbol{f}^{\mathcal{A}}(\boldsymbol{u}_1^{\mathcal{A}}[g], \dots, \boldsymbol{u}_n^{\mathcal{A}}[g]) & \text{se } \boldsymbol{t} = \boldsymbol{f}(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n). \end{cases}$$

Lemma 29.2. *Se $g, h\colon \textsc{Vbl} \to \|\mathcal{A}\|$ sono assegnazioni tali che $g \restriction \textsc{Vbl}(\boldsymbol{t}) = h \restriction \textsc{Vbl}(\boldsymbol{t})$, allora $\boldsymbol{t}^{\mathcal{A}}[g] = \boldsymbol{t}^{\mathcal{A}}[h]$.*

Dimostrazione. Per induzione su $\mathrm{ht}(\boldsymbol{t})$. Se $\boldsymbol{t} = \boldsymbol{c}$ con $\boldsymbol{c} \in \mathrm{Const}$ oppure $\boldsymbol{t} = \boldsymbol{x}$ con $\boldsymbol{x} \in \textsc{Vbl}$, il risultato è immediato. Supponiamo che $\boldsymbol{t} = \boldsymbol{f}(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)$. Allora $\textsc{Vbl}(\boldsymbol{t}) = \textsc{Vbl}(\boldsymbol{u}_1) \cup \dots \cup \textsc{Vbl}(\boldsymbol{u}_n)$ e quindi, per ipotesi induttiva, $\boldsymbol{u}_m^{\mathcal{A}}[g] = \boldsymbol{u}_m^{\mathcal{A}}[h]$, per $m = 1, \dots, n$, quindi

$$\boldsymbol{t}^{\mathcal{A}}[g] = \boldsymbol{f}^{\mathcal{A}}(\boldsymbol{u}_1^{\mathcal{A}}[g], \dots, \boldsymbol{u}_n^{\mathcal{A}}[g]) = \boldsymbol{f}^{\mathcal{A}}(\boldsymbol{u}_1^{\mathcal{A}}[h], \dots, \boldsymbol{u}_n^{\mathcal{A}}[h]) = \boldsymbol{t}^{\mathcal{A}}[h]. \qquad \square$$

In particolare: se $\boldsymbol{t}$ è chiuso allora possiamo definire $\boldsymbol{t}^{\mathcal{A}}$ l'interpretazione di $\boldsymbol{t}$ in $\mathcal{A}$ come $\boldsymbol{t}^{\mathcal{A}}[g]$ per una qualunque assegnazione g.

Esercizio 29.3. Se $\mathcal{A}'$ è un'espansione di $\mathcal{A}$ e $\mathcal{A} \subseteq \mathcal{B}$, dimostrare che

$$\boldsymbol{t}^{\mathcal{A}} = \boldsymbol{t}^{\mathcal{A}'} = \boldsymbol{t}^{\mathcal{B}}.$$

Se $\textsc{Vbl}(\boldsymbol{t}) \subseteq \{\boldsymbol{x}_1, \dots, \boldsymbol{x}_n\}$ e $a_1, \dots, a_n$ siano elementi di $\|\mathcal{A}\|$ non necessariamente distinti e g e h sono assegnazioni in $\mathcal{A}$ tali che $g(\boldsymbol{x}_m) = h(\boldsymbol{x}_m) = a_m$, per $1 \leq m \leq n$, allora, per il Lemma 29.2, $\boldsymbol{t}^{\mathcal{A}}[g] = \boldsymbol{t}^{\mathcal{A}}[h]$ e indicheremo quest'elemento con

$$\boldsymbol{t}^{\mathcal{A}}[a_1, \dots, a_n].$$

Un modo equivalente per definirlo è considerare l'espansione $\langle \mathcal{A}, a_1, \dots, a_n \rangle$ di $\mathcal{A}$ ottenuta aggiungendo ad L nuovi simboli di costante $\mathring{a}_1, \dots, \mathring{a}_n$ che devono essere interpretati come $a_1, \dots, a_n$ — si noti che gli $\mathring{a}_m$, a differenza degli a_m, *devono essere tutti distinti*. L'interpretazione in $\mathcal{A}'$ del termine chiuso

$$\boldsymbol{t}[\mathring{a}_1/\boldsymbol{x}_1, \dots, \mathring{a}_n/\boldsymbol{x}_n]$$

ottenuto sostituendo le costanti $\mathring{a}_1, \dots, \mathring{a}_n$ al posto delle variabili $\boldsymbol{x}_1, \dots, \boldsymbol{x}_n$ in $\boldsymbol{t}$, coincide con $\boldsymbol{t}^{\mathcal{A}}[a_1, \dots, a_n]$, cioè

$$(\boldsymbol{t}[\mathring{a}_1/\boldsymbol{x}_1, \dots, \mathring{a}_n/\boldsymbol{x}_n])^{\mathcal{A}'} = \boldsymbol{t}^{\mathcal{A}}[a_1, \dots, a_n].$$

Lemma 29.4. *Se $\boldsymbol{t}$ è un termine le cui variabili sono tra $\boldsymbol{x}_1, \dots, \boldsymbol{x}_n$ e se $\pi\colon \mathcal{A} \to \mathcal{B}$ è un morfismo, allora*

$$\forall a_1, \dots, a_n \in \|\mathcal{A}\| \; (\pi(\boldsymbol{t}^{\mathcal{A}}[a_1, \dots, a_n]) = \boldsymbol{t}^{\mathcal{B}}[\pi(a_1), \dots, \pi(a_n)]).$$

Dimostrazione. Per induzione su $\mathrm{ht}(\boldsymbol{t})$. Se $\mathrm{ht}(\boldsymbol{t}) = 0$, allora $\boldsymbol{t} = \boldsymbol{x}_m$ oppure $\boldsymbol{t} = \boldsymbol{c}_k$, quindi $\boldsymbol{t}^{\mathcal{A}}[\vec{a}] = a_m$ e $\boldsymbol{t}^{\mathcal{B}}[\pi(\vec{a})] = \pi(a_m)$ oppure $\boldsymbol{t}^{\mathcal{A}}[\vec{a}] = \boldsymbol{c}_k^{\mathcal{A}}$ e $\boldsymbol{t}^{\mathcal{B}}[\vec{a}] = \boldsymbol{c}_k^{\mathcal{B}}$. Se $\mathrm{ht}(\boldsymbol{t}) > 0$, allora $\boldsymbol{t} = \boldsymbol{f}_j(\boldsymbol{t}_1, \dots, \boldsymbol{t}_m)$ per qualche $j \in J$ e $\boldsymbol{t}_1, \dots, \boldsymbol{t}_m \in \mathrm{Term}$. Allora

$$\begin{aligned}
\pi(\boldsymbol{t}^{\mathcal{A}}[\vec{a}]) &= \pi(\boldsymbol{f}_j^{\mathcal{A}}(\boldsymbol{t}_1^{\mathcal{A}}[\vec{a}], \dots, \boldsymbol{t}_m^{\mathcal{A}}[\vec{a}])) \\
&= \boldsymbol{f}_j^{\mathcal{B}}(\pi(\boldsymbol{t}_1^{\mathcal{A}}[\vec{a}]), \dots, \pi(\boldsymbol{t}_m^{\mathcal{A}}[\vec{a}])) && \text{(per definizione di morfismo)} \\
&= \boldsymbol{f}_j^{\mathcal{B}}(\boldsymbol{t}_1^{\mathcal{B}}[\pi(\vec{a})], \dots, \boldsymbol{t}_m^{\mathcal{B}}[\pi(\vec{a})]) && \text{(per ipotesi induttiva)} \\
&= \boldsymbol{t}^{\mathcal{B}}[\pi(\vec{a})] && \text{(per definizione di sostituzione).}
\end{aligned}$$

□

29.B. La verità di una formula in una struttura. Definiamo quando una formula $\boldsymbol{\varphi}$ è **vera in** $\mathcal{A}$ **secondo un'assegnazione** g, in simboli

$$\mathcal{A} \vDash \boldsymbol{\varphi}[g].$$

L'espressione qui sopra si legge anche: $\mathcal{A}$ **soddisfa** $\boldsymbol{\varphi}$ **con l'assegnazione** g, ovvero $\mathcal{A}$ è un **modello di** $\boldsymbol{\varphi}$ **per l'assegnazione** g. Nel caso in cui ciò non valga, scriveremo $\mathcal{A} \nvDash \boldsymbol{\varphi}[g]$ e diremo che $\boldsymbol{\varphi}$ è **falsa in** $\mathcal{A}$ **per l'assegnazione** g. La definizione di $\mathcal{A} \vDash \boldsymbol{\varphi}[g]$ è per ricorsione sulla complessità di $\boldsymbol{\varphi}$:

- $\mathcal{A} \vDash (\boldsymbol{t}_1 \equiv \boldsymbol{t}_2)[g]$ se e solo se $\boldsymbol{t}_1^{\mathcal{A}}[g] = \boldsymbol{t}_2^{\mathcal{A}}[g]$;
- $\mathcal{A} \vDash (\boldsymbol{R}_i(\boldsymbol{t}_1, \dots, \boldsymbol{t}_m))[g]$ se e solo se $(\boldsymbol{t}_1^{\mathcal{A}}[g], \dots, \boldsymbol{t}_m^{\mathcal{A}}[g]) \in \boldsymbol{R}_i^{\mathcal{A}}$;
- $\mathcal{A} \vDash (\boldsymbol{\neg\varphi})[g]$ se e solo se $\mathcal{A} \nvDash \boldsymbol{\varphi}[g]$;
- $\mathcal{A} \vDash (\boldsymbol{\varphi \vee \psi})[g]$ se e solo se $\mathcal{A} \vDash \boldsymbol{\varphi}[g]$ o $\mathcal{A} \vDash \boldsymbol{\psi}[g]$;
- $\mathcal{A} \vDash (\boldsymbol{\exists x \varphi})[g]$ se e solo se c'è un $a \in \|\mathcal{A}\|$ tale che $\mathcal{A} \vDash \boldsymbol{\varphi}[g_{\boldsymbol{x} \mapsto a}]$.

Per evitare confusioni tra le formule di L (cioè particolari espressioni) e le formule (del linguaggio della teoria degli insiemi) che descrivono la relazione di soddisfazione, abbiamo usato le espressioni "se e solo se", "o", "c'è un $a \in \|\mathcal{A}\|$ tale che" invece dei connettivi $\Leftrightarrow$, $\vee$ e del quantificatore $\exists$. La versione formalizzata della definizione qui sopra diventa

$$\begin{aligned}
\mathcal{A} \vDash (\boldsymbol{t}_1 \equiv \boldsymbol{t}_2)[g] &\Leftrightarrow \boldsymbol{t}_1^{\mathcal{A}}[g] = \boldsymbol{t}_2^{\mathcal{A}}[g] \\
\mathcal{A} \vDash (\boldsymbol{R}_i(\boldsymbol{t}_1, \dots, \boldsymbol{t}_m))[g] &\Leftrightarrow (\boldsymbol{t}_1^{\mathcal{A}}[g], \dots, \boldsymbol{t}_m^{\mathcal{A}}[g]) \in \boldsymbol{R}_i^{\mathcal{A}} \\
\mathcal{A} \vDash (\boldsymbol{\neg\varphi})[g] &\Leftrightarrow \neg\,(\mathcal{A} \vDash \boldsymbol{\varphi}[g]) \\
\mathcal{A} \vDash (\boldsymbol{\varphi \vee \psi})[g] &\Leftrightarrow \mathcal{A} \vDash \boldsymbol{\varphi}[g] \vee \mathcal{A} \vDash \boldsymbol{\psi}[g] \\
\mathcal{A} \vDash (\boldsymbol{\exists x \varphi})[g] &\Leftrightarrow \exists a \in \|\mathcal{A}\|\,(\mathcal{A} \vDash \boldsymbol{\varphi}[g_{\boldsymbol{x} \mapsto a}])\,.
\end{aligned}$$

Esercizio 29.5. Dimostrare che:

(i) $\mathcal{A} \vDash (\boldsymbol{\varphi \wedge \psi})[g] \Leftrightarrow (\mathcal{A} \vDash \boldsymbol{\varphi}[g] \wedge \mathcal{A} \vDash \boldsymbol{\psi}[g])$;

(ii) $\mathcal{A} \vDash (\boldsymbol{\forall x \varphi})[g] \Leftrightarrow \forall a \in \|\mathcal{A}\|\ (\mathcal{A} \vDash \boldsymbol{\varphi}[g_{\boldsymbol{x} \mapsto a}])$;

(iii) $\mathcal{A} \vDash \neg\neg\boldsymbol{\varphi}[g] \Leftrightarrow \mathcal{A} \vDash \boldsymbol{\varphi}[g]$;
(iv) $\mathcal{A} \vDash (\boldsymbol{\varphi} \vee \boldsymbol{\psi})[g] \Leftrightarrow \mathcal{A} \vDash \neg\,(\neg\boldsymbol{\varphi} \wedge \neg\boldsymbol{\psi})\,[g]$;
(v) $\mathcal{A} \vDash (\boldsymbol{\varphi} \Rightarrow \boldsymbol{\psi})[g] \Leftrightarrow (\mathcal{A} \vDash \boldsymbol{\varphi}[g] \Rightarrow \mathcal{A} \vDash \boldsymbol{\psi}[g])$;
(vi) $\mathcal{A} \vDash (\boldsymbol{\varphi} \Leftrightarrow \boldsymbol{\psi})\,[g] \Leftrightarrow (\mathcal{A} \vDash \boldsymbol{\varphi}[g] \Leftrightarrow \mathcal{A} \vDash \boldsymbol{\psi}[g])$.

Definizione 29.6. Una formula $\boldsymbol{\varphi}$ si dice

- **soddisfacibile in una struttura** $\mathcal{A}$ se $\mathcal{A} \vDash \boldsymbol{\varphi}[g]$ per una qualche assegnazione g;
- **soddisfacibile** se è soddisfacibile in *qualche* struttura;
- **vera in una struttura** $\mathcal{A}$ se $\mathcal{A} \vDash \boldsymbol{\varphi}[g]$ per *ogni* valutazione g. In questo caso scriveremo che $\mathcal{A} \vDash \boldsymbol{\varphi}$,
- **valida** o **logicamente vera** se è vera in ogni struttura.

Una formula che non è soddisfacibile si dice **insoddisfacibile** o **logicamente falsa**. Quindi $\boldsymbol{\varphi}$ è insoddisfacibile se e solo se $\neg\boldsymbol{\varphi}$ è valida.

Lemma 29.7. *Se* $\boldsymbol{\varphi}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)$ *è una L-formula e* $g, h\colon \textsc{Vbl} \to \|\mathcal{A}\|$ *sono assegnazioni tali che* $g \restriction \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\} = h \restriction \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\}$,

$$\mathcal{A} \vDash \boldsymbol{\varphi}[g] \Leftrightarrow \mathcal{A} \vDash \boldsymbol{\varphi}[h].$$

Dimostrazione. Per induzione su $\mathrm{ht}(\boldsymbol{\varphi})$. Il caso di $\boldsymbol{\varphi}$ atomica discende direttamente dal Lemma 29.2. Se $\boldsymbol{\varphi} = \neg\boldsymbol{\psi}$ oppure $\boldsymbol{\varphi} = \boldsymbol{\psi} \vee \boldsymbol{\chi}$, il risultato è banale. Supponiamo quindi $\boldsymbol{\varphi}$ sia della forma $\exists \boldsymbol{y}\, \boldsymbol{\psi}$. Se $\mathcal{A} \vDash \exists \boldsymbol{y}\, \boldsymbol{\psi}[g]$, allora c'è un $a \in \|\mathcal{A}\|$ tale che $\mathcal{A} \vDash \boldsymbol{\psi}[g_{\boldsymbol{y}\mapsto a}]$. Per ipotesi induttiva $\mathcal{A} \vDash \boldsymbol{\psi}[g_{\boldsymbol{y}\mapsto a}] \Leftrightarrow \mathcal{A} \vDash \boldsymbol{\psi}[h_{\boldsymbol{y}\mapsto a}]$ e quindi $\mathcal{A} \vDash \exists \boldsymbol{y}\, \boldsymbol{\psi}[h]$. □

Quindi per ogni formula $\boldsymbol{\varphi}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)$ ed elementi non necessariamente distinti $a_1, \ldots, a_n \in \|\mathcal{A}\|$

$$\mathcal{A} \vDash \boldsymbol{\varphi}[a_1, \ldots, a_n]$$

se e solo se $\mathcal{A} \vDash \boldsymbol{\varphi}[g]$ per qualche (equivalentemente: per ogni) assegnazione g tale che $g(\boldsymbol{x}_m) = a_m$, $(1 \leq m \leq n)$. In particolare, se $\boldsymbol{\varphi}$ ha una variabile libera $\boldsymbol{x}$ scriveremo

$$\mathcal{A} \vDash \boldsymbol{\varphi}[a]$$

per qualche (equivalentemente: per ogni) assegnazione g tale che $g(\boldsymbol{x}) = a$. Se σ è un enunciato, allora le assegnazioni diventano irrilevanti, per cui poniamo

$$\mathcal{A} \vDash \boldsymbol{\sigma}$$

se vale $\mathcal{A} \vDash \boldsymbol{\sigma}[g]$ per una (equivalentemente: per tutte) le assegnazioni.

Esercizio 29.8. Sia $L' \subseteq L$ e $\boldsymbol{\varphi} \in \mathrm{Fml}(L')$. Verificare per induzione su $\mathrm{ht}(\boldsymbol{\varphi})$ che per ogni $\mathcal{A} \in \mathrm{Str}(L)$ e ogni $g\colon \textsc{Vbl} \to \|\mathcal{A}\|$,

$$\mathcal{A} \vDash \boldsymbol{\varphi}[g] \Leftrightarrow (\mathcal{A} \restriction L') \vDash \boldsymbol{\varphi}[g].$$

Proposizione 29.9. *Sia* $\boldsymbol{\varphi}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)$ *una L-formula,* $\mathcal{A}$ *una L-struttura e* $a_1, \ldots, a_n \in \|\mathcal{A}\|$.

(a) *Se* $\boldsymbol{y} \notin \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\}$, *allora*

$$\begin{aligned}\mathcal{A} \vDash \exists \boldsymbol{y}\boldsymbol{\varphi}[a_1, \ldots, a_n] &\Leftrightarrow \mathcal{A} \vDash \forall \boldsymbol{y}\boldsymbol{\varphi}[a_1, \ldots, a_n] \\ &\Leftrightarrow \mathcal{A} \vDash \boldsymbol{\varphi}[a_1, \ldots, a_n].\end{aligned}$$

(b) *Se* $\boldsymbol{y} = \boldsymbol{x}_m$ *per qualche* $1 \leq m \leq n$, *allora*

$$\begin{aligned}&\mathcal{A} \vDash (\exists \boldsymbol{x}_m \boldsymbol{\varphi})[a_1, \ldots, a_n] \\ &\qquad \Leftrightarrow \exists a \in \|\mathcal{A}\| \, (\mathcal{A} \vDash \boldsymbol{\varphi}[a_1, \ldots, a_{m-1}, a, a_{m+1}, \ldots, a_n]) \,, \\ &\mathcal{A} \vDash (\forall \boldsymbol{x}_m \boldsymbol{\varphi})[a_1, \ldots, a_n] \\ &\qquad \Leftrightarrow \forall a \in \|\mathcal{A}\| \, (\mathcal{A} \vDash \boldsymbol{\varphi}[a_1, \ldots, a_{m-1}, a, a_{m+1}, \ldots, a_n]) \,.\end{aligned}$$

Dimostrazione. (a) Supponiamo che $\mathcal{A} \vDash \exists \boldsymbol{y}\boldsymbol{\varphi}[a_1, \ldots, a_n]$, vale a dire che $\mathcal{A} \vDash \exists \boldsymbol{y}\boldsymbol{\varphi}[g]$ per una (equivalentemente: per ogni) assegnazione g tale che $g(\boldsymbol{x}_m) = a_m$ $(1 \leq m \leq n)$. Allora $\mathcal{A} \vDash \boldsymbol{\varphi}[g_{\boldsymbol{y} \mapsto a}]$ per qualche $a \in \|\mathcal{A}\|$. Per l'ipotesi su $\boldsymbol{y}$, $g_{\boldsymbol{y} \mapsto a}(\boldsymbol{x}_i) = a_i$ e quindi $\mathcal{A} \vDash \boldsymbol{\varphi}[a_1, \ldots, a_n]$. L'implicazione $(\mathcal{A} \vDash \boldsymbol{\varphi}[a_1, \ldots, a_n]) \Rightarrow (\mathcal{A} \vDash \exists \boldsymbol{y}\boldsymbol{\varphi}[a_1, \ldots, a_n])$ è analoga, quindi

$$\mathcal{A} \vDash \boldsymbol{\varphi}[a_1, \ldots, a_n] \Leftrightarrow \mathcal{A} \vDash \exists \boldsymbol{y}\boldsymbol{\varphi}[a_1, \ldots, a_n]. \tag{29.2}$$

Dato che le variabili libere di $\neg\boldsymbol{\varphi}$ sono esattamente le stesse di $\boldsymbol{\varphi}$, abbiamo che

$$\begin{aligned}\mathcal{A} \vDash \forall \boldsymbol{y}\boldsymbol{\varphi}[a_1, \ldots, a_n] &\Leftrightarrow \mathcal{A} \nvDash \exists \boldsymbol{y} \neg \boldsymbol{\varphi}[a_1, \ldots, a_n] \\ &\Leftrightarrow \mathcal{A} \nvDash \neg \boldsymbol{\varphi}[a_1, \ldots, a_n] \\ &\Leftrightarrow \mathcal{A} \vDash \boldsymbol{\varphi}[a_1, \ldots, a_n],\end{aligned}$$

dove nella seconda riga abbiamo usato l'equivalenza (29.2) per $\neg\boldsymbol{\varphi}$.

La parte (b) è lasciata al lettore. □

Esercizio 29.10. Generalizzare la Proposizione 29.9 al caso di formule con più quantificatori dello stesso tipo (per esempio $\exists \boldsymbol{y}_1 \exists \boldsymbol{y}_2 \ldots \exists \boldsymbol{y}_m \boldsymbol{\varphi}$, oppure $\forall \boldsymbol{y}_1 \forall \boldsymbol{y}_2 \ldots \forall \boldsymbol{y}_m \boldsymbol{\varphi}$).

Diamo ora la definizione formale di una nozione introdotta nel Capitolo I a pagina 31:

Definizione 29.11. La **chiusura universale** di una formula $\boldsymbol{\varphi}$ è l'enunciato $\forall \boldsymbol{v}_{k_1} \ldots \forall \boldsymbol{v}_{k_n} \boldsymbol{\varphi}$ dove $\{\boldsymbol{v}_{k_1}, \ldots, \boldsymbol{v}_{k_n}\}$ sono le variabili libere di $\boldsymbol{\varphi}$, dove $\langle \boldsymbol{v}_n \mid n \in \omega \rangle$ è la lista ufficiale delle variabili introdotte a pagina 434.

Diremo che una struttura $\mathcal{A}$ soddisfa una formula (con eventualmente variabili libere) $\boldsymbol{\varphi}$ se e solo se soddisfa la sua chiusura universale $\boldsymbol{\varphi}^{\forall}$,

$$\mathcal{A} \vDash \boldsymbol{\varphi} \text{ se e solo se } \mathcal{A} \vDash \boldsymbol{\varphi}^{\forall}.$$

Proposizione 29.12. *Se* $\mathrm{Subst}(\boldsymbol{\varphi}, \vec{\boldsymbol{x}}, \vec{\boldsymbol{t}})$ *e* $a = \boldsymbol{t}^{\mathcal{A}}[g] \in \|\mathcal{A}\|$ *dove* g *è un'assegnazione in una* L*-struttura* $\mathcal{A}$*, allora*

$$\mathcal{A} \vDash \boldsymbol{\varphi}[\![\boldsymbol{t}/\boldsymbol{x}]\!][g] \quad \Leftrightarrow \quad \mathcal{A} \vDash \boldsymbol{\varphi}[g_{\boldsymbol{x}\mapsto a}].$$

Dimostrazione. Se $\boldsymbol{\varphi}$ è atomica, o $\boldsymbol{\varphi}$ è $\boldsymbol{\neg\psi}$, oppure $\boldsymbol{\varphi}$ è $\boldsymbol{\psi \vee \chi}$, il risultato è banale. Supponiamo $\boldsymbol{\varphi}$ sia $\boldsymbol{\exists y \psi}$ e distinguiamo due casi.

Caso 1: $\boldsymbol{y = x}$. Allora $\boldsymbol{x}$ non occorre libera in $\boldsymbol{\varphi}$ e quindi $\boldsymbol{\varphi}[\boldsymbol{t}/\boldsymbol{x}]$ è $\boldsymbol{\varphi}$ e g e $g_{\boldsymbol{x}\mapsto a}$ coincidono sulle variabili libere di $\boldsymbol{\varphi}$. Segue che

$$\begin{aligned} \mathcal{A} \vDash \boldsymbol{\varphi}[\![\boldsymbol{t}/\boldsymbol{x}]\!][g] &\Leftrightarrow \mathcal{A} \vDash \boldsymbol{\varphi}[g] \\ &\Leftrightarrow \mathcal{A} \vDash \boldsymbol{\varphi}[g_{\boldsymbol{x}\mapsto a}] \qquad \text{(per il Lemma 29.7).} \end{aligned}$$

Caso 2: $\boldsymbol{y \neq x}$. Allora $\boldsymbol{\varphi}[\![\boldsymbol{t}/\boldsymbol{x}]\!]$ è $\boldsymbol{\exists y \psi}[\![\boldsymbol{t}/\boldsymbol{x}]\!]$ e dato che $\boldsymbol{y}$ non occorre in $\boldsymbol{t}$, per ogni $b \in A$ si ha

$$a = \boldsymbol{t}^{\mathcal{A}}[g] = \boldsymbol{t}^{\mathcal{A}}[g_{\boldsymbol{y}\mapsto b}]. \tag{29.3}$$

Quindi

$$\begin{aligned} \mathcal{A} \vDash \boldsymbol{\varphi}[\![\boldsymbol{t}/\boldsymbol{x}]\!][g] &\Leftrightarrow \exists b \in A\ \mathcal{A} \vDash \boldsymbol{\psi}[\![\boldsymbol{t}/\boldsymbol{x}]\!][g_{\boldsymbol{y}\mapsto b}] \\ &\Leftrightarrow \exists b \in A\ \mathcal{A} \vDash \boldsymbol{\psi}[(g_{\boldsymbol{y}\mapsto b})_{\boldsymbol{x}\mapsto a}] \quad \text{(per ipo. ind. e per (29.3))} \\ &\Leftrightarrow \exists b \in A\ \mathcal{A} \vDash \boldsymbol{\psi}[(g_{\boldsymbol{x}\mapsto a})_{\boldsymbol{y}\mapsto b}] \quad \text{(per (29.1))} \\ &\Leftrightarrow \mathcal{A} \vDash \boldsymbol{\exists y \psi}[g_{\boldsymbol{x}\mapsto a}] \\ &\Leftrightarrow \mathcal{A} \vDash \boldsymbol{\varphi}[g_{\boldsymbol{x}\mapsto a}]. \qquad \square \end{aligned}$$

Teorema 29.13. *Sia* $\mathcal{A}$ *una* L*-struttura. Supponiamo che* $\boldsymbol{\varphi \Rightarrow \psi}$ *sia vera in* $\mathcal{A}$ *e che* $\boldsymbol{x}$ *non occorra libera in* $\boldsymbol{\psi}$*. Allora* $\boldsymbol{\exists x \varphi \Rightarrow \psi}$ *è vera in* $\mathcal{A}$*.*

Dimostrazione. Supponiamo, per assurdo, che $\mathcal{A} \nvDash (\boldsymbol{\exists x \varphi \Rightarrow \psi})[g]$ per qualche assegnazione g. Allora $\mathcal{A} \vDash \boldsymbol{\exists x \varphi}[g]$ e $\mathcal{A} \nvDash \boldsymbol{\psi}[g]$. Sia $a \in \|\mathcal{A}\|$ tale che $\mathcal{A} \vDash \boldsymbol{\varphi}[g_{\boldsymbol{x}\mapsto a}]$. Poiché $\boldsymbol{x}$ non occorre libera in $\boldsymbol{\psi}$, allora $\mathcal{A} \nvDash \boldsymbol{\psi}[g_{\boldsymbol{x}\mapsto a}]$ per il Lemma 29.7, e dato che $\mathcal{A} \vDash (\boldsymbol{\varphi \Rightarrow \psi})[g_{\boldsymbol{x}\mapsto a}]$ per ipotesi, allora $\mathcal{A} \nvDash \boldsymbol{\varphi}[g_{\boldsymbol{x}\mapsto a}]$: assurdo. $\square$

Il risultato precedente è noto come la

Regola del quantificatore esistenziale. Se $\boldsymbol{x}$ non occorre libera in $\boldsymbol{\psi}$, allora da $\boldsymbol{\varphi \Rightarrow \psi}$ possiamo inferire $\boldsymbol{\exists x \varphi \Rightarrow \psi}$, in simboli

$$\frac{\boldsymbol{\varphi \Rightarrow \psi},\ \boldsymbol{x} \notin \mathrm{VBL}(\boldsymbol{\psi})}{\boldsymbol{\exists x \varphi \Rightarrow \psi}}$$

29.C. Esempi di formule valide.

29.C.1. *Tautologie.* Ricordiamo dalla Sezione 3.C.1 che una formula si dice **primitiva** se è atomica oppure della forma $\exists \boldsymbol{x}\boldsymbol{\psi}$. Ad ogni $\boldsymbol{\varphi}$ possiamo associare un insieme $\mathcal{P}(\boldsymbol{\varphi})$ di formule primitive come segue:

- se $\boldsymbol{\varphi}$ è primitiva, allora $\mathcal{P}(\boldsymbol{\varphi}) = \{\boldsymbol{\varphi}\}$,
- se $\boldsymbol{\varphi} = \neg\boldsymbol{\psi}$, allora $\mathcal{P}(\boldsymbol{\varphi}) = \mathcal{P}(\boldsymbol{\psi})$,
- se $\boldsymbol{\varphi} = \boldsymbol{\psi} \vee \boldsymbol{\chi}$, allora $\mathcal{P}(\boldsymbol{\varphi}) = \mathcal{P}(\boldsymbol{\psi}) \cup \mathcal{P}(\boldsymbol{\chi})$.

