

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
3	Funzioni	42
3.1	Come funzionano le funzioni	42
3.2	Come fare le cose una dopo l'altra	47
3.3	Come fare le cose al contrario	48
3.4	Esercizi	53
4	Relazioni	57
4.1	Mettere le cose in relazione	57
4.2	Prima, dopo, nessuna delle due, o entrambe	60
4.3	Perdere informazione (e vivere felici)	62
4.4	Portarsi appresso una relazione	69
4.5	Esercizi	72
5	Costruire nuovi numeri	75
5.1	Voglio poter sottrarre quello che mi pare!	75
5.2	Voglio poter dividere per quello che mi pare!	79
5.3	Voglio dividere e tenermi il resto!	82
5.4	Voglio fare i conti sull'orologio!	85
5.5	Digressione: voglio costruire altri numeri!	86

INDICE	ii
6 Successioni e ricorsione	89
6.1 Numeri in fila	89
6.2 Saltare la fila	90
6.3 Esercizi	95
Suggerimenti	97
Bibliografia	99

Readme

Cos'è questo documento? Gli appunti di Matematica Discreta, corso 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 di revisione e con probabilità molto alta contengono errori, refusi, etc. Se ne trovate, vi incoraggio a segnalarmeli all'indirizzo email a pagina [iv](#). Una lista di chi ha segnalato degli errori è a pagina [v](#).

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? 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 programma preferito, e.g. `latexdiff` oppure `ediff` (una funzione di `emacs`).

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.

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. Link di invito si trova sulla pagina elearning.

Versione e codice Questa versione è stata compilata in data 27 ottobre 2026 alle 23:41. Il sorgente è disponibile facendo clic destro² sulla prima graffetta a sinistra, quello della bibliografia sulla seconda, e non vi spoilerò la terza.



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

Ringraziamenti Grazie a: Jack D'Aurizio per gli Esercizi 6.21 e 6.23, Antonio De Lucreziis per l'Esempio 4.11.5, Giorgio Mossa per l'Esempio 4.9.4.

Un grazie per aver trovato e segnalato errori in queste dispense a: Matteo Marilli.

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 $B \not\subseteq C$

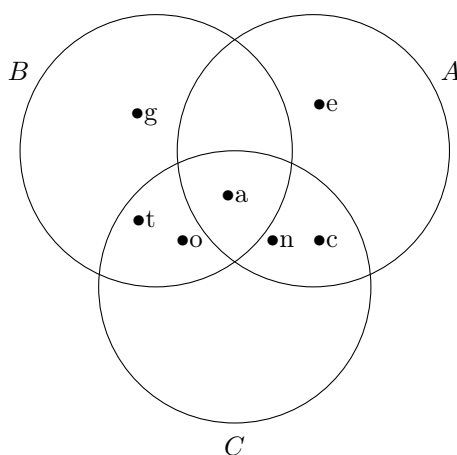


Figura 1.1: Diagramma di Venn degli insiemi A , B , C delle lettere che compaiono rispettivamente nelle parole “cane”, “gatto” e “canto”.

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.

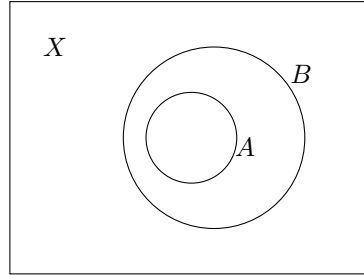


Figura 1.2: Un diagramma di Venn che rappresenta due sottoinsiemi A , B di un insieme X tali che $A \subseteq B$.

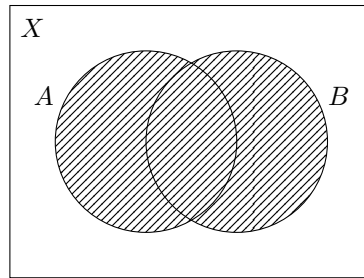


Figura 1.3: Due sottoinsiemi A , B di un insieme X , con la loro unione $A \cup B$ evidenziata a righe diagonali.

