

Matematica Discreta
2026/2027
Appunti del corso

Rosario Mennuni
Università degli studi di Bari Aldo Moro

Indice

1	Insiemi	1
1.1	Insiemi e come denotarli	1
1.2	Avere gli stessi elementi (o qualcuno in meno)	3
1.3	Operazioni fra insiemi	6
1.4	Esercizi	13
1.5	Digressione: fare bootstrapping della matematica	15
2	Logica	19
2.1	Enunciati	19
2.2	Connettivi	20
2.3	Ancora altri connettivi	24
2.4	Variabili e quantificatori	29
2.5	Come (non) usare i quantificatori	32
2.6	Simboli con gli angoli vs. simboli tondi	36
2.7	Logica del second'ordine e numeri naturali	37
2.8	Esercizi	39
2.9	Digressione: altre logiche	41

Readme

Cos'è questo documento? Questi sono gli appunti del corso di Matematica Discreta, canale E–M, tenuto all'Università degli studi di Bari Aldo Moro da Rosario Mennuni.

Cosa non è questo documento?

Completo. Sono appunti per le lezioni scritti mentre il corso progredisce, e quella che state vedendo è una versione parziale.

Senza errori. Questi appunti non hanno subito alcun processo editoriale di revisione e con probabilità molto alta contengono errori, refusi, etc. Se ne trovate, vi incoraggio caldamente a segnalarmeli all'indirizzo email a pagina [pagina iii](#).

Un libro. Il materiale di questo corso è coperto da tanti libri, che spesso contengono molti esercizi, etc.

L'unica cosa che dovrete leggere. Meglio integrare con libri (ad esempio [[BG05](#); [PC08](#); [Ros19](#)]¹), altri appunti (come quelli di altri canali dello stesso corso [[Azz26b](#); [Iac25a](#)]), vecchie tracce d'esame e relative soluzioni [[Iac26](#)], pagine Wikipedia (meglio se in inglese), video... Sugli argomenti di questo corso è stato prodotto veramente tanto materiale. Usatelo!

Cosa ci facciamo con questo documento? Quello che vi pare. Leggetelo, studiatelo, condividetelo, modificalo... Questo documento è rilasciato sotto una licenza parecchio permissiva e il codice sorgente (in $\text{\LaTeX}$) è più sotto. Quindi se volete farne versioni annotate, cambiare il font o il layout, mettere su un repository e modificarli in maniera collaborativa, rifarli in `typst` perché vi piace più di $\text{\LaTeX}$, etc, fate pure.

Dove trovo l'ultima versione di questi appunti? Sulla mia pagina, al link https://www.dm.uniba.it/it/members/rosario-mennuni/md2627_mennuni.pdf

Ho una versione precedente di questi appunti, come scopro cosa è cambiato? Se i pdf non sono troppo diversi potete provare a darli in pasto a `diffpdf`. Altrimenti, recuperate i file sorgente (vedi sotto) e usate il vostro

¹Questo è un riferimento bibliografico e punta alla bibliografia, che si trova verso la fine delle documento. Se state guardando questi appunti in pdf, il colore denota dei link.

programma preferito. Raccomando `latexdiff` oppure `ediff` (una funzione di `emacs`).

Ho imparato questi appunti a memoria ma ho molta difficoltà con gli esercizi, passerò l'esame? La probabilità che questo succeda è *molto* bassa. Per lo stesso motivo per cui non c'è verso che impariate a programmare leggendo vagonate di codice senza mai scriverne una riga.

Ho imparato gli argomenti di questi appunti e so fare gli esercizi, passerò l'esame? Forse.

Ma quindi per passare l'esame...? Bisogna superare lo scritto e, se si decide di sostenere l'orale, passare anche quello [Iac25b]. Se conoscete bene il contenuto di questi appunti, siete in grado di esporre quello che contengono in maniera soddisfacente, e sapete risolvere a occhi chiusi esercizi simili a quelli delle tracce d'esame degli anni passati, la probabilità di passarlo è *molto* alta.

Come imparo a fare gli esercizi? Fatene tanti, fate gli scritti degli appelli precedenti, confrontate quello che avete fatto con le soluzioni, confrontatevi fra di voi, chiedete al docente, al tutor, a chi ha già fatto il corso, etc. Queste ultime cose sono particolarmente importanti per gli esercizi che chiedono di dimostrare qualcosa dato che, specie all'inizio, è facile convincersi di aver dimostrato qualcosa e non accorgersi che l'argomento ha delle mancanze o dei bug.

Ma se gli esercizi li faccio con un LLM va bene? Fate quello che vi pare, ma i primi studi dicono che probabilmente all'esame fate peggio. [SLW26] (No, all'esame potete usare solo penna e calcolatrice (non quella del cellulare), vedi regole d'esame [Iac25b]).

Info

- Per contattarmi a riguardo di queste note (domande, chiarimenti, segnalazione di errori, etc), scrivete a rosario.mennuni@uniba.it.
- Pagina elearning del corso: <https://elearning.uniba.it/course/view.php?id=14635>
- Esiste un canale Telegram per annunci dell'ultimo minuto (ad esempio, lezioni annullate per imprevisti) e per domande di interesse generale per le partecipanti del corso. Il link di invito si trova sulla pagina elearning del corso.

Versione e codice Questa versione è stata compilata in data 1 ottobre 2026 alle 18:24. Il sorgente di questi appunti è disponibile facendo clic destro² sulla graffetta a sinistra, quello della bibliografia è nella graffetta a destra.



²O quello che il vostro visualizzatore di pdf usa per aprire gli allegati. Sì, i pdf possono avere allegati.

Rosario Mennuni

Quest'opera è distribuita con licenza [Creative Commons «Attribuzione 4.0 Internazionale»](#).



Capitolo 1

Insiemi

In questo capitolo parliamo di insiemi e delle loro proprietà di base. Ne approfittiamo per introdurre un po' di gergo matematico, fare le nostre prime dimostrazioni, e imparare qualche tecnica per farle.

1.1 Insiemi e come denotarli

Un *insieme* è una collezione di elementi.

Esempio 1.1. Qualche esempio di insieme.

1. L'insieme il cui unico elemento è il numero 2.
2. L'insieme il cui unico elemento è l'Italia.
3. L'insieme vuoto, denotato con $\emptyset$. È l'unico insieme che non ha nessun elemento.
4. L'insieme degli stati che confinano con San Marino.
5. L'insieme i cui elementi sono: 1, 3, 5, 7, 9.
6. L'insieme i cui elementi sono: 5, l'Italia, e GNU/Linux.
7. L'insieme il cui unico elemento è l'insieme vuoto. Questo insieme *non* è l'insieme vuoto: a differenza di quest'ultimo, ha un elemento.¹
8. L'insieme dei numeri naturali, cioè dei numeri interi non negativi²: 0, 1, 2, 3, 4, ...
Questo insieme si denota con $\mathbb{N}$.
9. L'insieme dei numeri naturali dispari minori di 10.
10. L'insieme i cui elementi sono: 5, l'Italia, GNU/Linux, l'insieme dei numeri naturali, l'insieme vuoto, e l'insieme di cui al punto 5 sopra.

Sì, gli insiemi possono essere elementi di altri insiemi.

¹La maniera migliore in cui abbia sentito spiegare la differenza fra questo insieme e l'insieme vuoto è: è la stessa differenza fra avere il portafogli vuoto e non avere nemmeno il portafogli.

²In queste note consideriamo 0 un numero naturale, ma è bene sapere che in alcuni testi $\mathbb{N}$ denota l'insieme degli interi strettamente positivi.

Notazione 1.2. Per dire che a è un elemento dell'insieme B , scriviamo $a \in B$. Questa scrittura si può pronunciare in varie maniere, tipicamente “ a in B ”, “ a appartiene a B ”, “ a è un elemento di B ”. Per dire che a non è un elemento di B si scrive $a \notin B$, pronunciato “ a non in B ”, o “ a non appartiene a B ”, etc.

Esempio 1.3. Se X è l'insieme dell'Esempio 1.1.5, allora $5 \in X$ e $6 \notin X$, e anche $13 \notin X$.

Spesso gli insiemi vengono denotati con lettere (latine) maiuscole, e.g.³ A, B, C, X, Y, Z , e i loro elementi con lettere minuscole. Questo non è un obbligo, e ha perfettamente senso scrivere cose come $A \in B$ o $a \in b$.

Ora, scrivere cose come “l'insieme i cui elementi sono:” ogni volta diventa molto noioso molto in fretta. Tipicamente, invece di scriverlo a parole si usano le parentesi graffe. Dentro, o si elencano gli elementi dell'insieme separati da virgole, o si dà una descrizione degli elementi in una maniera che faccio prima a mostrarvi che a spiegare a parole.

Esempio 1.4. Gli insiemi nell'Esempio 1.1 possono essere anche denotati rispettivamente⁴ come segue:

1. $\{2\}$
2. $\{\text{Italia}\}$
3. $\{\}$
4. $\{x \text{ stato} \mid x \text{ confina con San Marino}\}$ o anche, chiamando S l'insieme degli stati, $\{x \in S \mid x \text{ confina con San Marino}\}$. Tipicamente la barretta $\mid$ si legge “tale che” o “tali che” o similmente. La prima descrizione si può leggere, ad esempio, “l'insieme degli x stato tale che x confina con San Marino”, oppure “l'insieme degli stati x tali che x confina con San Marino”, e la seconda “l'insieme degli x in S tali che x confina con San Marino”.
5. $\{1, 3, 5, 7, 9\}$
6. $\{5, \text{Italia}, \text{GNU/Linux}\}$
7. $\{\emptyset\}$, o anche $\{\{\}\}$
8. Per l'insieme dei numeri naturali, in letteratura⁵, è comune scrivere cose come $\{0, 1, 2, 3, 4, \dots\}$ e lasciare al lettore il compito di capire dal contesto cosa ci va al posto dei puntini. Questa non è veramente una definizione formale, ma spesso si prendere per buono che l'insieme $\mathbb{N}$ dei numeri naturali “sia lì” in qualche maniera. Se non vi va bene prendere l'insieme $\mathbb{N}$ per buono, potete leggere la Sezione 1.5.
9. $\{x \in \mathbb{N} \mid (\exists y \in \mathbb{N} \ x = 2y + 1) \wedge (x \leq 10)\}$. Questo si legge “l'insieme degli x in $\mathbb{N}$ tali che esiste y in $\mathbb{N}$ tale che $x = 2y + 1$ e x è minore o uguale di 10”. Anche qui, su simboli come $\exists, \wedge$, ci torniamo.

³Abbreviazione per “ad esempio” (*exempli gratia*).

⁴Nel senso che il numero n dell'esempio Esempio 1.1 corrisponde al numero n di questo esempio.

⁵Quando un testo di matematica parla di “letteratura”, di solito di sta riferendo a libri e articoli di matematica.

10. $\{5, \text{Italia}, \text{GNU/Linux}, \mathbb{N}, \emptyset, \{1, 3, 5, 7, 9\}\}$.

Invece della barretta $|$, per denotare gli insiemi vengono usati anche i due punti, ad esempio $\{x \text{ stato} : x \text{ confina con San Marino}\}$.

1.2 Avere gli stessi elementi (o qualcuno in meno)

Un tema ricorrente in matematica è che delle cose non ci interessa tanto *cosa sono*, ma piuttosto *cosa fanno* e come si relazionano con altre cose simili. Nel caso degli insiemi, la proprietà fondamentale è la seguente.

Assioma 1.5 (di Estensionalità). Siano A e B insiemi con la proprietà che, per ogni elemento x , abbiamo che $x \in A$ se e solo se $x \in B$. Allora $A = B$.

Due commenti:

- “ P se e solo se Q ” è un’abbreviazione per “se P allora Q e se Q allora P ”. In altre parole, P e Q sono *equivalenti*. Ci torniamo.
- Il viceversa di questo assioma⁶ è banalmente vero: se $A = B$ allora A e B sono due nomi per la stessa cosa, e il fatto che un elemento x appartenga a questa cosa non dipende da come la chiamiamo.

In altre parole, l’Assioma di Estensionalità (insieme al suo ovvio viceversa) dice che:

due insiemi sono uguali se e solo se hanno gli stessi elementi.

Osservazione 1.6. In particolare, non importa in che ordine elenchiamo gli elementi di un insieme, o se invece di elencarne gli elementi lo descriviamo in un’altra maniera. Per fare un altro esempio:

$$\begin{aligned} \{1, 2, 3\} &= \{1, 3, 2\} = \{x \in \mathbb{N} \mid 0 < x < 4\} = \{x \in \mathbb{N} \mid (0 < x) \wedge (x < 4)\} \\ &= \{x \in \mathbb{N} \mid (\text{il nome di } x \text{ in italiano ha 3 lettere}) \wedge (x \neq 6)\} \end{aligned}$$

Osservazione 1.7. Inoltre, non importa se elenchiamo un qualche elemento più volte. Ad esempio, $\{2, 2, 3, 4, 6, 6, 5, 5, 5, 5\} = \{2, 3, 4, 5, 6\}$. In altre parole, un elemento non può far parte di un insieme “più di una volta”. Per esempio,

$$\begin{aligned} &\{x \text{ lettera} \mid x \text{ compare in “pappe”}\} \\ &= \{x \text{ lettera} \mid x \text{ compare in “ape”}\} \\ &= \{a, e, p\} \end{aligned}$$

Esercizio 1.8. Trovare le coppie di insiemi uguali fra quelli dell’Esempio 1.1.

Esempio 1.9. Sia A l’insieme $\{0, 1, 6\}$. Per fare prima, possiamo scrivere anche “sia $A := \{0, 1, 6\}$ ” (letto “sia A uguale per definizione a $\{0, 1, 6\}$ ”).⁷ Siano poi $B := \{6, 1, 5, 0\}$ e $C := \{6, 1, 0\}$. Allora, per estensionalità, $A = C$, e sempre per estensionalità $A \neq B$ perché $5 \in B$ e $5 \notin A$.

⁶Perché “assioma” e non “teorema”? Vedi Sezione 1.5.

⁷Notare che $:=$ e $=$ sono animali diversi. Con $A := B$ stiamo dicendo che definiamo A come B . Con $A = B$ stiamo dicendo che A e B , che sono oggetti già introdotti, o magari variabili, sono uguali. È un po’ come, in $\mathbb{C}$, la differenza fra $=$ e $==$ (con la fastidiosa differenza che $=$ in $\mathbb{C}$ corrisponde a $:=$, non a $=$).

Tuttavia, A e B sembrano chiaramente più “imparentati” fra loro che, per esempio, A e $\{3, 1, 12\}$. Questa “parentela” è il contenuto della nostra prima⁸ definizione.

Definizione 1.10. Diciamo che A è un *sottoinsieme* di B , in simboli $A \subseteq B$ sse⁹ per ogni x , se $x \in A$ allora $x \in B$.

In altre parole, $A \subseteq B$ vuol dire che ogni elemento di A è anche un elemento di B . Alcuni sinonimi di $A \subseteq B$:

- $B \supseteq A$
- B è un *sovrainsieme* di A
- A è *incluso* in B
- B *include* A

Esempio 1.11. Alcuni esempi di sottoinsiemi.

1. Per ogni insieme A , abbiamo $A \subseteq A$: ogni insieme è sottoinsieme di sé stesso. Per indicare che $A \subseteq B$ e $A \neq B$ si scrive¹⁰ $A \subsetneq B$, e si dice che A è un sottoinsieme *proprio* di B .
2. $\{4, 73\} \subseteq \mathbb{N}$.
3. $\{x \text{ lettera} \mid x \text{ compare in “pappe”}\} \subseteq \{x \text{ lettera} \mid x \text{ compare in “aperte”}\}$.
4. $\{x \text{ lettera} \mid x \text{ compare in “aperte”}\} \not\subseteq \{x \text{ lettera} \mid x \text{ compare in “chiuse”}\}$, dove $\not\subseteq$ vuol dire “non è incluso in”.¹¹ Il motivo per cui questo è vero è che, per esempio, l’insieme a sinistra contiene la lettera p , mentre l’insieme a destra no.

Prima di andare avanti, ne approfittiamo per guardare una primissima (e molto facile) dimostrazione. Il fatto che $A \subseteq A$ potrebbe aver lasciato qualcuno interdetto. Vediamo perché è vero.

Proposizione 1.12. Per ogni insieme A si ha che $A \subseteq A$.

Dimostrazione. Dobbiamo dimostrare che, dato un insieme qualunque A , l’inclusione $A \subseteq A$ è vera. Fissiamo quindi un insieme arbitrario—cioè un insieme su cui non sappiamo niente se non che è un insieme—¹²e chiamiamolo A . Per la Definizione 1.10, per dimostrare che $A \subseteq A$ dobbiamo dimostrare che dato un elemento arbitrario x , se $x \in A$ allora $x \in A$. Ma questo è ovvio. $\square$

⁸Se *non* ti stai chiedendo se “un *insieme* è una collezione di elementi” è una definizione, ignora questa nota. Se te lo stai chiedendo, vedi Sezione 1.5.

⁹La doppia *s* non è un errore di stampa. In queste note, “sse” nè un abbreviazione per “se e solo se, per definizione,”. Vuol dire che stiamo dando alla cosa a destra del “sse” il nome tipicamente enfaticizzato *in corsivo* a sinistra. È un po’ come la differenza fra il simbolo $:=$ introdotto prima e $=$, vedi Nota 7. In letteratura è molto comune, nelle definizioni, scrivere semplicemente “se”. Anche se poco comune, a volte “sse” viene usato come abbreviazione per “se e solo se” anche se non per definizione; questa pratica espone al rischio di vigorosi grattacapi come risultato di errori di stampa, e l’autore di queste note la sconsiglia vivamente.