Ad ogni $\boldsymbol{\varphi} \in \mathrm{Fml}(L)$ possiamo associare una proposizione $\boldsymbol{p}_{\boldsymbol{\varphi}}$ del calcolo proposizionale sulle lettere $\{\boldsymbol{\psi}_1, \dots, \boldsymbol{\psi}_n\} = \mathcal{P}(\boldsymbol{\varphi})$:

$$\boldsymbol{p}_{\boldsymbol{\varphi}} = \begin{cases} \boldsymbol{\varphi} & \text{se } \boldsymbol{\varphi} \text{ è primitiva,} \\ \neg \boldsymbol{p}_{\boldsymbol{\psi}} & \text{se } \boldsymbol{\varphi} = \neg\boldsymbol{\psi}, \\ \boldsymbol{p}_{\boldsymbol{\psi}} \vee \boldsymbol{p}_{\boldsymbol{\chi}} & \text{se } \boldsymbol{\varphi} = \boldsymbol{\psi} \vee \boldsymbol{\chi}. \end{cases}$$

Lemma 29.14. *Siano $\boldsymbol{\varphi}$, $\boldsymbol{p}_{\boldsymbol{\varphi}}$ e $\boldsymbol{\psi}_1, \dots, \boldsymbol{\psi}_n$ come sopra. Sia $\mathcal{A}$ una L-struttura e g un'assegnazione. Sia v la valutazione definita da*

$$v(\boldsymbol{\psi}_i) = 1 \Leftrightarrow \mathcal{A} \vDash \boldsymbol{\psi}_i[g].$$

Allora

$$v(\boldsymbol{p}_{\boldsymbol{\varphi}}) = 1 \Leftrightarrow \mathcal{A} \vDash \boldsymbol{\varphi}[g].$$

Dimostrazione. Per induzione sull'altezza della proposizione $\boldsymbol{p}_{\boldsymbol{\varphi}}$. Se $\mathrm{ht}(\boldsymbol{p}_{\boldsymbol{\varphi}}) = 0$ allora $\boldsymbol{\varphi}$ è primitiva e il risultato segue immediatamente. Se $\mathrm{ht}(\boldsymbol{p}_{\boldsymbol{\varphi}}) > 0$ allora $\boldsymbol{\varphi} = \neg\boldsymbol{\psi}$ oppure $\boldsymbol{\varphi} = \boldsymbol{\psi} \vee \boldsymbol{\chi}$, cioè $\boldsymbol{p}_{\boldsymbol{\varphi}} = \neg\boldsymbol{p}_{\boldsymbol{\psi}}$ oppure $\boldsymbol{p}_{\boldsymbol{\varphi}} = \boldsymbol{p}_{\boldsymbol{\psi}} \vee \boldsymbol{p}_{\boldsymbol{\chi}}$ e il risultato segue dalla definizione di $\vDash$. □

Diremo che una formula $\boldsymbol{\varphi} \in \mathrm{Fml}(L)$ è una **tautologia** se e solo se la formula proposizionale $\boldsymbol{p}_{\boldsymbol{\varphi}}$ è una tautologia proposizionale (Definizione 23.37).

Corollario 29.15. *Se $\boldsymbol{\varphi} \in \mathrm{Fml}(L)$ è una tautologia, allora $\boldsymbol{\varphi}$ è logicamente valida.*

29.C.2. *Assiomi di sostituzione.* Un **assioma di sostituzione** è una formula della forma

$$\boldsymbol{\varphi}[\![\boldsymbol{t}_1/\boldsymbol{x}_1, \dots, \boldsymbol{t}_n/\boldsymbol{x}_n]\!] \Rightarrow \exists \boldsymbol{x}_1 \dots \exists \boldsymbol{x}_n \boldsymbol{\varphi}.$$

Verifichiamo che gli assiomi di sostituzione sono validi. Fissiamo una struttura $\mathcal{A}$ ed un'assegnazione $g\colon \mathrm{Vbl} \to \|\mathcal{A}\|$ tale che

$$\mathcal{A} \vDash \boldsymbol{\varphi}[\![\boldsymbol{t}_1/\boldsymbol{x}_1, \dots, \boldsymbol{t}_n/\boldsymbol{x}_n]\!][g].$$

Applicando ripetutamente la Proposizione 29.12 si ha che $\mathcal{A} \vDash \boldsymbol{\varphi}[g']$ dove

$$g'(\boldsymbol{y}) = \begin{cases} \boldsymbol{y} & \text{se } \boldsymbol{y} \notin \{\boldsymbol{x}_1, \dots, \boldsymbol{x}_n\} \\ \boldsymbol{t}_i^{\mathcal{A}}[g] & \text{se } \boldsymbol{y} = \boldsymbol{x}_i. \end{cases}$$

e quindi $\mathcal{A} \vDash \exists \boldsymbol{x}_1 \ldots \exists \boldsymbol{x}_n \boldsymbol{\varphi}[g]$. Abbiamo quindi dimostrato che

$$\mathcal{A} \vDash (\boldsymbol{\varphi}[\![\boldsymbol{t}_1/\boldsymbol{x}_1, \ldots, \boldsymbol{t}_n/\boldsymbol{x}_n]\!] \Rightarrow \exists \boldsymbol{x}_1 \ldots \exists \boldsymbol{x}_n \boldsymbol{\varphi})[g]$$

per ogni struttura $\mathcal{A}$ e ogni assegnazione g.

29.C.3. *Assiomi dell'uguaglianza.* Un **assioma di uguaglianza** è una formula della forma

- $\boldsymbol{t} \equiv \boldsymbol{t}$,
- $\boldsymbol{s} \equiv \boldsymbol{t} \Rightarrow \boldsymbol{t} \equiv \boldsymbol{s}$,
- $\boldsymbol{s} \equiv \boldsymbol{t} \wedge \boldsymbol{t} \equiv \boldsymbol{u} \Rightarrow \boldsymbol{s} \equiv \boldsymbol{u}$,
- $\boldsymbol{s}_1 \equiv \boldsymbol{t}_1 \wedge \ldots \wedge \boldsymbol{s}_n \equiv \boldsymbol{t}_n \Rightarrow \boldsymbol{f}_j(\boldsymbol{s}_1, \ldots, \boldsymbol{s}_n) \equiv \boldsymbol{f}_j(\boldsymbol{t}_1, \ldots, \boldsymbol{t}_n)$,
- $\boldsymbol{s}_1 \equiv \boldsymbol{t}_1 \wedge \ldots \wedge \boldsymbol{s}_n \equiv \boldsymbol{t}_n \wedge \boldsymbol{R}_i(\boldsymbol{s}_1, \ldots, \boldsymbol{s}_n) \Rightarrow \boldsymbol{R}_i(\boldsymbol{t}_1, \ldots, \boldsymbol{t}_n)$.

È immediato verificare che gli assiomi di uguaglianza sono validi.

29.C.4. *Qualche esempio non banale.*

- La formula $\exists \boldsymbol{x}\,(\boldsymbol{\varphi} \Rightarrow \forall \boldsymbol{x} \boldsymbol{\varphi})$ è logicamente valida.

  Infatti, per ogni struttura $\mathcal{A}$ e assegnazione g, se $\mathcal{A} \nvDash \forall \boldsymbol{x} \boldsymbol{\varphi}[g]$, allora c'è un $a \in \|\mathcal{A}\|$ tale che $\mathcal{A} \nvDash \boldsymbol{\varphi}[g_{\boldsymbol{x} \mapsto a}]$, cioè $\mathcal{A} \vDash (\boldsymbol{\varphi} \Rightarrow \forall \boldsymbol{x} \boldsymbol{\varphi})\,[g_{\boldsymbol{x} \mapsto a}]$ in quanto l'antecedente nell'implicazione è falsa, e quindi $\mathcal{A} \vDash \exists \boldsymbol{x}\,(\boldsymbol{\varphi} \Rightarrow \forall \boldsymbol{x} \boldsymbol{\varphi})\,[g]$.

  Viceversa, se $\mathcal{A} \vDash \forall \boldsymbol{x} \boldsymbol{\varphi}[g]$, allora $\mathcal{A} \vDash \boldsymbol{\varphi}[g]$ e quindi $\mathcal{A} \vDash (\boldsymbol{\varphi} \Rightarrow \forall \boldsymbol{x} \boldsymbol{\varphi})\,[g]$, da cui $\mathcal{A} \vDash \exists \boldsymbol{x}\,(\boldsymbol{\varphi} \Rightarrow \forall \boldsymbol{x} \boldsymbol{\varphi})\,[g]$.
- L'enunciato del linguaggio che ha soltanto un simbolo di operazione binaria $*$ (cioè il linguaggio dei semigruppi)

  $$\forall \boldsymbol{x} \forall \boldsymbol{y} \forall \boldsymbol{z}\,((\boldsymbol{x} * \boldsymbol{y}) * \boldsymbol{z} \equiv \boldsymbol{y}) \Rightarrow \forall \boldsymbol{x} \forall \boldsymbol{y}\,(\boldsymbol{x} \equiv \boldsymbol{y})$$

  è valido. Infatti come mostrato nell'Esempio 5.12 a pagina 89, una qualsiasi struttura algebrica $\langle A, \cdot \rangle$ che soddisfi $\forall \boldsymbol{x} \forall \boldsymbol{y} \forall \boldsymbol{z}\,((\boldsymbol{x} * \boldsymbol{y}) * \boldsymbol{z} \equiv \boldsymbol{y})$ ha un solo elemento.

29.D. Definibilità. Richiamiamo qualche nozione introdotta informalmente nella Sezione 3.F.5.

Definizione 29.16. Sia $\mathcal{A} \in \mathrm{Str}(L)$, $P \subseteq A = \|\mathcal{A}\|$ e $n \geq 1$.

- Un insieme $X \subseteq A^n$ è definibile con parametri in P mediante una formula $\boldsymbol{\varphi}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n, \boldsymbol{y}_1, \ldots, \boldsymbol{y}_k)$ se esistono $p_1, \ldots, p_k \in P$ per cui

  $X = \{\langle a_1, \ldots, a_n \rangle \in A^n \mid \mathcal{A} \vDash \boldsymbol{\varphi}[a_1, \ldots, a_n, p_1, \ldots, p_k]\}$

  $= \{\langle a_1, \ldots, a_n \rangle \in A^n \mid \langle a_1, \ldots, a_n, p_1, \ldots, p_k \rangle \in \mathbf{T}^{\mathcal{A}}_{\boldsymbol{\varphi}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n, \boldsymbol{y}_1, \ldots, \boldsymbol{y}_k)}\}$.

  L'intero n si dice dimensione di X.
- Quando $P = A$ diremo che X è definibile con parametri in $\mathcal{A}$. Se $P = \emptyset$ o equivalentemente $k = 0$ e quindi la formula è della forma $\boldsymbol{\varphi}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)$ e

  $$X = \{\langle a_1, \ldots, a_n \rangle \in A^n \mid \mathcal{A} \vDash \boldsymbol{\varphi}[a_1, \ldots, a_n]\}\,,$$

diremo che X è definibile senza parametri.

- $\mathrm{Def}^n_{\mathcal{A}}(P) = \{X \subseteq A^n \mid X \text{ è definibile con parametri in } P\}$.

Lemma 29.17. (a) *Se* $X \in \mathrm{Def}^n_{\mathcal{A}}(\{q_1, \ldots, q_m\} \cup P')$ *e* $\{q_1\}, \ldots, \{q_m\} \in \mathrm{Def}^1_{\mathcal{A}}(P)$ *allora* $X \in \mathrm{Def}^n_{\mathcal{A}}(P \cup P')$.

(b) *Supponiamo* $R \in \mathrm{Def}^m_{\mathcal{A}}(P)$ *e* $X \in \mathrm{Def}^n_{\langle \mathcal{A}, R\rangle}(Q)$, *dove* $\langle \mathcal{A}, R\rangle$ *è l'espansione di* $\mathcal{A}$ *ottenuta aggiungendo la relazione* R. *Allora* $X \in \mathrm{Def}^n_{\mathcal{A}}(P \cup Q)$.

Dimostrazione. (a) Per semplicità notazionale consideriamo il caso in cui $m = 1$. Sia $\boldsymbol{\varphi}(\boldsymbol{y}, \boldsymbol{z}_1, \ldots, \boldsymbol{z}_k)$ una formula che definisce q_1 con parametri $p_1, \ldots, p_k \in P$ e sia $\boldsymbol{\psi}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n, \boldsymbol{y}, \boldsymbol{w}_1, \ldots, \boldsymbol{w}_h)$ una formula che definisce X con parametri q_1 e $p'_1, \ldots, p'_h \in P'$. Allora la formula

$$\boldsymbol{\exists y}\, (\boldsymbol{\varphi}(\boldsymbol{y}, \boldsymbol{z}_1, \ldots, \boldsymbol{z}_k) \boldsymbol{\wedge} \boldsymbol{\psi}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n, \boldsymbol{y}, \boldsymbol{w}_1, \ldots, \boldsymbol{w}_h))$$

definisce X in $\mathcal{A}$ con parametri in $\{p_1, \ldots, p_k\} \cup \{p'_1, \ldots, p'_h\} \subseteq P \cup P'$.

(b) Per semplicità notazionale supponiamo R 1-aria e X n-aria. Sia $\boldsymbol{\varphi}(\boldsymbol{x}, p_1, \ldots, p_k)$ una L-formula che definisce R e sia $\tilde{\boldsymbol{\psi}}(\boldsymbol{y}_1, \ldots, \boldsymbol{y}_n, p'_1, \ldots, p'_h)$ una $L \cup \{\mathring{R}\}$-formula che definisce X in $\langle \mathcal{A}, R\rangle$. La L-formula

$$\boldsymbol{\psi}(\boldsymbol{y}_1, \ldots, \boldsymbol{y}_n, p_1, \ldots, p_k, p'_1, \ldots, p'_h)$$

ottenuta da $\tilde{\boldsymbol{\psi}}$ rimpiazzando tutte le occorrenze della forma "$\mathring{R}(\boldsymbol{x})$" con "$\boldsymbol{\varphi}(\boldsymbol{x}, p_1, \ldots, p_k)$" (per ogni scelta di variabile $\boldsymbol{x}$) definisce X in $\mathcal{A}$ con parametri $p_1, \ldots, p_k, p'_1, \ldots, p'_h \in P$,come richiesto. □

Per l'Esercizio 30.7, se $X \subseteq A^n$ è definito da $\boldsymbol{\varphi}$ e parametri $p_1, \ldots, p_m$, allora l'immagine di X via $\pi \in \mathrm{Aut}(\mathcal{A})$

$$\pi[X] = \{\pi(\vec{a}) \mid \vec{a} \in X\}$$

è definito da $\boldsymbol{\varphi}$ e parametri $\pi(p_1), \ldots, \pi(p_m)$. In particolare, se $p_1, \ldots, p_m$ sono lasciati fissi da π, allora $\pi[X] = X$. In altre parole abbiamo dimostrato che

Lemma 29.18. *Se* $\pi \in \mathrm{Aut}(\mathcal{A})$, $\pi(p_i) = p_i$ *(*$i = 1, \ldots, m$*) e* $\pi[X] \neq X$, *allora* X *non è definibile in* $\mathcal{A}$ *con parametri* $p_1, \ldots, p_m$.

Esercizi

Esercizio 29.19. Dimostrare che

$$\boldsymbol{s \equiv t \Rightarrow \big(\varphi[\![s/x]\!] \Leftrightarrow \varphi[\![t/x]\!]\big)},$$

è logicamente valida.

Esercizio 29.20. Dimostrare che le seguenti formule sono logicamente valide:

(i) $\boldsymbol{\exists x\,(\varphi \vee \psi) \Leftrightarrow (\exists x\varphi \vee \exists x\psi)}$.

(ii) $\boldsymbol{\forall x\,(\varphi \wedge \psi) \Leftrightarrow (\forall x\varphi \wedge \forall x\psi)}$.

(iii) $\boldsymbol{\exists x\,(\varphi \wedge \psi) \Rightarrow (\exists x\varphi \wedge \exists x\psi)}$.

(iv) $\boldsymbol{(\forall x\varphi \vee \forall x\psi) \Rightarrow \forall x\,(\varphi \vee \psi)}$.

(v) $\boldsymbol{\forall x\,(\varphi \Rightarrow \psi) \Leftrightarrow (\varphi \Rightarrow \forall x\psi)}$, se $\boldsymbol{x}$ non occorre libera in $\boldsymbol{\varphi}$.

Esercizio 29.21. Dimostrare che le seguenti formule non sono valide:

(i) $\boldsymbol{(\exists x\varphi \wedge \exists x\psi) \Rightarrow \exists x\,(\varphi \wedge \psi)}$

(ii) $\boldsymbol{\forall x\,(\varphi \vee \psi) \Rightarrow (\forall x\varphi \vee \forall x\psi)}$.

(iii) $\boldsymbol{\forall x\,(\varphi \Rightarrow \psi) \Rightarrow (\varphi \Rightarrow \forall x\psi)}$,se $\boldsymbol{x}$ occorre libera in $\boldsymbol{\varphi}$.

Esercizio 29.22. Dimostrare che

(i) una formula φ è valida se e solo se $\varphi^{\forall}$ è valida;

(ii) φ è soddisfacibile se e solo se $\varphi^{\exists}$ è soddisfacibile.

30. Teorie e modelli

Richiamiamo alcuni concetti già introdotti informalmente nel Capitolo I.

Definizione 30.1. Fissiamo un linguaggio L e sia Γ un insieme di formule. Se $\mathcal{A} \in \mathrm{Str}(L)$ diremo che $\mathcal{A}$ è un **modello di** Γ

$$\mathcal{A} \vDash \Gamma$$

se $\mathcal{A} \vDash \boldsymbol{\varphi}$, per ogni $\boldsymbol{\varphi} \in \Gamma$. Equivalentemente

$$\mathcal{A} \vDash \Gamma \quad \text{se e solo se} \quad \mathcal{A} \vDash \Gamma^{\forall}$$

dove $\Gamma^{\forall} = \left\{\boldsymbol{\varphi}^{\forall} \mid \boldsymbol{\varphi} \in \Gamma\right\}$ è l'insieme delle chiusure universali delle formule in Γ.

La classe delle L-strutture che sono modelli di un insiemi di formule Γ è

$$\mathrm{Mod}_L(\Gamma) = \mathrm{Mod}(\Gamma) = \{\mathcal{A} \in \mathrm{Str}(L) \mid \mathcal{A} \vDash \Gamma\}.$$

Se Γ è un singoletto $\{\boldsymbol{\varphi}\}$, scriveremo $\mathrm{Mod}(\boldsymbol{\varphi})$ invece di $\mathrm{Mod}(\{\boldsymbol{\varphi}\})$.

Definizione 30.2. Se $\{\boldsymbol{\varphi}, \boldsymbol{\psi}\}, \Gamma, \Delta \subseteq \mathrm{Fml}(L)$, diremo che

- Δ è una **conseguenza logica di** Γ **nel linguaggio** L, in simboli $\Gamma \models_L \Delta$, se $\mathrm{Mod}(\Gamma) \subseteq \mathrm{Mod}(\Delta)$. Se $\Gamma = \emptyset$ scriveremo $\models \Delta$ e se Γ e Δ sono i singoletti $\{\boldsymbol{\varphi}\}$ e $\{\boldsymbol{\psi}\}$, scriveremo $\boldsymbol{\varphi} \models \boldsymbol{\psi}$;

- Γ e Δ sono **logicamente equivalenti** se $\mathrm{Mod}(\Gamma) = \mathrm{Mod}(\Delta)$;
- $\boldsymbol{\varphi}$ e $\boldsymbol{\psi}$ sono **logicamente equivalenti modulo** Γ se $\Gamma \models_L \boldsymbol{\varphi} \boldsymbol{\Leftrightarrow} \boldsymbol{\psi}$.

Come abbiamo detto nell'Osservazione 3.18, la nozione di equivalenza logica tra formule è più forte rispetto alla nozione di equivalenza logica delle chiusure universali.

Esercizio 30.3. Se $L' \subseteq L$ e $\Gamma, \Delta \subseteq \mathrm{Fml}(L')$, allora

$$\Gamma \models_L \Delta \quad \Leftrightarrow \quad \Gamma \models_{L'} \Delta.$$

Quando il linguaggio è chiaro dal contesto, scriveremo semplicemente $\Sigma \models \Delta$.

Ricordiamo (Definizione 3.8) che una teoria è un insieme T di enunciati e che ogni altra teoria logicamente equivalente ad essa si dice sistema di assiomi per T. Una teoria T è soddisfacibile se $\mathrm{Mod}(T) \neq \emptyset$; se inoltre $T \models \boldsymbol{\sigma}$ oppure $T \models \boldsymbol{\neg\sigma}$ per ogni enunciato $\boldsymbol{\sigma}$, allora la teoria si dice completa (Definizione 3.14). Una teoria T è **semanticamente chiusa** se è un insieme di enunciati chiuso per conseguenza logica, cioè se $T \models \sigma$ allora $\sigma \in T$, per ogni enunciato σ. La **teoria di una L-struttura** $\mathcal{A}$ è

$$\mathrm{Th}(\mathcal{A}) = \{\boldsymbol{\sigma} \in \mathrm{Sent}(L) \mid \mathcal{A} \vDash \boldsymbol{\sigma}\}.$$

Esercizio 30.4. Dimostrare che:

(i) Ogni teoria semanticamente chiusa è completa se e solo se è una teoria soddisfacibile e massimale, cioè se $T \subset S$ allora S è insoddisfacibile.

(ii) Se T è una teoria semanticamente chiusa e se $\boldsymbol{\sigma}, \boldsymbol{\tau} \in \mathrm{Sent}(L)$, allora

$$\boldsymbol{\sigma} \boldsymbol{\wedge} \boldsymbol{\tau} \in T \quad \Leftrightarrow \quad \boldsymbol{\sigma} \in T \wedge \boldsymbol{\tau} \in T.$$

(iii) Se T è una teoria completa e se $\boldsymbol{\sigma}, \boldsymbol{\tau} \in \mathrm{Sent}(L)$, allora

$$T \models \boldsymbol{\sigma} \boldsymbol{\vee} \boldsymbol{\tau} \quad \Leftrightarrow \quad T \models \boldsymbol{\sigma} \vee T \models \boldsymbol{\tau}.$$

(iv) Se T è una teoria semanticamente chiusa e completa e se $\boldsymbol{\sigma} \in \mathrm{Sent}(L)$, allora

$$\boldsymbol{\sigma} \notin T \quad \Leftrightarrow \quad \boldsymbol{\neg\sigma} \in T.$$

30.A. Preservazione di formule in strutture. La nozione di $\exists$-formula, $\forall$-formula, $\forall\exists$-formula, ecc. sono state introdotte a pag. 36 del Capitolo I.

Proposizione 30.5. *Siano $\boldsymbol{\varphi}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)$ una formula, $\vec{a} \in A$ e $\mathcal{A} \subseteq \mathcal{B}$.*

(a) *Se $\boldsymbol{\varphi}$ è priva di quantificatori*

$$\mathcal{A} \vDash \boldsymbol{\varphi}[\vec{a}] \quad \Leftrightarrow \quad \mathcal{B} \vDash \boldsymbol{\varphi}[\vec{a}].$$

(b) *Se $\boldsymbol{\varphi}$ è una $\forall$-formula*

$$\mathcal{B} \vDash \boldsymbol{\varphi}[\vec{a}] \quad \Rightarrow \quad \mathcal{A} \vDash \boldsymbol{\varphi}[\vec{a}].$$

(c) *Se* $\boldsymbol{\varphi}$ *è una* $\exists$*-formula*

$$\mathcal{A} \vDash \boldsymbol{\varphi}[\vec{a}] \quad \Rightarrow \quad \mathcal{B} \vDash \boldsymbol{\varphi}[\vec{a}].$$

Dimostrazione. (a) Per induzione su $\mathrm{ht}(\boldsymbol{\varphi})$. Se $\boldsymbol{\varphi}$ è atomica (vale a dire $\boldsymbol{t}_1 \equiv \boldsymbol{t}_2$ o $R(\boldsymbol{t}_1, \dots, \boldsymbol{t}_n)$) allora il risultato segue dall'Esercizio 29.3 e dalla definizione di sotto-struttura. Se $\boldsymbol{\varphi}$ è $\boldsymbol{\neg\psi}$, allora

$$\begin{aligned} \mathcal{A} \vDash \boldsymbol{\varphi}[\vec{a}] &\Leftrightarrow \neg(\mathcal{A} \vDash \boldsymbol{\psi}[\vec{a}]) \\ &\Leftrightarrow \neg(\mathcal{B} \vDash \boldsymbol{\psi}[\vec{a}]) \qquad \text{(per ip. ind.)} \\ &\Leftrightarrow \mathcal{B} \vDash \boldsymbol{\varphi}[\vec{a}]. \end{aligned}$$

Se $\boldsymbol{\varphi}$ è $\boldsymbol{\psi \vee \chi}$, allora

$$\begin{aligned} \mathcal{A} \vDash \boldsymbol{\varphi}[\vec{a}] &\Leftrightarrow (\mathcal{A} \vDash \boldsymbol{\psi}[\vec{a}] \vee \mathcal{A} \vDash \boldsymbol{\chi}[\vec{a}]) \\ &\Leftrightarrow (\mathcal{B} \vDash \boldsymbol{\psi}[\vec{a}] \vee \mathcal{B} \vDash \boldsymbol{\chi}[\vec{a}]) \qquad \text{(per ip. ind.)} \\ &\Leftrightarrow \mathcal{B} \vDash \boldsymbol{\varphi}[\vec{a}]. \end{aligned}$$

(b) Sia $\boldsymbol{\varphi}$ la formula $\boldsymbol{\forall y}_1 \dots \boldsymbol{\forall y}_m \boldsymbol{\psi}$ e supponiamo $\mathcal{B} \vDash \boldsymbol{\varphi}[\vec{a}]$, vale a dire $\forall b_1 \dots b_m \in B\, (\mathcal{B} \vDash \boldsymbol{\psi}[\vec{b}, \vec{a}])$. Quindi, per ogni $b_1, \dots, b_m \in A \subseteq B$, vale $\mathcal{B} \vDash \boldsymbol{\psi}[\vec{b}, \vec{a}]$ e allora, per la parte (a), vale $\mathcal{A} \vDash \boldsymbol{\psi}[\vec{b}, \vec{a}]$. Abbiamo mostrato che $\forall b_1 \dots b_m \in A\, (\mathcal{A} \vDash \boldsymbol{\psi}[\vec{b}, \vec{a}])$, cioè $\mathcal{A} \vDash \boldsymbol{\varphi}[\vec{a}]$.

(c) segue da (b). □

Proposizione 30.6. *Sia* $\boldsymbol{\varphi}$ *una* $\forall\exists$*-formula soddisfatta in ogni* $\mathcal{A}_n$*, dove* $\mathcal{A}_0 \subseteq \mathcal{A}_1 \subseteq \dots$*. Allora* $\bigcup_n \mathcal{A}_n \vDash \boldsymbol{\varphi}$*.*

Dimostrazione. Poiché la chiusura universale di una $\forall\exists$-formula è una $\forall\exists$-formula, possiamo supporre che $\boldsymbol{\varphi}$ sia un enunciato. Fissiamo $\boldsymbol{\psi}$ priva di quantificatori tale che

$$\boldsymbol{\varphi} = \boldsymbol{\forall x}_1 \dots \boldsymbol{\forall x}_n \boldsymbol{\exists y}_1 \dots \boldsymbol{\exists y}_m \boldsymbol{\psi}.$$

Fissiamo $a_1, \dots, a_n \in \bigcup_i A_i$ e sia N sufficientemente grande per cui $a_1, \dots, a_n \in A_N$. Allora $\mathcal{A}_N \vDash \boldsymbol{\varphi}$ implica che

$$\mathcal{A}_N \vDash (\boldsymbol{\exists y}_1 \dots \boldsymbol{\exists y}_m \boldsymbol{\psi})\, [a_1, \dots, a_n].$$

Per la parte (c) della Proposizione 30.5 segue che $\bigcup_n \mathcal{A}_n \vDash \boldsymbol{\varphi}$. □

30.B. Equivalenza elementare. Per le Definizioni 3.14 e 3.26 del Capitolo I diciamo che due L-strutture $\mathcal{A}$ e $\mathcal{B}$ sono **elementarmente equivalenti** $\mathcal{A} \equiv \mathcal{B}$ se e solo se

$$\mathrm{Th}(\mathcal{A}) = \mathrm{Th}(\mathcal{B}),$$

e che un morfismo $\pi\colon \mathcal{A} \to \mathcal{B}$ è un'**immersione elementare** se per ogni formula $\boldsymbol{\varphi}(\boldsymbol{x}_1, \dots, \boldsymbol{x}_n)$ e ogni $\vec{a} \in A^n$

$$\mathcal{A} \vDash \boldsymbol{\varphi}[\vec{a}] \quad \Leftrightarrow \quad \mathcal{B} \vDash \boldsymbol{\varphi}[\pi(\vec{a})].$$

Esercizio 30.7. Sia $\pi\colon \mathcal{A} \to \mathcal{B}$ un morfismo. Dimostrare che:

(i) Se π è un isomorfismo allora è un'immersione elementare.

(ii) Se π è elementare allora è iniettiva.

(iii) Se per ogni formula $\boldsymbol{\varphi}$ e ogni $\vec{a}$

$$\mathcal{A} \vDash \boldsymbol{\varphi}[\vec{a}] \quad \Rightarrow \quad \mathcal{B} \vDash \boldsymbol{\varphi}[\pi(\vec{a})]$$

allora π è elementare.

Se c'è un'immersione elementare di $\mathcal{A}$ in $\mathcal{B}$ diremo che $\mathcal{A}$ **si immerge elementarmente in** $\mathcal{B}$,

$$\mathcal{A} \preccurlyeq \mathcal{B}.$$

Se $\mathcal{A} \subseteq \mathcal{B}$ e la funzione di inclusione è un'immersione elementare diremo che $\mathcal{A}$ è una **sotto-struttura elementare** di $\mathcal{B}$,

$$\mathcal{A} \preccurlyeq \mathcal{B},$$

e se $\mathcal{A} \neq \mathcal{B}$ diremo che $\mathcal{A}$ è una **sotto-struttura elementare propria** di $\mathcal{B}$, in simboli $\mathcal{A} \prec \mathcal{B}$. Le espressioni $\mathcal{A} \subseteq \mathcal{B}$ e $\mathcal{A} \subset \mathcal{B}$ significano che $\mathcal{A}$ è isomorfa ad una sotto-struttura di $\mathcal{B}$ e, rispettivamente, ad una sotto-struttura propria di $\mathcal{B}$.

Sia $\mathcal{A} \in \mathrm{Str}(L)$, sia

$$L_A = L \cup \{\mathring{a} \mid a \in A\}$$

il linguaggio espanso con un nuovo simbolo di costante per ogni elemento di A e sia $\langle \mathcal{A}, a\rangle_{a\in A}$ l'espansione canonica di $\mathcal{A}$ ad A.

Definizione 30.8. Il **diagramma di** $\mathcal{A}$ è l'insieme di tutte le formule atomiche e loro negazioni che valgono in $\langle \mathcal{A}, a\rangle_{a\in A}$

$$\mathrm{Diag}(\mathcal{A}) = \mathrm{Th}(\langle \mathcal{A}, a\rangle_{a\in A}) \cap (\mathrm{AtFml}(L_A) \cup \{\boldsymbol{\neg\psi} \mid \boldsymbol{\psi} \in \mathrm{AtFml}(L_A)\}).$$

Il **diagramma elementare** di $\mathcal{A}$ è l'insieme di tutti gli enunciati che valgono in $\langle \mathcal{A}, a\rangle_{a\in A}$

$$\mathrm{EDiag}(\mathcal{A}) = \mathrm{Th}(\langle \mathcal{A}, a\rangle_{a\in A}).$$

Teorema 30.9. *Le seguenti affermazioni sono equivalenti:*

(a) $\mathcal{A} \preccurlyeq \mathcal{B}$,

(b) *c'è un'espansione* $\tilde{\mathcal{B}}$ *di* $\mathcal{B}$ *nel linguaggio* $L_A = L \cup \{\mathring{a} \mid a \in A\}$ *tale che* $\tilde{\mathcal{B}} \vDash \mathrm{EDiag}(\mathcal{A})$.