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.

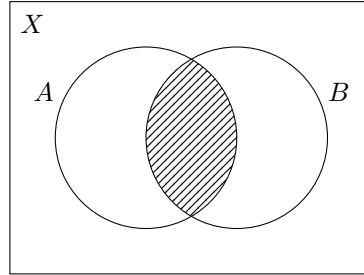


Figura 1.4: Due sottoinsiemi A, B di un insieme X , con la loro intersezione $A \cap B$ evidenziata a righe diagonali.

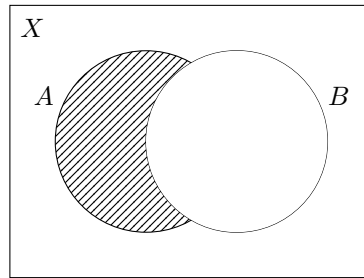


Figura 1.5: Due sottoinsiemi A, B di un insieme X , con la differenza $A \setminus B$ evidenziata a righe diagonali.

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. $A \setminus B = \{1, a, y\}$

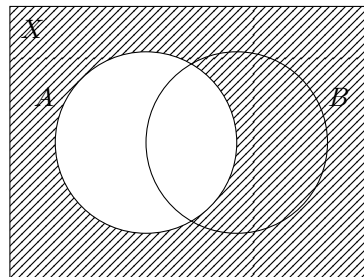


Figura 1.6: Due sottoinsiemi A, B di un insieme X , con il complementare A^c di A rispetto a X evidenziato a righe diagonali.

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. Vedi Suggerimento 1. I suggerimenti sono in un capitolo a parte per evitare spoiler per chi non li volesse. $\square$

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 [Wiki] 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 [Wikm].

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 [Wikd].

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 [Wike]. 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 [Wikh], vedi ad esempio [Wikb].

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 [Wikic].

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: vedi Suggerimento 2. $\square$

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:

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

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

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.

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 27 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 scucire 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. Vedi Suggerimento 3. □

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

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

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.

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

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) $\forall x \neg(s(x) = 0)$
- (PA2) $\forall x \forall y ((s(x) = s(y)) \Rightarrow x = y)$
- (PA3) $\forall A \left((0 \in A \wedge \forall x (x \in A \Rightarrow s(x) \in A)) \Rightarrow \forall x x \in A \right)$

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 ricavarne 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 $(\mathbb{N}, 0, s)$.

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.

³⁵Ci torniamo, qualche anticipazione in Nota 36.

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”.

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 0 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 0 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 $0 \in A$.

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. $((B \Rightarrow A) \Rightarrow A) \Rightarrow A$ | 5. $B \Rightarrow (A \Rightarrow (A \Rightarrow A))$ |
| 2. $((A \Rightarrow B) \Rightarrow A) \Rightarrow A$ | 6. $A \Rightarrow (B \Rightarrow (A \Rightarrow A))$ |
| 3. $((A \Rightarrow A) \Rightarrow B) \Rightarrow A$ | 7. $A \Rightarrow (A \Rightarrow (B \Rightarrow A))$ |
| 4. $((A \Rightarrow A) \Rightarrow A) \Rightarrow B$ | 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 [Wikg].

Capitolo 3

Funzioni

3.1 Come funzionano le funzioni

Intuitivamente, una funzione è una cosa che prende tutte le robe che vivono da una parte, e le manda in robe che vivono magari da un'altra parte. Ma facciamo le cose per bene.

Definizione 3.1. Una *funzione* f è una tripla ordinata $(\text{dom}(f), \text{codom}(f), \Gamma_f)$, dove

- $\text{dom}(f)$ è un insieme, chiamato il *dominio* di f ,
- $\text{codom}(f)$ è un insieme, chiamato il *codominio* di f , e
- Γ_f , chiamato il *grafico* di f , è un sottoinsieme di $\text{dom}(f) \times \text{codom}(f)$ tale che per ogni $x \in \text{dom}(f)$ esiste un unico $y \in \text{codom}(f)$ tale che $(x, y) \in \Gamma_f$.