¹⁰In letteratura, il simbolo $\subset$ viene usato a volte al posto di $\subseteq$ e a volte al posto di $\subsetneq$. Personalmente preferisco tagliare la testa al toro e non usarlo proprio.

¹¹Attenzione: $\subsetneq$ e $\not\subseteq$ vogliono dire cose diverse!

¹²È possibile usare gli emdash anche se non si è un LLM.

Il quadratino nella riga sopra vuol dire “la dimostrazione è finita”, ed è usuale metterne uno alla fine di ogni dimostrazione.

Già che ci siamo, introduciamo un po’ di gergo. Il termine “proposizione” è più o meno un sinonimo di “teorema”, ma di solito se qualcosa si chiama “teorema” tende ad avere un po’ più importanza. In entrambi i casi, è un enunciato matematico di cui esiste una dimostrazione.

Quando una proposizione segue da un’altra, a volte la si chiama *corollario* della prima. Per esempio, vediamo un corollario della Proposizione 1.12.

Corollario 1.13. Siano A e B insiemi. Allora $A = B$ se e solo se $A \subseteq B$ e $B \subseteq A$.

Dimostrazione. Per dimostrare un “se e solo se” dobbiamo dimostrare due cose: che se è vero l’enunciato a sinistra allora è vero quello a destra, e che se è vero l’enunciato a destra allora è vero quello a sinistra.

Da sinistra a destra quindi, assumiamo che $A = B$. Per la Proposizione 1.12, abbiamo $A \subseteq A$. Dato che $A = B$, possiamo sostituire B al posto della seconda A in questa inclusione e ottenere $A \subseteq B$. Sostituendo con B la prima A in $A \subseteq A$ scopriamo che $B \subseteq A$.

Da destra a sinistra, assumiamo che $A \subseteq B$ e $B \subseteq A$. Per l’Assioma di Estensionalità (Assioma 1.5), per dimostrare che $A = B$ ci basta dimostrare che, dato un elemento qualunque x , se $x \in A$ allora $x \in B$ e se $x \in B$ allora $x \in A$. Prendiamo quindi un elemento qualunque x . Se $x \in A$, dato che per ipotesi $A \subseteq B$, allora $x \in B$ per definizione di inclusione (Definizione 1.10). Similmente, se $x \in B$, dato che per ipotesi $B \subseteq A$ allora $x \in A$. $\square$

Come anticipato, un’altra maniera di dire “ P se e solo se Q ” è dire che P e Q sono equivalenti. Prima di vedere un esempio, vediamo un lemma che ci servirà per dimostrarlo. Un *lemma* è un teoremino ausiliario che tipicamente serve come passo intermedio per dimostrare qualcos’altro.

Lemma 1.14. Sia X un insieme. Se $X \subseteq \emptyset$, allora $X = \emptyset$.

Dimostrazione. Se $X \subseteq \emptyset$, per definizione di “ $\subseteq$ ” ogni elemento di X è un elemento di $\emptyset$. Dato che $\emptyset$ non ha elementi (per sua definizione), allora anche X non ne ha. Ma allora $X = \emptyset$. $\square$

Se da un lato l’insieme vuoto ha solo sé stesso come sottoinsieme, d’altra parte è sottoinsieme di tutti gli insiemi: per ogni insieme A , si ha che $\emptyset \subseteq A$. C’è di più, questa proprietà lo *caratterizza*, cioè l’insieme vuoto è l’unico insieme che ha questa proprietà. Dimostriamolo.

Proposizione 1.15. Per un insieme X , le seguenti sono equivalenti.

1. $X = \emptyset$.
2. Per ogni insieme A , abbiamo $X \subseteq A$.

Dimostrazione. Per dimostrare che $1 \Rightarrow 2$ (che si legge “1 implica 2” ed è una maniera compatta per dire che se vale 1 allora vale 2) dobbiamo mostrare che, se A è un insieme qualunque, allora $\emptyset \subseteq A$. Procediamo *per assurdo*, cioè facciamo vedere che assumendo $\emptyset \not\subseteq A$ otteniamo una contraddizione. Dato che $B \subseteq C$ vuol dire che tutti gli elementi di B sono anche elementi di C , dire che $B \not\subseteq C$

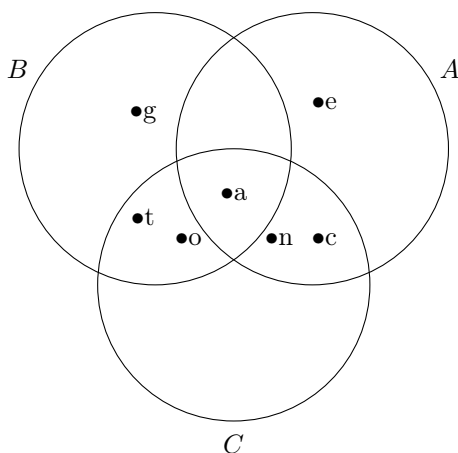


Figura 1.1: Diagramma di Venn degli insiemi A , B , C delle lettere che compaiono rispettivamente nelle parole “cane”, “gatto” e “canto”.

vuol dire che c è un elemento di B che non è un elemento di C . Quindi, se $\emptyset \not\subseteq A$, allora c è un elemento di $\emptyset$ che non è un elemento di A . Ma, a prescindere da chi sia A , se è vero questo, in particolare c è un elemento di $\emptyset$. Ma $\emptyset$, per definizione, non ha elementi. Questa è una contraddizione, e quindi $1 \Rightarrow 2$ è dimostrato.

Per dimostrare che $2 \Rightarrow 1$, facciamo una scelta di A furba. Se $X \subseteq A$ vale per tutti gli insiemi, allora in particolare vale per $A = \emptyset$. Ma allora $X \subseteq \emptyset$, e quindi $X = \emptyset$ per il Lemma 1.14 $\square$

Osservazione 1.16. L'appartenenza $\in$ e l'inclusione $\subseteq$ sono due cose diverse, e nessuna delle due implica l'altra. Per esempio, se $A = \{1, \{2, 3\}\}$, allora $\emptyset \subseteq A$ ma $\emptyset \notin A$; e se $B = \{2, 3\}$ e A è come sopra allora $B \in A$ ma $B \not\subseteq A$.

1.3 Operazioni fra insiemi

1.3.1 Diagrammi di Venn

In questa sezione introduciamo alcune comuni operazioni che si possono fare sugli insiemi e le loro proprietà di base. Per visualizzare cosa fanno queste operazioni tornano comodi i *diagrammi di Venn*, che con tutta probabilità avete già visto almeno una volta nella vita: sono quei disegni dove gli insiemi sono rappresentati da regioni nel piano delimitate da curve, e a volte i loro elementi (o anche solo alcuni di essi) sono rappresentati da pallini, stelline o quel che è. Due esempi sono nelle Figure 1.1 e 1.2.

1.3.2 Unione, intersezione e differenza

Definizione 1.17. Siano A e B due insiemi.

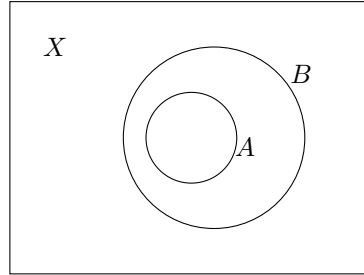


Figura 1.2: Un diagramma di Venn che rappresenta due sottoinsiemi A , B di un insieme X tali che $A \subseteq B$.

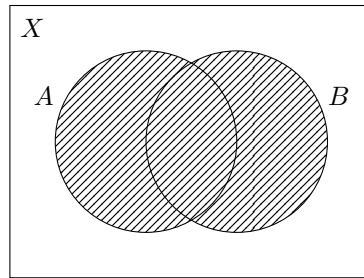


Figura 1.3: Due sottoinsiemi A , B di un insieme X , con la loro unione $A \cup B$ evidenziata a righe diagonali.

1. L'*unione* $A \cup B$ è l'insieme degli elementi x tali che $x \in A$ o $x \in B$; in altre parole, degli elementi che appartengono ad almeno uno¹³ fra A e B (vedi Figura 1.3).
2. L'*intersezione* $A \cap B$ è l'insieme degli elementi x tali che $x \in A$ e $x \in B$; in altre parole, degli elementi che appartengono sia ad A che a B (vedi Figura 1.4).
3. Se $A \cap B = \emptyset$, si dice che A e B sono *disgiunti* o che *non si intersecano*.
4. La *differenza* $A \setminus B$ è l'insieme degli elementi x tali che $x \in A$ e $x \notin B$; in altre parole, degli elementi che appartengono ad A e non appartengono a B (vedi Figura 1.5).

Alcuni commenti:

1. $A \cup B$ si pronuncia “ A unito B ”, o anche “ A unione B ”.
2. $A \cap B$ si pronuncia “ A intersecato B ”, o anche “ A intersezione B ”.
3. $A \setminus B$ si pronuncia “ A meno B ”. Un'altra notazione è $A - B$.
4. Se $B \subseteq A$, allora $A \setminus B$ si denota anche con $\complement_A(B)$ e si può chiamare anche il *complementare* di B in A . Se stiamo ragionando di sottoinsiemi di un

¹³In matematica, salvo indicazione contraria, la “o” è *inclusiva*, cioè “ P o Q ” è vera se almeno una di P , Q è vera, e in particolare se lo sono entrambe. C'è anche una “o” *esclusiva*, che è vera quando una fra P e Q è vera, ma non entrambe. Ci torniamo.

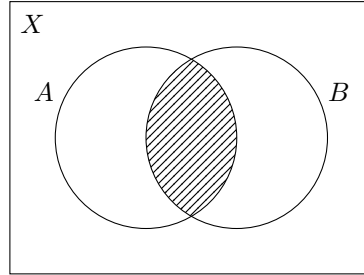


Figura 1.4: Due sottoinsiemi A, B di un insieme X , con la loro intersezione $A \cap B$ evidenziata a righe diagonali.

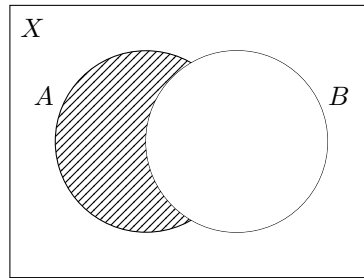


Figura 1.5: Due sottoinsiemi A, B di un insieme X , con la differenza $A \setminus B$ evidenziata a righe diagonali.

qualche A fissato o chiaro dal contesto, si può anche scrivere B^c invece di $\complement_A(B)$. (vedi Figura 1.6)

Esempio 1.18. Se $A := \{1, 3, a, x, y\}$ e $B := \{2, 3, x, z\}$, allora abbiamo quanto segue.

1. $A \cup B = \{1, 2, 3, a, x, y, z\} = B \cup A$
2. $A \cap B = \{3, x\} = B \cap A$
3. $A \setminus B = \{1, a, y\}$

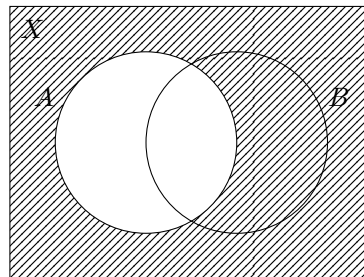


Figura 1.6: Due sottoinsiemi A, B di un insieme X , con il complementare A^c di A rispetto a X evidenziato a righe diagonali.

4. $B \setminus A = \{2, z\}$
5. Rispetto a $X := \{1, 2, 3, 8, a, b, c, x, y, z\}$ abbiamo $A^c = \mathbb{C}_X(A) = \{2, 8, b, c, z\} = X \setminus A$
6. Rispetto a $Y := \{1, 2, 3, 8, a, b, c, x, y, z, \alpha, \beta\}$ abbiamo $A^c = \mathbb{C}_Y(A) = \{2, 8, b, c, z, \alpha, \beta\} = Y \setminus A$
7. Se $A := \{n \in \mathbb{N} \mid \exists k \in \mathbb{N} n = 2k\}$ è l'insieme dei numeri naturali multipli di 2 e $B := \{n \in \mathbb{N} \mid \exists k \in \mathbb{N} n = 3k\}$ è l'insieme dei numeri naturali multipli di 3, allora $A \cap B$ è l'insieme dei numeri naturali multipli di 6.
8. Se A è l'insieme dei numeri naturali pari e B è l'insieme dei numeri naturali dispari, allora $A \cap B = \emptyset$ e $A \cup B = \mathbb{N}$. Chi sono $A \setminus B$ e $B \setminus A$?

Vediamo subito qualche proprietà fondamentale di queste operazioni.

Proposizione 1.19. Sia X un insieme. Le operazioni sui sottoinsiemi di X soddisfano le seguenti proprietà

1. Commutatività
 - (a) dell'unione: $A \cup B = B \cup A$;
 - (b) e dell'intersezione: $A \cap B = B \cap A$.
2. Associatività
 - (a) dell'unione: $(A \cup B) \cup C = A \cup (B \cup C)$;
 - (b) e dell'intersezione: $(A \cap B) \cap C = A \cap (B \cap C)$.
3. Distributività
 - (a) dell'unione sull'intersezione: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;
 - (b) e dell'intersezione sull'unione: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
4. Leggi di De Morgan:
 - (a) $(A \cup B)^c = A^c \cap B^c$;
 - (b) $(A \cap B)^c = A^c \cup B^c$.

Dimostrazione. Vediamo una dimostrazione della (4a). La dimostrazione delle altre proprietà è lasciata come esercizio.

Dimostriamo che $(A \cup B)^c = A^c \cap B^c$ per *doppia inclusione*, cioè dimostriamo separatamente che $(A \cup B)^c \subseteq A^c \cap B^c$ e che $(A \cup B)^c \supseteq A^c \cap B^c$. Questo basta per dimostrare l'uguaglianza per il Corollario 1.13.

Per dimostrare che $(A \cup B)^c \subseteq A^c \cap B^c$ sia $x \in X$ un qualunque elemento del membro di sinistra dell'inclusione, che chiameremo LHS per fare prima; dobbiamo mostrare che appartiene al RHS, cioè al membro di destra.¹⁴ Dire che $x \in (A \cup B)^c$ vuol dire che $x \notin (A \cup B)$. Dato che $x \notin A \cup B$, in particolare $x \notin A$, dato che tutti gli elementi di A sono anche elementi di $A \cup B$. In altre parole, $x \in A^c$. Nella stessa maniera si dimostra che $x \in B^c$. Dato che x appartiene sia ad A^c che a B^c , allora appartiene alla loro intersezione $A^c \cap B^c$. Questo completa la dimostrazione dell'inclusione $\subseteq$.

¹⁴Sono rispettivamente gli acronimi di *Left Hand Side* e *Right Hand Side*.

Per dimostrare che il RHS è incluso nel LHS, sia $x \in X$ tale che $x \in A^c \cap B^c$. Dato che $A^c \cap B^c \subseteq A^c$, in particolare $x \in A^c$, quindi $x \notin A$. Similmente, $x \notin B$. Dato che x non appartiene a nessuno di A, B , per definizione non appartiene alla loro unione, cioè $x \notin A \cup B$, che è la stessa cosa di $x \in (A \cup B)^c$. Questo completa la dimostrazione dell'inclusione $\supseteq$. $\square$

Se le dimostrazioni viste finora vi sembrano lunghe e verbose, è perché lo sono. Questo è intenzionale, dato che sono le prime dimostrazioni del corso, ma inizieremo presto ad essere più concisi. Ad esempio, la dimostrazione sopra la potremmo riscrivere come segue.

Dimostrazione. Se $x \in (A \cup B)^c$ allora $x \notin A \cup B$, quindi $x \notin A$ e $x \notin B$, cioè $x \in A^c$ e $x \in B^c$, quindi $x \in A^c \cap B^c$.

Viceversa, se $x \in A^c \cap B^c$ allora $x \notin A$ e $x \notin B$, quindi per definizione $x \notin A \cup B$ e quindi $x \in (A \cup B)^c$.

Concludiamo per il Corollario 1.13. $\square$

E volendo essere ancora più stringati potremmo scrivere qualcosa del genere, scrivendo “ $\iff$ ” per “se e solo se”:

Dimostrazione. Abbiamo che:

$$x \in (A \cup B)^c \iff x \notin A \cup B \iff (x \notin A) \wedge (x \notin B) \iff x \in A^c \cap B^c \quad \square$$

1.3.3 L'insieme delle parti

Definizione 1.20. Sia X un insieme. L'*insieme delle parti* $\mathcal{P}(X)$ è l'insieme di tutti i sottoinsiemi di X .

Esempio 1.21. Alcuni esempi di insieme delle parti.

1. L'insieme vuoto $\emptyset$ ha un solo sottoinsieme: sé stesso. Quindi $\mathcal{P}(\emptyset) = \{\emptyset\}$.
2. Qualunque sia a , l'insieme $\{a\}$ ha due sottoinsiemi: sé stesso e l'insieme vuoto. Quindi $\mathcal{P}(\{a\}) = \{\emptyset, \{a\}\}$.
3. Qualunque siano $a \neq b$, l'insieme $\{a, b\}$ ha quattro sottoinsiemi: il vuoto, tutto l'insieme, e due *singoletti* (insiemi con esattamente un elemento): $\mathcal{P}(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$.
4. Qualunque siano a, b, c , abbiamo

$$\mathcal{P}(\{a, b, c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$$

Se a, b, c sono *a due a due distinti* (cioè “tutti diversi”: $a \neq b$, $a \neq c$, e $b \neq c$), allora $\mathcal{P}(\{a, b, c\})$ ha 8 elementi.