Dimostrazione. (a) $\Rightarrow$ (b): Se $\pi\colon \mathcal{A} \to \mathcal{B}$ è elementare, allora ponendo

$$(\mathring{a})^{\tilde{\mathcal{B}}} = \pi(a) \text{ per } a \in A,$$

otteniamo l'espansione $\tilde{\mathcal{B}} = \langle \mathcal{B}, \pi(a)\rangle_{a\in A}$. Verifichiamo che $\tilde{\mathcal{B}} \vDash \boldsymbol{\sigma}$ per ogni $\boldsymbol{\sigma} \in \mathrm{EDiag}(\mathcal{A})$. Se $\boldsymbol{\sigma} \in \mathrm{Sent}(L_A)$ allora $\boldsymbol{\sigma}$ è della forma $\boldsymbol{\varphi}[\![\mathring{a}_1/\boldsymbol{x}_1, \dots, \mathring{a}_n/\boldsymbol{x}_n]\!]$, dove $\boldsymbol{\varphi}(\boldsymbol{x}_1, \dots, \boldsymbol{x}_n)$ è una L-formula e quindi

$$\begin{aligned}\langle \mathcal{A}, a\rangle_{a\in A} \vDash \boldsymbol{\sigma} &\Leftrightarrow \mathcal{A} \vDash \boldsymbol{\varphi}[a_1, \dots, a_n]\\ &\Leftrightarrow \mathcal{B} \vDash \boldsymbol{\varphi}[\pi(a_1), \dots, \pi(a_n)]\\ &\Leftrightarrow \tilde{\mathcal{B}} \vDash \boldsymbol{\sigma}.\end{aligned}$$

(b) $\Rightarrow$ (a): Supponiamo che $\tilde{\mathcal{B}}$ sia una L_A-struttura che soddisfa $\mathrm{EDiag}(\mathcal{A})$. Allora, per ogni coppia $a_1, a_2 \in A$

$$\begin{aligned}a_1 \neq a_2 &\Leftrightarrow (\mathring{a}_1 \not\equiv \mathring{a}_2) \in \mathrm{EDiag}(\mathcal{A})\\ &\Leftrightarrow \tilde{\mathcal{B}} \vDash \mathring{a}_1 \not\equiv \mathring{a}_2\\ &\Leftrightarrow (\mathring{a}_1)^{\tilde{\mathcal{B}}} \neq (\mathring{a}_2)^{\tilde{\mathcal{B}}}.\end{aligned}$$

Quindi $\pi\colon A \to B$, $\pi(a) = (\mathring{a})^{\tilde{\mathcal{B}}}$, è una funzione iniettiva. Se $\boldsymbol{\varphi}(\boldsymbol{x}_1, \dots, \boldsymbol{x}_n)$ è una L-formula e $a_1, \dots, a_n \in A$, allora

$$\begin{aligned}\mathcal{A} \vDash \boldsymbol{\varphi}[a_1, \dots, a_n] &\Leftrightarrow \boldsymbol{\varphi}[\![\mathring{a}_1/\boldsymbol{x}_1, \dots, \mathring{a}_n/\boldsymbol{x}_n]\!] \in \mathrm{EDiag}(\mathcal{A})\\ &\Leftrightarrow \tilde{\mathcal{B}} \vDash \boldsymbol{\varphi}[\![\mathring{a}_1/\boldsymbol{x}_1, \dots, \mathring{a}_n/\boldsymbol{x}_n]\!]\\ &\Leftrightarrow \mathcal{B} \vDash \boldsymbol{\varphi}[\pi(a_1), \dots, \pi(a_n)].\end{aligned}$$

Quindi π è elementare. □

Esercizio 30.10. Siano $\mathcal{A}, \mathcal{B} \in \mathrm{Str}(L)$. Dimostrare che le seguenti condizioni sono equivalenti:

(i) $\mathcal{A} \subseteq \mathcal{B}$,

(ii) c'è un'espansione $\tilde{\mathcal{B}}$ di $\mathcal{B}$ nel linguaggio $L \cup \{\mathring{a} \mid a \in \|\mathcal{A}\|\}$ tale che $\tilde{\mathcal{B}} \vDash \mathrm{Diag}(\mathcal{A})$.

Teorema 30.11 (Tarski-Vaught)**.** *Se $\pi\colon \mathcal{A} \to \mathcal{B}$ è un'immersione le seguenti condizioni sono equivalenti:*

(a) *π è elementare,*

(b) *per ogni formula $\boldsymbol{\varphi}(\boldsymbol{y}, \boldsymbol{x}_1, \dots, \boldsymbol{x}_n)$ e ogni $\vec{a} \in A^n$*

$$\mathcal{B} \vDash (\boldsymbol{\exists y}\boldsymbol{\varphi})[\pi(\vec{a})] \quad \Leftrightarrow \quad \exists b \in A\, (\mathcal{B} \vDash \boldsymbol{\varphi}[\pi(b), \pi(\vec{a})])\,.$$

Dimostrazione. (a) $\Rightarrow$ (b): Se $\mathcal{B} \vDash (\boldsymbol{\exists y}\boldsymbol{\varphi})[\pi(\vec{a})]$ allora $\mathcal{A} \vDash (\boldsymbol{\exists y}\boldsymbol{\varphi})[\vec{a}]$ per l'elementarità di π, e quindi $\mathcal{A} \vDash \boldsymbol{\varphi}[b, \vec{a}]$ per qualche $b \in A$, da cui $\mathcal{B} \vDash \boldsymbol{\varphi}[\pi(b), \pi(\vec{a})]$.

(b) $\Rightarrow$ (a): Per induzione su $\mathrm{ht}(\boldsymbol{\psi})$ dimostriamo che

$$\mathcal{A} \vDash \boldsymbol{\psi}[\vec{a}] \quad \Leftrightarrow \quad \mathcal{B} \vDash \boldsymbol{\psi}[\pi(\vec{a})]. \tag{30.1}$$

Se $\boldsymbol{\psi}$ è atomica allora (30.1) vale per l'Esercizio 30.17. Se $\boldsymbol{\psi}$ è $\boldsymbol{\neg}\boldsymbol{\psi}_1$ o $\boldsymbol{\psi}_1 \boldsymbol{\vee} \boldsymbol{\psi}_2$, allora (30.1) vale per ipotesi induttiva e per la definizione di soddisfazione. Quindi possiamo supporre che $\boldsymbol{\psi}$ sia $\boldsymbol{\exists y \varphi}$:

$$\begin{aligned} \mathcal{A} \vDash (\boldsymbol{\exists y \varphi})[\vec{a}] &\Leftrightarrow \exists b \in A\, (\mathcal{A} \vDash \boldsymbol{\varphi}[b, \vec{a}]) \\ &\Leftrightarrow \exists b \in A\, (\mathcal{B} \vDash \boldsymbol{\varphi}[\pi(b), \pi(\vec{a})]) \qquad \text{(per ipotesi induttiva)} \\ &\Leftrightarrow \mathcal{B} \vDash (\boldsymbol{\exists y \varphi})[\pi(\vec{a})] \qquad \text{(per la nostra ipotesi).} \end{aligned}$$ □

Corollario 30.12. *Le seguenti condizioni sono equivalenti:*

(a) $\mathcal{A} \preccurlyeq \mathcal{B}$

(b) $\mathcal{A} \subseteq \mathcal{B}$ *e per ogni formula* $\boldsymbol{\varphi}(\boldsymbol{y}, \boldsymbol{x}_1, \dots, \boldsymbol{x}_n)$ *e ogni* $\vec{a} \in A^n$

$$\mathcal{B} \vDash (\boldsymbol{\exists y \varphi})[\vec{a}] \quad \Leftrightarrow \quad \exists b \in A\, (\mathcal{B} \vDash \boldsymbol{\varphi}[b, \vec{a}])\,.$$

Proposizione 30.13. *Supponiamo che* $\mathcal{A}_0 \preccurlyeq \mathcal{A}_1 \preccurlyeq \mathcal{A}_2 \preccurlyeq \dots$. *Allora* $\mathcal{A}_m \preccurlyeq \mathcal{A}_\infty \stackrel{\text{def}}{=} \bigcup_{k\in\omega} \mathcal{A}_k$, *per ogni* $m \in \omega$.

Dimostrazione. Verifichiamo per induzione su $\operatorname{ht} \boldsymbol{\varphi}(\boldsymbol{x}_1, \dots, \boldsymbol{x}_n)$ che per ogni $m \in \omega$ e ogni $a_1, \dots, a_n \in A_m$

$$\mathcal{A}_m \vDash \boldsymbol{\varphi}[\vec{a}] \quad \Leftrightarrow \quad \mathcal{A}_\infty \vDash \boldsymbol{\varphi}[\vec{a}].$$

Chiaramente $\mathcal{A}_m \subseteq \mathcal{A}_\infty$, quindi per il Corollario 30.12 è sufficiente dimostrare che se $\boldsymbol{\varphi} = \boldsymbol{\exists y \psi}(\boldsymbol{y}, \boldsymbol{x}_1, \dots, \boldsymbol{x}_n)$ e $\mathcal{A}_\infty \vDash (\boldsymbol{\exists y \psi})[\vec{a}]$ con $a_1, \dots, a_n \in A_m$, allora $\mathcal{A}_\infty \vDash \boldsymbol{\psi}[b, \vec{a}]$, per qualche $b \in A_m$. Sia $b' \in \bigcup_k A_k$ tale che

$$\mathcal{A}_\infty \vDash \boldsymbol{\psi}[b', \vec{a}]$$

e sia $m' \geq m$ tale che $b' \in A_{m'}$. Per ipotesi induttiva $\mathcal{A}_{m'} \vDash \boldsymbol{\psi}[b', \vec{a}]$ e quindi $\mathcal{A}_{m'} \vDash (\boldsymbol{\exists y \psi})[\vec{a}]$ da cui $\mathcal{A}_m \vDash (\boldsymbol{\exists y \psi})[\vec{a}]$. Ne segue che $\mathcal{A}_m \vDash \boldsymbol{\psi}[b, \vec{a}]$ per un opportuno $b \in A_m$. □

30.C. Funzioni di Skolem. Sia $\mathcal{A}$ una L-struttura e sia $\lhd$ un buon ordine di $A = \|\mathcal{A}\|$. Ad ogni formula $\boldsymbol{\varphi}$ con variabili libere $\boldsymbol{y}, \boldsymbol{x}_1, \dots, \boldsymbol{x}_n$ associamo

$$h_{\boldsymbol{\varphi}} \colon A^n \to A$$

la **funzione di Skolem per** $\boldsymbol{\exists y \varphi}$ definita da

$$h_{\boldsymbol{\varphi}}(a_1, \dots, a_n) = \begin{cases} \text{il } \lhd\text{-minimo } b \text{ tale che } \mathcal{A} \vDash \boldsymbol{\varphi}[b, \vec{a}] & \text{se } \mathcal{A} \vDash (\boldsymbol{\exists y \varphi})[\vec{a}] \\ a^* & \text{altrimenti,} \end{cases}$$

dove a^* è il $\lhd$-minimo di A. Osserviamo che se $\boldsymbol{y}$ è l'unica variabile libera di $\boldsymbol{\varphi}$, allora $h_{\boldsymbol{\varphi}} \colon A^0 \to A$ è — essenzialmente — un elemento di A: un testimone del fatto che $\mathcal{A} \vDash \boldsymbol{\exists y \varphi}$ oppure a^*. L'insieme delle funzioni di Skolem per $\mathcal{A}$ è denotato con

$$\operatorname{Sk}(\mathcal{A}).$$

Teorema 30.14. *Supponiamo $\mathcal{A}$ sia una L-struttura bene ordinabile. Per ogni $X \subseteq A$, la chiusura di X sotto le funzioni in* $\mathrm{Sk}(\mathcal{A})$ *è una sotto-struttura elementare di $\mathcal{A}$,*

$$\mathrm{Cl}_{\mathrm{Sk}(\mathcal{A})}(X) \preccurlyeq \mathcal{A}.$$

Dimostrazione. La funzione di Skolem della formula $\boldsymbol{y} \not\equiv \boldsymbol{y}$ garantisce che $a^* \in C = \mathrm{Cl}_{\mathrm{Sk}(\mathcal{A})}(X)$, quindi $C \neq \emptyset$. Per ogni simbolo di costante $\boldsymbol{c}$ la chiusura di C sotto la funzione 0-aria di Skolem $h_{\boldsymbol{\varphi}}$, dove $\boldsymbol{\varphi}$ è $\boldsymbol{y} \equiv \boldsymbol{c}$, garantisce che $\boldsymbol{c}^{\mathcal{A}} \in C$. Per ogni simbolo $\boldsymbol{f}$ di funzione n-aria, la chiusura di C sotto la funzione di Skolem $h_{\boldsymbol{\psi}}$, dove $\boldsymbol{\psi}$ è $\boldsymbol{y} \equiv \boldsymbol{f}(\boldsymbol{x}_1, \dots, \boldsymbol{x}_n)$, garantisce che C è chiuso sotto $\boldsymbol{f}^{\mathcal{A}}$. Poiché l'interpretazione dei simboli di relazione non costituisce un problema, segue che C è (l'universo di) una sottostruttura di $\mathcal{A}$. Per il Teorema di Tarski-Vaught è sufficiente verificare che se $\mathcal{A} \vDash (\boldsymbol{\exists y \varphi})[\vec{c}]$ per qualche $\vec{c} \in C^n$, allora c'è un $b \in C$ tale che $\mathcal{A} \vDash \boldsymbol{\varphi}[b, \vec{c}]$. Ma ciò è immediato prendendo $b = h_{\boldsymbol{\varphi}}(\vec{c})$. □

Il seguente risultato, noto come il "Teorema di Löwenheim-Skolem all'ingiù" asserisce, in particolare, che ogni struttura più che numerabile in un linguaggio numerabile ha una sotto-struttura elementare numerabile.

Teorema 30.15. *Supponiamo L sia bene ordinabile. Se $\mathcal{A} \in \mathrm{Str}(L)$ e κ è un cardinale infinito tale che*

$$\mathrm{card}(L) \leq \kappa \leq \mathrm{card}(\mathcal{A}),$$

allora per ogni $X \subseteq A$ con $|X| \leq \kappa$ c'è una $\mathcal{B} \preccurlyeq \mathcal{A}$ con $X \subseteq B$ e $\mathrm{card}(\mathcal{B}) = \kappa$.

Dimostrazione. Sia $Y \subseteq A$ tale che $X \subseteq Y$ e $|Y| = \kappa$. Poiché

$$|\mathrm{Sk}(\mathcal{A})| \leq |\mathrm{Fml}(L)| = \mathrm{card}(L),$$

segue dal Teorema 16.5 che

$$\kappa \leq |Y| \leq |\mathrm{Cl}_{\mathrm{Sk}(\mathcal{A})}(Y)| \leq \kappa.$$

Per il Teorema 30.14 possiamo prendere $B = \mathrm{Cl}_{\mathrm{Sk}(\mathcal{A})}(Y)$. □

30.D. Classi elementari e varietà. Una classe di strutture $\mathcal{K} \subseteq \mathrm{Str}(L)$ è una

- **classe elementare in** L, in simboli: $\mathrm{EC}(L)$, sse
$$\mathcal{K} = \mathrm{Mod}(\boldsymbol{\sigma})$$
per qualche L-enunciato $\boldsymbol{\sigma}$;
- **classe elementare generalizzata in** L, in simboli: $\mathrm{EC}_\Delta(L)$, sse
$$\mathcal{K} = \mathrm{Mod}(\Sigma)$$
per qualche insieme di L-enunciati Σ.

- **classe pseudo-elementare in** L, in simboli: $\mathrm{PC}(L)$, sse
$$\mathcal{K} = \{\mathcal{A}' \restriction L \mid \mathcal{A}' \in \mathcal{K}'\}$$
dove $\mathcal{K}'$ è elementare in qualche linguaggio $L' \supseteq L$;
- **classe pseudo-elementare generalizzata in** L, in simboli: $\mathrm{PC}_\Delta(L)$, sse
$$\mathcal{K} = \{\mathcal{A}' \restriction L \mid \mathcal{A}' \in \mathcal{K}'\}$$
dove $\mathcal{K}'$ è elementare generalizzata in qualche linguaggio $L' \supseteq L$.[2]

Dalla definizione discende che

$$\begin{array}{ccc} \mathrm{EC} & \Longrightarrow & \mathrm{PC} \\ \Downarrow & & \Downarrow \\ \mathrm{EC}_\Delta & \Longrightarrow & \mathrm{PC}_\Delta \end{array}$$

Se $\mathcal{K} = \mathrm{Mod}(\Sigma)$ e Σ è finito allora $\mathcal{K} = \mathrm{Mod}(\bigwedge \Sigma)$ è EC. Per questo motivo, le classi elementari si dicono anche **finitamente assiomatizzabili**, mentre le classi elementari generalizzate si dicono **assiomatizzabili**. Osserviamo che $\emptyset$ e $\mathrm{Str}(L)$ sono sempre finitamente assiomatizzabili, per ogni L. Se $\mathcal{K}$ è $\mathrm{Mod}(\boldsymbol{\sigma})$ allora anche $\mathrm{Str}(L) \setminus \mathcal{K} = \mathrm{Mod}(\boldsymbol{\neg\sigma})$. In altre parole: il complemento di una classe elementare è elementare.

30.E. Esempi. Vedremo ora alcuni esempi di classi di strutture matematiche che sono assiomatizzabili.

30.E.1. *Ordini.* Consideriamo il linguaggio L_{ORDINI}. La classe dei pre-ordini, degli ordini, degli ordini lineari, etc. sono elementari. La classe degli ordini mal-fondati è PC_Δ in L_{ORDINI}: infatti basta considerare gli enunciati che caratterizzano gli ordini (proprietà riflessiva, antisimmetrica e transitiva) con in aggiunta gli enunciati

$$(\boldsymbol{c}_{n+1} \leq \boldsymbol{c}_n) \boldsymbol{\wedge} \boldsymbol{\neg} (\boldsymbol{c}_n \leq \boldsymbol{c}_{n+1})$$

dove le $\boldsymbol{c}_n$ sono delle costanti.

30.E.2. *Il calcolo proposizionale.* Fissato un insieme S di lettere, nella sezione **??** abbiamo definito l'insieme $\mathrm{Prop}(S)$ delle proposizioni su S. Il linguaggio L associato ad S ha un unico simbolo di relazione 1-ario $\boldsymbol{U}$ e un simbolo di costante $\mathring{A}$, per ogni $A \in S$. Ad ogni $\boldsymbol{p} \in \mathrm{Prop}(S)$ possiamo associare un enunciato $\boldsymbol{\sigma_p} \in \mathrm{Sent}(L)$: alle lettere proposizionali $A \in S$ associamo l'enunciato $\boldsymbol{U}(\mathring{A})$, e poi estendiamo l'assegnazione in modo ovvio, ponendo $\boldsymbol{p \vee q} \mapsto \boldsymbol{\sigma_p \vee \sigma_q}$, $\boldsymbol{\neg p} \mapsto \boldsymbol{\neg \sigma_p}$, etc. Sempre nella sezione **??** abbiamo definito una valutazione per $\mathrm{Prop}(S)$ come una funzione $v\colon L \to \{0,1\}$. Ogni valutazione v determina una L-struttura

$$\mathcal{M}_v = \langle S, \{A \in S \mid v(A) = 1\}, A \rangle_{A \in S}$$

[2]Gli acronimi EC e PC stanno per *Elementary Class* e *Pseudo-elementary Class*.

dove $\{A \in L \mid v(A) = 1\}$ è l'interpretazione di $\boldsymbol{U}$ e A è l'interpretazione di $\mathring{A}$. Viceversa, ad ogni L-struttura $\mathcal{M} = \langle M, \boldsymbol{U}^{\mathcal{M}}, \mathring{A}^{\mathcal{M}} \rangle_{A \in S}$ associamo la valutazione

$$v_{\mathcal{M}}(A) = 1 \Leftrightarrow \mathring{A}^{\mathcal{M}} \in \boldsymbol{U}^{\mathcal{M}}.$$

Una facile induzione sull'altezza delle formule dimostra che

$$v(\boldsymbol{p}) = 1 \quad \Leftrightarrow \quad \mathcal{M}_v \vDash \boldsymbol{\sigma_p} \qquad \text{e}$$
$$\mathcal{M} \vDash \boldsymbol{\sigma_p} \quad \Leftrightarrow \quad v_{\mathcal{M}}(\boldsymbol{p}) = 1.$$

Esercizi

Esercizio 30.16. Sia $L = \{U\}$ il linguaggio con un unico simbolo di relazione 1-aria. Le L-strutture $\langle A, B \rangle$ sono insiemi non-vuoti con un sottoinsieme privilegiato.

(i) Quante sono — a meno di isomorfismo — le L-strutture di cardinalità n? Di cardinalità $\kappa \geq \omega$?

(ii) Trovare un insieme di enunciati Σ tale che $\langle A, B \rangle \vDash \Sigma$ se e solo se A, B, $A \setminus B$ sono infiniti.

Esercizio 30.17. Verificare che le Proposizioni 30.5 e 30.6 si generalizzano al caso delle immersioni. Per esempio: se $\boldsymbol{\varphi}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)$ è priva di quantificatori e $\pi \colon \mathcal{A} \to \mathcal{B}$ è un'immersione,

$$\mathcal{A} \vDash \boldsymbol{\varphi}[\vec{a}] \quad \Leftrightarrow \quad \mathcal{B} \vDash \boldsymbol{\varphi}[\pi(\vec{a})].$$

Esercizio 30.18. Consideriamo ora il caso di un ultrapotenza $\mathcal{A}^X/U$, cioè $\prod_U \mathcal{A}_x$ con $\mathcal{A}_x = \mathcal{A}$ per ogni $x \in X$. Per ogni $a \in A$ sia $c_a \colon X \to A$ la funzione costante $c_a(x) = a$ per ogni $x \in X$ e sia $\pi \colon \mathcal{A} \to \mathcal{A}^X/U$, $\pi(a) = [c_a]$. Dimostrare che π è elementare.

Note e osservazioni

31. Il teorema di compattezza

Un insieme di enunciati Σ si dice **finitamente soddisfacibile** se e solo se ogni sottoinsieme finito $\Sigma_0 \subseteq \Sigma$ è soddisfacibile. Chiaramente ogni insieme di enunciati soddisfacibile è finitamente soddisfacibile e se l'insieme è finito vale anche il converso. Il seguente **Teorema di Compattezza**, dimostrato da K. Gödel nel 1930, asserisce questo fatto è vero in generale:

Teorema 31.1. *Sia $\Sigma \subseteq \mathrm{Sent}(L)$ è finitamente soddisfacibile. Se assumiamo* BPI *oppure se L è bene ordinabile, allora Σ è soddisfacibile.*

Osserviamo che per l'Esempio 30.E.2, questo risultato generalizza il Teorema 23.42 di Compattezza per il calcolo proposizionale.

Corollario 31.2. *Se Σ è un insieme di enunciati e $\boldsymbol{\sigma}$ un enunciato, allora $\Sigma \models \boldsymbol{\sigma}$ se e solo se $\Sigma_0 \models \boldsymbol{\sigma}$ per qualche $\Sigma_0 \subseteq \Sigma$ finito.*

Dimostrazione. Se, per assurdo, $\Sigma_0 \not\models \boldsymbol{\sigma}$ per ogni $\Sigma_0 \subseteq \Sigma$ finito, allora $\Sigma \cup \{\boldsymbol{\neg\sigma}\}$ sarebbe finitamente soddisfacibile e quindi soddisfacibile. Ma ogni modello di $\Sigma \cup \{\boldsymbol{\neg\sigma}\}$ è un modello di Σ: contraddizione. □

31.A. Dimostrazione del Teorema di Compattezza. Il Teorema di Compattezza è una conseguenza del seguente risultato sugli ultraprodotti.

Teorema 31.3 (Łos)**.** *Siano $\langle \mathcal{A}_x \mid x \in X\rangle$ delle L-strutture e sia U un ultrafiltro su X. Sia $\lhd_x$ un buon ordine su $\|\mathcal{A}_x\|$. Per ogni formula $\boldsymbol{\varphi}(\boldsymbol{x}_1, \dots, \boldsymbol{x}_n)$ e per ogni $g_1, \dots, g_n \in \bigtimes_{x\in X} A_x$*

$$\prod_U \mathcal{A}_x \vDash \boldsymbol{\varphi}[[g_1], \dots, [g_n]] \quad \Leftrightarrow \quad X_{\boldsymbol{\varphi},g_1,\dots,g_n} \in U,$$

dove $X_{\boldsymbol{\varphi},g_1,\dots,g_n} = \{x \in X \mid \mathcal{A}_x \vDash \boldsymbol{\varphi}[g_1(x), \dots, g_n(x)]\}$.

Dimostrazione. La dimostrazione procede per induzione su $\mathrm{ht}(\boldsymbol{\varphi})$. Se $\boldsymbol{\varphi}$ è atomica, il risultato discende dalla definizione di $\prod_U \mathcal{A}_x$. Negli altri casi, al fine di semplificare la notazione, supponiamo che $n = 2$. Se $\boldsymbol{\varphi} = \boldsymbol{\neg\psi}$, allora

$$\begin{aligned}\prod_U \mathcal{A}_x \vDash \boldsymbol{\varphi}[[g_1],[g_2]] &\Leftrightarrow \prod_U \mathcal{A} \nvDash \boldsymbol{\psi}[[g_1],[g_2]]\\ &\Leftrightarrow X_{\boldsymbol{\psi},g_1,g_2} \notin U\\ &\Leftrightarrow X_{\boldsymbol{\varphi},g_1,g_2} \in U\end{aligned}$$

dove nell'ultimo passaggio abbiamo usato che $X_{\boldsymbol{\varphi},g_1,g_2} = X \setminus X_{\boldsymbol{\psi},g_1,g_2}$.

Se $\boldsymbol{\varphi} = \boldsymbol{\psi} \boldsymbol{\vee} \boldsymbol{\chi}$, allora

$$\begin{aligned}\prod_U \mathcal{A}_x \vDash \boldsymbol{\varphi}[[g_1],[g_2]] &\Leftrightarrow (\prod_U \mathcal{A} \vDash \boldsymbol{\psi}[[g_1],[g_2]]) \vee (\prod_U \mathcal{A} \vDash \boldsymbol{\chi}[[g_1],[g_2]])\\ &\Leftrightarrow X_{\boldsymbol{\psi},g_1,g_2} \in U \vee X_{\boldsymbol{\chi},g_1,g_2} \in U\\ &\Leftrightarrow X_{\boldsymbol{\psi},g_1,g_2} \cup X_{\boldsymbol{\chi},g_1,g_2} \in U\\ &\Leftrightarrow X_{\boldsymbol{\psi}\vee\boldsymbol{\chi},g_1,g_2} \in U\end{aligned}$$

dove abbiamo usato che $X_{\boldsymbol{\psi}\vee\boldsymbol{\chi},g_1,g_2} = X_{\boldsymbol{\psi},g_1,g_2} \cup X_{\boldsymbol{\chi},g_1,g_2}$.

Supponiamo ora $\boldsymbol{\varphi} = \boldsymbol{\exists y \psi}$. Se $\prod_U \mathcal{A}_x \vDash \boldsymbol{\varphi}[[g_1],[g_2]]$ allora c'è un $h \in \bigtimes_{x\in X} A_x$ tale che $\prod_U \mathcal{A}_x \vDash \boldsymbol{\psi}[[h],[g_1],[g_2]]$ e quindi, per ipotesi induttiva, $X_{\boldsymbol{\psi},h,\bar{g}} \in U$. Poiché $X_{\boldsymbol{\varphi},g_1,g_2} \supseteq X_{\boldsymbol{\psi},h,g_1,g_2}$, segue che $X_{\boldsymbol{\varphi},g_1,g_2} \in U$. Viceversa, supponiamo $X_{\boldsymbol{\varphi},g_1,g_2} \in U$. Sia $h \in \bigtimes_{x\in X} A_x$ la funzione

$$h(x) = \begin{cases}\text{il } \lhd_x\text{-minimo } a \text{ tale che } \mathcal{A}_x \vDash \boldsymbol{\psi}[a, g_1(x), g_2(x)] & \text{se } x \in X_{\boldsymbol{\varphi},g_1,g_2},\\ a^*_x & \text{altrimenti,}\end{cases}$$

dove a^*_x è il $\lhd_x$-minimo elemento di A_x. Allora $X_{\boldsymbol{\varphi},g_1,g_2}$ è contenuto in $X_{\boldsymbol{\psi},h,g_1,g_2}$ (anzi: i due insiemi coincidono) e quindi $X_{\boldsymbol{\psi},h,g_1,g_2} \in U$. Per ipotesi induttiva, questo implica che $\prod_U \mathcal{A}_x \vDash \boldsymbol{\psi}[[h],[g_1],[g_2]]$ e quindi $\prod_U \mathcal{A}_x \vDash \boldsymbol{\varphi}[[g_1],[g_2]]$. □

Corollario 31.4. *Se $\mathcal{A} \in \mathrm{Str}(L)$ è bene ordinabile allora*

$$\mathcal{A} \equiv \prod_U \mathcal{A}.$$

Corollario 31.5 (AC)**.** *Ogni classe EC_Δ è chiusa per ultraprodotti.*

La dimostrazione che ora presentiamo del Teorema di Compattezza utilizza l'Assioma di Scelta, ma, come vedremo nella Sezione 35, AC può essere rimpiazzato con il principio più debole BPI.

Dimostrazione del Teorema di Compattezza (AC). Sia

$$X = \{x \subseteq \Sigma \mid x \text{ è finito}\}$$

e per ogni $x \in X$ scegliamo un $\mathcal{A}_x \vDash x$. Sia

$$S(x) = \{y \in X \mid x \subseteq y\}.$$

Poiché $S(x_1) \cap \cdots \cap S(x_n) = S(x_1 \cup \cdots \cup x_n)$, l'insieme

$$\{S(x) \mid x \in X\} \subseteq \mathscr{P}(X)$$

è una base per un filtro F su X. Sia $U \supseteq F$ un ultrafiltro che estende F. Vogliamo dimostrare che per ogni $\boldsymbol{\sigma} \in \Sigma$

$$\prod_U \mathcal{A}_x \vDash \boldsymbol{\sigma}.$$

Ciò segue immediatamente dal Teorema di Łos e da $\{x \in X \mid \mathcal{A}_x \vDash \boldsymbol{\sigma}\} \supseteq S(\{\boldsymbol{\sigma}\}) \in F \subseteq U$. □

31.B. Classi elementari.

Teorema 31.6. *Supponiamo che T, T_0 e T_1 siano teorie soddisfacibili tali che*

$$\mathrm{Mod}(T) = \mathrm{Mod}(T_0) \cup \mathrm{Mod}(T_1) \quad e \quad \mathrm{Mod}(T_0) \cap \mathrm{Mod}(T_1) = \emptyset.$$

Allora esistono insiemi finiti di enunciati Σ_0 e Σ_1 tali che $T \cup \Sigma_i$ è un sistema di assiomi per T_i, ($i = 0, 1$).