Esempio 3.2. Siano $X := \{1, 2\}$ e $Y := \{3, 4\}$.

1. $(X, Y, \{(1, 3), (2, 3)\})$ è una funzione, rappresentata in Figura 3.1.
2. $(X, Y, \{(1, 3)\})$ non è una funzione.
3. $(X, Y, \{(1, 3), (2, 3), (1, 4)\})$ non è una funzione.
4. $(X, Y, \{(1, 3), (2, 5)\})$ non è una funzione.¹
5. $(X, Y, \{(3, 3), (2, 3)\})$ non è una funzione.²
6. Se X e Y sono insiemi non vuoti, per ogni $c \in Y$ c'è una funzione *costante* definita da $\forall x \in X \ f(x) = c$. Ad esempio, la funzione del punto 1 è costante.

Anche se una funzione è una tripla ordinata, la notazione usata di solito è diversa da quella vista sopra:

Notazione 3.3. 1. Scriviamo $f: X \rightarrow Y$ per dire che f è una funzione con dominio X e codominio Y .

¹Ma $(X, \{3, 5\}, \{(1, 3), (2, 5)\})$ lo è.

²Ma $(\{2, 3\}, Y, \{(3, 3), (2, 3)\})$ lo è.

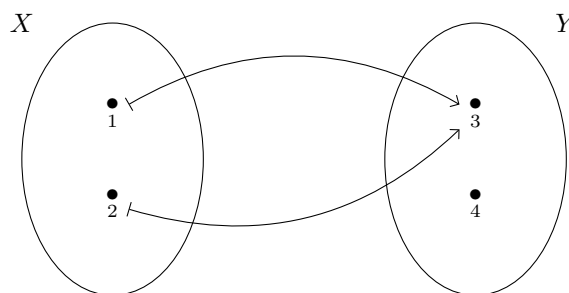


Figura 3.1: La funzione dell'Esempio 3.2.1.

2. Per dire che $(x, y) \in \Gamma_f$ scriviamo anche $y = f(x)$, o anche $f: x \mapsto y$. Notare la differenza fra $\rightarrow$ che va fra il dominio e il codominio e $\mapsto$ che va fra un elemento del dominio e l'elemento corrispondente nel codominio.
3. Se $f: X \rightarrow Y$ è una funzione e $x \in X$, l'elemento $f(x)$ si chiama *immagine* di x secondo f .
4. Invece di “funzione” si può dire anche *mappa* o anche *applicazione*.
5. Per dire che $f(x) = y$ si dice anche che “ f manda x in y ” o che “ f mappa x in y ”.

È comune specificare una funzione f dando una qualche espressione per $f(x)$ in termini di x . Per esempio:

Esempio 3.4. La funzione $f: \mathbb{N} \rightarrow \mathbb{N}$ che manda ogni numero naturale nel suo doppio aumentato di 1 può venire denotata con “ $f(n) = 2n + 1$ ”, o anche con “ $n \mapsto 2n + 1$ ”. Si intende che, per ogni n nel dominio, $(n, 2n + 1)$ appartiene al grafico.

Però, come un insieme può contenere quello che gli pare, una funzione può mandare gli elementi del dominio dove gli pare nel codominio: nella Definizione 3.1, non c'è scritto da nessuna parte che le coppie di Γ_f debbano sottostare a qualche “regola” come $n \mapsto 2n + 1$.

Esercizio 3.5. Per ogni $(X, Y) \in \{\emptyset, \{1\}, \{1, 2\}\}^2$, elencare le $f: X \rightarrow Y$.

Esercizio 3.6. Quali di queste scritture definiscono il grafico di una funzione $\mathbb{N} \rightarrow \mathbb{N}$?