1.3.4 Tuple ordinate e prodotto cartesiano

Come dicevamo nell'Osservazione 1.6, un insieme è una collezione *non ordinata* di elementi. Chiaramente, per molte cose potremmo aver bisogno di “strutture dati” ordinate. Per esempio, per specificare le coordinate di un punto nel piano, è importante distinguere l'ascissa e l'ordinata. Dato che $\{a, b\} = \{b, a\}$, buttarle entrambe dentro un insieme e basta non è una buona idea: per esempio, guardando l'insieme $\{0, 10000\}$, non sapremmo se stiamo parlando di un punto molto a destra centrato verticalmente, o molto in alto centrato orizzontalmente.

Il rimedio è introdurre il concetto di *coppie ordinate*, di solito denotate con le parentesi tonde, per esempio (a, b) . Come per gli insiemi, delle coppie ordinate non ci interessa tanto “cosa sono” quanto “cosa fanno”. Quello che “fanno” le coppie ordinate è la seguente cosa:

Proprietà 1.22. Due coppie ordinate (a, b) e (c, d) sono uguali se e solo se $a = c$ e $b = d$.

In altre parole, una coppia ordinata “sa” chi è la sua prima coordinata e chi è la sua seconda coordinata. Inoltre, le due coordinate di una coppia ordinata possono tranquillamente essere uguali.

Esempio 1.23. Le coppie ordinate $(0, 1)$, $(1, 0)$ e $(1, 1)$ sono a due a due distinte: $(0, 1) \neq (1, 1)$ perché differiscono sulla prima coordinata, $(1, 0) \neq (1, 1)$ perché differiscono sulla seconda coordinata, e $(1, 0) \neq (0, 1)$ perché, ad esempio, differiscono sulla prima coordinata; o, se preferite, sulla seconda: l'importante per dire che sono diverse è che differiscano in almeno una delle coordinate.

Tratteremo le coppie ordinate come oggetti di un tipo diverso da quello degli insiemi, per cui riterremo, per convenzione, scritte come $0 \in (0, 1)$ prive di senso. In altre parole, possiamo pensare alle coppie ordinate come ad una “struttura dati” diversa dalla “struttura dati” degli insiemi. Dati a e B , se B è un insieme ha senso chiedersi se $a \in B$. Se invece B è una coppia ordinata, ha senso chiedersi se a è la sua prima coordinata e ha senso chiedersi se a è la sua seconda coordinata, ma non ha senso chiedersi se a appartiene a B .¹⁵

Spesso è utile considerare tutte le coppie ordinate con la prima coordinata proveniente da un qualche insieme A la seconda da un qualche insieme B , per A e B fissati.

Definizione 1.24. Siano A, B insiemi. Il *prodotto cartesiano* $A \times B$ è l'insieme $\{(a, b) \mid a \in A, b \in B\}$.

Esempio 1.25. 1. Siano $A = \{1, 2\}$ e $B = \{1, 4\}$. Allora

$$A \times B = \{(1, 1), (1, 4), (2, 1), (2, 4)\}$$

mentre, per esempio, $(4, 1) \notin A \times B$.

2. Se almeno uno fra A e B è uguale a $\emptyset$, allora $A \times B = \emptyset$.

Dimostrazione. Se così non fosse, $A \times B$ conterrebbe un elemento (a, b) con $a \in A$ e $b \in B$. Ma dato che $a \in A$ e $b \in B$, nessuno fra A e B è vuoto. $\square$

¹⁵Può essere interessante però sapere che le coppie ordinate si possono “implementare” usando gli insiemi; per l'implementazione più popolare, vedi Esercizio 1.41.

3. Viceversa, se $A \times B = \emptyset$ allora almeno uno fra A e B è vuoto.

Dimostrazione. Se A e B sono entrambi non vuoti, allora esistono $a \in A$ e $b \in B$. Quindi $(a, b) \in A \times B$, che è perciò non vuoto. $\square$

4. A scuola avete probabilmente visto identificare la retta con l'insieme dei numeri reali $\mathbb{R}$ (su cui torneremo) e il piano con l'insieme $\mathbb{R} \times \mathbb{R}$, anche denotato come $\mathbb{R}^2$.

5. Più in generale, se $A = B$, l'insieme $A \times B = A \times A$ è anche denotato A^2 .

Osservazione 1.26. Il prodotto cartesiano non è commutativo: se $A \neq B$ e sia A che B sono diversi da $\emptyset$, allora $A \times B \neq B \times A$.

Per esempio, se $A = \{1, 2, 3\}$ e $B = \{1, 2, 4\}$, allora $(1, 4) \in A \times B$. Ma approfittiamone per dimostrarlo in generale.

Dimostrazione. Per estensionalità, se $A \neq B$ deve esistere o un elemento $a \in A \setminus B$, o un elemento $b \in B \setminus A$.

Nel primo caso, fissiamo un tale $a \in A \setminus B$. Dato che per ipotesi $B \neq \emptyset$, esiste qualche $c \in B$. Ma allora $(a, c) \in A \times B$, ma $(a, c) \notin B \times A$, perché la prima coordinata di (a, c) non sta in B .

Nel secondo caso, le ipotesi sono che esista un $b \in B \setminus A$, e che $A \neq \emptyset$. Potremmo scrivere una dimostrazione simile a quella del caso precedente e andrebbe benissimo. Oppure, possiamo *ricondurci al caso precedente*; una maniera veloce di dirlo è “dato che la conclusione è simmetrica in A, B , possiamo applicare il paragrafo precedente a B, A invece che ad A, B ”, ma almeno una volta nella vita, è bene vedere esplicitamente cosa vuol dire questo in tutti i dettagli.¹⁶ Osserviamo che l'argomento nel paragrafo precedente funziona se al posto di A, B mettiamo qualunque C, D rispettivamente (cioè C al posto di A e D al posto di B) purché rispettino le ipotesi che esista qualche $x \in C \setminus D$ e che esista qualche $y \in D$ (che prima si chiamavano a e c , ma ovviamente non è importante se gli cambiamo nome). Sotto le ipotesi di questo paragrafo però, $C := B$ e $D := A$ soddisfano queste ipotesi, e quindi per il paragrafo precedente abbiamo che $C \times D \neq D \times C$. Se ci ricordiamo chi erano C e D , scopriamo che $B \times A \neq A \times B$. Dato che *la conclusione è simmetrica* in A, B , cioè che non cambia se scambiamo B con A dato che $B \times A \neq A \times B$ è equivalente $A \times B \neq B \times A$, abbiamo finito. $\square$

Chiaramente non c'è nessun motivo di fermarsi a 2. Per qualunque $n \in \mathbb{N}$, diciamo con $n \geq 2$, si può parlare di n -uple ordinate.¹⁷ L'analogo della Proprietà 1.22 è il seguente.

Proprietà 1.27. Due n -uple ordinate $(a_1, \dots, a_n)$ e $(b_1, \dots, b_n)$ sono uguali se e solo se, per ogni $i \in \mathbb{N}$ con $1 \leq i \leq n$ abbiamo $a_i = b_i$.

¹⁶“Ma non era più facile scrivere direttamente l'adattamento delle prime tre righe?” Sì, certo, in questo caso, perché stiamo dimostrando qualcosa di molto facile. A volte però “il primo caso” richiede molto più lavoro, e potersi ricondurre a un caso precedente ne richiede molto meno.

¹⁷In realtà si può fare anche per $n = 1$ e, buffamente, per $n = 0$. Se la cosa vi incuriosisce, provate a pensare cosa viene fuori, e cosa succede alla Definizione 1.28. Suggerimento: potreste voler tornare a ripensarci dopo che avremo parlato di funzioni.

In altre parole, due n -uple ordinate sono uguali se e solo se, per ogni i fra 1 ed n compresi, hanno la stessa i -esima coordinata; più in breve, se “hanno tutte le coordinate uguali”.

Diamo quindi la seguente definizione.

Definizione 1.28. Sia $n \in \mathbb{N}$ con $n \geq 2$ e siano $A_1, \dots, A_n$ insiemi. Il *prodotto cartesiano* $A_1 \times \dots \times A_n$ è l'insieme

$$A_1 \times \dots \times A_n := \{(a_1, \dots, a_n) \mid a_1 \in A_1, \dots, a_n \in A_n\}$$

Anche qui, se gli A_i sono tutti uguali ad A , si può scrivere A^n .

Se sopra vi danno fastidio i puntini “...”, non siete sole. Approfittiamone per introdurre il simbolo $\forall$, che si legge “per ogni”, e dire che sopra avremmo potuto scrivere $\{(a_1, \dots, a_n) \mid \forall i \leq n \ a_i \in A_i\}$.

La definizione sopra *generalizza* la Definizione 1.24, che è il suo *caso particolare* con $n = 2$.

1.4 Esercizi

Questi esercizi sono *pochi*. È fortemente raccomandato cercare altri esercizi in altri libri o appunti che trattano argomenti simili, ad esempio [Azz26a] e altre fonti in bibliografia. E farli, ovviamente.

Esercizio 1.29. Generate degli insiemi di lettere a caso, ad esempio scegliendo delle parole a caso da un testo e prendendo gli insiemi delle lettere che li compongono. Per ogni coppia di insiemi così ottenuti:

1. dire se uno dei due è un sottoinsieme dell'altro,
2. calcolarne unione, intersezione, differenza, complemento rispetto all'insieme delle lettere dell'alfabeto,
3. disegnare i relativi diagrammi di Venn.

Esercizio 1.30. Per quali coppie ordinate (A, B) di insiemi in questa lista vale che $A \subseteq B$?

1. $A_0 := \mathbb{N} \setminus \{0\}$
2. $A_1 := \{n \in \mathbb{N} \mid n \text{ è pari}\}$
3. $A_2 := \{n \in \mathbb{N} \mid n \text{ è dispari}\}$
4. $A_3 := \{n \in \mathbb{N} \mid n \text{ è il successore di un naturale dispari}\}$
5. $A_4 := \{n \in \mathbb{N} \mid n \text{ è un multiplo di } 3\}$
6. $A_5 := A_0 \cap A_2$
7. $A_6 := A_1 \cap A_2$
8. $A_7 := A_1 \cup A_2$

Esercizio 1.31. Calcolare unione e intersezione di ogni coppia di insiemi A_i, A_j nell'Esercizio 1.31.

Esercizio 1.32. Completare la dimostrazione della Proposizione 1.19.

Esercizio 1.33. Sia un insieme fissato e siano A, B, C sottoinsiemi di X . Per ognuna delle seguenti proprietà, dire se è vero che, per tutte le scelte di X, A, B, C , la proprietà è vera. Per le proprietà vere, scrivere una dimostrazione. Per quelle false, trovare un controesempio (vedi sotto). Tutti i complementari si intendono calcolati rispetto ad X .

- | | | |
|-----------------------------------|------------------------------------|---|
| 1. $A \cap A = \emptyset$ | 13. $A \cup A^c = \emptyset$ | 25. $A \cap \emptyset = A^c$ |
| 2. $A \cup A = \emptyset$ | 14. $A \cup A^c = A$ | 26. $A \cap \emptyset = X$ |
| 3. $A \setminus A = \emptyset$ | 15. $A \cup A^c = X$ | 27. $(A^c)^c = \emptyset$ |
| 4. $A \cup A = A$ | 16. $A \cap A^c = \emptyset$ | 28. $(A^c)^c = A$ |
| 5. $A \cap A = A$ | 17. $A \cap A^c = A$ | 29. $(A^c)^c = X$ |
| 6. $A \setminus A = A$ | 18. $A \cap A^c = X$ | 30. $A \setminus B = B \setminus A$ |
| 7. $A \subseteq A \cup B$ | 19. $A \cup \emptyset = \emptyset$ | 31. $A \setminus (B \setminus C) = (A \setminus B) \setminus C$ |
| 8. $A \subseteq A \cap B$ | 20. $A \cup \emptyset = A$ | 32. $A \setminus B = A^c \cup B$ |
| 9. $A \supseteq A \cup B$ | 21. $A \cup \emptyset = A^c$ | 33. $A \setminus B = A \cap B^c$ |
| 10. $A \supseteq A \cap B$ | 22. $A \cup \emptyset = X$ | 34. $A \setminus B = (A \cup B)^c \cap A$ |
| 11. $A \cup B \subseteq A \cap B$ | 23. $A \cap \emptyset = \emptyset$ | 35. $B \setminus A = B \cap A^c$ |
| 12. $A \cap B \subseteq A \cup B$ | 24. $A \cap \emptyset = A$ | 36. $A^c = B$ |

Soluzione parziale. Il punto 1 è chiaramente falso. Per dimostrarlo, esibiamo un controesempio. Un *controesempio* è un esempio che fa vedere che un enunciato della forma “per ogni A, B, C [succede qualcosa ad A, B, C]” è falso, trovando A, B, C per cui il “qualcosa” non succede. In questo caso, dobbiamo trovare un A tale che $A \cap A \neq \emptyset$. Basta prendere un qualunque A non vuoto, ad esempio $\{9\}$. Allora $A \cap A = \{9\} \cap \{9\} = \{9\}$, che non è vuoto perché contiene 9. $\square$

Definizione 1.34. La *differenza simmetrica* $A \triangle B$ è l’insieme degli elementi x tali che $(x \in A \text{ o } x \in B)$ e non $(x \in A \text{ e } x \in B)$; in altre parole, degli elementi che appartengono ad esattamente uno fra A e B .

Un’altra notazione per $A \triangle B$ è $A \oplus B$.

Esercizio 1.35. Disegnare l’analogo della Figura 1.3 per la differenza simmetrica.

Esercizio 1.36. Esprimere $A \triangle B$ usando $\cup, \cap, \setminus$ (non per forza tutti e tre).

Esercizio 1.37. Che proprietà ha la differenza simmetrica fra quelle viste per le altre operazioni (commutatività, associatività, distributività su un’altra operazione, o di un’altra operazione su di essa)?

Esercizio 1.38. Dimostrare che le seguenti sono equivalenti, per ogni coppia di insiemi A, B .

1. $A \subseteq B$
2. $A \cap B = A$
3. $A \cup B = B$

Esercizio 1.39.

1. Se a, b, c, d sono a due a due distinti, quanti elementi ha $\mathcal{P}(\{a, b, c, d\})$?
2. Più in generale, se $n \in \mathbb{N}$ e $a_1, a_2, a_3, \dots, a_n$ sono a due a due distinti, quanti elementi ha $\mathcal{P}(\{a_1, a_2, a_3, \dots, a_n\})$?

Suggerimento. Fissiamo un sottoinsieme $X \subseteq \{a_1, a_2, a_3, \dots, a_n\}$. Quante maniere ci sono di estenderlo a un sottoinsieme di $\{a_1, a_2, a_3, \dots, a_n, a_{n+1}\}$? $\square$

Esercizio 1.40. Calcolare i seguenti insiemi di coppie o triple ordinate, scrivendone per ognuno tutti gli elementi.

1. $\{(a, b) \in \mathbb{N}^2 \mid a < b < 4\}$
2. $\{(a, b) \in \mathbb{N}^2 \mid a + b = 4\}$
3. $\{(a, b) \in \mathbb{N}^2 \mid a < b < 6 \text{ e } b - a \text{ è divisibile per } 3\}$
4. $\{(a, b, c) \in \mathbb{N}^3 \mid a^2 + b^2 + c^2 = 5\}$
5. $\{(a, b, c) \in \mathbb{N}^3 \mid a^2 + b^2 + c^2 = 7\}$
6. $\{(a, b, c) \in \mathbb{N}^3 \mid a^2 + b^2 + c^2 = 9\}$

1.5 Digressione: fare bootstrapping della matematica

La Sezione 1.4 *non* può essere ignorata ai fini dell'esame, come tutte le altre sezioni di esercizi. Questa sezione invece sì¹⁸, così come tutte le altre il cui nome inizia con "Digressione: ". È qui per dare una risposta (parziale) a chi si sta ponendo domande come "perché la definizione di insieme all'inizio di questo capitolo non è numerata?" o anche "perché la letteratura dice che quello di insieme è un concetto primitivo e non può essere definito?".

Quando in matematica si dà una definizione, deve essere possibile, almeno in linea di principio, stabilire se un dato qualcosa la soddisfa o meno.

Per esempio, "un numero naturale n è *irriducibile* sse, per ogni $a \in \mathbb{N}$, se a divide n allora $a = 1$ o $a = n$ " è una definizione matematica: preso un numero n , mi basta osservare che i divisori di n sono contenuti nell'insieme $\{1, \dots, n\}$, e controllare se c'è un $k \in \{2, 3, \dots, n-1\}$ che divide n . Questa non è la maniera più efficiente per farlo¹⁹, e se n è, per esempio, 2^{2^N} dove N è il numero di atomi

¹⁸Tranne che per la sua prima frase. Sul serio, fate gli esercizi.

¹⁹Ad esempio, basterebbe guardare solo i primi, e solo fino a $\sqrt{n}$, e si può fare moooooooooolto meglio di così, ma non è questo il punto.

nell'universo la cosa è nella pratica infattibile, ma appunto *in linea di principio*, dato abbastanza tempo e abbastanza pazienza, potrebbe essere fatto.²⁰

Invece “un insieme è *bello* sse tutti i suoi elementi sono belli” *non* è una definizione matematica... a meno che non abbiamo già dato una definizione di “elemento bello”. Di fatto, nella definizione di “irriducibile” sopra stiamo assumendo di aver già definito cosa è un numero naturale e cosa vuol dire “divide”. Nel caso degli insiemi, abbiamo detto che un insieme è una collezione di elementi. Ma cos'è un elemento?