Dimostrazione. $T_0 \cup T_1$ è insoddisfacibile e quindi, per compattezza, esistono $\Sigma_0 \subseteq T_0$ e $\Sigma_1 \subseteq T_1$ tali che $\Sigma_0 \cup \Sigma_1$ è insoddisfacibile. Chiaramente $\mathrm{Mod}(T_0) \subseteq \mathrm{Mod}(T \cup \Sigma_0) \subseteq \mathrm{Mod}(T)$ e $\mathrm{Mod}(T_1) \subseteq \mathrm{Mod}(T \cup \Sigma_1) \subseteq \mathrm{Mod}(T)$, e poiché $\mathrm{Mod}(T \cup \Sigma_0) \cap \mathrm{Mod}(T \cup \Sigma_1) = \emptyset$,

$$\mathrm{Mod}(T_0) = \mathrm{Mod}(T \cup \Sigma_0) \quad \text{e} \quad \mathrm{Mod}(T_1) = \mathrm{Mod}(T \cup \Sigma_1)$$

come richiesto. □

Quindi otteniamo come corollario il Teorema 3.33 del Capitolo I:

Corollario 31.7. *Supponiamo* $\mathcal{C}_0$ *sia* EC_Δ *ma non* EC *e che* $\mathcal{C}$ *sia* EC. *Se* $\mathcal{C}_0 \subseteq \mathcal{C}$, *allora* $\mathcal{C} \setminus \mathcal{C}_0$ *non è* EC_Δ.

Dimostrazione. Supponiamo che $\mathcal{C}_0 = \mathrm{Mod}(T_0)$ e che $\mathcal{C} = \mathrm{Mod}(\boldsymbol{\sigma})$ per qualche enunciato $\boldsymbol{\sigma}$. Se, per assurdo, $\mathcal{C} \setminus \mathcal{C}_0 = \mathrm{Mod}(T_1)$ per qualche teoria T_1, allora esisterebbe un insieme finito di enunciati Σ_0 tali che $\{\boldsymbol{\sigma}\} \cup \Sigma_0$ è un sistema di assiomi per T, contro la nostra ipotesi. □

In particolare:

Corollario 31.8. *Se* $\mathcal{K}$ *e* $\mathrm{Str}(L) \setminus \mathcal{K}$ *sono* EC_Δ, *allora* $\mathcal{K}$ *e* $\mathrm{Str}(L) \setminus \mathcal{K}$ *sono* EC.

Il seguente risultato generalizza il Teorema 3.10, mostrando che una classe assiomatizzabile può non essere finitamente assiomatizzabile, anche ampliando il linguaggio.

Teorema 31.9. *Sia* Δ *un insieme di enunciati di* L *e siano* $\boldsymbol{\sigma}_n$ *degli enunciati di un linguaggio* $L' \supseteq L$. *Sia* $\mathcal{K} = \mathrm{Mod}(\Sigma)$, *dove* $\Sigma = \Delta \cup \{\boldsymbol{\sigma}_n \mid n \in \omega\}$, *così che* $\mathcal{K}$ *è una classe* $\mathrm{EC}_\Delta(L')$ *e quindi* $\mathrm{PC}_\Delta(L)$. *Supponiamo che*

$$\forall m \in \omega \, (\Delta \cup \{\boldsymbol{\sigma}_n \mid n < m\} \not\models_{L'} \Sigma) \, .$$

Allora $\mathcal{K}$ *non è* $\mathrm{PC}(L)$.

Dimostrazione. Per assurdo supponiamo esista un linguaggio $L'' \supseteq L$ ed un enunciato $\boldsymbol{\tau} \in \mathrm{Sent}(L'')$ tali che $\mathcal{K}$ è la classe delle contrazioni dei modelli di $\boldsymbol{\tau}$,

$$\mathcal{K} = \{\mathcal{A}'' \restriction L \mid \mathcal{A}'' \in \mathrm{Mod}_{L''}(\boldsymbol{\tau})\}.$$

Sostituendo, se necessario, L'' con $L' \cup L''$ possiamo supporre che $L' \subseteq L''$. Poiché $\Sigma \models_{L''} \boldsymbol{\tau}$, per il Corollario 31.2 c'è un $\Sigma_0 \subseteq \Sigma$ finito tale che $\Sigma_0 \models_{L"} \boldsymbol{\tau}$ e quindi c'è un $m \in \omega$ tale che

$$\Delta \cup \{\boldsymbol{\sigma}_n \mid n < m\} \models_{L"} \boldsymbol{\tau}.$$

Poiché $\boldsymbol{\tau} \models_{L''} \Sigma$, per transitività della nozione di conseguenza logica si ha che $\Delta \cup \{\boldsymbol{\sigma}_n \mid n < m\} \models_{L''} \Sigma$ e quindi, per l'Esercizio 30.3, $\Delta \cup \{\boldsymbol{\sigma}_n \mid n < m\} \models_{L'} \Sigma$, contro la nostra ipotesi. □

Corollario 31.10. *Le seguenti classi sono* $\mathrm{EC}_\Delta(L)$ *ma non* $\mathrm{PC}(L)$*:*

(a) *La classe degli insiemi (gruppi, anelli, campi, ordini, algebre di Boole) infiniti, nel linguaggio minimale* $L_\emptyset$ *(rispettivamente in* L_{GRUPPI}, L_{ANELLI}, *etc.)*

(b) *La classe dei gruppi privi di torsione.*

(c) *La classe dei campi di caratteristica* 0.

Quindi, utilizzando il Corollario 31.7 si ha

Corollario 31.11. *Le seguenti classi non sono* PC_Δ*:*

(a) *La classe degli insiemi (gruppi, anelli, campi, ordini, algebre di Boole) finiti.*

(b) *La classe dei gruppi che hanno elementi di torsione.*

(c) *La classe dei campi di caratteristica finita.*

Osservazione 31.12. Il Teorema 31.9 *non dice* che se una classe che ha soltanto strutture infinite allora non è elementare! Infatti ci sono molte classi elementari che hanno solo strutture infinite, per esempio la classe degli ordini lineari densi, la classe delle algebre di Boole prive di atomi, la classe dei corpi non commutativi (Teorema di Wedderburn, vedi pag. 490), etc.

Esercizi

Esercizio 31.13. Dimostrare che l'ultrapotenza $\prod_U \mathbb{R}$ dove U è un ultrafiltro su ω, è un campo non-archimedeo elementarmente equivalente ad $\mathbb{R}$.

Esercizio 31.14. Assumiamo BPI e la seguente versione del Corollario 31.4 per strutture arbitrarie, cioè

(*) Se $\mathcal{A} \in \mathrm{Str}(L)$, dove L è un linguaggio contenente un simbolo di relazione binaria, allora $\mathcal{A}$ è elementarmente equivalente ad ogni sua ultrapotenza.

Sia $R \subseteq A \times A$ tale che $\forall x \in A\, \exists y \in A\ (x\ R\ y)$ e supponiamo che non esista $f\colon A \to A$ tale che $\forall x \in A\ (x\ R\ f(x))$, cioè $S(f) \neq A$ per ogni $f \in A^A$ dove $S(f) = \{a \in A \mid a\ R\ f(a)\}$.

(i) Dimostrare che $\left\{S(f) \mid f \in A^A\right\}$ è chiusa per unioni e genera un ideale proprio J su A.

(ii) Sia U un ultrafiltro che estende $\check{J}$ e ottenere una contraddizione considerando l'ultrapotenza $\prod_U \mathcal{A}$ dove $\mathcal{A} = \langle A, R\rangle$.

(iii) Concludere che BPI + (*) $\Rightarrow$ AC.

Esercizio 31.15. Dimostrare che c'è un gruppo G che contiene un elemento privo di torsione e che è elementarmente equivalente al gruppo delle radici dell'unità $\{z \in \mathbb{C} \mid \exists n \in \mathbb{Z}\,(z^n = 1)\}$.

Note e Osservazioni

Le applicazioni del Teorema di Łos 31.3 utilizzano sempre la scelta, ma l'enunciato, anche esteso a strutture non necessariamente ordinabili, *non implica* AC. Infatti l'esistenza di ultrafiltri non principali non è dimostrabile a partire da MK o da ZF [**Bla77**], quindi se ogni ultrafiltro è principale, allora $\prod_U \mathcal{A}_x \cong \mathcal{A}_{x_0}$ dove $\{x_0\}$ è il generatore di U, e quindi il Teorema di Łos vale per motivi banali. Tuttavia, come mostra l'Esercizio 31.14 (tratto da [**Bel09**]), il Teorema di Łos e BPI implicano AC.

32. Applicazioni della compattezza

32.A. Il metodo dei diagrammi.

32.A.1. *Dimostrazione della Proposizione 6.18.* Dato che strutture isomorfe possono essere identificate, la Proposizione 6.18 segue dal seguente risultato.

Proposizione 32.1. *Sia L un linguaggio con almeno un simbolo di costante $\boldsymbol{c}$, sia T una L-teoria, e sia $\boldsymbol{\varphi}(\boldsymbol{y}, \boldsymbol{x}_1, \dots, \boldsymbol{x}_n)$ una L-formula che è congiunzione di formule atomiche o negazioni di formule atomiche. Le seguenti affermazioni sono equivalenti:*

(a) *c'è una L-formula aperta $\boldsymbol{\theta}$ con le medesime variabili libere di $\boldsymbol{\exists y \varphi}$ tale che*

$$T \models \boldsymbol{\forall \vec{x}}[\boldsymbol{\exists y \varphi} \boldsymbol{\Leftrightarrow} \boldsymbol{\theta}]$$

(b) *se M e N sono modelli di T e se K è una L-struttura contenuta in $M \cap N$, allora*

$$M \vDash \boldsymbol{\exists y \varphi}[a_1, \dots, a_n] \Leftrightarrow N \vDash \boldsymbol{\exists y \varphi}[a_1, \dots, a_n],$$

per ogni $a_1, \dots, a_n \in K$.

Dimostrazione. L'unica direzione non banale è (b)⇒(a). Supponiamo che $\boldsymbol{\varphi}$ sia come sopra, e per semplicità notazionale, scriveremo $\boldsymbol{\psi}$ invece di $\boldsymbol{\exists y \varphi}$. Se $T \models \boldsymbol{\forall \vec{x} \psi}$, allora sia $\boldsymbol{\theta}$ la formula $\boldsymbol{x}_1 \equiv \boldsymbol{x}_1 \boldsymbol{\wedge} \dots \boldsymbol{\wedge} \boldsymbol{x}_n \equiv \boldsymbol{x}_n$, se $n \geq 1$, oppure $\boldsymbol{c} \equiv \boldsymbol{c}$ altrimenti. Analogamente, se $T \models \boldsymbol{\forall \vec{x} \neg \psi}$, allora sia $\boldsymbol{\theta}$ la formula $\boldsymbol{x}_1 \not\equiv \boldsymbol{x}_1 \boldsymbol{\wedge} \dots \boldsymbol{\wedge} \boldsymbol{x}_n \not\equiv \boldsymbol{x}_n$, se $n \geq 1$, oppure $\boldsymbol{c} \not\equiv \boldsymbol{c}$ altrimenti. Quindi possiamo supporre che $\boldsymbol{\exists \vec{x} \psi}$ e $\boldsymbol{\exists \vec{x} \neg \psi}$

□

32.A.2. *Buoni ordini.* Fissiamo un ordinale $\alpha \geq \omega$. Sia

$$\Sigma = \mathrm{EDiag}(\langle \alpha, < \rangle) \cup \{\boldsymbol{c}_{n+1} < \boldsymbol{c}_n \mid n \in \omega\}$$

dove le $\boldsymbol{c}_n$ sono nuovi simboli di costante. Fissato $N \in \omega$, consideriamo la struttura $\mathcal{A}$ di universo α dove

$$\boldsymbol{c}_n^{\mathcal{A}} = \begin{cases} N - n & \text{se } n \leq N, \\ 0 & \text{altrimenti.} \end{cases}$$

Allora $\mathcal{A}$ è un modello per $\mathrm{EDiag}(\langle \alpha, < \rangle) \cup \{\boldsymbol{c}_{n+1} < \boldsymbol{c}_n \mid n < N\}$. Poiché N è arbitrario, ne segue che Σ è finitamente soddisfacibile. Quindi c'è un ordine lineare $\langle A, < \rangle$ mal-fondato tale che $\langle \alpha, < \rangle \preccurlyeq \langle A, < \rangle$.

32.A.3. *Anelli di interi algebrici.*

Teorema 32.2. *Sia R un dominio di integrità in cui ogni elemento appartiene al più ad un numero finito di ideali primi.* Per esempio, l'anello degli interi algebrici in una qualunque estensione dei razionali. *Sia $\boldsymbol{\sigma}$ un enunciato di $L = L_{\text{ANELLI C.}} \cup \{\mathring{a} \mid a \in R\}$*

Allora $\boldsymbol{\sigma}$ *vale in ogni campo che estende* R *se e solo se* $\boldsymbol{\sigma}$ *vale in ogni campo che estende* R/I*, per tutti gli ideali primi* I*, salvo, al più un numero finito.*

Dimostrazione. Il teorema è banalmente vero se R ha una quantità finita di ideali primi, quindi supponiamo altrimenti. Per ipotesi

$$\Sigma_{\text{CAMPI}} \cup \operatorname{Diag}(R) \models \boldsymbol{\sigma}$$

quindi per compattezza possiamo trovare $\boldsymbol{\tau}_1, \dots, \boldsymbol{\tau}_n \in \operatorname{Diag}(R)$ tali che $\Sigma_{\text{CAMPI}} \cup \{\boldsymbol{\tau}_1, \dots, \boldsymbol{\tau}_n\} \models \boldsymbol{\sigma}$. Gli enunciati $\boldsymbol{\tau}_i$ sono formule atomiche, cioè della forma

$$\mathring{a} \equiv \mathring{b}, \quad \mathring{a} + \mathring{b} \equiv \mathring{c}, \quad \mathring{a} \cdot \mathring{b} \equiv \mathring{c}$$

con $a, b, c \in R$, oppure negazioni di formule atomiche. Osserviamo che la formula $\boldsymbol{\neg}(\mathring{a} + \mathring{b} \equiv \mathring{c})$ è conseguenza logica delle due formule $\mathring{a} + \mathring{b} \equiv \mathring{d}$ e $\boldsymbol{\neg}(\mathring{c} \equiv \mathring{d})$, dove $d = a + b \in R$; analogamente $\boldsymbol{\neg}(\mathring{a} \cdot \mathring{b} \equiv \mathring{c})$ è conseguenza logica delle due formule $\mathring{a} \cdot \mathring{b} \equiv \mathring{d}$ e $\boldsymbol{\neg}(\mathring{c} \equiv \mathring{d})$, dove $d = a \cdot b \in R$. Infine le formule della forma $\boldsymbol{\neg}(\mathring{a} \equiv \mathring{b})$ con $a, b \in R \setminus \{0_R\}$ sono conseguenza logica di $\boldsymbol{\neg}(\mathring{c} \equiv \mathbf{0})$, con $c = a - b \in R \setminus \{0_R\}$. Quindi possiamo supporre che gli enunciati $\boldsymbol{\tau}_1, \dots, \boldsymbol{\tau}_n$ siano positivi o della forma $\boldsymbol{\neg}(\mathring{a} \equiv \mathbf{0})$ con $a \in R \setminus \{0_R\}$. Siano $a_1, \dots, a_m$ gli elementi non nulli di R tali che $\mathring{a}_1, \dots, \mathring{a}_n$ sono le costanti che occorrono nei $\boldsymbol{\tau}_i$. Per ipotesi, tutti gli ideali I, eccetto al più un numero finito, non contengono $\{a_1, \dots, a_m\}$. Fissiamo un ideale siffatto, sia $\pi\colon R \to R/I$ la proiezione canonica: questa preserva gli enunciati positivi e poiché $\pi(a_j) \neq 0_{R/I}$ preserva anche gli enunciati della forma $\boldsymbol{\neg}(\mathring{a} \equiv \mathbf{0})$. Allora R/I, o meglio, la sua espansione canonica al linguaggio L, soddisfa $\{\boldsymbol{\tau}_1, \dots, \boldsymbol{\tau}_n\}$, da cui segue che ogni sua estensione che sia un campo soddisfa $\boldsymbol{\sigma}$. □

Ricordiamo che un polinomio $f \in R[X_1, \dots, X_n]$ è irriducibile su R se non può essere fattorizzato come $f = g \cdot h$, con $g, h \in R[X_1, \dots, X_n]$ non costanti. Se f è irriducibile su ogni campo che estende R diremo che è assolutamente irriducibile su R.

Corollario 32.3. *Sia* R *un dominio di integrità in cui ogni elemento appartiene al più ad un numero finito di ideali primi e supponiamo che* $f \in R[X_1, \dots, X_n]$ *sia assolutamente irriducibile su* R*. Allora* f *è assolutamente irriducibile su* R/I*, per tutti gli ideali primi* I*, salvo, al più un numero finito.*

Dimostrazione. È sufficiente verificare che la proprietà "f è irriducibile" è formalizzabile come un enunciato di $L_{\text{ANELLI C.}} \cup \{\mathring{a} \mid a \in R\}$: per ogni coppia (d_1, d_2) tale che $d = d_1 + d_2$ e $1 \leq d_1, d_2$, si definisce l'enunciato $\boldsymbol{\sigma}_{(d_1,d_2)}$ che asserisce che non è possibile una fattorizzazione di f in polinomi di grado d_1 e d_2 quindi si prende la congiunzione di questi enunciati. □

32.B. I teoremi di Löwenheim-Skolem. Il seguente risultato è noto come "Teorema di Löwenheim-Skolem all'insù".

Teorema 32.4. *Se Σ è un insieme di enunciati tale che per ogni $n > 0$ esiste un modello di Σ con almeno n elementi. (In particolare questo vale se Σ ha un modello infinito.) Allora Σ ha modelli di cardinalità arbitrariamente grande,*

$$\forall \kappa \exists \mathcal{B} \in \mathrm{Mod}(\Sigma)\,(\mathrm{card}(\mathcal{B}) \geq \kappa)\,.$$

Dimostrazione. Sia $\tilde{L} = L \cup \{\boldsymbol{d}_\alpha \mid \alpha < \kappa\}$ l'espansione di L mediante nuove costanti e sia $\tilde{\Sigma} = \Sigma \cup \{\boldsymbol{d}_\alpha \not\equiv \boldsymbol{d}_\beta \mid \alpha < \beta < \kappa\} \subseteq \mathrm{Sent}(\tilde{L})$. Sia $\Delta \subseteq \tilde{\Sigma}$ un sottoinsieme finito: allora esiste $n \in \omega$ ed esistono $\{\alpha_i \mid i < n\} \subseteq \kappa$ tali che

$$\Delta \subseteq \Sigma \cup \{\boldsymbol{d}_{\alpha_i} \not\equiv \boldsymbol{d}_{\alpha_j} \mid 0 \leq i < j < n\}.$$

Sia $\mathcal{A} \vDash \Sigma$ un modello con almeno n elementi $a_0, \ldots, a_{n-1}$ e sia $\tilde{\mathcal{A}}$ l'espansione di $\mathcal{A}$ al linguaggio $\tilde{L}$ così definita:

$$\boldsymbol{d}_\alpha^{\tilde{\mathcal{A}}} = \begin{cases} a_i & \text{se } \alpha = \alpha_i \\ a_0 & \text{altrimenti.} \end{cases}$$

È immediato verificare che $\tilde{\mathcal{A}} \vDash \Delta$. Abbiamo quindi dimostrato che $\tilde{\Sigma}$ è finitamente soddisfacibile. Per compattezza c'è un modello $\tilde{\mathcal{B}} \vDash \tilde{\Sigma}$ la cui cardinalità è maggiore o uguale a κ, poiché $\boldsymbol{d}_\alpha^{\tilde{\mathcal{A}}} \neq \boldsymbol{d}_\beta^{\tilde{\mathcal{A}}}$ quando $0 < \alpha < \beta < \kappa$. Sia $\mathcal{B}$ la contrazione di $\tilde{\mathcal{B}}$ ad L. Allora $\mathcal{B}$ è il modello cercato. □

Corollario 32.5. *Sia Σ un insieme di enunciati i cui modelli sono tutti di cardinalità finita. Allora i modelli di Σ hanno cardinalità uniformemente limitata, cioè*

$$\exists n \in \omega \forall \mathcal{A} \in \mathrm{Mod}(\Sigma)\,(\mathrm{card}(\mathcal{A}) \leq n)\,.$$

Il Teorema 32.4 implica, in particolare, che ci sono gruppi (o gruppi privi di torsione, campi di caratteristica fissata, campi algebricamente chiusi, algebre di Boole, ecc.) di cardinalità arbitrariamente grande.

Mettendo assieme questo risultato e il Teorema di Löwenheim-Skolem all'ingiù 30.15, si ottiene:

Corollario 32.6. *Se $\mathcal{A}$ è una struttura infinita, allora*

$$\forall \kappa \geq \max(\mathrm{card}(L), \mathrm{card}(\mathcal{A}))\, \exists \mathcal{B}\ (\mathcal{A} \preccurlyeq \mathcal{B} \wedge \kappa = \mathrm{card}(\mathcal{B}))\,.$$

Dimostrazione. Per il Teorema 30.9 è sufficiente trovare un modello di $\mathrm{EDiag}(\mathcal{A})$ di taglia κ. La teoria $\mathrm{EDiag}(\mathcal{A})$ è soddisfacibile e ha cardinalità $\leq \kappa$, quindi per il Teorema 32.4 ha un modello di cardinalità $\geq \kappa$ che per il Teorema 30.15 ha una sottostruttura elementare di taglia κ. □

32.C. Modelli non-standard dell'aritmetica. Una struttura

$$\mathcal{M} = \langle M; \boldsymbol{S}^{\mathcal{M}}, +^{\mathcal{M}}, \cdot^{\mathcal{M}}, <^{\mathcal{M}}, \mathbf{0}^{\mathcal{M}} \rangle$$

del linguaggio L_{PA} dell'aritmetica di Peano (Sezione 7.E) è standard se è isomorfo ad $\mathbb{N}$, altrimenti si dice **non-standard**.

Esercizio 32.7. La funzione $F\colon \mathbb{N} \to M$ definita da $F(0) = \mathbf{0}^{\mathcal{M}}$ e $F(n+1) = \boldsymbol{S}^{\mathcal{M}}(F(n))$ è un omomorfismo iniettivo di strutture e $\operatorname{ran}(F)$ è un segmento iniziale di M cioè

$$x <^{\mathcal{M}} F(n) \Rightarrow \exists m < n \; (F(m) = x)\,.$$

Quindi un modello $\mathcal{M}$ di PA è formato da due parti: un segmento iniziale isomorfo ad $\mathbb{N}$ che si dice parte standard, ed il suo complemento che si dice parte non-standard. (Naturalmente la parte non-standard è vuota se e solo se il modello è standard.) La parte standard di $\mathcal{M}$ è l'insieme

$$\{t^{\mathcal{M}} \mid t \text{ termine chiuso di } L_{\mathsf{PA}}\}.$$

Quindi un modello $\mathcal{M}$ è non-standard se e solo se c'è un $x \in M$ tale che $\mathcal{M} \vDash \boldsymbol{S}^{(n)}(\mathbf{0}) < x$ per ogni n, dove il termine $\boldsymbol{S}^{(n)}(\mathbf{0})$ è definito induttivamente da $\boldsymbol{S}^{(0)}(\mathbf{0}) = \mathbf{0}$ e $\boldsymbol{S}^{(n+1)}(\mathbf{0}) = \boldsymbol{S}(\boldsymbol{S}^{(n)}(\mathbf{0}))$.

Identificheremo la parte standard di $\mathcal{M}$ con $\mathbb{N}$, cioè $\mathbb{N} \subseteq M$ e useremo $S, +, \cdot, <, 0$ al posto di $\boldsymbol{S}^{\mathcal{M}}, +^{\mathcal{M}}, \cdot^{\mathcal{M}}, <^{\mathcal{M}}, \mathbf{0}^{\mathcal{M}}$. Useremo le lettere $n, m, k, l, \ldots$ per gli interi standard cioè gli elementi di $\mathbb{N}$ e le lettere $a, b, c, d, \ldots$ per gli interi non-standard, cioè per gli elementi della parte non-standard.

Per il Teorema di Löwenheim-Skolem 32.4 ci sono modelli (necessariamente non-standard) più che numerabili di PA, e in questa sezione costruiremo dei modelli non-standard numerabili di PA. Naturalmente se $\mathcal{M}$ è una struttura induttiva, cioè se soddisfa il principio di induzione del second'ordine Ind^2 a pagina 130 della Sezione 7.A, allora $\mathcal{M}$ è standard per il Teorema 7.3, ma Ind^2 non è un enunciato della logica del prim'ordine.

Teorema 32.8. *Ogni teoria soddisfacibile T in un linguaggio $L \supseteq L_{\mathsf{PA}}$ tale che $T \models \mathsf{PA}$ ammette un modello non-standard.*

Dimostrazione. Estendiamo L ad $L' = L \cup \{\boldsymbol{c}\}$ mediante un nuovo simbolo di costante e sia

$$\Sigma = T \cup \{\boldsymbol{S}^{(n)}(\mathbf{0}) < \boldsymbol{c} \mid n \in \omega\}.$$

Se $\Sigma_0 \subseteq \Sigma$ è finito, allora $\Sigma_0 \subseteq T \cup \left\{\boldsymbol{S}^{(n)}(\mathbf{0}) < \boldsymbol{c} \mid n < k\right\}$ per qualche $k \in \omega$. Se $\mathcal{N}$ è un modello di T indichiamo con $\mathcal{N}'$ la sua espansione a L' dove assegniamo a $\boldsymbol{c}$ il valore $\left(\boldsymbol{S}^{(k)}(\mathbf{0})\right)^{\mathcal{N}}$. Allora $\mathcal{N}' \vDash \Sigma_0$ e poiché Σ_0 è arbitrario ne segue che Σ è finitamente soddisfacibile. Per compattezza c'è una L'-struttura $\mathcal{M}'$ tale che $\mathcal{M}' \vDash \Sigma$, quindi la sua contrazione $\mathcal{M} = \mathcal{M}' \restriction L$ è un modello non-standard di T. □

Fissiamo un modello non-standard $\mathcal{M}$ di PA ed un suo intero non-standard a. Per la parte (e) del Teorema 7.15, $a = S(a')$ per qualche a' e poiché $\mathbb{N}$ è chiuso sotto la funzione S, anche a' è non-standard. Dato che $S(a)$ è anch'esso non-standard, possiamo dare la seguente definizione

Definizione 32.9. Se a è un intero non-standard di un modello $\mathcal{M}$ di PA, la sua **galassia** è l'insieme

$$G(a) = \{a + n \mid n \in \mathbb{Z}\}.$$

Chiaramente $G(a)$ è un insieme convesso nell'ordinamento, cioè

$$x, y \in G(a) \wedge (x < z < y) \Rightarrow z \in G(a).$$

Se $G(a_1) = G(a_2)$ e $G(b_1) = G(b_2)$ allora $G(a_1 + b_1) = G(a_2 + b_2)$ quindi la funzione addizione induce un'operazione associativa e commutativa $\oplus$ sulle galassie definita da

$$G(a) \oplus G(b) = G(a + b).$$

Esercizio 32.10. Dimostrare che la funzione G definisce una partizione della parte non standard e che

$$(a_1 \in G(a) \wedge b_1 \in G(b) \wedge a < b \wedge G(a) \cap G(b) = \emptyset) \Rightarrow a_1 < b_1.$$

Poiché l'ordinamento $<$ è totale possiamo quindi definire un ordinamento sulle galassie ponendo

$$G(a) \lhd G(b) \Leftrightarrow G(a) \neq G(b) \wedge a < b.$$

Per la parte (g) del Teorema 7.15, per ogni a non-standard c'è un $b < a$ tale che $2 \cdot b \leq a \leq 2 \cdot b + 1$ e poiché $\mathbb{N}$ è chiuso sotto l'addizione si ha che b è non-standard e che $b \notin G(a)$ e quindi $G(b) \lhd G(a)$. In altre parole: non c'è una galassia minima. Analogamente non c'è una galassia massima, dato che $G(a) \lhd G(a + a)$. Infine, se $G(a_1) \lhd G(a_2)$ fissiamo b tale che $a_1 + b + b \leq a_2 \leq a_1 + b + b + 1$: allora $G(a_1) \lhd G(a_1 + b) \lhd G(a_2)$, cioè tra due galassie c'è sempre una galassia. Quindi l'ordinamento della parte non-standard di $\mathcal{M}$ è isomorfo a $Q \times \mathbb{Z}$ con l'ordinamento lessicografico, dove $\langle Q, \prec \rangle$ è un ordine lineare denso senza primo o ultimo elemento. In particolare, se $\mathcal{M}$ è numerabile l'ordinamento della parte non-standard è $\mathbb{Q} \times \mathbb{Z}$.

32.C.1. *Indefinibilità del prodotto a partire dalla relazione di divisibilità.* Sia $\mathcal{M}$ un modello non-standard di $\mathrm{Th}(\mathbb{N})$. Costruiremo una biezione $F\colon M \to M$ che è un automorfismo per la struttura $\mathcal{M}' = \langle M, | \rangle$ ma tale che $F(x \cdot y) \neq F(x) \cdot F(y)$, per opportuni $x, y \in M$. Ogni $x \in M$ può essere fattorizzato in un unico modo come $2^y \cdot z$, dove $2 \nmid z$. Per semplicità notazionale poniamo $A(x) = y$ e $B(x) = z$, cioè

$$x = 2^{A(x)} \cdot B(x).$$

Fissiamo ora un intero non standard $K \in M$ e definiamo

$$F(x) = \begin{cases} 2^{A(x)+1} \cdot B(x) & \text{se } \exists n \in \mathbb{Z}\ (A(x) = 2 \cdot K + n), \\ x & \text{altrimenti.} \end{cases}$$

(La funzione F non è definibile in $\mathcal{M}$, ma questo è irrilevante.) Chiaramente

$$x_1 \mid x_2 \Leftrightarrow (A(x_1) \leq A(x_2) \wedge B(x_1) \mid B(x_2))$$

e quindi F è un isomorfismo della struttura $\mathcal{M}' = \langle M, | \rangle$, ma $F(2^{K+K}) \neq F(2^K) \cdot F(2^K)$.

32.D. Il teorema di Ramsey finito. Nella sezione 26 abbiamo dimostrato il Teorema 26.1 di Ramsey nel caso infinito: per ogni insieme infinito A, se coloriamo gli elementi di $[A]^r$ con k colori, allora c'è sempre un $H \subseteq A$ infinito tale che $[H]^r$ è monocromatico. Mediante il Teorema di Compattezza possiamo dimostrare la sua versione finita.