- | | |
|-----------------------|-------------------------------|
| 1. $n \mapsto 3n + 2$ | 6. $f(n) = n/2$ |
| 2. $n \mapsto 3n - 2$ | 7. $0 \mapsto 3, 1 \mapsto 4$ |
| 3. $x \mapsto 3x + 2$ | 8. $n \mapsto 5$ |
| 4. $x \mapsto 3x - 2$ | 9. $n \mapsto n$ |
| 5. $f(x) = 5$ | 10. $n \mapsto x$ |

Per definizione di funzione, ogni elemento x del dominio di f viene “mandato” da f in un unico elemento. Però, lo stesso elemento del codominio può essere “raggiunto” da tanti elementi del dominio, o da nessuno.

Esempio 3.7. Sia $f: \mathbb{N} \rightarrow \mathbb{N}$ la funzione che manda x nel resto della divisione di x per 10. In altre parole, nella sua ultima cifra quando scritto in base 10. Di numeri x tali che $f(x) = 7$ ce ne sono infiniti, e di numeri x tali che $f(x) = 25$ non ce n'è nessuno.

Introduciamo della terminologia per “i numeri che vengono mandati da f in 7” e cose analoghe:

Definizione 3.8. Se $f: X \rightarrow Y$ è una funzione e $y \in Y$, la *controimmagine* di y secondo f è l'insieme $f^{-1}(y) := \{x \in X \mid f(x) = y\}$.

Altri nomi per la stessa cosa: *preimmagine* di y secondo f , *fibra* di f in y .

Esercizio 3.9. Siano X, Y come nell'Esempio 3.2, e sia f la funzione del suo punto 1. Per ogni $y \in Y$, calcolare $f^{-1}(y)$.

Definizione 3.10. Sia $f: X \rightarrow Y$.

1. Se $A \subseteq X$, l'*immagine* $f(A)$ di A secondo f è

$$f(A) := \{f(x) \mid x \in A\}$$

2. L'*immagine* di f è $\text{im}(f) := f(X)$.

3. Se $B \subseteq Y$, la *controimmagine* $f^{-1}(B)$ è

$$f^{-1}(B) := \{x \in X \mid f(x) \in B\}$$

Osservazione 3.11. Commenti:

1. Sopra, la scrittura $\{f(x) \mid x \in A\}$ è un'altra maniera per denotare un insieme, chiaramente più snella di scrivere $\{y \in Y \mid \exists x \in A \ y = f(x)\}$. Scritture del genere, con a sinistra di $\mid$ una qualche espressione in delle variabili e a destra la specifica di dove spaziano le variabili, verranno usate ripetutamente nel resto del testo.
2. “Ma abbiamo definito $f(\text{roba})$ due volte?”. Ottima domanda. Questo è un *abuso di notazione*: stiamo “sovraccaricando” una scrittura, che può voler dire cose diverse a seconda del contesto. Senza sapere chi è “roba”, la scrittura $f(\text{roba})$ può effettivamente voler dire due cose:
 - (a) se “roba” è un elemento del dominio di f , allora $f(\text{roba})$ è l'unico robo tale che $(\text{roba}, \text{robo}) \in \Gamma_f$;
 - (b) se “roba” è un sottoinsieme del dominio di f , allora $f(\text{roba})$ è $\{f(x) \mid x \in \text{roba}\}$.
3. Discorsi analoghi si applicano a f^{-1} .
4. “Ma quindi come faccio a capire chi è $f(G)$?”. Di nuovo, dipende da chi è G . Per indicare in maniera non ambigua l'immagine di un sottoinsieme (quindi, come in Definizione 3.10.1), ci sarebbe la scrittura $f''G$, ma è poco usata.³

³Non conosco analoghi per disambiguare la scrittura f^{-1} , ma di solito questa viene intesa nel secondo senso introdotto.