Tutta 'sta manfrina per dire che, nel dare le definizioni, da qualche parte si deve partire, e quel qualcosa da dove partiamo, purtroppo, non può essere definito e va in un certo senso “preso per buono”.

La scelta “mainstream” è di partire dagli insiemi.²¹ Questo *non* vuol dire “cos'è un insieme lo sappiamo tutti e che proprietà hanno gli insiemi è ovvio”: un minimo di “specifiche tecniche” del concetto di insieme vanno date. La prima idea che può passare per la testa è di stipulare cose come “per ogni proprietà esiste l'insieme degli elementi che la soddisfano”. Il problema è che questa idea²² ha lo spiacevole inconveniente di far materializzare un signore inglese alla tua porta a dirti che questa cosa, se ci pensi bene, purtroppo non ha senso [Wikg] e rischia di trasformarti nel papa²³, per cui servono approcci un attimino più cauti. Per dare un'idea, l'approccio più diffuso ai *fondamenti della matematica* è il seguente:

1. Si stipula che quello di “insieme” è un “concetto primitivo”, come quello di “punto” in geometria euclidea.
2. Invece di dire “cosa è” un insieme, si dice “cosa fa”, nel senso di: come si relaziona con altri insiemi.
3. Di fatto, questo vuol dire che invece di definire cosa è un insieme, ci si mette d'accordo su alcune proprietà che devono essere soddisfatte dall'universo degli insiemi.
4. La lista di proprietà più popolare è nota come ZFC, che è un acronimo per *Zermelo–Fraenkel set theory with Choice*.
5. Per esempio, l'Assioma di Estensionalità è una delle proprietà che costituiscono ZFC. Giusto per nominarne un'altra, l'*Assioma della Coppia* dice che per ogni due insiemi A, B esiste l'insieme $\{A, B\}$.
6. Gli enunciati che fanno parte di ZFC li si chiama *assiomi*, li si usa per dimostrare *teoremi* tramite certe regole che vanno anche esse specificate,

²⁰Di fatto, per soddisfare quell’“in linea di principio” basta molto meno; ad esempio, ci sono definizioni che richiedono di controllare “in linea di principio” una quantità infinita di condizioni. Per esempio verificare che $\sqrt{2}$ è irrazionale richiederebbe, in linea di principio, di controllare per ogni $m, n \in \mathbb{N} \setminus \{0\}$ che $m^2/n^2 \neq 2$. Non si può controllare a mano infiniti casi, ma il fatto che $\sqrt{2}$ è irrazionale ha una dimostrazione (finita).

²¹Non è l'unica scelta possibile. In passato è stato anche popolare usare le n -uple ordinate come oggetti primitivi, e ci sono approcci che prendono come oggetti primitivi cose più elaborate.

²²Nota come “comprensione non ristretta”.

²³Su questo ci torniamo, ma vi assicuro che è meno campato in aria di quanto sembri. Coincidentalmente, l'intersezione fra l'insieme dei laureati in matematica e l'insieme dei papi è non vuota.

e tutti gli oggetti di cui stiamo parlando sono insiemi (inclusi gli “elementi” in “un insieme è una collezione di elementi”).

Senza addentrarci troppo nei dettagli²⁴, partendo da questo si può mettere in piedi quasi²⁵ tutta la matematica. Per dare un’idea, la maniera standard di “implementare” le coppie ordinate con gli insiemi è la seguente.

Esercizio 1.41 (Coppie di Kuratowski). Per a, b insiemi, definiamo $(a, b)_K := \{\{a\}, \{a, b\}\}$. Dimostrare che $(-, -)_K$ soddisfa la Proprietà 1.22, cioè che $(a, b)_K = (c, d)_K$ se e solo se $a = c$ e $b = d$.

Se pensate abbastanza a lungo a questo esercizio potreste rendervi conto che, per esempio, con questa implementazione succede “per sbaglio” che $\{\emptyset\} \in (\emptyset, \{\emptyset\})$, anche se avevamo detto che non ha veramente senso chiedersi se una coordinata di una coppia ordinata è un suo elemento. Questo è un artefatto di questa implementazione, non è presente in altre codifiche delle coppie ordinate, e nella pratica matematica quando si parla di coppie ordinate si assume solo che soddisfino la Proprietà 1.22. Se stessimo programmando, in sostanza staremmo chiamando una qualche libreria che gestisce le coppie ordinate, e il codice che stiamo usando deve funzionare anche se la libreria viene riscritta, purché continui a soddisfare la Proprietà 1.22.

Già che ci siamo: “cosa fanno” i numeri naturali lo vedremo più avanti nel corso. Però “cosa sono” nell’implementazione standard della matematica con gli insiemi” lo possiamo già dire ora. Lavorando in ZFC, i numeri naturali si definiscono come segue.

1. $0 := \emptyset$. In altre parole, l’insieme vuoto è il numero 0.
2. $1 := \{0\} = \{\emptyset\}$
3. $2 := \{0, 1\} = \{\emptyset, \{\emptyset\}\}$
4. $3 := \{0, 1, 2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$
5. Più in generale, $n + 1 := \{0, 1, 2, \dots, n - 2, n - 1, n\}$ o, più precisamente (e senza usare puntini), $n + 1 := n \cup \{n\}$.
6. $\mathbb{N}$ contiene quanto sopra e nient’altro. Più precisamente, $\mathbb{N}$ è il più piccolo insieme X tale che $\emptyset \in X$ e, se $x \in X$, allora $x \cup \{x\} \in X$.

Chi ci assicura che un qualche insieme X come sopra esista? Anche questo è un assioma di ZFC, noto come *Assioma dell’Infinito*. Il fatto che esista “il più piccolo” tale insieme segue dagli assiomi di ZFC, ma qui mi fermo perché altrimenti diventano gli appunti di un altro corso.

A titolo di curiosità, notiamo che questa codifica dei numeri naturali ha come conseguenze, per esempio, che $2 \in 3$, che $2 \subseteq 3$, che $2 = \mathcal{P}(1)$ e, combinandola con le coppie di Kuratowski, che $(0, 0) = \{1\}$ e che $(0, 1) = 3 \setminus 1$ (potete provare a dimostrare queste cose come esercizio nel seguire le definizioni). Di nuovo, nella pratica matematica quello che veramente ci interessa dei numeri naturali

²⁴Per sviscerare i quali fino in fondo servirebbe un mezzo corso, ma se volete approfondire per curiosità potete partire ad esempio da [Wikh].

²⁵Il perché di questo “quasi” e il come fare a sbarazzarsene è molto interessante, ma va decisamente oltre gli argomenti di questo corso. Per approfondire, un possibile punto di partenza è [Wikc].

è che soddisfino certe proprietà che vederemo più avanti, e il fatto che in questa implementazione diventi sensato chiedersi se $2 \in 3$ viene sostanzialmente ignorato.

Se avete letto fino a qui, complimenti, e se il contenuto di questa sezione appare fumoso è normale (ma tanto non fa parte dell'esame). Però, ehi, ora sapete (vedi Nota [1](#)) cosa c'entra il numero 1 con un portafogli vuoto.

Capitolo 2

Logica

Nel capitolo precedente abbiamo già incrociato brevemente alcuni simboli logici: il *connettivo* $\wedge$ e i *quantificatori* $\exists$ e $\forall$. Qui ne parliamo più in dettaglio.

2.1 Enunciati

Un *enunciato* è qualcosa di cui abbia senso dire se è vero o falso. Gli enunciati vengono chiamati anche *proposizioni*; purtroppo, la parola “proposizione” può essere usata per indicare due cose diverse: quello appena introdotto, e quello introdotto a pagina 5. La differenza è che nel senso di pagina 5, una proposizione non è mai falsa, perché ha una dimostrazione. In quale senso lo stiamo usando va capito dal contesto.

Esempio 2.1. Vediamo qualche esempio di cose che sono enunciati e di cose che non lo sono.

1. “ $+224 =$ ”. Questa non è nemmeno una formula ben formata, figuriamoci un enunciato.
2. “ $2 + 2 = 4$ ”. È un enunciato, ed è vero.
3. “ $2 + x = 4$ ”. Questa è una formula, ma il fatto che contenga la *variabile libera* x fa sì che non sia un enunciato.
4. “ $2 + 3 = 4$ ”. Se *sostituiamo* 3 al posto della variabile x nella formula precedente, otteniamo un enunciato. Un enunciato falso, ma comunque un enunciato.
5. “ $2 + x = 4$ dove $x = 3$ ”. È un enunciato, vedi punto precedente.
6. “ $\exists x \in \mathbb{N} \ x + 2 = 4$ ”. Questo è un enunciato, che dice che esiste un numero naturale che sommato a 2 dà 4. Notare che la *variabile* x qui è “catturata” dal quantificatore, e quindi non è libera, al contrario del punto 3 sopra.
7. “ $9 \leq 10$ ” è un enunciato.
8. “ $n \leq 10$ ” non è un enunciato, di nuovo, perché la variabile n è libera.

9. “Ogni numero pari maggiore di 2 è somma di due numeri primi”. Questo è un enunciato, nonostante il fatto che ad oggi non si sappia se è vero.
10. “Esiste un numero naturale che non è somma di tre quadrati.” Avete fatto gli esercizi del capitolo precedente, vero?
11. “Quanto fa $2 + 2$?” non è un enunciato.
12. “Vieni qui per favore” non è un enunciato.
13. “Dimostrare che $2 + 2 = 4$ ” non è un enunciato.
14. “Ciao!” non è un enunciato.
15. “A pranzo ho mangiato limoni” è un enunciato.
16. “Signora, i limoni, signoraaaa” non è un enunciato.

2.2 Connettivi

Con i connettivi possiamo combinare enunciati dati, diciamo $A_1, \dots, A_n$, per formarne altri il cui valore di verità dipende da quelli di $A_1, \dots, A_n$.

Ad esempio, usando i connettivi, partendo da tre enunciati A_1, A_2, A_3 possiamo costruire un enunciato che è vero se e solo se tutti gli A_i sono veri, oppure che è vero se e solo se A_1 è vero e A_2 è falso oppure A_1 è falso e A_3 è vero.

Il primo connettivo che vediamo è *unario*: prende un argomento solo.

Definizione 2.2. Sia A un'enunciato. La *negazione* $\neg(A)$ (pronunciato “non A ”) è vera sse A è falsa.

Quando non c'è rischio di ambiguità, possiamo omettere le parentesi e scrivere semplicemente $\neg A$. Ma, formalmente, stipuliamo che le parentesi fanno parte del connettivo.

Esempio 2.3. Se A è l'enunciato “ $2 + 2 = 4$ ”, allora $\neg A$, (che possiamo anche scrivere direttamente come $\neg(2 + 2 = 4)$), è falso.

Se A è l'enunciato “ $2 + 2 = 5$ ”, allora $\neg A$ è vero.

Notiamo che, per decidere se $\neg A$ è vero o meno, non ci serve veramente sapere chi è A , ma solo se è vero o falso. In sostanza, possiamo trattare A come un segnaposto per un enunciato non specificato: una *variabile proposizionale* (o anche *variabile Booleana*), che può assumere i valori “vero” o “falso”. Come usuale, scriveremo 1 invece di “vero” e 0 al posto di “falso”.

Possiamo pensare a un connettivo a n argomenti $C(A_1, \dots, A_n)$ come a un programma che prende in input una n -upla di 0 e 1 (pensati come valori di verità, come sopra) e restituisce 0 o 1. O come a una funzione, nel senso matematico che approfondiremo a breve. O come a un certo tipo di circuito, letteralmente [Wikid]. Ad ogni modo, una maniera sintetica per specificare il comportamento di un connettivo C , è dare una *tavola di verità*: una tabella che ci dice qual è l'output per i vari possibili input. Per esempio, la tavola di verità della negazione è in Figura 2.1.

Vediamo subito i due più popolari connettivi *binari*, cioè a due argomenti. Il primo l'abbiamo già incontrato.

A	$\neg A$
0	1
1	0

Figura 2.1: Tavola di verità della negazione.

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

Figura 2.2: Tavola di verità della congiunzione e della disgiunzione.

Definizione 2.4. Siano A, B enunciati.

1. La *congiunzione* $(A \wedge B)$ (pronunciato “ A e B ”) è vera sse sia A che B sono vere.
2. La *disgiunzione* $(A \vee B)$ (pronunciato “ A o B ”) è vera sse almeno una fra A e B è vera.

Le tavole di verità della congiunzione e della disgiunzione sono in Figura 2.2.

Osservazione 2.5. Alcuni commenti.

1. Sia $\wedge$ che $\vee$ sono commutative e associative. Dimostrarlo come esercizio, ad esempio costruendo le tavole di verità di $A \wedge (B \wedge C)$ e $(A \wedge B) \wedge C$.
2. La congiunzione “e” in italiano a volte ha anche significato causale o temporale (“ti ho visto e ti ho salutato”, “pioveva e ho preso l’ombrello”). La “e” matematica, $\wedge$, non ha niente di tutto ciò (come testimonia la sua tavola di verità, è commutativa!). $A \wedge B$ vuol dire che A e B sono tutte e due vere, stop. Non che B è una conseguenza di A , non che B viene dopo A , niente di tutto ciò.
3. La “o” è inclusiva¹, cioè se sia A che B sono vere allora $A \vee B$ è vera. Se qualcuno vi dicesse “Mi mandi 1 bitcoin a questo indirizzo $\vee$ ti faccio brutte cose”, voi pagate, e le brutte cose succedono comunque, questo qualcuno non sta mentendo.² C’è anche una “o” esclusiva, vedi Definizione 2.10.
4. Al solito, se togliere le parentesi non genera ambiguità, possiamo farlo. Per esempio, dato che $\wedge$ è associativa, è comune scrivere cose come $A_1 \wedge A_2 \wedge A_3$, tanto il risultato è lo stesso a prescindere da come mettiamo le parentesi. Però attenzione, perché mischiando $\wedge$ e $\vee$ si possono scrivere cose ambigue,

¹Come già spoilerato nella Nota 13 del Capitolo 1.

²Anche se immagino che in una situazione del genere valutare l’integrità logica di questa persona sia l’ultimo dei vostri problemi.

per esempio non c'è una convenzione standard su come mettere le parentesi in $A \wedge B \vee C$. Vedi Esercizio 2.50.

5. Al contrario, si conviene che $\neg$ abbia precedenza sugli altri connettivi. Per esempio, $\neg A \wedge B$ vuol dire, per convenzione, che $(\neg A) \wedge B$.
6. Una cosa come $(\neg A) \wedge B$, ottenuta combinando variabili proposizionali con i connettivi, si chiama *formula proposizionale*. Questa “combinazione” deve essere fatta in maniera sensata, ad esempio “ $\vee \vee A \wedge B \wedge$ ” non è una formula proposizionale. Per rendere preciso quel “in maniera sensata” si specifica una *grammatica formale* stipulando che:
 - (a) se A è una variabile proposizionale, allora A è una formula proposizionale;
 - (b) se φ, ψ sono formule proposizionali, allora $(\neg\varphi)$, $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$ sono formule proposizionali;³
 - (c) [regole simili per gli altri connettivi che introdurremo in seguito];
 - (d) nient'altro è una formula proposizionale, cioè ogni formula proposizionale è ottenuta usando le regole precedenti.

Una maniera concisa di dire quanto sopra è: l'insieme delle formule proposizionali è il più piccolo insieme che contiene le variabili proposizionali ed è chiuso per connettivi. Ora, dato che questo non è un corso di logica, nel seguito daremo definizioni più informali di così, ma è bene avere un'idea di come si fa a rendere queste cose precise.

Per quanto sia comodo avere a disposizione $\vee$, questo connettivo è superfluo, nel senso specificato nella Proposizione 2.8 sotto.

Definizione 2.6. Siano $n \in \mathbb{N}$ e φ e ψ due formule nelle variabili proposizionali $A_1, \dots, A_n$. Diciamo che φ e ψ sono *equivalenti* sse, per ogni assegnazione di valori di verità a $A_1, \dots, A_n$, il corrispondente valore di verità di φ è uguale a quello di ψ .

Se pensiamo alle formule come al codice di un programma, dire che due formule equivalenti vuol dire che forniscono lo stesso output su ogni input o, se preferite, se hanno la stessa tavola di verità.

Esempio 2.7. Le formule proposizionali $\varphi := \neg A$ e $\psi := \neg(\neg(\neg A))$: sono equivalenti: se assegniamo ad A il valore 0, un semplice calcolo mostra che sia φ che ψ hanno valore 1, e se assegniamo ad A il valore 1, sia φ che ψ hanno valore 0.

Proposizione 2.8. Per ogni A, B enunciati, $A \vee B$ è equivalente a $\neg(\neg A \wedge \neg B)$.

Un'altra maniera di enunciare questa proposizione è dire che le formule proposizionali $A \vee B$ e $\neg(\neg A \wedge \neg B)$ sono equivalenti. Nel primo caso, stiamo pensando ad A e B come a enunciati non specificati (e.g. “ $1 + 1 = 2$ e $1 + 1 = 3$ ”). Nel secondo caso, le stiamo pensando come variabili proposizionali (cioè cose al cui posto ci può andare 0 o 1). La differenza quasi non c'è, dato che di A, B ci interessa solo il valore di verità.