Teorema 32.11 (Teorema di Ramsey nel caso finito)**.** *Per ogni $r, k, n > 0$ esiste un m tale che ogni colorazione $f\colon [m]^r \to k$ ammette un sottoinsieme $H \subseteq m$ monocromatico di cardinalità n.*

Dimostrazione. Per semplicità notazionale supponiamo $r = 2$. Fissiamo $k \geq 2$. Consideriamo il linguaggio L che ha k predicati 2-ari $\boldsymbol{C}_0, \dots, \boldsymbol{C}_{k-1}$ che rappresentano i colori. Consideriamo l'insieme degli enunciati che asseriscono che ogni coppia non ordinata di oggetti è colorata con un unico colore e che ci sono infiniti elementi:

(i) $\boldsymbol{\forall x \forall y}\,(\boldsymbol{C}_h(\boldsymbol{x}, \boldsymbol{y}) \boldsymbol{\Rightarrow} \boldsymbol{C}_h(\boldsymbol{y}, \boldsymbol{x}))$, per tutti gli $h < k$,

(ii) $\boldsymbol{\forall x \forall y}\left(\boldsymbol{x} \not\equiv \boldsymbol{y} \boldsymbol{\Rightarrow} \bigvee_{h \leq k} \boldsymbol{C}_h(\boldsymbol{x}, \boldsymbol{y})\right)$,

(iii) $\boldsymbol{\neg \exists x \exists y}\,(\boldsymbol{C}_h(\boldsymbol{x}, \boldsymbol{y}) \boldsymbol{\wedge} \boldsymbol{C}_i(\boldsymbol{x}, \boldsymbol{y}))$, per tutti gli $h < i < k$,

(iv) $\boldsymbol{\varepsilon}_{\geq n}$, per $n > 1$, dove $\boldsymbol{\varepsilon}_{\geq n}$ è l'enunciato definito a pagina 15.

Per (iv) se una L-struttura $\mathcal{A} = \left\langle A, \boldsymbol{C}_0^{\mathcal{A}}, \dots, \boldsymbol{C}_{k-1}^{\mathcal{A}} \right\rangle$ soddisfa Σ allora A è infinito e posto $\bar{C}_i = \{\{x, y\} \in [A]^2 \mid (x, y) \in \boldsymbol{C}_i^{\mathcal{A}}\}$, gli insiemi $\bar{C}_0, \dots, \bar{C}_{k-1}$ sono disgiunti e $\bar{C}_0 \cup \dots \cup \bar{C}_{k-1} = [A]^2$. Viceversa, se A è infinito e $[A]^2$ è colorato con k colori, cioè ci sono $\bar{C}_0, \dots, \bar{C}_{k-1}$ sottoinsiemi disgiunti di A tali che $\bar{C}_0 \cup \dots \cup \bar{C}_{k-1} = [A]^2$, allora posto $\boldsymbol{C}_i^{\mathcal{A}} = \{(x, y) \mid \{x, y\} \in \bar{C}_i\}$ si ha che $\mathcal{A} \vDash \Sigma$. Fissiamo un modello $\mathcal{A}$ di Σ. Per il Teorema 26.1 di Ramsey nel caso infinito c'è un sottoinsieme omogeneo infinito di A. Per ogni n fissato, $\mathcal{A}$ soddisfa l'enunciato $\boldsymbol{\varphi}_n$ che dice:

($\boldsymbol{\varphi}_n$) Ci sono elementi distinti $\boldsymbol{x}_0, \dots, \boldsymbol{x}_{n-1}$ tali che $[\{\boldsymbol{x}_0, \dots, \boldsymbol{x}_{n-1}\}]^2$ è monocromatico di colore $\boldsymbol{C}_h$, per qualche $h < k$

in simboli

$$\exists \boldsymbol{x}_0 \ldots \exists \boldsymbol{x}_{n-1} \Big[\bigwedge_{i<j<n} \boldsymbol{x}_i \not\equiv \boldsymbol{x}_j \wedge \big(\bigvee_{h<k} \bigwedge_{i<j<n} \boldsymbol{C}_h(\boldsymbol{x}_i, \boldsymbol{x}_j) \big) \Big].$$

Essendo $\mathcal{A}$ arbitrario in $\mathrm{Mod}(\Sigma)$ questo prova che

$$\Sigma \models \boldsymbol{\varphi}_n$$

per ogni n. Per il Teorema di Compattezza, fissato n possiamo trovare un $\Sigma' \subset \Sigma$ finito tale che $\Sigma' \models \boldsymbol{\varphi}_n$. Sia m massimo tale che $\boldsymbol{\varepsilon}_{\geq m} \in \Sigma'$. Una colorazione con k colori di $[m]^2$ induce un modello $\mathcal{A}'$ di Σ' di cardinalità m. Poiché $\mathcal{A}' \vDash \boldsymbol{\varphi}_n$, ne consegue che c'è un $H \subset m$ di cardinalità n che è monocromatico. □

Esercizi

Esercizio 32.12. Dimostrare che la relazione di conseguenza logica è un pre-ordine su $\mathscr{P}(\mathrm{Sent}(L))$ i cui elementi minimali sono gli insiemi Σ non soddisfacibili.

Esercizio 32.13. Dimostrare che un gruppo abeliano è ordinabile (vedi pag. 77) se e solo se è privo di torsione

Esercizio 32.14. Sia G un gruppo tale che elementi di torsione finita arbitrariamente elevata, cioè

$$\forall n \, \exists g \in G \ (n \leq o(g) < \infty) \, .$$

Dimostrare che c'è un gruppo H con un elemento privo di torsione e tale che $G \preccurlyeq H$.

Esercizio 32.15. Dimostrare che un grafo è k-colorabile se e solo se ogni suo sottografo finito è k-colorabile.

Esercizio 32.16. Generalizzare il Corollario 31.8 dimostrando che se $\mathcal{K}$ e $\mathrm{Str}(L) \setminus \mathcal{K}$ sono PC_Δ, allora $\mathcal{K}$ e $\mathrm{Str}(L) \setminus \mathcal{K}$ sono PC.

Esercizio 32.17. Dimostrare in dettaglio i Corollari 31.10 e 31.11.

Esercizio 32.18. Ricordiamo (vedi pagina **??**) che un ordine lineare è omogeneo se presi due intervalli aperti, questi sono isomorfi; è ultraomogeneo se ogni automorfismo parziale può essere esteso ad un automorfismo. Dimostrare che la classi degli ordini lineari omogenei e ultraomogenei sono, rispettivamente, PC e PC_Δ nel linguaggio L_{ORDINI}.

Esercizio 32.19. Dimostrare che la classe degli ordini mal-fondati è pseudo-elementare generalizzata (PC_Δ) nel linguaggio L_{ORDINI}, ma non è pseudo-elementare (PC) cioè non è finitamente assiomatizzabile in nessun linguaggio che estenda L_{ORDINI}.

Esercizio 32.20. Dimostrare che le seguenti classi di strutture non sono PC_Δ.

(i) Le strutture (insiemi, gruppi, anelli, ordini, ecc.) finite.

(ii) I gruppi di torsione.

(iii) I campi di caratteristica positiva.

(iv) Gli ordini ben fondati.

Esercizio 32.21. Sia U un ultrafiltro su un insieme $I \neq \emptyset$ e siano $\mathcal{A}_i \in \mathrm{Str}(L)$, con $i \in I$. Dimostrare che se $L' \subseteq L$ allora

$$\big(\prod_U \mathcal{A}_i\big) \restriction L' = \prod_U \big(\mathcal{A}_i \restriction L'\big) \, .$$

Concludere che una classe PC_Δ è chiusa per ultraprodotti.

Esercizio 32.22. Dimostrare che ogni campo ordinato ha un'estensione elementary non archimedea.

Esercizio 32.23. Dedurre il Teorema 26.1 di Ramsey nel caso infinito dalla sua versione nel caso finito (Teorema 32.11).

Esercizio 32.24. Dimostrare che un gruppo abeliano è semplice se è isomorfo a $\mathbb{Z}/p\mathbb{Z}$ per qualche primo p. Concludere che non esiste alcun sistema di assiomi Σ in un qualche linguaggio $L \supseteq L_{\text{SEMIGRUPPI}}$ tale che

$$\{\mathcal{G} \restriction L_{\text{SEMIGRUPPI}} \mid \mathcal{G} \in \text{Mod}(\Sigma)\}$$

è la classe dei gruppi semplici.

Esercizio 32.25. Dimostrare che la classe dei grafi connessi non è assiomatizzabile.

Esercizio 32.26. Generalizzare la Proposizione 30.13 dimostrando che se

$$\left(\langle \mathcal{A}_x \mid x \in D\rangle, \langle \pi_{x,y} \mid x, y \in D \wedge x \leq y\rangle\right)$$

è un sistema diretto superiormente di strutture e mappe elementari, allora

$$\pi_{y,\infty} \colon \mathcal{A}_x \to \varinjlim_{x \in D} \mathcal{A}_x$$

è elementare, per ogni $y \in D$.

Esercizio 32.27. Dimostrare che se Σ è un insieme di enunciati in un linguaggio arbitrario che ha modelli finiti di cardinalità arbitrariamente grande, allora ha un modello $\mathcal{M}$ il cui universo è immagine suriettiva dei reali. Quindi se assumiamo AC (o anche solo che $\mathbb{R}$ sia bene ordinabile) $\text{card}(\mathcal{M}) \leq 2^{\aleph_0}$.

Dare un esempio di una teoria (in un linguaggio necessariamente più che numerabile) che ha modelli finiti di cardinalità arbitrariamente grande, che ha un modello di cardinalità del continuo, ma non ha nessun modello infinito di cardinalità infinita strettamente minore della cardinalità di $\mathbb{R}$.

Esercizio 32.28. In questo esercizio daremo una nuova dimostrazione del Teorema 23.26 di Stone.

Sia L il linguaggio $\{\mathring{Y}, \mathring{\mathcal{F}}, \mathring{\in}, \mathring{C}, \mathring{U}, \mathring{I}\}$ dove

- $\mathring{Y}, \mathring{\mathcal{F}}$ sono simboli di relazione 1-arie,
- $\mathring{\in}, \mathring{C}$ sono simboli di relazione 2-arie,
- $\mathring{U}, \mathring{I}$ sono simboli di relazione 3-arie.

Dare un insieme finito di assiomi Σ nel linguaggio L tale che ogni suo modello è isomorfo ad una struttura con universo $Y \cup \mathcal{F}$, dove $Y \neq \emptyset$, $Y \cap \mathcal{F} = \emptyset$, $\mathcal{F} \subseteq \mathscr{P}(Y)$ è una sub-algebra, e $\mathring{Y}, \mathring{\mathcal{F}}, \mathring{\in}$ sono interpretate come Y, $\mathcal{F}$ e l'appartenenza tra elementi di Y ed elementi di $\mathcal{F}$ e i simboli $\mathring{C}, \mathring{U}, \mathring{I}$ sono interpretati, rispettivamente, come i grafi delle funzioni complementi, unione e intersezione in $\mathcal{F}$.

Sia B un'algebra di Boole e sia $\tilde{L} = L \cup \{\mathring{b} \mid b \in B\} \cup \{\curlyvee, \curlywedge, \mathbf{0}, \mathbf{1}\}$. Dimostrare che $\text{Diag}(B) \cup \Sigma$ è un insieme finitamente soddisfacibile di $\tilde{L}$-enunciati. Concludere che B è isomorfa ad una sub-algebra di $\mathscr{P}(Y)$, per qualche insieme Y.

Esercizio 32.29. Usare l'Esercizio 8.76 della Sezione 8 per dimostrare che ogni reticolo distributivo è isomorfo ad un sotto-reticolo di qualche $\mathscr{P}(X)$.

Esercizio 32.30. Dimostrare il Teorema 5.18 dei Quattro Colori per le carte piane con un numero arbitrario (vale a dire: infinito) di regioni, cioè: ogni grafo che non contiene K_5 o $\text{K}_{3,3}$ come minore è 4-colorabile.

Esercizio 32.31. Se $(P, \leq)$ è un insieme parzialmente ordinato, un $I \subseteq P$ si dice **indipendente** se

$$\forall x, y \in P\, [x \neq y \Rightarrow (x \not\leq y \wedge y \not\leq x)]\,.$$

Un insieme indipendente interseca una catena in al più un punto, quindi se P è unione di n catene, allora ogni insieme indipendente ha cardinalità $\leq n$. Dilworth nel 1950 dimostrò il converso per gli ordini parziali *finiti*.

Teorema (Dilworth)**.** *Sia $(P, \leq)$ un ordine parziale finito tale che ogni insieme indipendente ha cardinalità $\leq n$. Allora ci sono delle catene $C_0, \ldots, C_{n-1} \subseteq P$ tali che $\bigcup_{i<n} C_i = P$.*

Generalizzare questo risultato a *tutti* gli insiemi parzialmente ordinati.

Esercizio 32.32. Dimostrare che:

(i) l'insieme degli elementi di torsione $\mathrm{Tor}(G)$, di un gruppo (vedi pagina 76)

(ii) la parte divisibile di un gruppo abeliano (vedi pag. 76)

non sono definibili nel linguaggio dei gruppi.

Esercizio 32.33. Sia T una teoria di $L' \supseteq L$. Dimostrare che $\mathcal{M} \in \mathrm{Str}(L)$ è immergibile in un modello di T se e solo se ogni sottostruttura finitamente generata di $\mathcal{M}$ è immergibile in un modello di T.

In particolare:

- un semigruppo (o più in generale una magma, vedi pagina **??**) è immergibile in un gruppo (abeliano, ordinato, divisibile, ecc.) se e solo se ogni suo sottosemigruppo finitamente generato lo è,
- un anello (o più in generale un semianello, Definizione 5.5) è immergibile in un campo (ordinato, differenziale, ecc.) se e solo se ogni suo sottoanello finitamente generato lo è.

33. Categoricità

Una teoria si dice

- **categorica** se ammette un unico modello (a meno di isomorfismi);
- κ-**categorica** se ha un modello bene ordinabile di cardinalità κ, dove κ è un cardinale infinito, e questo modello è unico a meno di isomorfismi.

Per il Teorema di Lowenheim-Skolem all'insù, se T è categorica, allora il suo unico modello è finito.

Teorema 33.1. *Sia L un linguaggio bene ordinabile di cardinalità $\leq \kappa$ e sia T una teoria κ-categorica che ha solo modelli infiniti. Allora T è completa.*

Dimostrazione. Se $\boldsymbol{\sigma} \in \mathrm{Sent}(L)$ testimonia che T non è completa, siano $\mathcal{A}$ e $\mathcal{B}$ modelli di T che soddisfano $\boldsymbol{\sigma}$ e $\boldsymbol{\neg\sigma}$, rispettivamente. Per ipotesi $\mathcal{A}$ e $\mathcal{B}$ sono infiniti, per il Teorema 32.4 di Löwenheim-Skolem all'insù possiamo supporre che $\mathrm{card}(\mathcal{A}) = \mathrm{card}(\mathcal{B}) \geq \kappa$ e per il Teorema 30.15 di Löwenheim-Skolem all'ingiù possiamo supporre che $\mathrm{card}(\mathcal{A}) = \mathrm{card}(\mathcal{B}) = \kappa$. Ma quindi $\mathcal{A} \cong \mathcal{B}$, contraddicendo l'assunzione che $\mathcal{A} \vDash \boldsymbol{\sigma}$ e $\mathcal{B} \vDash \boldsymbol{\neg\sigma}$. □

Osservazione 33.2. Le ipotesi che T abbia solo modelli infiniti e che il linguaggio abbia taglia $\leq \kappa$ sono necessarie (Esercizio33.8–33.9).

33.A. Esempi.

33.A.1. *Insiemi infiniti.* La teoria T che ha per assiomi gli enunciati $\boldsymbol{\varepsilon}_{\geq n}$ definiti a pagina 15 è κ-categorica per ogni κ, dato che un modello di T di cardinalità κ è semplicemente un insieme di cardinalità κ.

33.A.2. *Gruppi abeliani.* Per ogni cardinale infinito κ i gruppi $\bigoplus_{\alpha<\kappa}\mathbb{Z}$ e $\bigoplus_{\alpha<\kappa}\mathbb{Z}/2\mathbb{Z}$ sono di cardinalità κ e non sono mai isomorfi. Quindi la teoria dei gruppi abeliani non è mai κ-categorica.

33.A.3. *Ordini lineari densi senza né primo né ultimo elemento.* Ricordiamo che un ordine lineare (stretto) si dice denso se tra due punti c'è sempre un punto. La classe degli ordini lineari densi, senza né primo né ultimo elemento è elementare e $\mathbb{Q}$ ed $\mathbb{R}$ sono esempi di ordini siffatti. Per il Teorema 10.32, la teoria degli ordini lineari densi, senza né primo né ultimo elemento è ω-categorica e quindi è completa. Per l'Esercizio **??**, questa teoria non è $2^{\aleph_0}$-categorica: infatti si dimostra che per ogni cardinale più che numerabile κ è possibile costruire esempi di ordini lineari densi senza né primo né ultimo elemento di cardinalità κ e non isomorfi.

33.A.4. *Campi algebricamente chiusi.* ACF_p è la teoria dei campi algebricamente chiusi di caratteristica p, dove p è un numero primo oppure $p = 0$. (Il linguaggio è quello per gli anelli $L_{\text{ANELLI-1}}$.) Sia $\mathbb{F} \vDash \mathrm{ACF}_p$, sia $\mathbb{F}'$ il suo sottocampo primo e sia $X \subseteq \mathbb{F}$ una base di trascendenza di $\mathbb{F}$ su $\mathbb{F}'$. Osserviamo che $\mathbb{F}'$ è $\mathbb{Z}/p\mathbb{Z}$, se p è primo, o $\mathbb{Q}$ se $p = 0$; quindi $\mathbb{F}'$ è numerabile. La base di trascendenza X esiste per il Lemma di Zorn ed ha la cardinalità di $\mathbb{F}$, se $\mathbb{F}$ è più che numerabile. Se X e Y sono due basi di trascendenza per i campi $\mathbb{F}$ e $\mathbb{G}$ di ugual caratteristica e se $\pi\colon X \to Y$ è una biezione, allora π si estende ad un isomorfismo $\pi\colon \mathbb{F} \to \mathbb{G}$. Quindi, se $\mathbb{F}$, $\mathbb{G}$ sono campi algebricamente chiusi di ugual caratteristica e più che numerabili, allora hanno basi di trascendenza di ugual cardinalità e quindi sono isomorfi. Abbiamo quindi verificato che ACF_p è κ-categorica, se $\kappa > \omega$.

33.B. Applicazioni.

33.B.1. *Principio di Lefschetz.* Dall'Esempio 5.D.4 del Capitolo I e dal Corollario 31.2 otteniamo

> Se $\boldsymbol{\sigma}$ è un enunciato nel linguaggio degli anelli $L_{\text{ANELLI-1}}$ che vale in ogni campo di caratteristica 0, allora vale in ogni campo di caratteristica p, con p sufficientemente elevato.

In altre parole

$$\mathrm{ACF}_0 \models \boldsymbol{\sigma} \quad \Leftrightarrow \quad \exists n \forall p > n \, (p \text{ primo } \Rightarrow \mathrm{ACF}_p \models \boldsymbol{\sigma}) \, .$$

Una generalizzazione di questo è il seguente *Principio di Lefschetz*:

Teorema 33.3. *Sia* $\boldsymbol{\sigma}$ *un enunciato di* $L_{\text{ANELLI-1}}$. *Allora* $\boldsymbol{\sigma}$ *vale in un campo algebricamente chiuso di caratteristica* 0 *se e solo se vale in campi algebricamente chiusi di caratteristica* p, *con* p *primo arbitrariamente grande.*

Dimostrazione. Sia ACF_p la teoria dei campi algebricamente chiusi di caratteristica p, con p primo oppure $p = 0$. Se $\mathbb{F}$ un campo algebricamente

chiuso di caratteristica 0 e $\mathbb{F} \vDash \boldsymbol{\sigma}$, allora $\mathrm{ACF}_0 \models \boldsymbol{\sigma}$ per la completezza di ACF_0. Quindi per quanto sopra $\mathrm{ACF}_p \models \boldsymbol{\sigma}$, per tutti i primi p sufficientemente grandi.

Vice versa, supponiamo che

$$\forall n \in \mathbb{N} \exists p > n \exists \mathbb{F} \text{ campo algebricamente chiuso di caratteristica } p \text{ e } \mathbb{F} \vDash \boldsymbol{\sigma}.$$

Osserviamo che se $\mathbb{F}$ è algebricamente chiuso di caratteristica p e $\mathbb{F} \vDash \boldsymbol{\sigma}$, allora, per la completezza della teoria dei campi algebricamente chiusi di caratteristica p, ogni altro campo $\mathbb{F}'$ algebricamente chiuso di caratteristica p soddisfa $\boldsymbol{\sigma}$. Fissiamo un'enumerazione $\langle p_n \mid n \in \omega \rangle$ di tutti i numeri primi e sia $\mathbb{F}_n$ un campo algebricamente chiuso di caratteristica p_n. Sia $X = \{n \in \omega \mid \mathbb{F}_n \vDash \boldsymbol{\sigma}\}$ e sia U un ultrafiltro su ω tale che $X \in U$. Per il Teorema 31.3 di Łos $\prod_U \mathbb{F}_n$ è un campo algebricamente chiuso di caratteristica 0 che soddisfa $\boldsymbol{\sigma}$ e quindi $\mathrm{ACF}_0 \models \boldsymbol{\sigma}$. □

33.B.2. *Variabili complesse.* Se A è un anello, una funzione $f\colon A^n \to A^n$ si dice polinomiale se $f = (f_1, \dots, f_n)$, con $f_i \in A[X_1, \dots, X_n]$. Il grado di f è $\max(\deg(f_1), \dots, \deg(f_n))$. Dimostreremo il seguente

Teorema 33.4 (Ax)**.** *Ogni funzione polinomiale iniettiva $f\colon \mathbb{C}^n \to \mathbb{C}^n$ è suriettiva.*

Osserviamo che per ogni $n, d > 0$ c'è un enunciato $\boldsymbol{\sigma}_{n,d}$ del linguaggio degli anelli tale che $A \vDash \boldsymbol{\sigma}_{n,d}$ se e solo se

ogni funzione polinomiale iniettiva $A^n \to A^n$ di grado $\leq d$ è suriettiva,

per ogni anello commutativo unitario A. Quindi vogliamo dimostrare che per ogni $n, d > 0$

$$\mathbb{C} \vDash \boldsymbol{\sigma}_{n,d}$$

o, equivalentemente, che $\mathrm{ACF}_0 \models \boldsymbol{\sigma}_{n,d}$. Per il Principio di Lefschetz è sufficiente dimostrare che $\mathrm{ACF}_p \models \boldsymbol{\sigma}_{n,d}$ per primi p arbitrariamente grandi: dimostreremo che ciò vale per *ogni* p.

Sia $\mathbb{F}$ un campo algebricamente chiuso di caratteristica p: vogliamo verificare che $\mathbb{F} \vDash \boldsymbol{\sigma}_{n,d}$. Per completezza di ACF_p, possiamo supporre che $\mathbb{F}$ sia $\overline{\mathbb{Z}/p\mathbb{Z}}$, la chiusura algebrica di $\mathbb{Z}/p\mathbb{Z}$. Allora $\mathbb{F} = \bigcup_k \mathbb{F}_k$ dove gli $\mathbb{F}_k$ sono campi finiti (non algebricamente chiusi) di caratteristica p. Sia $f\colon \mathbb{F}^n \to \mathbb{F}^n$ una funzione polinomiale iniettiva di grado $\leq d$ e sia $\vec{b} \in \mathbb{F}^n$: vogliamo mostrare che c'è un $\vec{a}$ tale che $f(\vec{a}) = \vec{b}$. Sia k sufficientemente elevato tale che tutti i coefficienti di f e $b_1, \dots, b_n$ sono in $\mathbb{F}_k$. Quindi $f \restriction \mathbb{F}_k^n\colon \mathbb{F}_k^n \to \mathbb{F}_k^n$ è una funzione polinomiale iniettiva: ma ogni funzione iniettiva da un insieme finito in sé stesso è suriettiva, quindi esistono $a_1, \dots, a_n \in \mathbb{F}_k \subseteq \mathbb{F}$ tali che $f(\vec{a}) = \vec{b}$.

Esercizi

Esercizio 33.5. Dimostrare che se $f_1, \dots, f_n \in \mathbb{Q}[x_1, \dots, x_m]$ il sistema

$$\begin{cases} f_1(x_1, \dots, x_m) \\ \vdots \\ f_n(x_1, \dots, x_m) \end{cases}$$

ha al più k soluzioni in un'estensione di $\mathbb{Q}$ se e solo se il sistema ha al più k soluzioni in un campo di caratteristica p, per tutti i primi p salvo un numero finito.

Ripetere l'esercizio quando *al più* è sostituito da *esattamente* e da *al meno*.

Esercizio 33.6. Verificare che ACF_p non è $\aleph_0$-categorica.

Esercizio 33.7. Assumere AC e dimostrare che le seguenti teorie sono κ-categoriche per $\kappa > \omega$, ma non sono ω-categoriche:

(i) la teoria degli spazi vettoriali su un campo infinito numerabile $\Bbbk$, (Sezione 5.D.6),

(ii) la teoria dei gruppi abeliani divisibili e privi di torsione,

(iii) le teorie $\Sigma_{(\mathbb{N},S)}$, $\Sigma_{(\mathbb{N},<)}$, $\Sigma_{(\mathbb{N},+)}$ della Sezione 6.A,

(iv) la teoria dei gruppi abeliani divisibili ordinati,

(v) la teoria degli $\mathbb{Z}$-gruppi (vedi pag. 78).

In particolare, questi sono esempi di teorie complete.

Esercizio 33.8. Assumere AC e sia $\Bbbk$ è un campo finito. Dimostrare che:

(i) la teoria dei $\Bbbk$-spazi vettoriali è κ-categorica per ogni $\kappa \geq \omega$, ma non è completa;

(ii) la teoria dei $\Bbbk$-spazi vettoriali di dimensione infinita (si veda Esercizio 5.38) è completa.

Esercizio 33.9. Sia L il linguaggio per gli ordini esteso con un simbolo $\mathring{r}$ per ogni reale $r \in \mathbb{R}$. Sia T la L-teoria con gli assiomi per gli ordini lineari densi e

- $\mathring{0} \equiv \mathring{1} \Rightarrow \mathring{r} \equiv \mathring{0}$ per ogni $r \in \mathbb{R}$,
- $\mathring{0} \not\equiv \mathring{1} \Rightarrow \mathring{r} < \mathring{s}$ per ogni $r < s$ con $r, s \in \mathbb{R}$.

Dimostrare che T è ω- categorica, ma non completa.

Esercizio 33.10. Dimostrare che gli ordini lineari omogenei (vedi pag. 57) non sono assiomatizzabili nel linguaggio contenente soltanto il simbolo $\leq$ (Esercizio 3.59, Capitolo I).

34. Sintassi

34.A. Derivazioni. Un **assioma logico** di un linguaggio L è una formula di L che è:

- una tautologia, oppure
- un assioma di sostituzione (Sezione 29.C.2), oppure
- un assioma di uguaglianza (Sezione 29.C.3).

Richiamiamo due regole di derivazione viste rispettivamente a pagina 8 e a pagina 446.

Regola del *modus ponens*. Da $\boldsymbol{\psi \Rightarrow \varphi}$ e $\boldsymbol{\psi}$ si deduce $\boldsymbol{\varphi}$.

e introduciamo la seguente

Regola del quantificatore esistenziale. Se $\boldsymbol{x}$ non occorre libera in $\boldsymbol{\psi}$, allora da $\boldsymbol{\varphi \Rightarrow \psi}$ si deduce $\boldsymbol{\exists x \varphi \Rightarrow \psi}$.

Una **derivazione a partire da** Γ è una successione finita di L-formule $\langle \boldsymbol{\varphi}_0, \dots, \boldsymbol{\varphi}_n \rangle$ tale che per ogni $i \leq n$:

(1) $\boldsymbol{\varphi}_i \in \Gamma$, oppure

(2) $\boldsymbol{\varphi}_i$ è un assioma logico, oppure

(3) esistono $j, k \leq i$ tali che $\boldsymbol{\varphi}_i$ è ottenuta da $\boldsymbol{\varphi}_j$ e $\boldsymbol{\varphi}_k$ mediante la regola (MP); oppure

(4) $\boldsymbol{\varphi}_i$ è ottenuta da $\boldsymbol{\varphi}_j$ mediante la regola del quantificatore esistenziale per qualche $j < i$.

Diremo che $\boldsymbol{\varphi}$ è **derivabile da** Γ (ovvero che $\boldsymbol{\varphi}$ è un **teorema** di Γ) nel linguaggio L, in simboli

$$\Gamma \vdash_L \boldsymbol{\varphi},$$

se esiste $\langle \boldsymbol{\varphi}_0, \dots, \boldsymbol{\varphi}_n \rangle$, derivazione da Γ in L, tale che $\boldsymbol{\varphi} = \boldsymbol{\varphi}_n$. Quando il linguaggio L è chiaro dal contesto scriveremo semplicemente $\Gamma \vdash \boldsymbol{\varphi}$; se $\Gamma = \{\boldsymbol{\psi}\}$ o $\Gamma = \emptyset$, scriveremo, rispettivamente, $\boldsymbol{\psi} \vdash \boldsymbol{\varphi}$ e $\vdash \boldsymbol{\varphi}$. Se $\boldsymbol{\varphi} \vdash \boldsymbol{\psi}$ e $\boldsymbol{\psi} \vdash \boldsymbol{\varphi}$ diremo che $\boldsymbol{\varphi}$ e $\boldsymbol{\psi}$ sono derivabili l'una dall'altra, ovvero che $\boldsymbol{\varphi}$ e $\boldsymbol{\psi}$ sono **equiderivabili**. Una teoria T è **sintatticamente chiusa** se

$$T \vdash \boldsymbol{\sigma} \quad \Rightarrow \quad \boldsymbol{\sigma} \in T,$$

per ogni enunciato $\boldsymbol{\sigma}$.

Osservazioni 34.1. (a) Se $\Gamma \vdash_L \boldsymbol{\varphi}$, $\Gamma \subseteq \Gamma'$, $L \subseteq L'$ e $\Gamma' \subseteq \mathrm{Fml}(L')$, allora $\Gamma' \vdash_{L'} \boldsymbol{\varphi}$.

(b) La relazione $\vdash$ è transitiva: se $\Gamma \vdash \boldsymbol{\varphi}$ e $\boldsymbol{\varphi} \vdash \boldsymbol{\psi}$, allora $\Gamma \vdash \boldsymbol{\psi}$.

(c) $\Gamma \vdash \boldsymbol{\varphi}$ se e solo se $\Gamma_0 \vdash \boldsymbol{\varphi}$ per qualche $\Gamma_0 \subseteq \Gamma$ finito.

Le due regole di derivazione (la regola del *Modus Ponens* e quella del quantificatore esistenziale) sono formulate utilizzando il connettivo $\boldsymbol{\Rightarrow}$ che è, nella nostra trattazione formale dei linguaggi del prim'ordine, un'abbreviazione di una formula contenente $\boldsymbol{\neg}$ e $\boldsymbol{\vee}$. In altre parole: la regole (3) e (4) nella definizione di derivazione dovrebbero essere formulate così:

(3′) esistono $j, k < i$ tali che $\boldsymbol{\varphi}_j = \boldsymbol{\neg \varphi}_k \boldsymbol{\vee} \boldsymbol{\varphi}_i$,

(4′) $\boldsymbol{\varphi}_i = \boldsymbol{\neg \exists x \varphi \vee \psi}$, $\boldsymbol{x}$ non occorre libera in $\boldsymbol{\psi}$ e $\boldsymbol{\neg \varphi \vee \psi} = \boldsymbol{\varphi}_j$ per qualche $j < i$.