Esempio 3.12. Per ogni $f: X \rightarrow Y$ sono vere le seguenti.

1. $f^{-1}(Y) = X$, per definizione di funzione.
2. $f^{-1}(\emptyset) = \emptyset$.
3. Per ogni $y \in Y$ abbiamo $f^{-1}(y) = \emptyset \iff y \notin \text{im}(f)$.

Esempio 3.13. Se f è la funzione dell'Esempio 3.2.1, le immagini dei sottoinsiemi di X sono:

1. $f(\emptyset) = \emptyset$
2. $f(\{1\}) = \{3\}$
3. $f(\{2\}) = \{3\}$
4. $f(X) = \{3\}$

mentre le controimmagini dei sottoinsiemi di Y sono:

1. $f^{-1}(\emptyset) = \emptyset$
2. $f^{-1}(\{3\}) = X$
3. $f^{-1}(\{4\}) = \emptyset$
4. $f^{-1}(Y) = X$

Esercizio 3.14. Sia $f: \mathbb{N} \rightarrow \mathbb{N}$ data da $f(n) = 3n + 5$ e sia $A := \{n \in \mathbb{N} \mid 16 \leq x \leq 25\}$. Calcolare $f(A)$ e $f^{-1}(A)$.

Come il simbolo $\sum_{i=n}^m f(i)$ somma tante cose, c'è un simbolo che interseca tante cose, $\bigcap_{i=n}^m A_i$. Per definizione, $x \in \bigcap_{i=n}^m A_i$ sse per ogni i tale che $n \leq i \leq m$ si ha che $x \in A_i$. Se i lo facciamo “scorrere” su un insieme C , possiamo scrivere anche $\bigcap_{i \in C} A_i$, e la scrittura ha senso anche se C è infinito: per definizione, $x \in \bigcap_{i \in C} A_i$ sse, per ogni $i \in C$, abbiamo $x \in A_i$.

Analogamente, c'è un simbolo per l'unione di tante cose (anche infinite), che vi lascio definire per esercizio e che usiamo subito in un altro esercizio:

Esercizio 3.15. Per ogni $f: X \rightarrow Y$ e ogni $B \subseteq Y$ abbiamo

$$f^{-1}(B) = \bigcup_{y \in B} f^{-1}(y)$$

Osservazione 3.16. Commenti:

1. L'immagine di una funzione *non* è necessariamente il suo codominio. Ad esempio, il codominio della funzione nell'Esempio 3.4 è $\mathbb{N}$, mentre l'immagine è l'insieme dei numeri dispari. Ma, ovviamente, l'immagine è sempre un sottoinsieme del codominio. Le funzioni per cui immagine e codominio coincidono hanno un nome (ci torniamo a breve).

2. Checché vi abbiano detto alle superiori, no, il dominio di una funzione non si “calcola”. Il dominio di una funzione è qualcosa che si specifica quando si specifica la funzione stessa. In altre parole, quando si specifica chi è una funzione, bisogna dare il suo dominio e il suo codominio, dare (una regola per ricostruirsi) il grafico e basta *non* è sufficiente.⁴ Quando vi dicevano di “calcolare il dominio di $1/x$ ” avrebbero dovuto dire qualcosa tipo “trova il sottoinsieme più grande di $\mathbb{R}$ dove la scrittura $1/x$ è sensata”, o qualcosa di simile.

Il codominio di una funzione *non* si può ricostruire dal grafico.

Esempio 3.17. Se $f: \mathbb{N} \rightarrow \mathbb{N}$ mappa $n \mapsto n + 1$, e $g: \mathbb{N} \rightarrow \mathbb{N} \setminus \{0\}$ mappa $n \mapsto n + 1$, allora f e g sono due funzioni diverse con lo stesso grafico.