³E $\neg\psi$? Anche lei, ma dato che φ è arbitraria non serve dirlo anche con ψ .

A	B	$\neg A$	$\neg B$	$\neg A \wedge \neg B$	$\neg(\neg A \wedge \neg B)$
0	0	1	1	1	0
1	0	0	1	0	1
0	1	1	0	0	1
1	1	0	0	0	1

Figura 2.3: Tavola di verità di $\neg(\neg A \wedge \neg B)$.

In ogni caso, questo è un buon punto per dire che, in matematica, quando si enuncia un teorema usando variabili che non sono né assegnate né quantificate, si intende implicitamente che vengano quantificate universalmente all'inizio; in altre parole, se un teorema dice che “se $x, y \in \mathbb{N}$ allora $x + y = y + x$ ”, che come abbiamo visto sopra non sarebbe un enunciato, in realtà sta intendendo “per ogni x, y , se $x, y \in \mathbb{N}$ allora $x + y = y + x$ ”, che invece un enunciato lo è.

Ma vediamo come si dimostra la Proposizione 2.8.

Dimostrazione. Verifichiamo a mano la definizione di equivalenza controllando tutti i possibili assegnamenti di valori di verità. In altre parole, costruiamo la tavola di verità di $\neg(\neg A \wedge \neg B)$ e osserviamo che (la sua ultima colonna) è la stessa di (quella di) $A \vee B$. Questo lo facciamo “a pezzi” aggiungendo colonne per le *sottoformule* di $\neg(\neg A \wedge \neg B)$. Vedi Figura 2.3. $\square$

Alternativamente:

Dimostrazione. Fissiamo un assegnamento di valori di verità arbitrario ad A e B . Facciamo vedere che, senza sapere chi è questo assegnamento, se rende vero [rispettivamente, falso] il LHS allora rende anche [rispettivamente, falso] il RHS.

Se il nostro assegnamento rende vera $A \vee B$, allora deve rendere vera una delle due, che possiamo assumere *senza perdita di generalità*⁴ essere A perché l'enunciato è simmetrico in A, B . Allora $\neg A$ è falsa, e quindi a maggior ragione è falsa $\neg A \wedge \neg B$; per cui, la sua negazione, cioè il RHS, è vera. Se invece $A \vee B$ è falsa, allora sia A che B sono false, quindi $\neg A \wedge \neg B$ è vera, e quindi la sua negazione è falsa. $\square$

Vi potreste chiedere perché sprecare tutte queste righe invece di fare una tavola di verità. Immaginiamo di aver per le mani la formula

$$\varphi := (A \wedge [\text{formula lunghissima in } 10^{10^{10}} \text{ variabili}]) \wedge \neg A$$

Per stabilire che φ è equivalente alla formula sempre falsa (che si denota con $\perp$; ci torniamo), non c'è bisogno di fare nessuna tavola di verità: è facile dimostrare che φ è equivalente a $A \wedge \neg A \wedge [\text{roba}]$ (esercizio), e una formula del genere è sempre falsa, a prescindere da quante variabili contiene e che valore di verità gli si assegna (esercizio). In altre parole, a volte ci sono dimostrazioni estremamente più efficienti di guardare tutti i casi a mano per forza bruta. Trovarne una è ottimo, perché la dimensione delle tavole di verità cresce molto

⁴Una maniera un po' fancy per dire “è un caso particolare, ma il caso generale segue immediatamente”; cioè, dovremmo controllare anche il caso in cui l'assegnamento rende vera B , ma questo caso segue immediatamente da quello prima per simmetria scambiando A e B .

A	B	C	$(A \wedge B) \vee \neg C$
0	0	0	1
1	0	0	1
0	1	0	1
1	1	0	1
0	0	1	0
1	0	1	0
0	1	1	0
1	1	1	1

Figura 2.4: Tavola di verità di $(A \wedge B) \vee \neg C$.

in fretta quando cresce il numero di variabili, vedi e.g. la Figura 2.4. Se è una tale semplificazione sia sempre possibile⁵ è equivalente a uno dei problemi più importanti in informatica teorica [Wikf], vedi ad esempio [Wika].

Tornando a $\vee$, il fatto che sia esprimibile usando solo $\neg$ e $\wedge$ non è un caso: tutti i connettivi possono essere rimpiazzati da una combinazione di $\neg$ e $\wedge$ (Esercizio 2.56). Questa non è l'unica scelta possibile. Per esempio, potremmo anche usare $\neg$ e $\vee$, perché $\wedge$ si può esprimere a partire da loro:

Proposizione 2.9. $A \wedge B$ è equivalente a $\neg(\neg A \vee \neg B)$.

Dimostrazione. Esercizio. □

2.3 Ancora altri connettivi

Il fatto che sia possibile programmare tutto in assembly⁶ non vuol dire che sia una buona idea farlo, e c'è un motivo se esistono linguaggi di programmazione più di alto livello. Analogamente, introduciamo degli altri connettivi usati molto spesso e di cui fastidioso fare a meno.

Definizione 2.10. Definiamo i seguenti connettivi.

1. Il connettivo “falso” $\perp$, il cui valore di verità è sempre 0.
2. Il connettivo “vero” $\top$, il cui valore di verità è sempre 1.
3. L'*implicazione* $(A \Rightarrow B)$ (pronunciato “ A implica B ” o anche “se A allora B ”, o “se A B ”⁷, o “ B se A ” o anche “ A solo se B ”), equivalente per definizione a $\neg A \vee B$. Vedi Figura 2.5.
4. La *coimplicazione* $(A \Leftrightarrow B)$, (“ A coimplica B ”, o più comunemente “ A se e solo se B ”), equivalente per definizione a $(A \Rightarrow B) \wedge (B \Rightarrow A)$. Vedi Figura 2.5.

⁵Più precisamente, se è possibile trovare un algoritmo “veloce” per decidere se una formula è vera per almeno un assegnamento delle variabili.

⁶O in Whitespace, o in Brainfuck, o in Monicelli... [Eso].

⁷Pronuncia sconsigliatissima quando A, B sono enunciati matematici, specie quando hanno una certa complessità. Metterci in mezzo “allora” costa poco.

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

Figura 2.5: Tavole di verità di implicazione e coimplicazione.

5. La *o esclusiva* ($A \oplus B$), anche chiamata *xor*⁸, equivalente per definizione a $(A \vee B) \wedge \neg(A \wedge B)$. Vedi Esercizio 2.51.

Osservazione 2.11. Alcuni commenti:

1. Come esistono i connettivi unari, che prendono un argomento, e quelli binari, che ne prendono due, un connettivo 0-ario è un connettivo che non prende argomenti. Questa cosa è meno un grattacapo di quello che può sembrare: pensate a un programma senza input, che ritorna sempre la stessa cosa.⁹ Di connettivi 0-ari ce ne sono, a meno di equivalenza, solo due.
2. L'implicazione $A \Rightarrow B$ è un'altra cosa che tende ad essere fonte di grattacapi la prima volta che la si vede. *Non* esprime valore causale né temporale (vedremo vari esempi più avanti). Tutto quello che fa $A \Rightarrow B$ è dire che se A è vera allora anche B deve essere vera; se A è falsa allora B può fare quello che le pare. In particolare:
 - (a) Se B è vera, allora $A \Rightarrow B$ è sempre vera. Per esempio “se $2 + 2 = 5$ allora $2 = 2$ ” è vera, e anche “se nel 2026 la Spagna ha vinto i mondiali di calcio allora nel 2020 c'è stata una pandemia” è vera. Ovviamente è possibile fare esempi più ridicoli (esercizio).
 - (b) Se A è falsa, allora $A \Rightarrow B$ è sempre vera. Sempre. Per esempio, se A è “Parigi ha il mare” e B è “Parigi è Bari”, allora $A \Rightarrow B$ è vera.¹⁰ Idem nel caso in cui A è “ $1 = 2$ ” e B è “io sono il papa”.¹¹ Una maniera per convincersi di tutto questo è: immaginate di dire a un'amica “se il Bari vince ti offro la cena”; l'unico caso in cui la vostra amica può avere da ridire è se il Bari vince e non offrite la cena. In tutti gli altri tre casi, non avete mentito.
3. L'implicazione *non* è commutativa: confrontare l'esempio sopra con “se ti offro la cena il Bari vince”.
4. $A \Leftrightarrow B$ è vera se e solo se A e B sono equivalenti (esercizio). Ad esempio, $\neg A \Leftrightarrow \neg(\neg(\neg A))$ è vera per l'Esempio 2.7. Le formule proposizionali

⁸Sta per *exclusive or*, “o esclusiva”.

⁹Vedi anche le manpage dei comandi `true` e `false` nelle coreutils di GNU.

¹⁰Ovviamente $A \Rightarrow B$, con la stessa B , è vera anche se come A prendiamo “Berlino ha il mare”. Ma se invece prendiamo come A “Napoli ha il mare”, allora $A \Rightarrow B$ è falsa!

¹¹La seguente dimostrazione è attribuita a Bertrand Russell: l'insieme {io, il papa} ha 2 elementi. I suoi sottoinsiemi {io} e {il papa} hanno 1 elemento. Quindi, se $1 = 2$, per estensionalità io sono il papa.

“sempre vere”, o in altre parole vere per tutti gli assegnamenti di verità alle variabili, o ancora in altre parole le formule proposizionali equivalenti a $\top$, sono note anche come *tautologie*. Detto ancora in un'altra maniera, vuol dire che nella colonna a destra nella loro tabella di verità appare solo l'1. Quelle per cui appare solo lo 0 sono “sempre false”, e si chiamano *contraddizioni*. Se φ è una tautologia allora $\neg\varphi$ è una contraddizione, e se φ è una contraddizione allora $\neg\varphi$ è una tautologia (esercizio).

5. Abbiamo detto che, per usare meno parentesi, si conviene che $\neg$ ha la precedenza su $\wedge$ e $\vee$, e che per questi due non si stabilisce un ordine di precedenza. Tutti e tre hanno la precedenza su $\Rightarrow$ e $\Leftrightarrow$, e fra questi due non se ne stabilisce una. Per esempio, $\neg A \vee B \Rightarrow B \wedge \neg C$ è un'abbreviazione per $((\neg A) \vee B) \Rightarrow (B \wedge (\neg C))$.
6. Il connettivo $\Rightarrow$ non è associativo (esercizio), ma i libri di matematica sono pieni di scritture del tipo $A \Rightarrow B \Rightarrow C$. Questa di solito¹² viene trattata come un'abbreviazione per $(A \Rightarrow B) \wedge (B \Rightarrow C)$. È meno bizzarro di quanto pensi, dato che torna comodo per scrivere dimostrazioni o loro pezzi in maniera compatta, ad esempio

$$(2 \leq 3) \Rightarrow (2 \leq 4) \Rightarrow (2 + 2 \leq 4 + 2)$$

7. Invece di $\Rightarrow$ e $\Leftrightarrow$, in letteratura a vengono anche usati $\rightarrow$ e $\leftrightarrow$, il che libera i simboli $\Rightarrow$ e $\Leftrightarrow$ che vengono allora usati per denotare implicazione o equivalenza fra formule proposizionali, e gli si viene data priorità più bassa. Ad esempio, si può “ $A \rightarrow B \Leftrightarrow \neg A \vee B$ ” al posto di “ $A \rightarrow B$ è equivalente a $\neg A \vee B$ ”.

Per quanto alcune tautologie possano risultare poco interessanti (che ne so, $A \Leftrightarrow A$), altre tornano utili in pratica perché forniscono tecniche dimostrative. Ad esempio:

Esercizio 2.12. Mostrare che le seguenti sono tautologie.

1. $A \vee \neg A$ (*principio del terzo escluso*). Questo si può usare per fare dimostrazioni per casi (“o A è vera, nel qual caso [...] oppure A è falsa, nel qual caso [...]”)
2. $\neg\neg A \Leftrightarrow A$ (*eliminazione della doppia negazione*). Questa ci permette di semplificare le formule.

Di tautologie con dei nomi ce ne sono parecchie; un altro esempio è la *legge di non contraddizione* $\neg(A \wedge \neg A)$: una cosa non può essere contemporaneamente vera e falsa.

Un altro esempio importante è il fatto che, nonostante la freccia $\Rightarrow$ “non si possa girare” nel senso che $A \Rightarrow B$ non è equivalente a $B \Rightarrow A$, è possibile “girarla” al prezzo di negare sia A che B :

Esercizio 2.13. Dimostrare che la seguente è una tautologia.

$$(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$$

¹²In alcuni contesti (per esempio nei tipi di un linguaggio di programmazione) ha invece senso convenire che le frecce associno a destra: $A \rightarrow (B \rightarrow C)$.

Definizione 2.14. La formula $\neg B \Rightarrow \neg A$ viene chiamata la *contronominale* di $A \Rightarrow B$.

Osservazione 2.15. Nell'Osservazione 2.11.2 dicevamo che $\Rightarrow$ non indica né un rapporto di causa-effetto né forme di successione temporale. Questo è molto chiaro guardando l'equivalenza sopra: ad esempio, “se piove allora prendo l'ombrello” è equivalente a “se non prendo l'ombrello allora non piove”!

Il fatto che un'implicazione e la sua contronominale siano equivalenti ci permette di dimostrare un'istanza della seconda dimostrandone invece una della prima che magari ha una dimostrazione semplice. Vediamo subito un esempio.

Dimostrazione. Dimostriamo che, per ogni $n \in \mathbb{N}$, se n^2 è pari allora n è pari. La contronominale è: se n non è pari, allora n^2 non è pari. Quindi ci basta dimostrare che, se n è dispari, allora n^2 è dispari. Se n è dispari, per definizione esiste un numero naturale a tale che $n = 2a + 1$. Allora un facile calcolo mostra che $n^2 = 2(2a^2 + a) + 1$, quindi n^2 è della forma $2b + 1$ con $b \in \mathbb{N}$, ed è quindi dispari. $\square$

A proposito di tecniche di dimostrazione, siete invitate a comparare l'equivalenza seguente con il metodo di dimostrazione per assurdo (usato ad esempio per dimostrare la Proposizione 1.15).

Esercizio 2.16. Dimostrare che A è equivalente a $\neg A \Rightarrow \perp$.

Osservazione 2.17. Ad essere precisi e pignoli fino al midollo, il punto 1 dell'Osservazione 2.5 è falso. “Ma come, ho fatto l'esercizio e le tavole di verità tornano!”. Ok, se $\wedge$ la intendiamo come una funzione che prende in input una coppia ordinata di elementi dell'insieme $\{0, 1\}$ e ritorna un elemento dell'insieme $\{0, 1\}$, allora sì, $\wedge$ è commutativa.

Se invece $\wedge$ la intendiamo come una funzione che prende in input una coppia ordinata di formule proposizionali e restituisce una formula proposizionale, allora $\wedge$ non è commutativa perché, per esempio, le formule $A \wedge B$ e $B \wedge A$ sono diverse: le formule sono (delle particolari) stringhe simboli, l'ordine dei simboli conta, e qui una comincia con A e una con B . Quello che (chi)ha(fatto l'eserc)io ha dimostrato è che $A \wedge B$ e $B \wedge A$ sono equivalenti. In altre parole, $\wedge$ come operazione sulle formule non è veramente commutativa, ma *commutativa a meno di equivalenza*.

Per la cronaca, quando invece abbiamo detto che se A e B sono insiemi allora $A \cap B = B \cap A$, lì $\cap$ è un'operazione che prende in input una coppia ordinata di insiemi e restituisce un insieme, stop.

Come potreste aver notato, c'è un parallelo fra operazioni su insiemi e connettivi logici, dovuto al fatto che, fissato un insieme X e assumendo $x \in X$ e $A, B \subseteq X$ ¹³,

$$x \in A \cup B \iff x \in A \vee x \in B \quad (2.1)$$

$$x \in A \cap B \iff x \in A \wedge x \in B \quad (2.2)$$

$$x \in A^c \iff x \notin A \quad (2.3)$$

¹³Questa, ovviamente, è un'abbreviazione per “ $A \subseteq X$ e $B \subseteq X$ ”.

e le varie proprietà che abbiamo visto per $\cup, \cap$,⁶ si traducono in proprietà di $\vee, \wedge, \neg$ (d'altra parte, se si usano simboli simili ci sarà un motivo). Ad esempio, abbiamo la seguente versione delle leggi di De Morgan:

$$\neg(A \vee B) \iff \neg A \wedge \neg B \quad (2.4)$$

$$\neg(A \wedge B) \iff \neg A \vee \neg B \quad (2.5)$$

che potete dimostrare, ad esempio calcolando tavole di verità (esercizio). Oppure, $\wedge$ distribuisce su $\vee$ e viceversa (esercizio), $A \vee \neg A$ è una tautologia, etc. Non sto a tediarevi, ma vi raccomando di riguardare in questa luce il capitolo precedente, esercizi inclusi (che avete fatto, vero?). In ogni caso, ci torniamo.

Esercizio 2.18. Disegnare i diagrammi di Venn per le operazioni su insiemi che corrispondono a $A \Rightarrow B$ ed a $A \Leftrightarrow B$.