Tuttavia questa presentazione delle due regole di derivazione risulta esser meno chiara di quella data, per cui non verrà mai utilizzata. Un discorso analogo vale per gli altri due connettivi $\boldsymbol{\wedge}$ e $\boldsymbol{\Leftrightarrow}$, quanto per il quantificatore universale $\boldsymbol{\forall}$.

Per 29.C.2, 29.C.3 e il Corollario 29.15, ogni assioma logico è logicamente valido.

Il seguente **Teorema di Correttezza** mostra che le derivazioni generano conseguenze logiche.

Teorema 34.2 (Gödel)**.** *Se* $\Gamma \subseteq \mathrm{Fml}$ *e* $\boldsymbol{\varphi} \in \mathrm{Fml}$*, allora*

$$\Gamma \vdash \boldsymbol{\varphi} \Rightarrow \Gamma \models \boldsymbol{\varphi}.$$

Dimostrazione. Supponiamo $\mathcal{A} \vDash \Gamma$ e sia $\langle \boldsymbol{\varphi}_0, \dots, \boldsymbol{\varphi}_n \rangle$ una derivazione da Γ. È sufficiente verificare per induzione su $i \leq n$ che

$$\mathcal{A} \vDash \boldsymbol{\varphi}_i[g]$$

per ogni assegnazione g. Se $\boldsymbol{\varphi}_i$ è un assioma logico oppure $\boldsymbol{\varphi}_i \in \Gamma$ il risultato è immediato, quindi possiamo supporre che $\boldsymbol{\varphi}_i$ sia stata ottenuta mediante le regole.

Se $\boldsymbol{\varphi}_i$ è ottenuta per MP da $\boldsymbol{\varphi}_j$ e $\boldsymbol{\varphi}_k = \boldsymbol{\varphi}_j \boldsymbol{\Rightarrow} \boldsymbol{\varphi}_i$ per $j, k < i$, allora $\mathcal{A} \vDash \boldsymbol{\varphi}_j[g]$ e $\mathcal{A} \vDash (\boldsymbol{\varphi}_j \boldsymbol{\Rightarrow} \boldsymbol{\varphi}_i)[g]$ per ipotesi induttiva, e quindi $\mathcal{A} \vDash \boldsymbol{\varphi}_i[g]$.

Se $\boldsymbol{\varphi}_i = \boldsymbol{\exists x \psi \Rightarrow \chi}$ è ottenuta mediante la regola del quantificatore esistenziale a partire da $\boldsymbol{\varphi}_j = \boldsymbol{\psi \Rightarrow \chi}$, con $j < i$ e $\boldsymbol{x} \notin \mathrm{Fv}(\boldsymbol{\chi})$, si applica il Teorema 29.13. □

Nella Sezione 35 dimostreremo il Teorema di Completezza 35.2 che è il converso del Teorema di Correttezza, cioè dimostreremo che se $\Gamma \models \boldsymbol{\varphi}$ allora $\Gamma \vdash \boldsymbol{\varphi}$. Ne segue che la nozione di derivabilità e la nozione di conseguenza logica coincidono,

$$\Gamma \vdash \boldsymbol{\varphi} \Leftrightarrow \Gamma \models \boldsymbol{\varphi},$$

quindi una teoria T è *sintatticamente* chiusa se e solo se è *semanticamente* chiusa e per questo motivo (una volta dimostrato il Teorema di Completezza) diremo semplicemente che T è una **teoria chiusa**.

34.B. Regole derivate. La definizione ufficiale di derivazione prevede l'uso di due sole regole, ma a partire da queste è possibile ricavare numerose altre regole, dette **regole derivate**, che possono essere utilizzate all'interno delle derivazioni. Naturalmente le regole derivate possono sempre essere eliminate, visto che sono ottenibili a partire dalle due regole ufficiali (MP e la regola del quantficatore esistenziale), tuttavia rendono le derivazioni più semplici e chiare.

Regola della conseguenza tautologica. Se $\boldsymbol{\varphi}$ è conseguenza tautologica di $\boldsymbol{\psi}_1, \dots, \boldsymbol{\psi}_n$, allora $\boldsymbol{\varphi}$ si deduce da $\boldsymbol{\psi}_1, \dots, \boldsymbol{\psi}_n$, vale a dire

$$\text{se } \Gamma \vdash \boldsymbol{\psi}_1, \dots, \Gamma \vdash \boldsymbol{\psi}_n, \text{ allora } \Gamma \vdash \boldsymbol{\varphi}.$$

Dimostrazione. Dire che $\boldsymbol{\varphi}$ è conseguenza tautologica di $\boldsymbol{\psi}_1, \dots, \boldsymbol{\psi}_n$ è come dire che $\boldsymbol{\psi}_1 \boldsymbol{\Rightarrow} (\boldsymbol{\psi}_2 \boldsymbol{\Rightarrow} \dots (\boldsymbol{\psi}_n \boldsymbol{\Rightarrow} \boldsymbol{\varphi}) \dots)$ è una tautologia, quindi $\boldsymbol{\varphi}$ discende da n applicazioni della regola MP. □

Dato che $\boldsymbol{\varphi}_0 \boldsymbol{\wedge} \boldsymbol{\varphi}_1$ è conseguenza tautologica di $\boldsymbol{\varphi}_0, \boldsymbol{\varphi}_1$ e dato che $\boldsymbol{\varphi}_i$ è conseguenza tautologica di $\boldsymbol{\varphi}_0 \boldsymbol{\wedge} \boldsymbol{\varphi}_1$ otteniamo

Regola della congiunzione. Da $\boldsymbol{\varphi}$ e $\boldsymbol{\psi}$ si deduce $\boldsymbol{\varphi} \boldsymbol{\wedge} \boldsymbol{\psi}$ e da $\boldsymbol{\varphi} \boldsymbol{\wedge} \boldsymbol{\psi}$ si deduce tanto $\boldsymbol{\varphi}$ quanto $\boldsymbol{\psi}$. In altre parole

$$\Gamma \vdash \boldsymbol{\varphi} \text{ e } \Gamma \vdash \boldsymbol{\psi} \text{ se e solo se } \Gamma \vdash \boldsymbol{\varphi} \boldsymbol{\wedge} \boldsymbol{\psi}.$$

Poiché $\boldsymbol{\psi}$ è conseguenza tautologica di $\boldsymbol{\varphi} \boldsymbol{\Rightarrow} \boldsymbol{\psi}$ e $\boldsymbol{\neg\varphi} \boldsymbol{\Rightarrow} \boldsymbol{\psi}$ si ha

Regola della dimostrazione per casi. Se $\Gamma \vdash \boldsymbol{\varphi} \boldsymbol{\Rightarrow} \boldsymbol{\psi}$ e $\Gamma \vdash \boldsymbol{\neg\varphi} \boldsymbol{\Rightarrow} \boldsymbol{\psi}$ allora $\Gamma \vdash \boldsymbol{\psi}$.

Poiché $\boldsymbol{\varphi} \boldsymbol{\Rightarrow} \boldsymbol{\psi}$ è tautologicamente equivalente a $\boldsymbol{\neg\psi} \boldsymbol{\Rightarrow} \boldsymbol{\neg\varphi}$ si ha la

Regola di contrapposizione. Da $\boldsymbol{\varphi} \boldsymbol{\Rightarrow} \boldsymbol{\psi}$ si deduce $\boldsymbol{\neg\psi} \boldsymbol{\Rightarrow} \boldsymbol{\neg\varphi}$ e viceversa, cioè

$$\text{se } \Gamma \vdash \boldsymbol{\varphi} \boldsymbol{\Rightarrow} \boldsymbol{\psi} \text{ allora } \Gamma \vdash \boldsymbol{\neg\psi} \boldsymbol{\Rightarrow} \boldsymbol{\neg\varphi}.$$

Dalla regola di contrapposizione e dal fatto che $\boldsymbol{\forall x \psi}$ è un'abbreviazione di $\boldsymbol{\neg\exists x \neg\psi}$ si ottiene subito la

Regola del quantificatore universale. Se $\boldsymbol{x}$ non occorre libera in $\boldsymbol{\varphi}$ allora da $\boldsymbol{\varphi} \boldsymbol{\Rightarrow} \boldsymbol{\psi}$ si deduce $\boldsymbol{\varphi} \boldsymbol{\Rightarrow} \boldsymbol{\forall x \psi}$, cioè

$$\text{se } \boldsymbol{x} \notin \mathrm{Fv}(\boldsymbol{\varphi}) \text{ e } \Gamma \vdash \boldsymbol{\varphi} \boldsymbol{\Rightarrow} \boldsymbol{\psi} \text{ allora } \Gamma \vdash \boldsymbol{\varphi} \boldsymbol{\Rightarrow} \boldsymbol{\forall x \psi}.$$

Regola della generalizzazione. Se $\Gamma \vdash \boldsymbol{\varphi}$ allora $\Gamma \vdash \boldsymbol{\forall x \varphi}$.

Dimostrazione. Supponiamo $\Gamma \vdash \boldsymbol{\varphi}$. Allora $\Gamma \vdash \boldsymbol{\neg\forall x \varphi} \boldsymbol{\Rightarrow} \boldsymbol{\varphi}$ per la regola della conseguenza tautologica e quindi $\Gamma \vdash \boldsymbol{\neg\forall x \varphi} \boldsymbol{\Rightarrow} \boldsymbol{\forall x \varphi}$ per la regola del quantificatore universale. Ne segue che $\Gamma \vdash \boldsymbol{\forall x \varphi}$ per la regola della conseguenza tautologica. □

Lemma 34.3. *Se* $\Gamma \vdash \boldsymbol{\varphi}$ *allora* $\Gamma \vdash \boldsymbol{\varphi}[\![\boldsymbol{t}/\boldsymbol{x}]\!]$.

Dimostrazione. Per ipotesi $\Gamma \vdash \boldsymbol{\varphi}$ quindi per la regola di generalizzazione $\Gamma \vdash \boldsymbol{\forall x \varphi}$. Poiché $\boldsymbol{\varphi}[\![\boldsymbol{t}/\boldsymbol{x}]\!]$ è conseguenza tautologica di $\boldsymbol{\forall x \varphi}$ e dell'assioma di sostituzione $\boldsymbol{\neg\varphi}[\![\boldsymbol{t}/\boldsymbol{x}]\!] \boldsymbol{\Rightarrow} \boldsymbol{\exists x \neg\varphi}$, allora $\Gamma \vdash \boldsymbol{\varphi}[\![\boldsymbol{t}/\boldsymbol{x}]\!]$. □

Più ingenerale vale la seguente:

Regola della sostituzione. Se $\Gamma \vdash \boldsymbol{\varphi}$ allora $\Gamma \vdash \boldsymbol{\varphi}[\![\boldsymbol{t}_1/\boldsymbol{x}_1, \dots, \boldsymbol{t}_n/\boldsymbol{x}_n]\!]$.

Dimostrazione. Il caso $n = 1$ è il Lemma 34.3, quindi possiamo supporre che $n > 1$. Distinguiamo due casi.

- Caso 1: le variabili $\boldsymbol{x}_1, \dots, \boldsymbol{x}_n$ non occorrono nei termini $\boldsymbol{t}_1, \dots, \boldsymbol{t}_n$.
  Allora $\boldsymbol{\varphi}[\![\boldsymbol{t}_1/\boldsymbol{x}_1, \dots, \boldsymbol{t}_{k-1}/\boldsymbol{x}_{k-1}]\!][\![\boldsymbol{t}_k/\boldsymbol{x}_k]\!] = \boldsymbol{\varphi}[\![\boldsymbol{t}_1/\boldsymbol{x}_1, \dots, \boldsymbol{t}_k/\boldsymbol{x}_k]\!]$ e il risultato segue da n applicazioni del Lemma 34.3.
- Caso 2: altrimenti.
  Scegliamo delle variabili $\boldsymbol{y}_1, \dots, \boldsymbol{y}_n$ che non compaiono né in $\boldsymbol{\varphi}$ né in $\boldsymbol{t}_1, \dots, \boldsymbol{t}_n$. Per il Caso 1 $\Gamma \vdash \boldsymbol{\varphi}'$, dove $\boldsymbol{\varphi}' = \boldsymbol{\varphi}[\![\boldsymbol{y}_1/\boldsymbol{x}_1, \dots, \boldsymbol{y}_n/\boldsymbol{x}_n]\!]$, e sempre per il Caso 1, $\Gamma \vdash \boldsymbol{\varphi}'[\![\boldsymbol{t}_1/\boldsymbol{y}_1, \dots, \boldsymbol{t}_n/\boldsymbol{y}_n]\!]$, cioè $\Gamma \vdash \boldsymbol{\varphi}[\![\boldsymbol{t}_1/\boldsymbol{x}_1, \dots, \boldsymbol{t}_n/\boldsymbol{x}_n]\!]$.

□

Teorema 34.4. (a) *Se* $\Gamma \vdash \boldsymbol{\varphi}[\![\boldsymbol{t}_1/\boldsymbol{x}_1, \dots, \boldsymbol{t}_n/\boldsymbol{x}_n]\!]$ *allora* $\Gamma \vdash \boldsymbol{\exists x}_1 \dots \boldsymbol{\exists x}_n \boldsymbol{\varphi}$.
(b) *Se* $\Gamma \vdash \boldsymbol{\forall x}_1 \dots \boldsymbol{\forall x}_n \boldsymbol{\varphi}$ *allora* $\Gamma \vdash \boldsymbol{\varphi}[\![\boldsymbol{t}_1/\boldsymbol{x}_1, \dots, \boldsymbol{t}_n/\boldsymbol{x}_n]\!]$.

Dimostrazione. (a) La formula $\boldsymbol{\varphi} \boldsymbol{\Rightarrow} \boldsymbol{\exists x}_1 \dots \boldsymbol{\exists x}_n \boldsymbol{\varphi}$ è conseguenza tautologica delle formule

$$\boldsymbol{\varphi} \boldsymbol{\Rightarrow} \boldsymbol{\exists x}_n \boldsymbol{\varphi}, \quad \boldsymbol{\exists x}_n \boldsymbol{\varphi} \boldsymbol{\Rightarrow} \boldsymbol{\exists x}_{n-1} \boldsymbol{\exists x}_n \boldsymbol{\varphi}, \dots, \quad \boldsymbol{\exists x}_2 \dots \boldsymbol{\exists x}_n \boldsymbol{\varphi} \boldsymbol{\Rightarrow} \boldsymbol{\exists x}_1 \dots \boldsymbol{\exists x}_n \boldsymbol{\varphi},$$

che sono assiomi di sostituzione, quindi $\vdash \boldsymbol{\varphi} \boldsymbol{\Rightarrow} \boldsymbol{\exists x}_1 \dots \boldsymbol{\exists x}_n \boldsymbol{\varphi}$. Per la Regola di sostituzione $\vdash \boldsymbol{\varphi}[\![\boldsymbol{t}_1/\boldsymbol{x}_1, \dots, \boldsymbol{t}_n/\boldsymbol{x}_n]\!] \boldsymbol{\Rightarrow} \boldsymbol{\exists x}_1 \dots \boldsymbol{\exists x}_n \boldsymbol{\varphi}$, da cui il risultato.

(b) Per la parte (a) applicata alla formula $\boldsymbol{\neg\varphi}$ e la regola di contrapposizione $\vdash \boldsymbol{\forall x}_1 \dots \boldsymbol{\forall x}_n \boldsymbol{\varphi} \boldsymbol{\Rightarrow} \boldsymbol{\varphi}[\![\boldsymbol{t}_1/\boldsymbol{x}_1, \dots, \boldsymbol{t}_n/\boldsymbol{x}_n]\!]$, da cui il risultato. □

Per la regola di generalizzazione e per la parte (b) del Teorema 34.4 si ottiene

$$\Gamma \vdash \boldsymbol{\varphi} \text{ se e solo se } \Gamma \vdash \boldsymbol{\forall x} \boldsymbol{\varphi}$$

e più in generale

$$\Gamma \vdash \boldsymbol{\varphi} \text{ se e solo se } \Gamma \vdash \boldsymbol{\varphi}^{\forall}$$

Lemma 34.5. *Sia* Γ *un insieme di formule e sia* $\boldsymbol{\sigma}$ *un enunciato. Se* $\Gamma \cup \{\boldsymbol{\sigma}\} \vdash \boldsymbol{\varphi}$ *allora* $\Gamma \vdash \boldsymbol{\sigma} \boldsymbol{\Rightarrow} \boldsymbol{\varphi}$.

Dimostrazione. Supponiamo $\langle \boldsymbol{\varphi}_0, \dots, \boldsymbol{\varphi}_n \rangle$ sia una derivazione di $\boldsymbol{\varphi}$ a partire da $\Gamma \cup \{\boldsymbol{\sigma}\}$. Dimostreremo per induzione su $i \leq n$ che

$$\Gamma \vdash \boldsymbol{\sigma} \boldsymbol{\Rightarrow} \boldsymbol{\varphi}_i.$$

Consideriamo i vari casi:

- $\boldsymbol{\varphi}_i$ è un assioma logico oppure $\boldsymbol{\varphi}_i \in \Gamma$. Allora

$$\langle \boldsymbol{\varphi}_i \boldsymbol{\Rightarrow} (\boldsymbol{\sigma} \boldsymbol{\Rightarrow} \boldsymbol{\varphi}_i), \boldsymbol{\varphi}_i, \ \boldsymbol{\sigma} \boldsymbol{\Rightarrow} \boldsymbol{\varphi}_i \rangle$$

è una derivazione in Γ dal momento che la prima formula è una tautologia, la seconda è un assioma logico oppure è in Γ, la terza è ottenuta dalle prime due mediante MP.

- $\boldsymbol{\varphi}_i$ è $\boldsymbol{\sigma}$. Allora $\boldsymbol{\sigma} \Rightarrow \boldsymbol{\varphi}_i$ è una tautologia, quindi è derivabile.
- $\boldsymbol{\varphi}_i$ è ottenuta per MP da $\boldsymbol{\varphi}_m$ e $\boldsymbol{\varphi}_k$, dove $m, k < i$ e $\boldsymbol{\varphi}_k$ è $\boldsymbol{\varphi}_m \Rightarrow \boldsymbol{\varphi}_i$. Per ipotesi induttiva $\Gamma \vdash \boldsymbol{\sigma} \Rightarrow \boldsymbol{\varphi}_m$ e $\Gamma \vdash \boldsymbol{\sigma} \Rightarrow (\boldsymbol{\varphi}_m \Rightarrow \boldsymbol{\varphi}_i)$. Poiché $\boldsymbol{\sigma} \Rightarrow \boldsymbol{\varphi}_i$ è conseguenza tautologica di $\boldsymbol{\sigma} \Rightarrow (\boldsymbol{\varphi}_m \Rightarrow \boldsymbol{\varphi}_i)$ e di $\boldsymbol{\sigma} \Rightarrow \boldsymbol{\varphi}_m$, allora $\Gamma \vdash \boldsymbol{\sigma} \Rightarrow \boldsymbol{\varphi}_i$ per la regola della conseguenza tautologica.
- $\boldsymbol{\varphi}_i$ è ottenuta mediante la regola del quantificatore esistenziale a partire da $\boldsymbol{\varphi}_j$ con $j < i$, vale a dire $\boldsymbol{\varphi}_i = \exists \boldsymbol{x} \boldsymbol{\psi} \Rightarrow \boldsymbol{\chi}$, la variabile $\boldsymbol{x}$ non occorre libera in $\boldsymbol{\chi}$ e $\boldsymbol{\varphi}_j = \boldsymbol{\psi} \Rightarrow \boldsymbol{\chi}$. Per ipotesi induttiva $\Gamma \vdash \boldsymbol{\sigma} \Rightarrow (\boldsymbol{\psi} \Rightarrow \boldsymbol{\chi})$ e poiché $\boldsymbol{\sigma} \Rightarrow (\boldsymbol{\psi} \Rightarrow \boldsymbol{\chi})$ e $\boldsymbol{\psi} \Rightarrow (\boldsymbol{\sigma} \Rightarrow \boldsymbol{\chi})$ sono tautologicamente equivalenti, allora $\Gamma \vdash \boldsymbol{\psi} \Rightarrow (\boldsymbol{\sigma} \Rightarrow \boldsymbol{\chi})$. Dato che $\boldsymbol{\sigma}$ è un enunciato, $\boldsymbol{x} \notin \mathrm{Fv}(\boldsymbol{\sigma} \Rightarrow \boldsymbol{\chi})$, quindi $\Gamma \vdash \exists \boldsymbol{x} \boldsymbol{\psi} \Rightarrow (\boldsymbol{\sigma} \Rightarrow \boldsymbol{\chi})$ per la regola del quantificatore esistenziale, da cui $\Gamma \vdash \boldsymbol{\sigma} \Rightarrow (\exists \boldsymbol{x} \boldsymbol{\psi} \Rightarrow \boldsymbol{\chi})$ per la regola della conseguenza tautologica.

Quindi $\Gamma \vdash \boldsymbol{\sigma} \Rightarrow \boldsymbol{\varphi}_i$ per ogni $i \leq n$, come richiesto. □

L'ipotesi che $\boldsymbol{\sigma}$ sia una formula chiusa è essenziale. Per esempio, per la regola di generalizzazione $\boldsymbol{x} \equiv \boldsymbol{0} \vdash \forall \boldsymbol{x}(\boldsymbol{x} \equiv \boldsymbol{0})$, mentre non si può derivare $\vdash \boldsymbol{x} \equiv \boldsymbol{0} \Rightarrow \forall \boldsymbol{x}(\boldsymbol{x} \equiv \boldsymbol{0})$ dato che questa formula non è valida.

Spesso in matematica per dimostrare che $\forall \boldsymbol{x} \boldsymbol{\varphi}(\boldsymbol{x})$ si ragiona così: si prende un elemento generico $\boldsymbol{c}$ e si dimostra che vale $\boldsymbol{\varphi}$ per l'elemento $\boldsymbol{c}$; data l'arbitrarietà di $\boldsymbol{c}$ si conclude che $\forall \boldsymbol{x} \boldsymbol{\varphi}(\boldsymbol{x})$. Il seguente risultato formalizza tutto questo.

Teorema 34.6. *Sia $\Gamma \subseteq \mathrm{Fml}(L)$, sia $\boldsymbol{\varphi}$ una L-formula e sia $\boldsymbol{c}$ una nuova costante. Allora*

$$\Gamma \vdash_L \forall \boldsymbol{x} \boldsymbol{\varphi} \Leftrightarrow \Gamma \vdash_{L \cup \{\boldsymbol{c}\}} \boldsymbol{\varphi}[\![\boldsymbol{c}/\boldsymbol{x}]\!].$$

Dimostrazione. $\Gamma \vdash_L \forall \boldsymbol{x} \boldsymbol{\varphi}$ implica $\Gamma \vdash_{L \cup \{\boldsymbol{c}\}} \forall \boldsymbol{x} \boldsymbol{\varphi}$, quindi per il Teorema 34.4 $\Gamma \vdash_{L \cup \{\boldsymbol{c}\}} \boldsymbol{\varphi}[\![\boldsymbol{c}/\boldsymbol{x}]\!]$.

Viceversa supponiamo che $\langle \boldsymbol{\psi}_0, \dots, \boldsymbol{\psi}_n \rangle$ sia una derivazione in $L \cup \{\boldsymbol{c}\}$ di $\boldsymbol{\varphi}[\![\boldsymbol{c}/\boldsymbol{x}]\!]$ a partire da Γ. Sia $\boldsymbol{y}$ una variabile che non occorre in nessuna $\boldsymbol{\psi}_i$.

Fatto 34.6.1. *$\langle \boldsymbol{\psi}_0[\![\boldsymbol{y}/\boldsymbol{c}]\!], \dots, \boldsymbol{\psi}_n[\![\boldsymbol{y}/\boldsymbol{c}]\!] \rangle$ è una derivazione in L di $\boldsymbol{\varphi}[\![\boldsymbol{y}/\boldsymbol{x}]\!]$ a partire da Γ.*

Dimostrazione. Se $\boldsymbol{\psi}_i \in \Gamma$ allora $\boldsymbol{\psi}_i[\![\boldsymbol{y}/\boldsymbol{c}]\!] = \boldsymbol{\psi}_i$ dato che si tratta di L-formule.

Se $\boldsymbol{\psi}_i$ è l'assioma di sostituzione $\boldsymbol{\psi}[\![\boldsymbol{t}/\boldsymbol{z}]\!] \Rightarrow \exists \boldsymbol{z} \boldsymbol{\psi}$, allora $\boldsymbol{\psi}_i[\![\boldsymbol{y}/\boldsymbol{c}]\!]$ è l'assioma di sostituzione $\boldsymbol{\psi}'[\![\boldsymbol{u}/\boldsymbol{z}]\!] \Rightarrow \exists \boldsymbol{z} \boldsymbol{\psi}'$ dove $\boldsymbol{u} = \boldsymbol{t}[\![\boldsymbol{y}/\boldsymbol{c}]\!]$ e $\boldsymbol{\psi}' = \boldsymbol{\psi}[\![\boldsymbol{y}/\boldsymbol{c}]\!]$.

Se $\boldsymbol{\psi}_i$ è un assioma di uguaglianza o una tautologia, allora è immediato verificare che anche $\boldsymbol{\psi}_i[\![\boldsymbol{y}/\boldsymbol{c}]\!]$ è un assioma dello stesso tipo.

Se $\boldsymbol{\psi}_i$ è ottenuto per MP da $\boldsymbol{\psi}_j$ e $\boldsymbol{\psi}_k = \boldsymbol{\psi}_j \boldsymbol{\Rightarrow} \boldsymbol{\psi}_i$, con $j, k < i$, allora $\boldsymbol{\psi}_i[\![\boldsymbol{y}/\boldsymbol{c}]\!]$ è ottenuto per MP da $\boldsymbol{\psi}_j[\![\boldsymbol{y}/\boldsymbol{c}]\!]$ e $\boldsymbol{\psi}_k[\![\boldsymbol{y}/\boldsymbol{c}]\!]$.

Infine supponiamo che $\boldsymbol{\psi}_i$ sia ottenuto da qualche $\boldsymbol{\psi}_j$ con $j < i$ mediante la regola del quantificatore esistenziale, cioè $\boldsymbol{\psi}_i = \boldsymbol{\exists z \chi \Rightarrow \psi}$, $\boldsymbol{z} \notin \mathrm{Fv}(\boldsymbol{\psi})$ e $\boldsymbol{\psi}_j = \boldsymbol{\chi \Rightarrow \psi}$. Allora $\boldsymbol{\psi}_i[\![\boldsymbol{y}/\boldsymbol{c}]\!] = \boldsymbol{\exists z \chi}[\![\boldsymbol{y}/\boldsymbol{c}]\!] \boldsymbol{\Rightarrow} \boldsymbol{\psi}[\![\boldsymbol{y}/\boldsymbol{c}]\!]$, $\boldsymbol{z} \notin \mathrm{Fv}(\boldsymbol{\psi}[\![\boldsymbol{y}/\boldsymbol{c}]\!])$ e $\boldsymbol{\psi}_j[\![\boldsymbol{y}/\boldsymbol{c}]\!] = \boldsymbol{\chi}[\![\boldsymbol{y}/\boldsymbol{c}]\!] \boldsymbol{\Rightarrow} \boldsymbol{\psi}[\![\boldsymbol{y}/\boldsymbol{c}]\!]$, quindi $\boldsymbol{\psi}_i[\![\boldsymbol{y}/\boldsymbol{c}]\!]$ è ottenuta da $\boldsymbol{\psi}_j[\![\boldsymbol{y}/\boldsymbol{c}]\!]$ mediante la regola del quantificatore esistenziale. □

Allora $\Gamma \vdash_L \boldsymbol{\varphi}[\![\boldsymbol{y}/\boldsymbol{x}]\!]$ e quindi $\Gamma \vdash_L \boldsymbol{\varphi}$ per la regola di sostituzione. □

34.C. Coerenza. Sia $\Gamma \subseteq \mathrm{Fml}(L)$. Diremo che Γ è **incoerente** se $\Gamma \vdash_L \boldsymbol{\varphi}$ e $\Gamma \vdash_L \boldsymbol{\neg\varphi}$ per qualche formula $\boldsymbol{\varphi}$; equivalentemente, per la regola della congiunzione, se $\Gamma \vdash_L \boldsymbol{\varphi \wedge \neg\varphi}$. Poiché ogni formula è conseguenza tautologica di una contraddizione proposizionale, Γ è incoerente se e solo se da Γ si può derivare una qualsiasi formula. Se Γ non è incoerente allora si dice **coerente**; quindi Γ è coerente se $\Gamma \nvdash_L \boldsymbol{\varphi}$ per qualche $\boldsymbol{\varphi}$.

Esercizio 34.7. Dimostrare che:

(i) Γ è coerente se e solo se ogni suo sottoinsieme finito lo è;

(ii) se $\mathcal{C} \subseteq \mathscr{P}(\mathrm{Fml}(L))$ è linearmente ordinato da $\subseteq$ e se Γ è coerente per ogni $\Gamma \in \mathcal{C}$, allora $\bigcup \mathcal{C}$ è coerente.

Proposizione 34.8. *Sia* $\Gamma \subseteq \mathrm{Fml}(L)$ *e sia* $\boldsymbol{\sigma} \in \mathrm{Sent}(L)$. *Allora*

$$\Gamma \cup \{\boldsymbol{\sigma}\} \text{ } \textit{è coerente} \Leftrightarrow \Gamma \nvdash_L \boldsymbol{\neg\sigma}.$$

Dimostrazione. Se $\Gamma \vdash_L \boldsymbol{\neg\sigma}$, allora $\Gamma \cup \{\boldsymbol{\sigma}\} \vdash_L \boldsymbol{\sigma \wedge \neg\sigma}$. Viceversa supponiamo $\Gamma \cup \{\boldsymbol{\sigma}\}$ sia incoerente: allora $\Gamma \cup \{\boldsymbol{\sigma}\} \vdash_L \boldsymbol{\sigma \wedge \neg\sigma}$. Per il Lemma 34.5, $\Gamma \vdash_L \boldsymbol{\sigma \Rightarrow (\sigma \wedge \neg\sigma)}$ e quindi $\Gamma \vdash_L \boldsymbol{(\sigma \vee \neg\sigma) \Rightarrow \neg\sigma}$. Ma $\boldsymbol{\sigma \vee \neg\sigma}$ è una tautologia, quindi per *Modus ponens* $\Gamma \vdash_L \boldsymbol{\neg\sigma}$. □

La relazione

$$\boldsymbol{\varphi} \preceq_\Gamma \boldsymbol{\psi} \Leftrightarrow \Gamma \cup \{\boldsymbol{\varphi}\} \vdash_L \boldsymbol{\psi}$$

definisce un pre-ordine su $\mathrm{Fml}(L)$ e quindi induce una relazione d'equivalenza

$$\boldsymbol{\varphi} \sim_\Gamma \boldsymbol{\psi} \Leftrightarrow (\boldsymbol{\varphi} \preceq_\Gamma \boldsymbol{\psi} \wedge \boldsymbol{\psi} \preceq_\Gamma \boldsymbol{\varphi})$$

che si legge: $\boldsymbol{\varphi}$ e $\boldsymbol{\psi}$ sono **equiderivabili modulo** Γ. Quindi Γ è coerente se e solo se la relazione $\sim_\Gamma$ non è banale. Se $\Delta \subseteq \Gamma$ allora la relazione d'equivalenza $\sim_\Delta$ raffina $\sim_\Gamma$, vale a dire $\boldsymbol{\varphi} \sim_\Delta \boldsymbol{\psi} \Rightarrow \boldsymbol{\varphi} \sim_\Sigma \boldsymbol{\psi}$.