Se non è chiaro perché queste sono funzioni diverse:

Osservazione 3.18. Dato che le funzioni sono triple ordinate, $f = g$ se e solo se $\text{dom}(f) = \text{dom}(g) \wedge \text{codom}(f) = \text{codom}(g) \wedge \Gamma_f = \Gamma_g$. In altre parole, due funzioni sono uguali quando hanno lo stesso dominio, lo stesso codominio, e mandano ogni input nello stesso output.

Osservazione 3.19. Se grafico è lo stesso, non importa se è stato descritto in maniera diversa. Ad esempio, se f e g sono le funzioni $\mathbb{N} \rightarrow \mathbb{N}$ definite da

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

allora $f = g$ per l'Proposizione 2.46. Il fatto che la prima scrittura suggerisca un algoritmo molto più inefficiente che la scrittura a destra è irrilevante per dire se le due funzioni sono uguali o meno.⁵

Il dominio di una funzione invece *si può* ricostruire dal grafico. Per farlo, introduciamo delle funzioni particolarmente importanti.

Definizione 3.20. Sia $A_1 \times \dots \times A_n$ un prodotto cartesiano. Per $1 \leq i \leq n$, definiamo la *proiezione sull' i -esima coordinata* come la funzione $\pi_i: A_1 \times \dots \times A_n \rightarrow A_i$ che mappa

$$f(a_1, \dots, a_n) = a_i$$

Esercizio 3.21. Per ogni funzione f abbiamo che

1. $\text{dom}(f) = \pi_1(\Gamma_f)$, e che
2. $\text{im}(f) = \pi_2(\Gamma_2)$.

Il seguente esercizio dovrebbe puzzarvi di già visto.

Esercizio 3.22. Siano X un insieme e $A \subseteq X^2$. Dimostrare che $\{x \in X \mid \exists y (x, y) \in A\} = \pi_1(A)$ e che $\{y \in X \mid \exists x (x, y) \in A\} = \pi_2(A)$.

⁴Ma come al solito, può essere che dominio e codominio siano chiari dal contesto. Che ne so, magari uno scrive “consideriamo queste funzioni $\mathbb{N} \rightarrow \mathbb{N} [\dots] f_8(n) := n + 5 [\dots]$ ”.

⁵La situazione è diversa per funzioni scritte in un qualche linguaggio di programmazione, che possono prendere e ritornare argomenti dello stesso tipo e avere lo stesso output su ogni input ma essere comunque diverse, ad esempio una può essere significativamente più veloce dell'altra. Insomma, quando si parla di “funzioni” in informatica tipicamente si considera un concetto diverso che in matematica.

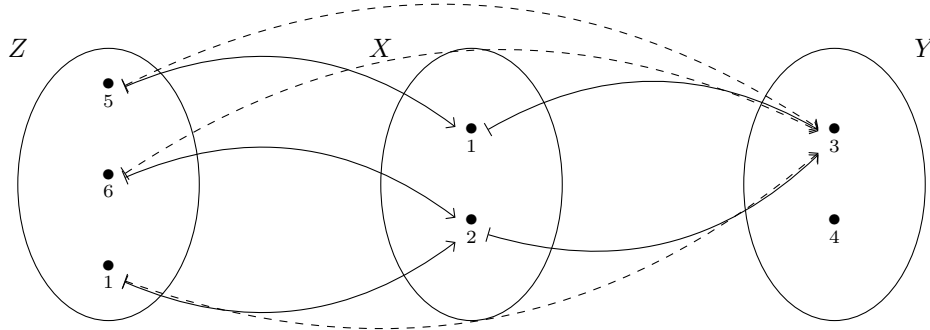


Figura 3.2: La composizione nell'Esempio 3.24.1. Freccie della composizione tratteggiate.

3.2 Come fare le cose una dopo l'altra

A volte, due funzioni si possono *comporre*, il che vuol dire fare prima una e poi l'altra. Perché questo abbia senso, bisogna che la prima ad essere applicata “arrivi” dove la seconda “parte”:

Definizione 3.23. Siano $f: X \rightarrow Y$ e $g: Y \rightarrow Z$. La *composizione* $g \circ f$ è la funzione $X \rightarrow Z$ definita da $(g \circ f)(x) := g(f(x))$.