Una cosa che è *vitale*¹⁴ non sbagliare a fare è “negare le formule”; non mi riferisco a, semplicemente, passare da $A \vee B$ a $\neg(A \vee B)$, ma ad usare cose come le leggi di De Morgan per spingere le negazioni “più dentro possibile” ed eventualmente operare altre semplificazioni, producendo una formula equivalente ma tipicamente più comprensibile. Ad esempio:

$$\begin{aligned} & \neg(A \wedge \neg(A \Rightarrow \neg B)) \\ \iff & \neg A \vee \neg\neg(A \Rightarrow \neg B) \\ \iff & \neg A \vee (A \Rightarrow \neg B) \\ \iff & \neg A \vee (\neg A \vee \neg B) \\ \iff & (\neg A \vee \neg A) \vee \neg B \\ \iff & \neg A \vee \neg B \end{aligned}$$

che, per la cronaca, è equivalente anche a $A \Rightarrow \neg B$ (o se preferite a, $B \Rightarrow \neg A$). Per essere precisi, invece di parlare di “negare le formule”, dovremmo parlare di *metterle in forma normale negativa*.

Definizione 2.19. Una formula è in *forma normale negativa* sse usa solo $\wedge, \vee, \neg$, e inoltre $\neg$ appare solo applicato a variabili proposizionali.

Si può dimostrare che ogni formula è equivalente a una in forma normale negativa. Questa forma, comunque, non è unica. In altre parole, ci sono formule equivalenti a diverse formule in forma normale negativa (che comunque sono tutte equivalenti, essendo equivalenti a quella di partenza). Per esempio, $A \vee \neg B$ e $\neg B \vee A$, ma si possono fare esempi meno banali, vedi Esercizio 2.55.

Last but not least, questa equivalenza vi servirà di continuo, ad esempio per dimostrare un'implicazione procedendo per assurdo.

Teorema 2.20. $\neg(A \Rightarrow B)$ è equivalente a $A \wedge \neg B$.

Dimostrazione. Esercizio. □

¹⁴Letteralmente. Non sto scherzando, vedi Sezione 2.9.

2.4 Variabili e quantificatori

Con le formule proposizionali ci si fa fino a un certo punto. Vorremmo poter fare cose come prendere una variabile, ad esempio x , farla spaziare su una *struttura* matematica, ad esempio $(\mathbb{N}, +, \cdot, \leq)$, e scrivere cose come $\forall x \forall y \forall z (x^4 + y^4 = z^4) \Rightarrow (x = 0 \vee y = 0 \vee z = 0)$. Definiremo queste cose solo in maniera informale ma, come nel punto 6 dell'Osservazione 2.5, è possibile fare tutto in maniera precisa specificando una grammatica formale.¹⁵

Supponiamo di voler studiare la struttura $(\mathbb{N}, 0, 1, +, \cdot, \leq)$. I simboli dopo $\mathbb{N}$ qui costituiscono un *vocabolario* per studiare questa struttura. Qui “0” e “1” sono *costanti*, “+” è una *funzione binaria*, “ $\cdot$ ” pure, mentre $\leq$ è una *relazione binaria*, e li abbiamo a disposizione perché stiamo lavorando in questa struttura. Possiamo usare lo stesso vocabolario anche per studiare altre strutture, ad esempio $(\mathbb{Z}, 0, 1, +, \cdot, \leq)$, dove $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ è l'insieme degli *interi*.¹⁶

Oltre ai simboli del vocabolario che ci siamo scelti, la logica del prim'ordine ci dà, “gratis” in ogni struttura, dei *simboli logici*: il simbolo $=$, che è un simbolo di relazione binaria che fa quello che vi aspettate, una quantità infinita di *variabili* $x, y, z, x_0, x_1, x_2, x_3, \dots$, i connettivi che abbiamo visto nelle scorse sezioni, e i *quantificatori* $\exists$ e $\forall$, su cui torniamo presto.¹⁷

Inoltre, quando siamo in una struttura, possiamo usare come *parametri* i suoi elementi. Se siamo in $\mathbb{N}$, ad esempio possiamo usare il parametro 7. In questa struttura non possiamo usare il parametro -5 , che non è in $\mathbb{N}$, ma lo possiamo usare se stiamo lavorando in $\mathbb{Z}$, che lo contiene.

Usando queste cose possiamo costruire le *formule del prim'ordine*, ad esempio $x + 1 \leq (y + 1) \cdot (1 + 1 + 1)$ oppure $(\exists y y^2 + 5 = x) \wedge (x \leq 18)$. In quest'ultima formula, la variabile y è *legata* dal quantificatore $\exists$, mentre la variabile x è *libera*, perché non è nello scope¹⁸ di alcun quantificatore.¹⁹ Di solito, quando una formula ha delle variabili libere lo si indica nel suo nome; ad esempio, le due formule precedenti potrebbero essere denotate rispettivamente $\varphi(x, y)$, pronunciato “ φ di x, y ”, e $\psi(x)$.²⁰

Se $A, B, C, \dots$ erano variabili proposizionali, dei “segnaposto” da sostituire con “vero” o “falso”, quelle appena introdotte sono *variabili del prim'ordine*: dei segnaposto da sostituire con elementi della struttura che stiamo studiando. Negli esempi sopra, al posto di x e y ci possiamo mettere elementi di $\mathbb{N}$.

In breve, la formula $\varphi(x) := x + 1 = 1 + 1 + 1$ non è un enunciato, perché senza sapere chi è x non ha senso dire se è vera o falsa. Però ci possiamo fare delle cose interessanti.

¹⁵E una semantica. Di nuovo, questo non è un corso di logica, ma un possibile punto di partenza per approfondire è [Wikb].

¹⁶Su cui torneremo più avanti, ma che confido abbiate già incontrato. Per il momento, mi scuso per i puntini.

¹⁷In letteratura si nominano anche le parentesi, ma qui le stiamo vedendo come parte dei connettivi e quantificatori: ricordiamo che formalmente $A \vee B$ è un'abbreviazione per $(A \vee B)$.

¹⁸Nel senso inglese, non nel senso degli attrezzi per pulire.

¹⁹Basta meno: basta comparire almeno una volta fuori dallo scope di tutti i quantificatori, ad esempio, x è libera in $(x + 1 = 1 + 1 + 1) \vee (\exists x x + 1 = 0)$. Nella pratica, riutilizzare le variabili in questo modo è ~~da evitare~~ poco chiaro e tende a non essere fatto.

²⁰Più precisamente, scrivere $\varphi(x, y)$ indica che l'insieme delle variabili libere di φ è incluso in $\{x, y\}$. Ad esempio, è lecito scrivere $\varphi(x, y) := x + 1 = 0$. Se volete, potete pensarla come abbreviazione per $\varphi(x, y) := x + 1 = 0 \wedge y = y$.

1. Al posto di x ci possiamo mettere un elemento della struttura che stiamo guardando, in questo caso $\mathbb{N}$. Per esempio, ci possiamo mettere 7. Questa cosa si denota con $\varphi(7/x)$, o anche direttamente $\varphi(7)$. Se lo facciamo per tutte le variabili libere, otteniamo un enunciato, e allora ha senso dire se è vero oppure falso. Per esempio, $\varphi(7)$ è $7 + 1 = 1 + 1 + 1$, che è falso.
2. Possiamo guardare tutte le cose che rendono la formula vera quando sostituite. In altre parole, possiamo usare una formula $\varphi(x)$ per *definire* un sottoinsieme di $\mathbb{N}$: l'insieme $\{x \in \mathbb{N} \mid \varphi(x)\}$. Con la $\varphi(x)$ di prima abbiamo

$$\{x \in \mathbb{N} \mid \varphi(x)\} = \{x \in \mathbb{N} \mid x + 1 = 1 + 1 + 1\} = \{2\}$$

Più in generale ogni formula in n variabili definisce un sottoinsieme dell' n -esima potenza cartesiana.²¹ Ad esempio possiamo prendere la formula $\varphi(x, y, z) := x^2 + y^2 \leq z^2$ e usarla per definire

$$\{(x, y, z) \in \mathbb{N}^3 \mid x^2 + y^2 \leq z^2\} \subseteq \mathbb{N}^3$$

In caso non ve ne foste accorti, questa cosa la sapete già: ad esempio l'avete vista nell'Esercizio 1.40.

3. Possiamo *quantificare* le variabili libere:

Definizione 2.21. Il *quantificatore esistenziale* $\exists$ (pronunciato “esiste”) funziona come segue. Data una formula $\varphi(x)$, anche $(\exists x \varphi(x))$ è una formula, ed è vera in una struttura M sse, per almeno un $a \in M$, è vera $\varphi(a)$.

Quindi, per esempio, $\exists x x \cdot x = 1 + 1$ è falsa in $\mathbb{N}$, dato che asserisce l'esistenza di un naturale il cui quadrato è 2, mentre $\exists x x \cdot x = 4$, sempre in $\mathbb{N}$, è vera, perché se rimuoviamo $\exists x$ e sostituiamo 2 alle altre due 2 otteniamo la formula $2 \cdot 2 = 4$, che è vera.

Osservazione 2.22. In altre parole, $\exists x \varphi(x)$ è vera in una struttura M se e solo se $\{x \in M \mid \varphi(x)\} \neq \emptyset$.

Possiamo anche limitare il quantificatore a un insieme dato. Per esempio, se $D \subseteq \mathbb{N}$ è l'insieme dei numeri dispari, possiamo scrivere²²

$$\exists x \in D x \cdot x = 4$$

e ora gli x che “vanno bene” per controllare se il resto della formula è vera devono per forza venire da D ; quelli fuori da D non contano. In altre parole, $\exists x \in A \varphi(x)$ è equivalente, per definizione, a $\exists x (x \in A \wedge \varphi(x))$, ed è vera

²¹Il caso 0 non fa eccezione. Forse ci torniamo più avanti.

²²Se state pensando “Ehi, ma non ci avevi detto che si poteva usare il simbolo $\in$ nelle formule!” avete ragione. Strettamente parlando, in logica del prim'ordine non si può (a meno che $\in$ non sia nel vocabolario, e comunque in quel caso si userebbe fra elementi della struttura, non fra un elemento e un sottoinsieme). Se D è definito da una formula $\psi(x)$ del vocabolario che già abbiamo, si può trattare $\exists x \in D \varphi(x)$ come abbreviazione per $\exists x \psi(x) \wedge \varphi(x)$. Se D non è definito da nessuna formula del vocabolario a disposizione, ci si può ricondurre al caso precedente *espandendo* il vocabolario e aggiungendo alla struttura un simbolo $P_D(x)$ di relazione unaria che è vero se e solo se $x \in D$.

se e solo se l'insieme delle soluzioni di $\varphi(x)$ interseca²³ A . In questo esempio, chiaramente, $\exists x \in D \ x \cdot x = 4$ è falsa.

A volte, invece di A , si mette direttamente una sua definizione; ad esempio, $\exists x \geq 5 \ \varphi(x)$, dove A in questo caso sarebbe $\{x \mid x \geq 5\}$.

Per la cronaca, in logica matematica per dire che, per esempio, $\exists x \ \varphi(x)$ è vera nella struttura $\mathbb{N}$, si scrive $\mathbb{N} \models \exists x \ \varphi(x)$. Nel resto della matematica il simbolo $\models$ è poco usato, e di solito si dice invece che $\exists x \in \mathbb{N} \ \varphi(x)$ è vera.²⁴

Al di là di quale convenzione si usa, la cosa importante è sapere dove sta spaziando il nostro quantificatore. L'enunciato $\exists x \ (x + 1 = 0)$ è falso nella struttura dei numeri naturali $\mathbb{N}$, ma è vero nella struttura dei numeri interi. Che scriviamo $\mathbb{N} \models \neg(\exists x \ (x + 1 = 0))$ oppure $\neg(\exists x \in \mathbb{N} \ (x + 1 = 0))$, che scriviamo $\mathbb{Z} \models \exists x \ (x + 1 = 0)$ oppure $\exists x \in \mathbb{Z} \ (x + 1 = 0)$ poco importa. Ma se scriviamo solo $\exists x \ (x + 1 = 0)$, è fondamentale che sia chiaro dal contesto quali x sta andando a guardare quell' $\exists$.

Vediamo ora un altro quantificatore.

Definizione 2.23. Il *quantificatore universale* $\forall$ (pronunciato “per ogni”) funziona come segue. Data una formula $\varphi(x)$, anche $(\forall x \ \varphi(x))$ è una formula, ed è vera in una struttura M sse, per tutti gli $a \in M$, è vera $\varphi(a)$.

Osservazione 2.24. In altre parole, $\forall x \ \varphi(x)$ è vera in una struttura M se e solo se $\{x \in M \mid \varphi(x)\} = M$.

Anche qui possiamo scrivere $\forall x \in A \ \varphi(x)$, che questa volta è equivalente per definizione a $\forall x \ (x \in A \Rightarrow \varphi(x))$. E adesso, perché $\forall x \in A \ \varphi(x)$ sia vera, basta che $\varphi(a)$ sia vera ogni volta che a lo prendiamo da A ; cosa succede fuori da A non conta, e $\forall x \in A \ \varphi(x)$ è vera se e solo se l'insieme delle soluzioni di $\varphi(x)$ include A .

Ovviamente le operazioni viste prima della Definizione 2.21 possono essere combinate, e possiamo per esempio definire l'insieme

$$\{x \in \mathbb{N} \mid \exists y \ x^2 + y^2 \leq 43\}$$

che potete per esempio calcolare come esercizio.

Come già accennato, se effettuiamo una di queste operazioni per tutte le variabili libere, alla fine otteniamo un *enunciato del prim'ordine*: una formula del prim'ordine che ha senso dire se sia vera oppure falsa in una struttura fissata (struttura per il vocabolario dell'enunciato).

Prima di andare avanti, cos'è una struttura quindi?

Osservazione 2.25. Possiamo pensare²⁵ alle strutture come a dei database. Per esempio, nel caso di $(\mathbb{N}, +, \cdot, \leq)$ c'è un'entrata per ogni numero naturale, c'è una tabella per il $+$ che ci dice quali sono le terne (x, y, z) tali che $x + y = z$, una tabella per il $\cdot$ che ci dice quali sono le terne (x, y, z) tali che $x \cdot y = z$, e una per il $\leq$ che ci dice quali sono le coppie (x, y) tali che $x \leq y$. Guardare l'insieme definito da una formula è come fare una query.

²³“ X interseca Y ” vuol dire che $X \cap Y \neq \emptyset$.

²⁴Di fatto, questo vuol dire lasciare al lettore il compito di dedurre dal contesto in che struttura stiamo lavorando, perché non è detto che sia il primo quantificatore a dirci in che struttura siamo. Ad esempio, se scriviamo $\forall x \in \mathbb{N} \ \exists y \in \mathbb{Z} \ x + y = 0$, questa formula va guardata in $\mathbb{Z}$, e $\mathbb{N}$ visto come un suo sottoinsieme.

²⁵Questa è *molto* più che un'analogia.

Notiamo che, se per esempio teniamo fisso l'insieme $\mathbb{N}$ ma cambiamo la tabella del $\leq$, la struttura cambia! In altre parole, per specificare una struttura in un vocabolario dobbiamo dare una tabella per ogni simbolo del vocabolario, e se cambiamo una di queste tabelle stiamo lavorando in un'altra struttura. Insomma, pensandole come database, le strutture sono read only, se parliamo di "cambiarla" in realtà stiamo parlando di farne una nuova con le modifiche specificate.

2.5 Come (non) usare i quantificatori

Anche in logica del prim'ordine ha senso parlare di enunciati equivalenti.

Definizione 2.26. Siano φ e ψ due enunciati del prim'ordine nello stesso vocabolario. Diciamo che φ e ψ sono *equivalenti* se, in ogni struttura nel loro vocabolario, φ è vera se e solo se ψ è vera.

Come per il simbolo $\Rightarrow$, i quantificatori si comportano in maniera che può sembrare all'inizio controintuitiva, e ci sono degli errori molto comuni che è *fondamentale* non fare.

Il primo di questi: pensare che $\neg\exists x (\varphi(x))$ sia equivalente a $\exists x (\neg\varphi(x))$. La prima ci sta dicendo che di x tali che $\varphi(x)$ non ce ne sono. La seconda, che c'è almeno un x tale che $\neg\varphi(x)$. Per convincersi che queste due cose non sono equivalenti, mettiamoci in $\mathbb{N}$ e prendiamo come $\varphi(x)$ la formula $x = 2 + 2$. Chiaramente $\varphi(4)$ è vera, quindi $\exists x (\varphi(x))$ è vera, e quindi la sua negazione $\neg(\exists x (\varphi(x)))$ è falsa. D'altra parte, di x tali che $\neg(x = 2 + 2)$ ce ne sono quanti ne vogliamo. Ad esempio, $\neg\varphi(17)$ è vera, e quindi $\exists x \neg\varphi(x)$ è vera.

Se preferite, se la nostra struttura è l'insieme degli abitanti di Bari con un simbolo di relazione $P(x)$ che sta per " x è al mare", allora $\neg\exists x P(x)$ dice che al mare non c'è nessuno, mentre $\exists x \neg P(x)$ dice che qualcuno è da un'altra parte.

Tuttavia, è possibile "spingere le negazioni all'interno" anche in presenza di quantificatori, grazie ai teoremi seguenti.

Teorema 2.27. Per ogni formula $\varphi(x)$, abbiamo che $\neg(\exists x \varphi(x))$ è equivalente a $\forall x (\neg\varphi(x))$.

Dimostrazione. Mostriamo le due implicazioni $\neg(\exists x \varphi(x)) \Rightarrow \forall x (\neg\varphi(x))$ e $\neg(\exists x \varphi(x)) \Leftarrow \forall x (\neg\varphi(x))$.