La relazione di equiderivabilità è particolarmente importante quando è ristretta agli enunciati e per il Lemma 34.5,

$$\boldsymbol{\sigma} \sim_\Gamma \boldsymbol{\tau} \Leftrightarrow \Gamma \vdash (\boldsymbol{\sigma \Leftrightarrow \tau}),$$

se $\boldsymbol{\sigma}, \boldsymbol{\tau} \in \mathrm{Sent}(L)$.

Esercizio 34.9. Supponiamo $\Gamma \subseteq \mathrm{Fml}(L)$ sia coerente e sia $\Sigma \subseteq \mathrm{Sent}(L)$. Dimostrare che:

(i) $\mathrm{Sent}(L)/{\sim_\Gamma}$ è un'algebra di Boole, detta **algebra di Lindenbaum generata da** Γ, con le operazioni

$$[\boldsymbol{\sigma}] \curlyvee [\boldsymbol{\tau}] = [\boldsymbol{\sigma} \vee \boldsymbol{\tau}]$$
$$[\boldsymbol{\sigma}] \curlywedge [\boldsymbol{\tau}] = [\boldsymbol{\sigma} \wedge \boldsymbol{\tau}]$$
$$[\boldsymbol{\sigma}]^* = [\neg \boldsymbol{\sigma}],$$

in cui $\mathbf{1}$ è la classe d'equivalenza contenente tutte le tautologie proposizionali e $\mathbf{0}$ è la classe d'equivalenza contenente tutte le contraddizioni proposizionali.

(ii) Σ è coerente se e solo se $\{[\boldsymbol{\sigma}] \mid \boldsymbol{\sigma} \in \Sigma\}$ è sottobase per un filtro proprio di $\mathrm{Sent}(L)/{\sim_\Gamma}$.

(iii) Σ è una teoria sintatticamente chiusa e coerente se e solo se $\{[\boldsymbol{\sigma}] \mid \boldsymbol{\sigma} \in \Sigma\}$ è un filtro proprio di $\mathrm{Sent}(L)/{\sim_\Gamma}$.

(iv) Σ è completa se e solo se $\{[\boldsymbol{\sigma}] \mid \boldsymbol{\sigma} \in \Sigma\}$ è un ultrafiltro.

Il seguente risultato è noto come **Lemma di Lindenbaum**.

Lemma 34.10 (Lindenbaum)**.** *Se L è un linguaggio bene ordinabile, allora ogni insieme coerente di L-enunciati può essere esteso ad un insieme coerente massimale di L-enunciati.*

In particolare, se vale BPI *(Definizione 23.24) e L è un linguaggio arbitrario, allora ogni insieme coerente di L-enunciati può essere esteso ad un insieme coerente massimale di L-enunciati.*

Dimostrazione. Sia Σ insieme coerente di L-enunciati. Per la nostra ipotesi $\mathrm{Sent}(L)$ è bene ordinabile e quindi lo è anche il suo quoziente, l'algebra di Lindenbaum $\mathrm{Sent}(L)/{\sim_\Sigma}$. Per l'Esercizio 34.9 $\{[\boldsymbol{\sigma}] \mid \boldsymbol{\sigma} \in \Sigma\}$ è un filtro che per il Teorema **??** può essere esteso ad un ultrafiltro U. L'insieme $\{\boldsymbol{\sigma} \mid [\boldsymbol{\sigma}] \in U\}$ è l'insieme coerente massimale cercato. □

Esercizi

Esercizio 34.11. Sia $\Gamma \subseteq \mathrm{Fml}(L)$. Poniamo $\boldsymbol{\varphi} \sim \boldsymbol{\tau}$ se $\Gamma \vdash \boldsymbol{\varphi} \Leftrightarrow \boldsymbol{\tau}$, cioè se $\boldsymbol{\varphi}$ e $\boldsymbol{\tau}$ sono equivalenti. Dimostrare che $\sim$ è una relazione di equivalenza su $\mathrm{Fml}(L)$ e che se Γ è coerente allora $\mathrm{Fml}(L)/{\sim}$ è un'algebra di Boole.

Esercizio 34.12. Supponiamo $\Sigma \subseteq \mathrm{Sent}(L)$ sia coerente e massimale rispetto all'inclusione. Allora

$$\Sigma \vdash \boldsymbol{\sigma} \Leftrightarrow \boldsymbol{\sigma} \in \Sigma$$
$$\boldsymbol{\sigma} \notin \Sigma \Leftrightarrow \boldsymbol{\neg\sigma} \in \Sigma$$
$$\boldsymbol{\sigma \vee \tau} \in \Sigma \Leftrightarrow \boldsymbol{\sigma} \in \Sigma \vee \boldsymbol{\tau} \in \Sigma.$$

Esercizio 34.13. Dimostrare che $\Gamma \vdash \boldsymbol{\varphi}$ se e solo se $\Gamma^\forall \vdash \boldsymbol{\varphi}^\forall$.

35. Il Teorema di Completezza

Proposizione 35.1. *Un insieme soddisfacibile di enunciati Σ è coerente.*

Dimostrazione. Supponiamo Σ sia incoerente, cioè $\Sigma \vdash \boldsymbol{\sigma \wedge \neg\sigma}$. Allora $\Sigma \models \boldsymbol{\sigma \wedge \neg\sigma}$, quindi se $\mathcal{A}$ è un modello di Σ, allora $\mathcal{A} \vDash \boldsymbol{\sigma \wedge \neg\sigma}$: assurdo. Quindi $\mathcal{A}$ è insoddisfacibile. □

Il Teorema di Completezza asserisce il converso del Teorema di Correttezza 34.2.

Teorema 35.2 (Completezza)**.** *Supponiamo L sia bene ordinabile, oppure assumiamo* BPI*. Allora*

$$\Gamma \models \boldsymbol{\varphi} \Rightarrow \Gamma \vdash \boldsymbol{\varphi}.$$

Il Teorema di Completezza discende dal converso della Proposizione 35.1, noto come Teorema di Esistenza di Modelli.

Teorema 35.3 (Esistenza di Modelli)**.** *Supponiamo $\Sigma \subseteq \mathrm{Sent}(L)$ sia coerente. Se L è bene ordinabile, allora Σ ha un modello di cardinalità $\leq \mathrm{card}(L)$.*

Se assumiamo BPI*, allora Σ ha un modello il cui universo è immagine suriettiva di $\mathrm{Fml}(L)^{<\omega}$.*

Dal Teorema di Esistenza di Modelli si ottiene una nuova, più perspicua, dimostrazione del Teorema di Compattezza 31.1.

Corollario 35.4. *Sia $\Sigma \subseteq \mathrm{Sent}(L)$ è finitamente soddisfacibile. Se L è bene ordinabile, allora Σ ha un modello bene ordinabile di cardinalità $\leq |L|$.*

Se assumiamo BPI *allora Σ ha un modello il cui universo è immagine suriettiva di $\mathrm{Fml}(L)^{<\omega}$.*

Dimostrazione. Se Σ è finitamente soddisfacibile, allora ogni suo sottoinsieme finito è coerente, quindi Σ è coerente. □

Vediamo come il Teorema di Completezza discende dal Teorema di Esistenza di Modelli.

Dimostrazione. Consideriamo prima il caso in cui $\boldsymbol{\varphi}$ sia un enunciato. Possiamo supporre che Γ sia coerente, altrimenti il risultato è banalmente vero. Se $\Gamma \nvdash \boldsymbol{\varphi}$ allora $\Gamma \cup \{\neg\boldsymbol{\varphi}\}$ è coerente per la Proposizione 34.8, quindi ammette un modello $\mathcal{A}$. Ma allora $\mathcal{A}$ testimonia che $\Gamma \not\models \boldsymbol{\varphi}$.

Supponiamo ora $\boldsymbol{\varphi}$ sia una formula con variabili libere $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$. Per la regola della generalizzazione e per il Teorema 34.4

$$\Gamma \vdash \boldsymbol{\varphi} \text{ se e solo se } \Gamma \vdash \forall \boldsymbol{x}_1 \ldots \forall \boldsymbol{x}_n \boldsymbol{\varphi}$$

e poiché $\Gamma \models \boldsymbol{\varphi}$ se e solo se $\Gamma \models \forall \boldsymbol{x}_1 \ldots \forall \boldsymbol{x}_n \boldsymbol{\varphi}$ il risultato segue. □

35.A. Il ruolo della teoria degli insiemi nel Teorema di Completezza. Nelle ipotesi dei Teoremi 35.2 e 35.3 si fa riferimento a qualche principio di scelta — il linguaggio deve essere bene ordinabile oppure bisogna assumere BPI. In particolare, se lavoriamo con una teoria T in un linguaggio finito o numerabile L, (per esempio: la teoria dei gruppi, dei campi, degli insiemi, ...) allora

$$T \vdash \boldsymbol{\sigma} \text{ se e solo se} T \models \boldsymbol{\sigma}.$$

Ma se consideriamo linguaggi arbitrari (come ci è capitato di fare nella Sezione 32.A), il ricorso a qualche forma di scelta è inevitabile, dato che il Teorema 35.3 per linguaggi arbitrari è equivalente a BPI l'affermazione che in un'algebra di Boole ogni filtro proprio è estendibile ad un ultrafiltro. Ricordiamo che BPI, così come il più forte AC, non è dimostrabile a partire dagli altri assiomi della teoria degli insiemi TI, sia che si utilizzi MK o che si utilizzi ZF. Quindi se lavoriamo in un universo degli insiemi in cui BPI non vale, allora c'è una teoria coerente T che non è soddisfacibile. (Chiaramente il linguaggio di T non può essere bene ordinabile.) Ne segue che in questo universo $T \nvdash \boldsymbol{\sigma} \wedge \neg\boldsymbol{\sigma}$ e tuttavia $T \models \boldsymbol{\sigma} \wedge \neg\boldsymbol{\sigma}$! Quindi anche il Teorema di Completezza 35.2 è equivalente a BPI.

Sia T una teoria con un sistema di assiomi ricorsivo in un linguaggio al più numerabile, così che le patologie del capoverso precedente non si manifestano. Supponiamo di aver dimostrato che $T \models \boldsymbol{\sigma}$ argomentando come si fa usualmente in matematica: si fissa un modello $\mathcal{M}$ di T arbitrario e si argomento che $\mathcal{M} \vDash \boldsymbol{\sigma}$. Supponiamo, però che in questa dimostrazione sia stato usato qualche principio insiemistico Ψ indimostrabile in TI, per esempio Ψ potrebbe essere l'Assioma di Scelta, l'Ipotesi del Continuo, ..., o le loro negazioni. Ne segue che per dimostrare un fatto finitario $T \models \boldsymbol{\sigma}$, cioè l'esistenza di una derivazione di $\boldsymbol{\sigma}$ da T, abbiamo usato un principio Ψ che trascende gli usuali assiomi delle teoria degli insiemi. Tuttavia, come vedremo nel Capitolo **??** l'uso di Ψ è superfluo quando Ψ appartiene ad una ampia classe di enunciati della teoria degli insiemi.

35.B. Il Teorema di Esistenza di Modelli. Per dimostrare il Teorema di Esistenza di Modelli, abbiamo bisogno di alcuni risultati preliminari.

Lemma 35.5. *Sia Σ una L-teoria coerente, sia $\boldsymbol{c}$ una nuova costante e sia $\boldsymbol{\varphi}(\boldsymbol{x})$ una L-formula con un'unica variabile libera. Allora la $L \cup \{\boldsymbol{c}\}$-teoria $\Sigma \cup \{\boldsymbol{\exists x \varphi \Rightarrow \varphi[c/x]}\}$ è coerente.*

Dimostrazione. Supponiamo, per assurdo, che

$$\Sigma \cup \{\boldsymbol{\exists x \varphi \Rightarrow \varphi[c/x]}\} \vdash_{L\cup\{\boldsymbol{c}\}} \boldsymbol{\sigma \wedge \neg \sigma}.$$

Per il Lemma 34.5 si ha $\Sigma \vdash_{L\cup\{\boldsymbol{c}\}} \boldsymbol{(\exists x \varphi \Rightarrow \varphi[c/x]) \Rightarrow \sigma \wedge \neg \sigma}$ e per la regola della conseguenza tautologica

$$\Sigma \vdash_{L\cup\{\boldsymbol{c}\}} \boldsymbol{\neg(\exists x \varphi \Rightarrow \varphi[c/x])},$$

cioè

$$\Sigma \vdash_{L\cup\{\boldsymbol{c}\}} \boldsymbol{(\exists x \varphi) \wedge \neg \varphi[c/x]}.$$

Il Teorema 34.6 implica che

$$\Sigma \vdash_L \boldsymbol{\forall x((\exists x \varphi) \wedge \neg \varphi)}$$

quindi $\Sigma \vdash_L \boldsymbol{(\exists x \varphi) \wedge \neg \varphi}$ per per la parte (b) del Teorema 34.4, da cui, per la regola della congiunzione $\Sigma \vdash_L \boldsymbol{\exists x \varphi}$ e $\Sigma \vdash_L \boldsymbol{\neg \varphi}$. Per la regola di generalizzazione $\Sigma \vdash_L \boldsymbol{\forall x(\neg \varphi)}$, cioè $\Sigma \vdash_L \boldsymbol{\neg(\exists x \varphi)}$, quindi Σ è incoerente. □

Lemma 35.6. *Se $\Sigma \subseteq \mathrm{Sent}(L)$ è coerente, allora esistono C un insieme di nuove costanti, e $\tilde{\Sigma} \subseteq \mathrm{Sent}(\tilde{L})$ dove $\tilde{L} = L \cup C$ tali che $\tilde{\Sigma} \supset \Sigma$ è coerente e se $\boldsymbol{\varphi}(\boldsymbol{x})$ è una L-formula con un'unica variabile libera, allora $\tilde{\Sigma} \vdash \boldsymbol{\exists x \varphi \Rightarrow \varphi[c/x]}$ per qualche $\boldsymbol{c} \in C$.*

Inoltre, se L è bene ordinabile, allora C può essere preso di cardinalità $\mathrm{card}(L)$.

Dimostrazione. Sia F l'insieme delle L-formule $\boldsymbol{\varphi}$ con un'unica variabile libera $\boldsymbol{x_\varphi}$, sia

$$C = \{\boldsymbol{c_\varphi} \mid \boldsymbol{\varphi} \in F\}$$

e sia

$$\tilde{\Sigma} = \Sigma \cup \{\boldsymbol{\exists x_\varphi \varphi \Rightarrow \varphi[c_\varphi/x_\varphi]} \mid \boldsymbol{\varphi} \in F\}.$$

Dobbiamo verificare che $\tilde{\Sigma}$ è coerente: se, per assurdo, $\tilde{\Sigma}$ fosse incoerente, allora potremmo trovare $\boldsymbol{\varphi}_1, \ldots, \boldsymbol{\varphi}_n \in F$ tali che

$$\Sigma \cup \{\boldsymbol{\exists x_{\varphi_i} \varphi_i \Rightarrow \varphi_i[c_{\varphi_i}/x_{\varphi_i}]} \mid 1 \leq i \leq n\}$$

è incoerente. Applicando $n+1$ volte il Lemma 35.5 si ottiene una contraddizione.

Se L è bene ordinabile, osserviamo che $|F| = \mathrm{card}(L)$ e quindi $|C| = \mathrm{card}(L)$. □

Definizione 35.7. Dato un linguaggio L, diremo che $\Gamma \subseteq \mathrm{Fml}(L)$ **ammette testimoni** se per ogni L-formula $\boldsymbol{\varphi}$ con al più una variabile libera $\boldsymbol{x}$ c'è una termine chiuso $\boldsymbol{t}$ tale che

$$\Gamma \vdash \boldsymbol{\exists x \varphi \Rightarrow \varphi[\![t/x]\!]}.$$

$\boldsymbol{t}$ si dice **testimone** per la formula $\boldsymbol{\exists x \varphi}$.

In altre parole: un insieme di formule ammette testimoni se ogni ogni qual volta dimostra un enunciato esistenziale $\boldsymbol{\exists x \varphi}$, allora dimostra $\boldsymbol{\varphi[\![t/x]\!]}$ per un opportuno termine chiuso $\boldsymbol{t}$.

Osservazioni 35.8. (a) Se Γ ammette testimoni, allora L ha delle costanti. Quindi non ogni teoria ammette testimoni — per esempio MK e ZF non ammettono testimoni.

(b) Se $\Gamma \subseteq \Gamma' \subseteq \mathrm{Fml}(L)$ e Γ ha testimoni, allora anche Γ' ha testimoni.

Teorema 35.9. *Se $\Sigma \subseteq \mathrm{Sent}(L)$ è coerente, allora esistono C un insieme di nuove costanti, e $\Sigma_\infty \subseteq \mathrm{Sent}(L_\infty)$ dove $L_\infty = L \cup C$ tali che $\Sigma_\infty \supset \Sigma$ è coerente e ha testimoni.*

Inoltre, se L è bene ordinabile, allora C può essere preso di cardinalità $\mathrm{card}(L)$.

Dimostrazione. Costruiremo induttivamente

- linguaggi $L = L_0 \subset L_1 \subset \cdots \subset L_n \subset \ldots$ tali che $L_{n+1} = L_n \cup C_n$ dove C_n è un insieme di costanti che non appartengono a L_n,
- insiemi coerenti $\Sigma_n \subseteq \mathrm{Sent}(L_n)$ tali che
  (i) $\Sigma = \Sigma_0 \subset \Sigma_1 \subset \cdots \subset \Sigma_n \subset \cdots$ e
  (ii) per ogni L_n-formula $\boldsymbol{\varphi}$ con un'unica variabile libera $\boldsymbol{x}$ c'è un $\boldsymbol{c} \in C_n$ tale che $\Sigma_{n+1} \vdash \boldsymbol{\exists x \varphi \Rightarrow \varphi[\![c/x]\!]}$.

Se $L_0, \ldots, L_n$, $C_0, \ldots, C_{n-1}$ e $\Sigma_0, \ldots, \Sigma_n$ sono stati costruiti e soddisfano i requisiti, allora il Lemma 35.6 garantisce l'esistenza di C_n (e quindi di L_{n+1}) e di Σ_{n+1} come richiesto. Posto $C = \bigcup_n C_n$, $L_\infty = \bigcup_n L_n$ e $\Sigma_\infty = \bigcup_n \Sigma_n$ abbiamo che

- $\Sigma_\infty \subseteq \mathrm{Sent}(L_\infty)$ è coerente (Esercizio 34.7 parte (ii))
- Σ_∞ ammette testimoni: fissata una L_∞ formula $\boldsymbol{\varphi(x)}$ con un'unica variabile libera, sia n minimo tale che $\boldsymbol{\varphi(x)} \in \mathrm{Fml}(L_n)$. Per costruzione c'è un $\boldsymbol{c} \in C_n$ tale che $\Sigma_{n+1} \vdash_{L_{n+1}} \boldsymbol{\exists x \varphi \Rightarrow \varphi[\![c/x]\!]}$ e quindi $\Sigma_\infty \vdash_{L_\infty} \boldsymbol{\exists x \varphi \Rightarrow \varphi[\![c/x]\!]}$.

Infine osserviamo che se L è bene ordinabile, allora $|C_n| = \mathrm{card}(L)$ e quindi $|C| = \mathrm{card}(L)$. □

35.B.1. *Dimostrazione del Teorema di Esistenza di Modelli 35.3.* Sia $\Sigma \subseteq \mathrm{Sent}(L)$ coerente: per il Lemma 35.6 fissiamo un insieme C di nuove costanti e possiamo estendere Σ ad un insieme coerente $\Sigma' \subseteq \mathrm{Sent}(\overline{L})$, dove $\overline{L} = L \cup C$ in modo che Σ' abbia testimoni. La nostra ipotesi (BPI oppure la bene ordinabilità di L) consente di applicare il Lemma di Lindenbaum 34.10, quindi c'è $\overline{\Sigma} \subseteq \mathrm{Sent}(\overline{L})$ un insieme coerente e massimale contenente Σ'. Per l'Esercizio 30.4 $\overline{\Sigma}$ è una teoria chiusa, quindi

$$\overline{\Sigma} \vdash_{\overline{L}} \boldsymbol{\sigma} \Leftrightarrow \boldsymbol{\sigma} \in \overline{\Sigma},$$

per ogni $\boldsymbol{\sigma} \in \mathrm{Sent}(\overline{L})$, e per l'Osservazione 35.8(b) se $\boldsymbol{\exists x \varphi} \in \overline{\Sigma}$ allora $\exists \boldsymbol{c} \in C \left(\boldsymbol{\exists x \varphi \Rightarrow \varphi[\![c/x]\!]} \in \overline{\Sigma}\right)$.

Costruiremo $\overline{\mathcal{A}} \in \mathrm{Str}(\overline{L})$ tale che $\overline{\mathcal{A}} \vDash \overline{\Sigma}$ e quindi, passando alla contrazione $\mathcal{A} = \overline{\mathcal{A}} \restriction L$ otterremo un modello di Σ.

Sia $\sim$ la relazione di equivalenza su $\mathrm{ClTerm}(\overline{L})$ definita da

$$\boldsymbol{t} \sim \boldsymbol{u} \Leftrightarrow (\boldsymbol{t} \equiv \boldsymbol{u}) \in \overline{\Sigma}.$$

L'universo della struttura $\overline{\mathcal{A}}$ (e quindi anche della struttura $\mathcal{A}$) è l'insieme

$$A = \mathrm{ClTerm}(\overline{L})/{\sim}$$

e l'interpretazione dei simboli non logici di $\overline{L}$ è definita come segue:

- Se $\boldsymbol{R} \in \mathrm{Rel}_{\overline{L}} = \mathrm{Rel}_L$ è n-ario, poniamo

  $$\boldsymbol{R}^{\overline{\mathcal{A}}} = \{\langle [\boldsymbol{t}_1]_\sim, \dots, [\boldsymbol{t}_n]_\sim \rangle \mid \boldsymbol{R}(\boldsymbol{t}_1, \dots, \boldsymbol{t}_n) \in \overline{\Sigma}\} \subseteq A^n.$$

  La relazione $\boldsymbol{R}^{\overline{\mathcal{A}}}$ è ben definita: se $\boldsymbol{R}(\boldsymbol{t}_1, \dots, \boldsymbol{t}_n) \in \bar{\Sigma}$ e se $\boldsymbol{t}_i \sim \boldsymbol{u}_i$ allora $\boldsymbol{t}_1 \equiv \boldsymbol{u}_1 \boldsymbol{\wedge} \dots \boldsymbol{\wedge} \boldsymbol{t}_n \equiv \boldsymbol{u}_n \in \overline{\Sigma}$ e poiché

  $$\boldsymbol{t}_1 \equiv \boldsymbol{u}_1 \boldsymbol{\wedge} \dots \boldsymbol{\wedge} \boldsymbol{t}_n \equiv \boldsymbol{u}_n \boldsymbol{\wedge} \boldsymbol{R}(\boldsymbol{t}_1, \dots, \boldsymbol{t}_n) \boldsymbol{\Rightarrow} \boldsymbol{R}(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)$$

  è un assioma di uguaglianza (Sezione 29.C.3), ne deduciamo che $\overline{\Sigma} \vdash_{\overline{L}} \boldsymbol{R}(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)$, cioè $\boldsymbol{R}(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n) \in \overline{\Sigma}$.
- Se $\boldsymbol{f} \in \mathrm{Func}_{\overline{L}} = \mathrm{Func}_L$ è n-ario, poniamo

  $$\boldsymbol{f}^{\overline{\mathcal{A}}} \colon A^n \to A \qquad \langle [\boldsymbol{t}_1]_\sim, \dots, [\boldsymbol{t}_n]_\sim \rangle \mapsto [\boldsymbol{f}(\boldsymbol{t}_1, \dots, \boldsymbol{t}_n)]_\sim.$$

  Anche in questo caso si verifica che la definizione di $\boldsymbol{f}^{\overline{\mathcal{A}}}$ non dipende dai rappresentanti scelti.
- Se $\boldsymbol{c} \in \mathrm{Const}_{\overline{L}} \supset \mathrm{Const}_L$, poniamo $\boldsymbol{c}^{\overline{\mathcal{A}}} = [\boldsymbol{c}]_\sim$.

Esercizio 35.10. Sia $\boldsymbol{t} \in \mathrm{ClTerm}$. Dimostrare che:

(i) $\boldsymbol{t}^{\overline{\mathcal{A}}} = [\boldsymbol{t}]_\sim$, dove $\boldsymbol{t}^{\overline{\mathcal{A}}}$ è l'interpretazione di $\boldsymbol{t}$ in $\overline{\mathcal{A}}$ definito nella Sezione 29.A;

(ii) $\boldsymbol{t} \sim \boldsymbol{c}$ per qualche $\boldsymbol{c} \in C$. In particolare,

$$A = \{[\boldsymbol{c}]_\sim \mid \boldsymbol{c} \in C\}\,.$$

Dobbiamo ora verificare che $\overline{\mathcal{A}} \vDash \overline{\Sigma}$. La definizione di $\mathcal{A}$ garantisce che

$$\boldsymbol{\sigma} \in \overline{\Sigma} \Leftrightarrow \overline{\mathcal{A}} \vDash \boldsymbol{\sigma}$$

per ogni enunciato atomico $\boldsymbol{\sigma}$. Verifichiamo per induzione su $\mathrm{ht}(\boldsymbol{\sigma})$ che questa equivalenza vale per ogni $\boldsymbol{\sigma} \in \mathrm{Sent}(\overline{L})$.

- Se $\boldsymbol{\sigma} = \boldsymbol{\neg\tau}$,

$$\begin{aligned} \boldsymbol{\neg\tau} \in \overline{\Sigma} &\Leftrightarrow \boldsymbol{\tau} \notin \overline{\Sigma} && \text{(Esercizio 34.12)} \\ &\Leftrightarrow \mathcal{A} \nvDash \boldsymbol{\tau} && \text{(ip. ind.)} \\ &\Leftrightarrow \mathcal{A} \vDash \boldsymbol{\neg\tau}. \end{aligned}$$

- Se $\boldsymbol{\sigma} = \boldsymbol{\tau \vee \chi}$ allora

$$\begin{aligned} \boldsymbol{\tau \vee \chi} \in \overline{\Sigma} &\Leftrightarrow \left(\boldsymbol{\tau} \in \overline{\Sigma}\right) \vee \left(\boldsymbol{\chi} \in \overline{\Sigma}\right) && \text{(Esercizio 34.12)} \\ &\Leftrightarrow \left(\overline{\mathcal{A}} \vDash \boldsymbol{\tau}\right) \vee \left(\overline{\mathcal{A}} \vDash \boldsymbol{\chi}\right) && \text{(ip. ind.)} \\ &\Leftrightarrow \overline{\mathcal{A}} \vDash \boldsymbol{\tau \vee \chi}. \end{aligned}$$

- Supponiamo $\boldsymbol{\sigma} = \boldsymbol{\exists x \varphi}$. Poiché $\overline{\Sigma}$ ha testimoni, $\boldsymbol{\exists x \varphi \Rightarrow \varphi[\![c/x]\!]} \in \overline{\Sigma}$ per qualche $\boldsymbol{c} \in C$.
  Quindi

$$\begin{aligned} \boldsymbol{\exists x \varphi} \in \overline{\Sigma} &\Rightarrow \boldsymbol{\varphi[\![c/x]\!]} \in \overline{\Sigma} \\ &\Rightarrow \overline{\mathcal{A}} \vDash \boldsymbol{\varphi[\![c/x]\!]} && \text{(ip. induttiva)} \\ &\Rightarrow \overline{\mathcal{A}} \vDash \boldsymbol{\varphi}[\boldsymbol{c}^{\overline{\mathcal{A}}}] && \text{(Proposizione 29.12)} \\ &\Rightarrow \overline{\mathcal{A}} \vDash \boldsymbol{\exists x \varphi}. \end{aligned}$$

  Viceversa supponiamo che $\overline{\mathcal{A}} \vDash \boldsymbol{\exists x \varphi}$ e quindi $\overline{\mathcal{A}} \vDash \boldsymbol{\varphi}[\boldsymbol{c}^{\overline{\mathcal{A}}}]$ per qualche $\boldsymbol{c} \in C$. Ne segue che $\overline{\mathcal{A}} \vDash \boldsymbol{\varphi[\![c/x]\!]}$per la Proposizione 29.12, quindi $\boldsymbol{\varphi[\![c/x]\!]} \in \overline{\Sigma}$ per ipotesi induttiva. L'assioma di sostituzione $\boldsymbol{\varphi[\![c/x]\!] \Rightarrow \exists x \varphi}$ appartiene a $\overline{\Sigma}$, quindi $\boldsymbol{\exists x \varphi} \in \overline{\Sigma}$ come richiesto.

Se L è bene ordinabile, allora $|A| \leq |C| = \mathrm{card}(L)$. Questo conclude la dimostrazione del Teorema di Esistenza di Modelli.

Esercizi

Esercizio 35.11. Dimostrare che il Teorema di Completezza e il Teorema di Compattezza implicano il Teorema di Esistenza di Modelli.

Esercizio 35.12. Dimostrare che il Teorema di Esistenza di Modelli per linguaggi arbitrari è equivalente a BPI.

Appendice A

Algebra e topologia

In questa appendice richiamiamo alcuni concetti di algebra e di topologia che dovrebbero essere familiari a tutti. Questa è solo una breve lista di definizioni—per una trattazione esauriente di questi argomenti il lettore può consultare [**Hun80, Lan02**] per l'algebra e [**Kur92, CTV76**] per la topologia.