Da sinistra a destra, se assumiamo $\neg(\exists x \varphi(x))$ allora $\exists x \varphi(x)$ è falsa, il che vuol dire che non c'è nessun elemento a tale che $\varphi(a)$. Quindi, qualunque elemento a prendiamo $\varphi(a)$ è falsa, e quindi $\neg\varphi(a)$ è vera. Dato che questo succede per tutti gli a , è vera $\forall x \neg\varphi(x)$.

Invece di dimostrare direttamente l'implicazione da destra a sinistra, dimostriamo invece la contronominale. Dopo aver eliminato le doppie negazioni, questa è (equivalente a) $(\exists x \varphi(x)) \Rightarrow \neg(\forall x \neg\varphi(x))$. Assumiamo quindi $\exists x \varphi(x)$. Allora, per qualche a , abbiamo $\varphi(a)$. Supponiamo per assurdo di avere $\forall x \neg\varphi(x)$. Allora, qualunque sia b , dobbiamo avere $\neg\varphi(b)$. In particolare, questo vale per $b = a$. Ma allora vale sia $\varphi(a)$ che $\neg\varphi(a)$. Questa è una contraddizione²⁶, per cui $\forall x \neg\varphi(x)$ deve essere per forza falsa, e otteniamo $\neg(\forall x \neg\varphi(x))$. $\square$

²⁶Se volete, è una contraddizione per il principio di non contraddizione.

Teorema 2.28. Per ogni formula $\varphi(x)$, abbiamo che $\neg(\forall x \varphi(x))$ è equivalente a $\exists x (\neg\varphi(x))$.

Dimostrazione. Esercizio. Suggerimento: una maniera è ricalcare la dimostrazione del Teorema 2.27 (e va benissimo). Una maniera più pigra è applicare il Teorema 2.27 non proprio a φ ma a qualcosa di imparentato e fare qualche manipolazione di connettivi. $\square$

Corollario 2.29. Per ogni formula $\varphi(x)$ è vero che

1. $\exists x \varphi(x)$ è equivalente a $\neg\forall x \neg\varphi(x)$, e che
2. $\forall x \varphi(x)$ è equivalente a $\neg\exists x \neg\varphi(x)$.

Quindi, come per $\forall$ che è ridondante se già abbiamo $\neg$ e $\wedge$, il quantificatore $\forall$ è ridondante se già abbiamo $\neg$ e $\exists$, nel senso che non ci permette di esprimere nulla di nuovo.²⁷

Esercizio 2.30. Dimostrare gli analoghi dei Teoremi 2.27 e 2.28 e del Corollario 2.29 ottenuti rimpiazzando $\exists x$ con $\exists x \in D$ e $\forall x$ con $\forall x \in D$.²⁸

Guardiamo il più classico degli esempi:

Esempio 2.31. Mettiamoci nella struttura $(\mathbb{R}, +, \cdot, 0, |\cdot|, f, <, \leq)$, dove $\mathbb{R}$ è l'insieme dei numeri reali, $|\cdot|$ è la funzione “valore assoluto”, e f è una qualche funzione unaria fissata ma arbitraria.²⁹ Neghiamo la formula

$$\varphi := \forall x \forall \varepsilon > 0 \exists \delta > 0 \forall y (|x - y| < \delta \Rightarrow |f(x) - f(y)| < \varepsilon)$$

che forse riconoscerete essere l'enunciato che dice “ f è continua”. Se questa è vera o meno, dipende da f (che è parte dei dati specificati nello specificare la struttura). In ogni caso, a prescindere da f , e a prescindere da se sappiamo qualcosa sulle funzioni continue o sui numeri reali, negare questa formula è una questione puramente meccanica, di mera manipolazione di simboli, che non dipende dal significato degli stessi. Svolgendo i passaggi uno alla volta:

$$\begin{aligned} & \neg(\forall x \forall \varepsilon > 0 \exists \delta > 0 \forall y (|x - y| < \delta \Rightarrow |f(x) - f(y)| < \varepsilon)) \\ \iff & \exists x \neg(\forall \varepsilon > 0 \exists \delta > 0 \forall y (|x - y| < \delta \Rightarrow |f(x) - f(y)| < \varepsilon)) \\ \iff & \exists x \exists \varepsilon > 0 \neg(\exists \delta > 0 \forall y (|x - y| < \delta \Rightarrow |f(x) - f(y)| < \varepsilon)) \\ \iff & \exists x \exists \varepsilon > 0 \forall \delta > 0 \neg \forall y (|x - y| < \delta \Rightarrow |f(x) - f(y)| < \varepsilon) \\ \iff & \exists x \exists \varepsilon > 0 \forall \delta > 0 \exists y \neg(|x - y| < \delta \Rightarrow |f(x) - f(y)| < \varepsilon) \\ \iff & \exists x \exists \varepsilon > 0 \forall \delta > 0 \exists y \neg(\neg(|x - y| < \delta) \vee |f(x) - f(y)| < \varepsilon) \\ \iff & \exists x \exists \varepsilon > 0 \forall \delta > 0 \exists y \neg \neg(|x - y| < \delta \wedge \neg(|f(x) - f(y)| < \varepsilon)) \\ \iff & \exists x \exists \varepsilon > 0 \forall \delta > 0 \exists y (|x - y| < \delta \wedge \neg(|f(x) - f(y)| < \varepsilon)) \end{aligned}$$

²⁷Questo parallelismo non è particolarmente sorprendente: dopo tutto, $\exists$ si comporta un po' come una “disgiunzione infinita”, e $\forall$ come una “congiunzione infinita”. Ad esempio, dire che in $\mathbb{N}$ è vera $\exists x \varphi(x)$ è un po' come dire che è vera $\varphi(0)$, oppure $\varphi(1)$, oppure $\varphi(2)$, eccetera. Però occhio, le formule della logica del primo ordine sono (delle particolari) stringhe *finite* di simboli, non possiamo letteralmente dire che una formula è una disgiunzione di infinite altre formule.

²⁸Tutti e due contemporaneamente! Se ne rimpiazziamo solo uno non funziona (esercizio: trovare un controesempio).

²⁹Nel senso: se cambiamo f , cambia la struttura, e quindi cambiano le formule vere nella struttura.

dove abbiamo usato i Teoremi 2.27 e 2.28, il fatto che $A \Rightarrow B$ è equivalente a $\neg A \vee B$, le leggi di De Morgan, e l'eliminazione della doppia negazione. Se poi ci ricordiamo anche che, in $\mathbb{R}$, abbiamo che $\neg(a < b)$ è equivalente a $a \geq b$, possiamo continuare:

$$\iff \exists x \exists \varepsilon > 0 \forall \delta > 0 \exists y (|x - y| < \delta \wedge |f(x) - f(y)| \geq \varepsilon)$$

Un'altro errore comune è scambiare quantificatori che non possono essere scambiati. Mentre $\exists x \exists y \varphi(x, y)$ e $\exists y \exists x \varphi(x, y)$ sono equivalenti (esercizio), così come lo sono $\forall x \forall y \varphi(x, y)$ e $\forall y \forall x \varphi(x, y)$ (esercizio anche questo), gli enunciati $\forall y \exists x \varphi(x, y)$ e $\exists x \forall y \varphi(x, y)$ *non* sono equivalenti.³⁰ Ad esempio, se lavoriamo nella struttura con elementi gli abitanti di Bari e un simbolo di relazione binaria $R(x, y)$ per “ x conosce y ”, allora $\forall y \exists x R(x, y)$ dice che ogni persona è conosciuta da almeno un'altra persona, mentre $\exists x \forall y R(x, y)$ dice che c'è una persona che conosce tutta Bari.

Per fare un esempio più matematico, $\forall x \in \mathbb{N} \exists y \in \mathbb{N} (y \geq x)$ dice che, per ogni numero naturale ne esiste un altro maggiore o uguale. Questo è banalmente vero:

Dimostrazione. Fissato un qualunque x , come *testimone* y dell'esistenziale possiamo prendere $y := x$ stesso; o se, se preferiamo, $y := x + 1$. $\square$

Invece, $\exists y \in \mathbb{N} \forall x \in \mathbb{N} (y \geq x)$ dice che i numeri naturali hanno un massimo, e questo è falso:

Dimostrazione. Supponiamo per assurdo che $\mathbb{N}$ abbia un massimo y . Quindi, per ogni $x \in \mathbb{N}$ dovremmo avere che $y \geq x$. Ma per $x := y + 1$ questo è falso, contraddizione. $\square$

Sempre per la rubrica “fonti di grattacapi”, nessuno ci vieta di quantificare sull'insieme vuoto. Quello che succede se usiamo il quantificatore esistenziale probabilmente ve lo aspettate:

Proposizione 2.32. In ogni struttura, per ogni formula $\varphi(x)$, l'enunciato $\exists x \in \emptyset \varphi(x)$ è falso.

Dimostrazione. Se fosse vero, esisterebbe un $a \in \emptyset$ tale che... non importa tale che cosa, già il fatto che ci sia un $a \in \emptyset$ ci dà un assurdo. $\square$

Quello che succede con il quantificatore universale invece può far alzare qualche sopracciglio.³¹

Proposizione 2.33. In ogni struttura, per ogni formula $\varphi(x)$, l'enunciato $\forall x \in \emptyset \varphi(x)$ è vero.

Quando questo succede, si parla di *essere vero a vuoto*. Ad esempio, dato che l'insieme dei cani su Marte è vuoto³², l'enunciato “tutti i cani su Marte guidano auto elettriche” è vero a vuoto. Essenzialmente, il motivo per cui è vero è che, se fosse falso, ci sarebbe un cane su Marte che... non importa cosa, in particolare ci sarebbe un cane su Marte, ma non c'è. Se l'argomento suona già sentito, non è un caso:

³⁰Come probabilmente già sapete se avete sentito dire le parole “uniformemente continua”.

³¹E generare discussioni sull'interpretazione di una carta nel bel mezzo di un gioco da tavolo. Aneddoto disponibile su richiesta.

³²Dati aggiornati al 1 ottobre 2026.

Dimostrazione. La Proposizione 2.32 vale per tutte le formule φ . Invece di applicarlo alla $\varphi(x)$ nell'enunciato di questa proposizione, lo applichiamo a $\neg\varphi(x)$, ottenendo che $\exists x \in \emptyset \neg\varphi(x)$ è falso. Quindi $\neg\exists x \in \emptyset \neg\varphi(x)$ è vero. Concludiamo applicando il Corollario 2.29 (o, più precisamente, l'Esercizio 2.30). $\square$

Se il sopracciglio ancora non si è abbassato, guardiamo una variante dell'Osservazione 2.11.3. Supponiamo che promettiate a un amico che “per ogni giornata di campionato in cui il Bari vince, la sera dopo ti offro la cena”. Supponiamo che il Bari abbia un campionato particolarmente disastroso fatto solo di pareggi e sconfitte. Chiaramente, potete non scuire un centesimo senza che il vostro amico possa accusarvi di aver mentito.

O ancora: “ogni numero sia pari che dispari è uguale al mio numero di telefono” è vera. E *non* vuol dire che il mio numero di telefono è sia pari che dispari: di tali numeri, non ce ne sono.³³

Osservazione 2.34. Il doversi confrontare con “casi estremi” come enunciati della forma $\forall x \in \emptyset \varphi(x)$ vi capiterà più spesso di quanto pensiate nel programmare. Ad esempio, potreste star scrivendo del codice e dover fare il caso base di una funzione ricorsiva.

Chiudiamo questa carrellata con un grande classico:

Proposizione 2.35. In ogni bar non vuoto c'è una persona che, se beve, bevono tutti.

Dimostrazione. Fissiamo un bar come nelle ipotesi e vediamo come struttura che ha come punti gli avventori del bar e come unico simbolo un simbolo di relazione unaria $B(x)$ che è vero sse x beve. L'enunciato della proposizione è che, in ogni tale struttura, è vera la formula $\exists y (B(y) \Rightarrow \forall x B(x))$. Abbiamo due casi:

1. Tutti nel bar stanno bevendo. Allora prendiamo una persona d qualunque nel bar, che esiste perché abbiamo assunto che il bar sia non vuoto. Dato che $\forall x B(x)$ è vera, $B(d) \Rightarrow \forall x B(x)$ è vera, e allora è vera $\exists y (B(y) \Rightarrow \forall x B(x))$.
2. C'è una persona a nel bar che non sta bevendo. Prendiamo proprio lei come persona che “se beve, bevono tutti”: infatti, dato che $B(a)$ è falsa, $B(a) \Rightarrow \forall x B(x)$ è vera (come tutte le implicazioni col membro di sinistra falso!), e quindi $\exists y (B(y) \Rightarrow \forall x B(x))$ è vera. $\square$

“Scusa ma cosa succede se questa persona a poi si mette a bere? Questo causa magicamente il comparire di bevande nelle mani di tutte le altre?” No, come dicevamo nell'Osservazione 2.11.2, non stiamo parlando di rapporti causa-effetto né di situazioni che si evolvono nel tempo, e questo è molto ben visibile in questo esempio. Quello che succede è la struttura non è più la stessa: nella prima struttura valeva $B(a)$, nella seconda vale $\neg B(a)$, quindi le due strutture non sono la stessa (vedi Osservazione 2.25). La proposizione è ancora vera

³³E tutti i numeri sono o pari o dispari. Per quanto spero che questo abominio sia finito, almeno un tempo si sentivano in giro baggiate come “0 e 1 non sono né pari né dispari” o peggio “0 e 1 sono parimpari”. A scanso di equivoci: 0 è pari perché è della forma $2k$ con k intero (nella fattispecie, $k = 0$), e 1 è dispari perché è della forma $2k + 1$ con k intero.

perché la stessa dimostrazione funziona ancora, ma se siamo nel secondo caso toccherà prendere un altro testimone dell'esistenziale.

Insomma, la logica del prim'ordine descrive situazioni “statiche”, e le strutture matematiche “non si muovono”: in questo caso, stiamo sostanzialmente ragionando su una fotografia del bar in un determinato momento.³⁴ Insomma, quello che la proposizione sta dicendo è che in ogni bar non vuoto, *in ogni determinato momento*, c'è una persona che, se lei sta bevendo, *tutti gli altri stanno già bevendo*.

2.6 Simboli con gli angoli vs. simboli tondi

Il fatto che i simboli $\wedge, \vee$ e $\cap, \cup$ si assomiglino non è un caso:

Esercizio 2.36. Siano $\varphi(x)$ e $\psi(x)$ due formule nel prim'ordine in una struttura M . Dimostrare che:

1. $\{x \in M \mid \varphi(x) \wedge \psi(x)\} = \{x \in M \mid \varphi(x)\} \cap \{x \in M \mid \psi(x)\}$
2. $\{x \in M \mid \varphi(x) \vee \psi(x)\} = \{x \in M \mid \varphi(x)\} \cup \{x \in M \mid \psi(x)\}$
3. $\{x \in M \mid \neg\varphi(x)\} = \{x \in M \mid \varphi(x)\}^c$

Esercizio 2.37. A che operazione su insiemi corrisponde $\Rightarrow$? A quale operazione corrisponde $\Leftrightarrow$?

Esercizio 2.38. Convincersi che $\{x \in M \mid \exists y \varphi(x, y)\}$ è la proiezione sulle x dell'insieme $\{(x, y) \in M^2 \mid \varphi(x, y)\}$.

Suggerimento. Scegliete un qualche insieme piccolo ma non troppo (boh, 7 elementi?) in $\mathbb{N}^2$, diciamo A , e calcolate chi è $\{x \mid \exists y (x, y) \in A\}$. $\square$

Esercizio 2.39. Dato $\{(x, y) \in M^2 \mid \varphi(x, y)\}$, che operazioni insiemistiche devo fare per ricavare $\{x \in M \mid \forall y \varphi(x, y)\}$?

Sopra abbiamo parlato più volte di enunciati equivalenti. Si può parlare di equivalenza anche per formule con variabili libere.

Definizione 2.40. Siano $\varphi(x_1, \dots, x_n)$ e $\psi(y_1, \dots, y_n)$ due formule libere nello stesso vocabolario.

1. Se M è una struttura, diciamo che $\varphi(x_1, \dots, x_n)$ e $\psi(x_1, \dots, x_n)$ sono *equivalenti in M* se in M è vera $\forall x_1 \dots \forall x_n (\varphi(x_1, \dots, x_n) \Leftrightarrow \psi(x_1, \dots, x_n))$.
2. Diciamo che $\varphi(x_1, \dots, x_n)$ e $\psi(x_1, \dots, x_n)$ sono *equivalenti* se sono equivalenti in tutte le strutture.

Esercizio 2.41. In $(\mathbb{Z}, +, \cdot)$, la formula $\varphi(x, y) := \exists k \, x + y = k + k$ è equivalente alla formula

$$\psi(x, y) := \left(((\exists k_0 \, x = k_0 + k_0) \wedge (\exists k_1 \, y = k_1 + k_1)) \right. \\ \left. \vee ((\exists k_2 \, x = k_2 + k_2 + 1) \wedge (\exists k_3 \, y = k_3 + k_3 + 1)) \right)$$

³⁴Ovviamente, questo non vuol dire che le strutture matematiche non possano essere usate per studiare cose che si muovono.

Osservazione 2.42. Essenzialmente tutto quello che abbiamo detto sopra *si generalizza* a formule con variabili libere. Ad esempio $\neg\forall x \varphi(x, y)$ è equivalente a $\exists x \neg\varphi(x, y)$, eccetera. È un ottimo esercizio riguardare tutta la sezione e rifare più dimostrazioni possibili per questo caso.

2.7 Logica del second'ordine e numeri naturali

Fissiamo una struttura M . Nelle sezioni precedenti abbiamo visto variabili e quantificatori del prim'ordine, che spaziano sugli elementi $x \in M$. Le variabili del *second'ordine*, di solito denotate con lettere maiuscole, e i loro quantificatori, spaziano sui sottoinsiemi $X \subseteq M$, e le formule possono parlare di appartenenza a queste variabili. Ad esempio, con la logica del second'ordine, possiamo scrivere cose come

$$\exists X \subseteq \mathbb{N} \forall x \in \mathbb{N} (x \in X \Leftrightarrow \exists k (x = 5 \cdot k))$$

che dice che esiste l'insieme dei multipli di 5.

Usando la logica del second'ordine possiamo “dire cosa fanno” i numeri naturali: elencare delle proprietà di base soddisfatte da loro, e “in sostanza”³⁵ solo da loro.

Definizione 2.43. Scriviamo s per denotare la funzione “successore” sui numeri naturali, definita da $s(x) := x + 1$.

Definizione 2.44. Gli *assiomi di Peano* sono i seguenti:

$$(PA1) \quad \forall x \neg(s(x) = 0)$$

$$(PA2) \quad \forall x \forall y ((s(x) = s(y)) \Rightarrow x = y)$$

$$(PA3) \quad \forall A \left((0 \in A \wedge \forall x (x \in A \Rightarrow s(x) \in A)) \Rightarrow \forall x x \in A \right)$$

Vediamo cosa dicono questi assiomi.

1. L'assioma (PA1) dice che nessun numero naturale ha 0 come successore.
2. L'assioma (PA2) dice che, se due numeri naturali x, y hanno lo stesso successore, allora sono uguali: se so chi è il successore di x , posso ricavarli chi è x . In altre parole, la funzione successore è *iniettiva*.
3. L'assioma (PA3) è anche noto come *principio di induzione*. È un principio potentissimo da usare nelle dimostrazioni, e imparare a usarlo è una delle cose più importanti da portarsi a casa da questo corso. Ma digeriamo un po' questa sleppa di simboli e vediamo cosa dice. Ci dice che, se abbiamo un sottoinsieme $A \subseteq \mathbb{N}$, e questo insieme contiene 0 ed è *chiuso per successore*, cioè il successore di qualunque elemento di A è ancora dentro A , allora A contiene tutti i numeri naturali, cioè $A = \mathbb{N}$. In altre parole, ci dice che se parto da 0 e continuo ad aggiungere 1, becco tutti i numeri naturali.

Fatto 2.45. Tutti gli assiomi di Peano sono veri nella struttura $(\mathbb{N}, 0, s)$.

³⁵Ci torniamo, qualche anticipazione in Nota 36.

Se avete (o quando avrete) letto la Sezione 1.5, potete prendere il fatto precedente come un teorema e provare a dimostrarlo. Altrimenti, potete sostanzialmente prenderlo come definizione dei numeri naturali, dato che sono, in un certo senso³⁶, l'unica struttura che li soddisfa.

Ad ogni modo, a titolo di primo assaggio, vediamo un esempio di utilizzo del principio di induzione per dimostrare qualcosa di non ovvio.

Proposizione 2.46. Per ogni n , la somma di tutti numeri naturali da 1 a n (estremi inclusi) è uguale a $n(n+1)/2$.

- Per esempio, $1 + 2 + 3 + \dots + 999 + 1000 = 500 \cdot 1001 = 500500$. Che è un calcolo un pelino più veloce di fare tutte le somme a mano.
- Qualunque sia n , uno fra n ed $(n+1)$ è pari, quindi $n(n+1)$ è sempre pari, e quindi $n(n+1)/2$ è sempre intero.
- È un buon momento per vedere come scrivere “la somma di tutti numeri naturali da 1 a n ” in matematica. Si scrive

$$\sum_{i=0}^n i$$

e si legge “somma per i che va da 0 a n di i ”.

Questa scrittura funziona un po' come un ciclo `for`: si prende i , si pone i uguale a quello che c'è scritto sotto, si somma quello che c'è scritto a destra (che tipicamente dipende da i), e ci si ferma quando i arriva a quello che c'è scritto sopra (incluso). Per esempio, possiamo scrivere $1^2 + 2^2 + 3^2 + 4^2$ come $\sum_{i=1}^4 i^2$.

Dimostrazione della Proposizione 2.46. Dobbiamo mostrare che, per ogni $n \in \mathbb{N}$, abbiamo

$$\sum_{i=0}^n i = \frac{n(n+1)}{2} \quad (2.6)$$

Chiamiamo A l'insieme degli n per cui la (2.6) è vera, e facciamo vedere che $A = \mathbb{N}$. Per l'assioma (PA3) ci basta far vedere due cose:

1. Che A contiene 0.
2. Che, per ogni $x \in \mathbb{N}$, se A contiene x allora contiene anche $x+1$.

Per verificare che $0 \in A$ (il caso base), iniziamo notando che $\sum_{i=0}^0 i = 0$. Ma anche $0(0+1)/2 = 0 \cdot 1/2 = 0/2 = 0$, quindi il caso $n = 0$ della (2.6) è vero, e allora $0 \in A$.

³⁶Più precisamente, l'unica nel vocabolario $\{0, s\}$ a meno di isomorfismo: ci torniamo più avanti ma, ad esempio, se M è la struttura dei numeri naturali col $+$, ed N è la struttura dei numeri naturali col $+$ ma ogni numero naturale è stato dipinto di rosso, queste due strutture sono isomorfe. Se state pensando alle strutture come a database, immaginate di fare una copia di una struttura su un altro computer. La copia non è letteralmente la stessa struttura (una è su un computer, una è su un altro), ma “fanno le stesse cose”.

Per la seconda parte (il *passo induttivo*), assumiamo di sapere già che la (2.6) vale per x e facciamo vedere che vale per $x + 1$. Prendiamo il LHS, sostituiamo $x + 1$ al posto di n , e scorporiamo l'ultimo pezzo della somma:

$$\sum_{i=0}^{x+1} i = \left(\sum_{i=0}^x i \right) + x + 1$$

Per *ipotesi induttiva*, cioè per il fatto che sappiamo già che la (2.6) è vera con x al posto di n , abbiamo $\sum_{i=0}^x i = x(x+1)/2$. Quindi

$$\left(\sum_{i=0}^x i \right) + x + 1 = \frac{x(x+1)}{2} + x + 1$$

e facendo il conto

$$\frac{x(x+1)}{2} + x + 1 = \frac{x(x+1) + 2(x+1)}{2} = \frac{(x+2)(x+1)}{2} = \frac{(x+1)(x+2)}{2}$$

che è proprio quello che otteniamo se mettiamo $x + 1$ al posto di n nel RHS della (2.6).

Ricapitolando, abbiamo mostrato che $0 \in A$ e che, per ogni $x \in \mathbb{N}$, se $x \in A$ allora anche $x + 1 \in A$. Per *induzione*, cioè per (PA3), $A = \mathbb{N}$. Per definizione di A , questo vuol dire che la (2.6) vale per tutti gli $n \in \mathbb{N}$, e abbiamo finito. $\square$

Anche qui, dato che era la prima dimostrazione per induzione del corso sono stato abbastanza verboso per chiarezza. Qui la stessa dimostrazione scritta in uno stile simile a come le vedremo in futuro:

Dimostrazione. Il caso base è ovvio. Per il passo induttivo,

$$\sum_{i=0}^{n+1} i = \frac{n(n+1)}{2} + n + 1 = \frac{(n+1)(n+2)}{2} \quad \square$$

Aggiungete alla checklist delle cose da imparare in questo corso: imparare a ricostruire un argomento completo come nella prima dimostrazione leggendo solo una sintesi come nella seconda.

2.8 Esercizi

Tutti gli esercizi lasciati nelle sezioni precedenti, ad esempio scrivendo “(esercizio)” sono, ovviamente, esercizi. Eccone qualcun altro. Come nel capitolo precedente, questa *non* è una lista esaustiva di esercizi ed è raccomandato cercarne altri in altre dispense, libri, online, etc. (e risolverli). Idem nei capitoli seguenti, non ve lo sto a riscrivere ogni volta.

Esercizio 2.47. Quali di queste sono tautologie?

1. $((B \Rightarrow A) \Rightarrow A) \Rightarrow A$
2. $((A \Rightarrow B) \Rightarrow A) \Rightarrow A$
3. $((A \Rightarrow A) \Rightarrow B) \Rightarrow A$
4. $((A \Rightarrow A) \Rightarrow A) \Rightarrow B$

5. $B \Rightarrow (A \Rightarrow (A \Rightarrow A))$

7. $A \Rightarrow (A \Rightarrow (B \Rightarrow A))$

6. $A \Rightarrow (B \Rightarrow (A \Rightarrow A))$

8. $A \Rightarrow (A \Rightarrow (A \Rightarrow B))$

Esercizio 2.48. Scrivere la tavola di verità di $((A \Rightarrow B) \wedge C) \Rightarrow (B \vee \neg C)$.

Esercizio 2.49. Scrivete un po' di formule proposizionali nelle variabili A, B, C usando (un sottoinsieme di) $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$ e calcolatene le tavole di verità.

Esercizio 2.50. Dimostrare che $(A \wedge B) \vee C$ e $A \wedge (B \vee C)$ non sono equivalenti.

Il “dimostrare che” lo iniziamo ad omettere. Se il testo di un esercizio è un enunciato, diamo per scontato che l'esercizio sia dimostrarlo.

Esercizio 2.51. Scrivere la tavola di verità di $\oplus$.

Esercizio 2.52. $A \oplus B$ è equivalente a $\neg(A \Leftrightarrow B)$.

Nessuno ci vieta di inventarci un connettivo ternario e denotarlo come ci pare. Per esempio potremmo definire il connettivo ternario “(se A allora B , altrimenti C)” che ha come tavola di verità quella di $(A \Rightarrow B) \wedge (\neg A \Rightarrow C)$. Oppure, che ne so, il connettivo ternario $\spadesuit(A, B, C)$ dicendo che ha come tavola di verità quella in Figura 2.4. Simboli ne possiamo usare quanti ne vogliamo, ma ovviamente quello che davvero ci interessa dei connettivi è la loro *classe di equivalenza*; in altre parole, la loro tavola di verità. Più in generale, possiamo definire, per ogni $n \in \mathbb{N}$, dei connettivi n -ari, che prendono n argomenti.

Esercizio 2.53. Quanti connettivi binari esistono, a meno di equivalenza?

Esercizio 2.54. Quanti connettivi n -ari esistono a meno di equivalenza?

Esercizio 2.55. Trovare due forme normali negative della formula $\neg(A \vee (B \wedge C))$ che non possano essere trasformate l'una nell'altra usando solo le proprietà commutative di $\wedge$ e $\vee$.

Esercizio 2.56. Dimostrare che, per ogni $n \in \mathbb{N}$, ogni connettivo n -ario può essere espresso usando solo $\neg$ e $\wedge$.

Esercizio 2.57. Scrivere delle formule che usano i quantificatori $\exists, \forall$ e negarle.

Un'altra abbreviazione che si incontra ogni tanto è $\exists!$, pronunciato “esiste ed è unico”. Per definizione, $\exists!x \varphi(x)$ è equivalente a

$$(\exists x \varphi(x)) \wedge (\forall y (\varphi(y) \Rightarrow y = x))$$

Esercizio 2.58. Digerire la formula sopra e convincersi che è vera se e solo se l'insieme definito da $\varphi(x)$ ha esattamente un elemento.

Ovviamente invece di “esattamente 1” possiamo fare anche cose come “al più 2”:

Esercizio 2.59. Il quantificatore $\exists^{\leq 2}x$ è definito dicendo che $\exists^{\leq 2}x \varphi(x)$ è vera se e solo se ci sono al più 2 elementi che soddisfano $\varphi(x)$. Esprimere questo quantificatore usando solo (i connettivi, l'uguaglianza, e) i quantificatori $\exists$ e $\forall$.

Esercizio 2.60. Fare la stessa cosa per i quantificatori $\exists^{\geq 2}$ e $\exists^{=2}$ (rispettivamente, “esistono al più 2” ed “esistono esattamente 2”).

Esercizio 2.61. Per $n > 2$, fare la stessa cosa per i quantificatori $\exists^{\leq n}$, $\exists^{\geq n}$ e $\exists^n$. Se non volete usare i puntini, sappiate che come esiste il simbolo $\sum_{i=1}^n$ per il $+$, per $\wedge$ e $\vee$ esistono rispettivamente $\bigwedge_{i=1}^n$ e $\bigvee_{i=1}^n$.

Esercizio 2.62. Quali coppie di formule fra le seguenti sono equivalenti in $(\mathbb{N}, 0, 1, +, \cdot)$? Quali sono equivalenti in tutte le strutture per il vocabolario $\{0, 1, +, \cdot\}$?

- $\varphi_0(x, y) := x = y + y$
- $\varphi_1(x, y) := x = (1 + 1) \cdot y$
- $\varphi_2(x, y) := x = x \wedge y = y$
- $\varphi_3(x, y) := x + y = y + x$
- $\varphi_4(x, y) := \top$
- $\varphi_5(x, y) := \perp$
- $\varphi_6(x, y) := \forall z \in \emptyset (x + y = y + x)$
- $\varphi_7(x, y) := \exists z \in \emptyset (x + y = y + x)$

Esercizio 2.63. Se il seguente enunciato è vero, dimostrarlo; in caso contrario, esibire un controesempio. “Per ogni D e $\varphi(x)$ e in ogni struttura è vero l’enunciato $(\forall x \in D \varphi(x)) \Rightarrow (\exists x \in D \varphi(x))$ ”.

2.9 Digressione: altre logiche

Si può andare oltre il second’ordine. Ad esempio, nella logica del terz’ordine si può quantificare su insiemi di insiemi, in quella del quart’ordine su insiemi di insiemi di insiemi, eccetera.

Inoltre, tutte le logiche di cui abbiamo parlato sopra (proposizionale, prim’ordine, ...) le abbiamo viste in versione *logica classica*. A titolo informativo, sappiate che esistono logiche diverse da quella classica, in cui possono succedere cose buffe. Ad esempio, ci possono essere più di due valori di verità, $\neg(\neg A)$ può non essere equivalente ad A , o ci possono essere operatori come “è possibile che”, e altre cose del genere.

Il motivo per cui vi sto dicendo questa cosa è che potreste effettivamente imbattervi più avanti negli studi: alcune di queste logiche sono importanti in informatica teorica, e altre sono usate direttamente nelle applicazioni. Applicazioni molto concrete, come (letteralmente) far funzionare gli ascensori e assicurarsi che non uccidano i loro occupanti [Wike].

Bibliografia

- [Azz26a] Sara Azzali. *Esercizi di matematica discreta*. https://www.dm.uniba.it/it/members/azzali/homepage/ex_md_2025-26.pdf. 2026.
- [Azz26b] Sara Azzali. *Matematica discreta*. https://www.dm.uniba.it/it/members/azzali/homepage/md_syllabus2025.pdf. 2026.
- [BG05] Mariagrazia Bianchi e Anna Gillio. *Introduzione alla matematica discreta*. seconda ed. McGraw-Hill, 2005. ISBN: 88-386-6229-0.
- [Eso] Esolang. *Esoteric programming languages wiki*. <https://esolangs.org/>.
- [Iac25a] Donatella Iacono. *Appunti delle lezioni di matematica discreta*. https://www.donatellaiacono.it/note_inf.html. 2025.
- [Iac25b] Donatella Iacono. *Regole e Frequently Asked Questions*. <https://www.donatellaiacono.it/faq.html>. 2025.
- [Iac26] Donatella Iacono. *Raccolta prove passate*. https://www.donatellaiacono.it/nuova_raccolta_tracceMD.pdf. 2026.
- [PC08] Giulia M. Piacentini Cattaneo. *Matematica discreta e applicazioni*. Zanichelli, 2008. ISBN: 978-88-08-06813.2.
- [Ros19] Kenneth H. Rosen. *Discrete Mathematics and Its Applications*. 8th ed. McGraw-Hill education, 2019. ISBN: 978-1-259-67651-2.
- [SLW26] David Strömberg, Victor Lei e Yanhui Wu. «The Generative AI Learning Penalty: Evidence from Chinese Secondary Education». In: DP21577 (2026). DOI: [10.2139/ssrn.6868618](https://doi.org/10.2139/ssrn.6868618).
- [Wika] Wikipedia. *Cook-Levin theorem*. https://en.wikipedia.org/wiki/Cook%E2%80%93Levin_theorem#Consequences.
- [Wikb] Wikipedia. *First-order logic*. https://en.wikipedia.org/wiki/First-order_logic.
- [Wikc] Wikipedia. *Hilbert's program*. https://en.wikipedia.org/wiki/Hilbert's_program.
- [Wikd] Wikipedia. *Logic gate*. https://en.wikipedia.org/wiki/Logic_gate.
- [Wike] Wikipedia. *Model checking*. https://en.wikipedia.org/wiki/Model_checking.
- [Wikf] Wikipedia. *P versus NP problem*. https://en.wikipedia.org/wiki/P_versus_NP_problem.

- [Wikg] Wikipedia. *Russell's paradox*. https://en.wikipedia.org/wiki/Russell%27s_paradox.
- [Wikh] Wikipedia. *Zermelo–Fraenkel set theory*. https://en.wikipedia.org/wiki/Zermelo%E2%80%93Fraenkel_set_theory.