1. Algebra

Un **semigruppo** è un insieme $S \neq \emptyset$ dotato di un'operazione binaria $*$ che è associativa, cioè $(a * b) * c = a * (b * c)$. Se esiste un elemento $e \in S$ tale che $\forall a \in S\,(a * e = e * a = a)$ diremo che è un **monoide**. L'elemento e è unico e si dice elemento neutro. Un **gruppo** è un monoide in cui ogni elemento ha un inverso, cioè $\forall x \in S\,\exists y \in S\,(x * y = y * x = e)$. L'inverso di x è unico e lo si denota con x^{-1}. Un gruppo si dice **commutativo** o **abeliano** se l'operazione è commutativa, cioè $\forall x, y \in S\,(x * y = y * x)$. Spesso l'operazione nei gruppi abeliani la si indica con $+$ e l'elemento neutro con 0. Un **anello** è un insieme $R \neq \emptyset$ dotato di due operazioni $+$ e $\cdot$ tali che

- $(R, +)$ è un gruppo abeliano in cui 0 denota l'elemento neutro,
- $(R, \cdot)$ è un semigruppo,
- vale la proprietà distributiva della somma rispetto al prodotto, cioè

$$(x + y) \cdot z = x \cdot z + y \cdot z,$$
$$z \cdot (x + y) = z \cdot x + z \cdot y.$$

Se c'è un elemento $e \in R$ tale che $x \cdot e = e \cdot x = x$, per tutti gli $x \in R$, diremo che l'anello è **unitario** e l'elemento e viene denotato con $1 = 1_R$. Un anello si dice **commutativo** se l'operazione $\cdot$ è commutativa. Un **dominio**

di integrità è un anello commutativo in cui non ci sono divisori dello 0, cioè $x \cdot y = 0 \Rightarrow x = 0 \vee y = 0$. Un **corpo**[1] è un anello unitario R in cui $0 \neq 1$ e ogni elemento non nullo ha un inverso, cioè

$$\forall x \in R \setminus \{0\}\, \exists y \in R \setminus \{0\}\, (x \cdot y = y \cdot x = 1)\,.$$

Un corpo commutativo si dice **campo**. Il tipico esempio di corpo non commutativo sono i quaternioni $\mathbb{H}$, mentre, per un teorema di Wedderburn, ogni corpo finito è un campo [**Wei95**]. La caratteristica di un campo è il più piccolo intero $p > 0$ tale che $\underbrace{1 + \cdots + 1}_{p \text{ volte}} = 0$ — se questo intero p esiste allora è un numero primo, se non esiste, diremo che il campo ha caratteristica 0.

Se R è un anello $R[X]$ è l'anello dei polinomi a coefficienti in R. Un campo $\Bbbk$ si dice **algebricamente chiuso** se ogni polinomio non nullo in $\Bbbk[X]$ ha una soluzione in $\Bbbk$. Un numero complesso si dice algebrico se è soluzione di un polinomio di $\mathbb{Q}[X]$ — equivalentemente, se è soluzione di un polinomio di $\mathbb{Z}[X]$. Un numero complesso che non sia algebrico si dice trascendente. L'insieme dei numeri algebrici forma un campo algebricamente chiuso $\overline{\mathbb{Q}}$ ed è il più piccolo campo algebricamente chiuso di caratteristica 0.

Uno **spazio vettoriale** su un campo $\Bbbk$ è un gruppo abeliano $\langle V, +, \mathbf{0}\rangle$ con una funzione $\Bbbk \times V \to V$, $(r, \mathbf{v}) \mapsto r\mathbf{v}$ detta prodotto per scalare, che soddisfa le seguenti identità, per ogni $r, s \in \Bbbk$ e ogni $\mathbf{u}, \mathbf{v} \in V$:

$$\begin{aligned} r(\mathbf{u} + \mathbf{v}) &= r\mathbf{u} + r\mathbf{v} \\ (r + s)\mathbf{u} &= r\mathbf{u} + s\mathbf{u} \\ (r \cdot s)\mathbf{u} &= r(s\mathbf{u}) \\ 1_{\Bbbk}\mathbf{u} &= \mathbf{u}. \end{aligned}$$

Gli elementi di V si dicono vettori, gli elementi di $\Bbbk$ si dicono scalari.

Un insieme $X \subseteq V$ si dice linearmente dipendente se esistono $\mathbf{v}_1, \ldots, \mathbf{v}_n \in X$ ed esistono scalari $r_1, \ldots, r_n \in \Bbbk$ tali che

- $(r_1, \ldots, r_n) \neq (0_{\Bbbk}, \ldots, 0_{\Bbbk})$ e
- $\sum_{i=1}^{n} r_i \mathbf{v}_i = \mathbf{0}$.

Se X non è linearmente dipendente, diremo che è linearmente indipendente. Un $X \subseteq V$ è un insieme di generatori di V, se ogni $\mathbf{v} \in V$ può essere espresso come combinazione lineare $\mathbf{v} = \sum_{i=1}^{n} r_i \mathbf{v}_i$, per qualche $\mathbf{v}_1, \ldots, \mathbf{v}_n \in X$ e $r_1, \ldots, r_n \in \Bbbk$. Uno spazio vettoriale si dice **finitamente generato** se ha un insieme finito di generatori. Una **base** di uno spazio vettoriale V è un insieme linearmente indipendente di generatori di V. Spesso nel caso degli spazi non finitamente generati si parla di **basi di Hamel**.

[1] In inglese *skew-field* o *division ring*

2. Topologia

Uno **spazio topologico** è un insieme X dotato di una famiglia $\mathcal{T} \subseteq \mathscr{P}(X)$ tale che

(1) $\emptyset, X \in \mathcal{T}$,

(2) se $A, B \in \mathcal{T}$ allora $A \cap B \in \mathcal{T}$,

(3) se $\{A_i \mid i \in I\} \subseteq \mathcal{T}$ allora $\bigcup_{i\in I} A_i \in \mathcal{T}$.

La famiglia $\mathcal{T}$ si dice **topologia** e i suoi elementi si dicono **aperti**. Quando la topologia $\mathcal{T}$ è chiara dal contesto diremo, con abuso di linguaggio, che X è uno spazio topologico.

Se $x \in V \subseteq X$ e se esiste U aperto tale che $x \in U \subseteq V$ diremo che V è un **intorno** del punto x. Se possiamo prendere $U = V$, cioè se V è aperto, parleremo di intorno aperto. Uno spazio si dice **primo-numerabile** ovvero che soddisfa al **primo assioma di numerabilità** se per ogni $x \in X$ esiste un insieme $\{V_n \mid n \in \omega\}$ di intorni di x tale che ogni intorno di x contiene uno dei V_n. Un $x \in X$ si dice **punto isolato** se $\{x\}$ è un aperto. Il complementare di un insieme aperto di dice **chiuso**. Un insieme che sia simultaneamente chiuso ed aperto si dice **chiuso-aperto**. Gli spazi X in cui gli unici insiemi chiusi-aperti sono $\emptyset$ e X si dicono **connessi**. In caso contrario si dicono sconnessi.

Se $Y \subseteq X$ l'**interno** di Y e la **chiusura** di Y sono, rispettivamente, il più grande aperto contenuto in Y e il più piccolo chiuso contenente Y, cioè

$$\mathrm{Int}(Y) = \bigcup\{U \subseteq Y \mid U \in \mathcal{T}\}$$
$$\mathrm{Cl}(Y) = \bigcap\{C \supseteq Y \mid X \setminus C \in \mathcal{T}\}.$$

La **frontiera** di Y è $\mathrm{Fr}(Y) = \mathrm{Cl}(Y) \setminus \mathrm{Int}(Y)$.

Se $Y \subseteq X$, la **topologia indotta** da X su Y è

$$\{Y \cap U \mid U \in \mathcal{T}\}$$

e diremo che Y, con questa topologia, è un sottospazio di X. Una funzione tra due spazi topologici si dice **continua** se la controimmagine di un aperto è un aperto — la funzione di inclusione tra un sottospazio e lo spazio ambiente è continua.

Un sottoinsieme Y si dice **denso** in X se $\mathrm{Cl}(Y) = X$. Uno spazio che abbia un sotto-insieme denso e numerabile si dice **separabile**.

2.A. Basi. Una **base** per una topologia su X è una $\mathcal{B} \subseteq \mathscr{P}(X)$ chiusa per intersezioni finite e tale che $\forall x \in X\, \exists B \in \mathcal{B}\, (x \in B)$. La **topologia generata da** $\mathcal{B}$ è

$$\hat{\mathcal{B}} = \{\textstyle\bigcup_{i\in I} B_i \mid \{B_i \mid i \in I\} \subseteq \mathcal{B}\}.$$

Diremo che $\mathcal{B}$ è una base per la topologia $\mathcal{T}$ se $\hat{\mathcal{B}} = \mathcal{T}$. Se uno spazio topologico ha una base numerabile diremo che è **secondo numerabile** ovvero che soddisfa al **secondo assioma di numerabilità**. Per l'assioma delle scelte numerabili, uno spazio secondo-numerabile è anche separabile (Esercizio 22.26). Per ogni $\mathcal{S} \subseteq \mathscr{P}(X)$ la famiglia

$$\{A_1 \cap \cdots \cap A_n \mid A_1, \dots, A_n \in \mathcal{S}\} \cup \{X\}$$

è una base per una topologia $\mathcal{T}$ su X e diremo che $\mathcal{S}$ è una **sottobase** per questa topologia.

Data una famiglia di spazi topologici $(Y_i, \mathcal{T}_i)$ $(i \in I)$, un insieme X e delle funzioni $F_i \colon X \to Y_i$, la topologia indotta su X dalle F_i è quella generata dagli insiemi $F_i^{-1}[U_i]$, con $U \in \mathcal{T}_i$ e $i \in I$. Una sottobase per questa topologia è

$$\{F_i^{-1}[U_i] \mid U_i \in \mathcal{T}_i, i \in I\}$$

e quindi un aperto di base è della forma

$$\left\{F_i^{-1}[U_i] \mid U_i \in \mathcal{T}_i, i \in J, J \subseteq I \text{ finito}\right\}.$$

Questa topologia $\mathcal{T}$ rende ogni F_i continua ed è la minima topologia siffatta, nel senso che ogni topologia su X che rende tutte le F_i continue deve contenere $\mathcal{T}$. Se prendiamo come $X = \bigtimes_{i\in I} Y_i$ il prodotto cartesiano degli spazi Y_i e $F_i \colon X \to Y_i$ è la funzione valutazione $f \mapsto f(i)$, si ottiene la **topologia prodotto** o **topologia di Tychonoff** i cui aperti di base sono della forma

$$\begin{aligned} \boldsymbol{N}(U_{i_0}, \dots, U_{i_n}) &= \{f \in \textstyle\bigtimes_{i\in I} Y_i \mid f(i_k) \in U_{i_k},\ k = 0, \dots, n\} \\ &= \textstyle\bigtimes_{j\in\{i_0,\dots,i_n\}} U_j \times \bigtimes_{i\in I\setminus\{i_0,\dots,i_n\}} Y_i \end{aligned}$$

dove $\{i_0, \dots, i_n\} \subseteq I$ e U_{i_k} è aperto in Y_{i_k}.

2.B. Assiomi di separazione. Gli spazi topologici possono essere classificati in base alla loro abilità di distinguere punti mediante aperti. Uno spazio topologico $(X, \mathcal{T})$ si dice

T_0 se punti distinti hanno famiglie degli intorni distinte,

$$x \neq y \Rightarrow \exists U \in \mathcal{T}\,((x \in U \wedge y \notin U) \vee (y \in U \wedge x \notin U))$$

T_1 se punti distinti sono distinguibili mediante aperti,

$$x \neq y \Rightarrow \exists U, V \in \mathcal{T}\,(x \in U \wedge y \notin U \wedge y \in V \wedge x \notin V)\,.$$

Equivalentemente: X è T_1 se $\{x\}$ è un chiuso, per ogni $x \in X$.

T_2 o di **Hausdorff** se punti distinti sono separabili mediante aperti,

$$x \neq y \Rightarrow \exists U, V \in \mathcal{T}\,(x \in U \wedge y \in V \wedge U \cap V = \emptyset)$$

T_3 o **regolare** se è possibile separare un punto x da un chiuso C mediante aperti, cioè

$$x \notin C \Rightarrow \exists U, V \in \mathcal{T}\,(x \in U \wedge C \subseteq V \wedge U \cap V = \emptyset)\,.$$

Equivalentemente: X è T_3 se per ogni aperto U e ogni $x \in U$, è possibile trovare un aperto V tale che $x \in V \subseteq \mathrm{Cl}(V) \subseteq U$. Se X è T_0, allora T_3 implica T_2.

2.C. Compattezza. Sia X uno spazio topologico e sia K un suo sottospazio. Un **ricoprimento aperto** di K è una famiglia $\{A_i \mid i \in I\}$ di aperti che ricoprono K, cioè $K \subseteq \bigcup_{i\in I} A_i$. Diremo che K è **compatto** se da ogni ricoprimento aperto $\{A_i \mid i \in I\}$ possiamo estrarre un sotto-ricoprimento finito, cioè se esiste $I_0 \subseteq I$ finito tale che $K \subseteq \bigcup_{i\in I_0} A_i$. In generale diremo che uno spazio topologico è compatto se lo è come sottospazio di sé stesso. Uno spazio è compatto se ogni famiglia $\mathcal{C}$ di chiusi ha la **proprietà dell'intersezione finita**: se $\forall C_1, \ldots, C_n \in \mathcal{C}\,(C_1 \cap \cdots \cap C_n \neq \emptyset)$, allora $\bigcap_{C\in\mathcal{C}} C \neq \emptyset$. Un chiuso di un compatto è compatto. Uno spazio compatto è T_3: se $x \notin C$ e C è chiuso (e quindi compatto), scegliamo aperti U_y e V_y disgiunti con $x \in U_y$ e $y \in V_y$. Poiché $\{V_y \mid y \in C\}$ ricopre C possiamo estrarre un sotto-ricoprimento finito $\{V_{y_1}, \ldots, V_{y_n}\}$. Allora $x \in U_{y_1} \cap \cdots \cap U_{y_n} = U$, $C \subseteq V_{y_1} \cup \cdots \cup V_{y_n} = V$ e $U \cap V = \emptyset$.

Uno spazio topologico si dice **localmente compatto** se è T_2 e ogni punto ha un intorno la cui chiusura è compatta. Equivalentemente: se U è aperto e $x \in U$ allora $\exists V$ aperto tale che $x \in V \subseteq \mathrm{Cl}(V) \subseteq U$ e $\mathrm{Cl}(V)$ è compatto.

2.D. Spazi metrici. Uno **spazio metrico** è un insieme X dotato di una **metrica** $d\colon X \times X \to [0; +\infty)$ che soddisfa alle tre proprietà:

- $d(x, y) = 0$ se e solo se $x = y$,
- $d(x, y) = d(y, x)$, per ogni $x, y \in X$,
- $d(x, y) \leq d(x, z) + d(z, y)$, per ogni $x, y, z \in X$.

La **palla aperta** di centro $x \in X$ e raggio $r > 0$ è l'insieme

$$\mathrm{B}(x; r) = \mathrm{B}_{(X,d)}(x; r) \stackrel{\text{def}}{=} \{y \in X \mid d(x, y) < r\}$$

mentre la palla chiusa $\mathrm{B}(x; r)^{\mathrm{cl}}$ ha la medesima definizione, con $\leq$ al posto di $<$. Il **diamtero** di un insieme $A \subseteq X$ è

$$\mathrm{diam}(A) = \sup\{d(x, y) \mid x, y \in A\}.$$

Un insieme si dice limitato se il suo diametro è $< \infty$.

Uno spazio metrico è anche uno spazio topologico, prendendo come sotto-base la famiglia delle palle aperte. Inoltre la topologia così ottenuta è T_0 e T_3 e soddisfa al primo assioma di numerabilità. Uno spazio metrico separabile è

anche secondo-numerabile: se D è un sottoinsieme denso e numerabile basta prendere come base $\{\mathrm{B}(x;q) \mid x \in D \wedge q \in \mathbb{Q}_+\}$.

Una successione $(x_n)_n$ in uno spazio metrico (X,d) converge ad un $x \in X$ se $\forall \varepsilon > 0\, \exists N\, \forall n > N\ (d(x_n,x) < \varepsilon)$. Una successione si dice di **Cauchy** se

$$\forall \varepsilon > 0\, \exists N\, \forall n,m > N\, d(x_n,x_m) < \varepsilon.$$

Uno spazio metrico si dice **completo** se ogni successione di Cauchy converge in X. In questo caso la metrica si dirà **completa**.

Indici

Qui sotto troverete tre indici: **Persone**, **Concetti** e **Simboli**. Nel primo troverete l'elenco dei matematici citati nel testo (per esempio: Kurt Gödel), ma non i teoremi o i concetti legati al nome di un matematico, che invece si trovano nel secondo indice (per esempio: Teorema|Primo — di incompletezza di Gödel). Il terzo indice contiene l'elenco dei più importanti simboli matematici usati nel testo (per quelli più comuni si vedano i Preliminari).

Concetti

Persone

Simboli

Bibliografia

[AH76] K. Appel and W. Haken. Every planar map is four colorable. *Bull. Amer. Math. Soc.*, 82(5):711–712, 1976.

[AM69] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[Bai88] David H. Bailey. The computation of π to $29,360,000$ decimal digits using Borweins' quartically convergent algorithm. *Math. Comp.*, 50(181):283–296, 1988.

[Bal84] Richard N. Ball. Distributive Cauchy lattices. *Algebra Universalis*, 18(2):134–174, 1984.

[Bel09] John L. Bell. *The axiom of choice*, volume 22 of *Studies in Logic (London)*. College Publications, London, 2009. Mathematical Logic and Foundations.

[Bès01] Alexis Bès. A survey of arithmetical definability. *Bull. Belg. Math. Soc. Simon Stevin*, (suppl.):1–54, 2001. A tribute to Maurice Boffa.

[Bla77] Andreas Blass. A model without ultrafilters. *Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys.*, 25(4):329–331, 1977.

[Bla79] Andreas Blass. Injectivity, projectivity, and the axiom of choice. *Trans. Amer. Math. Soc.*, 255:31–59, 1979.

[Bla84] Andreas Blass. Existence of bases implies the axiom of choice. In *Axiomatic set theory (Boulder, Colo., 1983)*, volume 31 of *Contemp. Math.*, pages 31–33. Amer. Math. Soc., Providence, RI, 1984.

[Boo88] George Boolos. Alphabetical order. *Notre Dame J. Formal Logic*, 29(2):214–215, 1988.

[Byr46] L. Byrne. Two brief formulations of Boolean algebra. *Bulletin (New Series) of the American Mathematical Society*, 52(4):269–272, 1946.

[CHR03] Patrick Cégielski, François Heroult, and Denis Richard. On the amplitude of intervals of natural numbers whose every element has a common prime divisor with at least an extremity. *Theoret. Comput. Sci.*, 303(1):53–62, 2003. Logic and complexity in computer science (Créteil, 2001).

[Con78] John B. Conway. *Functions of one complex variable*, volume 11 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1978.

[Coo93] Roger Cooke. Uniqueness of trigonometric series and descriptive set theory, 1870–1985. *Arch. Hist. Exact Sci.*, 45(4):281–334, 1993.

[Cra11] Marcel Crabbé. Cantor-Bernstein's Theorem in a Semiring. *The Mathematical Intelligencer*, 33(3):80, 2011.

[CTV76] Checcucci, Tognoli, and Vesentini. *Lezioni di topologia generale*. Feltrinelli, Milano, 1976.

[Dav55] Anne C. Davis. A characterization of complete lattices. *Pacific J. Math.*, 5:311–319, 1955.

[Die05] Reinhard Diestel. *Graph theory*, volume 173 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, third edition, 2005.

[Dow89] David L. Dowe. On the existence of sequences of co-prime pairs of integers. *J. Austral. Math. Soc. Ser. A*, 47(1):84–89, 1989.

[DP02] B. A. Davey and H. A. Priestley. *Introduction to lattices and order*. Cambridge University Press, New York, second edition, 2002.

[End01] Herbert B. Enderton. *A mathematical introduction to logic*. Harcourt/Academic Press, Burlington, MA, second edition, 2001.

[Eng89] Ryszard Engelking. *General topology*, volume 6 of *Sigma Series in Pure Mathematics*. Heldermann Verlag, Berlin, second edition, 1989. Translated from the Polish by the author.

[Fol99] Gerald B. Folland. *Real analysis*. Pure and Applied Mathematics (New York). John Wiley & Sons Inc., New York, second edition, 1999. Modern techniques and their applications, A Wiley-Interscience Publication.

[Fre03] D. H. Fremlin. *Measure theory. Vol. 2*. Torres Fremlin, Colchester, 2003. Broad foundations, Corrected second printing of the 2001 original.

[Fre04a] D. H. Fremlin. *Measure theory. Vol. 1*. Torres Fremlin, Colchester, 2004. The irreducible minimum, Corrected third printing of the 2000 original.

[Fre04b] D. H. Fremlin. *Measure theory. Vol. 3*. Torres Fremlin, Colchester, 2004. Measure algebras, Corrected second printing of the 2002 original.

[Fre06] D. H. Fremlin. *Measure theory. Vol. 4*. Torres Fremlin, Colchester, 2006. Topological measure spaces. Part I, II, Corrected second printing of the 2003 original.

[Fre08] D. H. Fremlin. *Measure theory. Vol. 5*. Torres Fremlin, Colchester, 2008. Topological measure spaces. Part I, II, Corrected second printing of the 2003 original.

[FW91] Matthew Foreman and Friedrich Wehrung. The Hahn-Banach theorem implies the existence of a non-Lebesgue measurable set. *Fund. Math.*, 138(1):13–19, 1991.

[Gol84] Robert Goldblatt. *Topoi*, volume 98 of *Studies in Logic and the Foundations of Mathematics*. North-Holland Publishing Co., Amsterdam, second edition, 1984. The categorial analysis of logic.

[Gol96] Dorian M. Goldfeld. Beyond the last theorem. *Math Horizons*, 1996.

[Goo91] K. R. Goodearl. *von Neumann regular rings*. Robert E. Krieger Publishing Co. Inc., Malabar, FL, second edition, 1991.

[Grä11] George Grätzer. *Lattice theory: foundation*. Birkhäuser/Springer Basel AG, Basel, 2011.

[GT02] Andrew Granville and Thomas J. Tucker. It's as easy as *abc*. *Notices Amer. Math. Soc.*, 49(10):1224–1231, 2002.

[Guy04] Richard K. Guy. *Unsolved problems in number theory*. Problem Books in Mathematics. Springer-Verlag, New York, third edition, 2004.

[HÖ5] Lars Hörmander. *The analysis of linear partial differential operators. II*. Classics in Mathematics. Springer-Verlag, Berlin, 2005. Differential operators with constant coefficients, Reprint of the 1983 original.

[Hen60] Leon Henkin. On mathematical induction. *The American Mathematical Monthly*, 67:323–338, 1960.

[Her97] Horst Herrlich. The Ascoli theorem is equivalent to the Boolean prime ideal theorem. *Rostock. Math. Kolloq.*, (51):137–140, 1997.

[Her06] Horst Herrlich. *Axiom of choice*, volume 1876 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 2006.

[HL71] J. D. Halpern and A. Lévy. The Boolean prime ideal theorem does not imply the axiom of choice. In *Axiomatic Set Theory (Proc. Sympos. Pure Math., Vol. XIII, Part I, Univ. California, Los Angeles, Calif., 1967)*, pages 83–134. Amer. Math. Soc., Providence, R.I., 1971.

[Hod79] Wilfrid Hodges. Krull implies Zorn. *J. London Math. Soc. (2)*, 19(2):285–287, 1979.

[Hod93] Wilfrid Hodges. *Model theory*, volume 42 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 1993.

[HR98] Paul Howard and Jean E. Rubin. *Consequences of the axiom of choice*, volume 59 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 1998. With 1 IBM-PC floppy disk (3.5 inch; WD).

[Hun80] Thomas W. Hungerford. *Algebra*, volume 73 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1980. Reprint of the 1974 original.

[Huu94] Taneli Huuskonen. Constants are definable in rings of analytic functions. *Proc. Amer. Math. Soc.*, 122(3):697–702, 1994.

[HW79] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. The Clarendon Press Oxford University Press, New York, fifth edition, 1979.

[IR90] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

[Jac85] Nathan Jacobson. *Basic algebra. I*. W. H. Freeman and Company, New York, second edition, 1985.

[Jec73] Thomas J. Jech. *The axiom of choice*. North-Holland Publishing Co., Amsterdam, 1973. Studies in Logic and the Foundations of Mathematics, Vol. 75.

[Jec03] Thomas Jech. *Set theory*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2003. The third millennium edition, revised and expanded.

[Joh84] P. T. Johnstone. Almost maximal ideals. *Fund. Math.*, 123(3):197–209, 1984.

[Kap95] Irving Kaplansky. *Fields and rings*. Chicago Lectures in Mathematics. University of Chicago Press, Chicago, IL, 1995. Reprint of the second (1972) edition.

[Kel55] John L. Kelley. *General Topology*. D. van Nostrand, 1955.

[Koe] Jochen Koenigsmann. Defining $\mathbb{Z}$ in $\mathbb{Q}$. arXiv:1011.3424v1.

[Kop89] Sabine Koppelberg. *Handbook of Boolean algebras. Vol. 1.* North-Holland Publishing Co., Amsterdam, 1989. Edited by J. Donald Monk and Robert Bonnet.

[Kun83] Kenneth Kunen. *Set theory*, volume 102 of *Studies in Logic and the Foundations of Mathematics*. North-Holland Publishing Co., Amsterdam, 1983. An introduction to independence proofs, Reprint of the 1980 original.

[Kur92] Casimir Kuratowski. *Topologie. I et II.* Éditions Jacques Gabay, Sceaux, 1992. Part I with an appendix by A. Mostowski and R. Sikorski, Reprint of the fourth (Part I) and third (Part II) editions.

[Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[Lev02] Azriel Levy. *Basic set theory*. Dover Publications Inc., Mineola, NY, 2002. Reprint of the 1979 Springer edition.

[LR84] D. H. Luecking and L. A. Rubel. *Complex analysis*. Universitext. Springer-Verlag, New York, 1984. A functional analysis approach.

[Man03] Zohar Manna. *Mathematical theory of computation*. Dover Publications Inc., Mineola, NY, 2003. Reprint of the 1974 original [McGraw-Hill, New York; MR0400771].

[Mar02] David Marker. *Model theory*, volume 217 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002. An introduction.

[Maz02] Stefano Mazzanti. Plain bases for classes of primitive recursive functions. *MLQ Math. Log. Q.*, 48(1):93–104, 2002.

[MB89a] J. Donald Monk and Robert Bonnet, editors. *Handbook of Boolean algebras. Vol. 2.* North-Holland Publishing Co., Amsterdam, 1989.

[MB89b] J. Donald Monk and Robert Bonnet, editors. *Handbook of Boolean algebras. Vol. 3.* North-Holland Publishing Co., Amsterdam, 1989.

[Men70] Elliott Mendelson. *Theory and problems of Boolean algebra and switching circuits*. McGraw-Hill Book Co., New York, 1970. Schaum's Outline Series.

[ML98] Saunders Mac Lane. *Categories for the working mathematician*, volume 5 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1998.

[Mon69] J. Donald Monk. *Introduction to set theory*. McGraw-Hill Book Co., New York, 1969.

[Mon75] Donald Monk. *Teoria assiomatica degli insiemi*. Boringhieri, Torino, 1975.

[Mor65] Anthony P. Morse. *A theory of sets*. Pure and Applied Mathematics, Vol. XVIII. Academic Press, New York, 1965.

[MPV03] William McCune, R. Padmanabhan, and Robert Veroff. Yet another single law for lattices. *Algebra Universalis*, 50(2):165–169, 2003.

[MS96] W. McCune and A. D. Sands. Computer and human reasoning: single implicative axioms for groups and for abelian groups. *Amer. Math. Monthly*, 103(10):888–892, 1996.

[MVF+02] W. McCune, R. Veroff, B. Fitelson, K. Harris, A. Feist, and L. Wos. Short single axioms for Boolean algebra. *Journal of Automated Reasoning*, 29(1):1–16, 2002.

[MW96] Angus Macintyre and A. J. Wilkie. On the decidability of the real exponential field. In *Kreiseliana*, pages 441–467. A K Peters, Wellesley, MA, 1996.

[OtR85] A. M. Odlyzko and H. J. J. te Riele. Disproof of the Mertens conjecture. *J. Reine Angew. Math.*, 357:138–160, 1985.

[Oxt80] John C. Oxtoby. *Measure and category*, volume 2 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1980. A survey of the analogies between topological and measure spaces.

[Paw91] Janusz Pawlikowski. The Hahn-Banach theorem implies the Banach-Tarski paradox. *Fund. Math.*, 138(1):21–22, 1991.

[PD11] Alexander Prestel and Charles N. Delzell. *Mathematical Logic and Model Theory*. Springer, 2011.

[Rav77] Yehuda Rav. Variants of Rado's selection lemma and their applications. *Math. Nachr.*, 79:145–165, 1977.

[Ric85] Denis Richard. Answer to a problem raised by J. Robinson: the arithmetic of positive or negative integers is definable from successor and divisibility ["Definability and decision problems in arithmetic", J. Symbolic Logic **14** (1949), 98–114; MR **11**, 151]. *J. Symbolic Logic*, 50(4):927–935 (1986), 1985.

[Rob49] Julia Robinson. Definability and decision problems in arithmetic. *J. Symbolic Logic*, 14:98–114, 1949.

[Rob51] Raphael M. Robinson. Undecidable rings. *Trans. Amer. Math. Soc.*, 70:137–159, 1951.

[Ros82] Joseph G. Rosenstein. *Linear orderings*, volume 98 of *Pure and Applied Mathematics*. Academic Press Inc. [Harcourt Brace Jovanovich Publishers], New York, 1982.

[Ros03] Haskell P. Rosenthal. The Banach spaces $C(K)$. In *Handbook of the geometry of Banach spaces, Vol. 2*, pages 1547–1602. North-Holland, Amsterdam, 2003.

[RR85] Herman Rubin and Jean E. Rubin. *Equivalents of the axiom of choice. II*, volume 116 of *Studies in Logic and the Foundations of Mathematics*. North-Holland Publishing Co., Amsterdam, 1985.

[Rud91] Walter Rudin. *Functional analysis*. International Series in Pure and Applied Mathematics. McGraw-Hill Inc., New York, second edition, 1991.

[Sag75] Gershon Sageev. An independence result concerning the axiom of choice. *Ann. Math. Logic*, 8:1–184, 1975.

[Sch97] Eric Schechter. *Handbook of analysis and its foundations*. Academic Press Inc., San Diego, CA, 1997.

[Smo91] Craig Smoryński. *Logical number theory. I.* Universitext. Springer-Verlag, Berlin, 1991. An introduction.

[Tar55] Alfred Tarski. A lattice-theoretical fixpoint theorem and its applications. *Pacific J. Math.*, 5:285–309, 1955.

[Thu82] William P. Thurston. Three-dimensional manifolds, Kleinian groups and hyperbolic geometry. *Bull. Amer. Math. Soc. (N.S.)*, 6(3):357–381, 1982.

[vdD98] Lou van den Dries. *Tame topology and o-minimal structures*, volume 248 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1998.

[Wag93] Stan Wagon. *The Banach-Tarski paradox*. Cambridge University Press, Cambridge, 1993. With a foreword by Jan Mycielski, Corrected reprint of the 1985 original.

[Wei95] André Weil. *Basic number theory*. Classics in Mathematics. Springer-Verlag, Berlin, 1995. Reprint of the second (1973) edition.

[Wil96] A. J. Wilkie. Model completeness results for expansions of the ordered field of real numbers by restricted Pfaffian functions and the exponential function. *J. Amer. Math. Soc.*, 9(4):1051–1094, 1996.

[Woo] Kevin Woods. Presburger arithmetic, rational generating functions, and quasi-polynomials.

[Woo81] Alan Robert Woods. *Some problems in logic and number theory, and their connections*. PhD thesis, Manchester University, 1981.