In altre parole, per calcolare $(g \circ f)(x)$ si calcola prima $f(x)$, e poi vi si applica g (sì, anche se sembra “al contrario” rispetto alla scrittura $g \circ f$)⁶.

Esempio 3.24. 1. Se $f: X \rightarrow Y$ è la funzione dell' Esempio 3.2.1 e g è la funzione con dominio $Z := \{1, 5, 6\}$ e codominio X , la composizione $g \circ f: Z \rightarrow Y$ è la costante 3, raffigurata in Figura 3.2.

2. Se f, g sono come sopra, la composizione $f \circ g$ non è definita (non ha senso), perché $\text{dom}(f) \neq \text{codom}(g)$.
3. Se $s: \mathbb{N} \rightarrow \mathbb{N}$ è la funzione successore $n \mapsto n + 1$ e $d: \mathbb{N} \rightarrow \mathbb{N}$ è la funzione “doppio” $n \mapsto 2n$, allora $d \circ s$ e $s \circ d$ sono entrambe definite, e uguali rispettivamente a $n \mapsto 2n + 2$ e $n \mapsto 2n + 1$. In particolare, anche per funzioni da un insieme fissato in sé stesso (in questo caso, $\mathbb{N}$), la composizione non è in generale commutativa.
4. Se $\text{dom}(f) = \text{codom}(f)$, allora possiamo comporre f con sé stessa quante volte ci pare, e la composizione di f con sé stessa n volte si denota con f^n .⁷ Ad esempio, $s^4(n) = n + 4$ e $d^5(n) = 32n$.

Magari vi state chiedendo: ma f^n vuol dire $f \circ (f \circ (\dots \circ f) \dots)$ oppure $(\dots (\dots \circ f) \circ f) \circ f$? La risposta è “non importa”:

⁶Il motivo per cui si usa quest'ultima è che torna bene con la scrittura $g(f(x))$. Non tutta la letteratura è d'accordo, e in alcuni libri (pochi) quella che noi chiamiamo $g \circ f$ viene chiamata $f \circ g$.

⁷Qui ci può essere un abuso di notazione: ad esempio, probabilmente avete visto scrivere $\sin^2(x)$ per intendere $(\sin(x))^2$, e non $\sin(\sin(x))$. Come al solito per gli abusi di notazione, il significato giusto va capito dal contesto.

Proposizione 3.25. La composizione di funzioni è *associativa*: per ogni $f: X \rightarrow Y$, $g: Y \rightarrow Z$, e $h: Z \rightarrow W$, abbiamo

$$(h \circ g) \circ f = h \circ (g \circ f)$$

Dimostrazione. Siano $\ell := (h \circ g) \circ f$ e $r := h \circ (g \circ f)$. Segue facilmente dalle definizioni che entrambe sono funzioni $X \rightarrow W$. Inoltre, i loro grafici sono uguali perché, per ogni $x \in X$, abbiamo

$$\begin{aligned} \ell(x) &= ((h \circ g) \circ f)(x) = (h \circ g)(f(x)) \\ &= h(g(f(x))) = h((g \circ f)(x)) = (h \circ (g \circ f))(x) = r(x) \quad \square \end{aligned}$$

Possiamo quindi scrivere cose come $h \circ g \circ f$ senza ambiguità.

L'altra proprietà fondamentale della composizione è che, per ogni insieme X , c'è una funzione speciale $X \rightarrow X$ che “non fa niente”, e che si può comporre (quando ha senso farlo) senza cambiare la funzione con cui la si sta componendo.

Definizione 3.26. La funzione *identità* $X \rightarrow X$ è definita da $\text{id}_X(x) = x$.

In altre parole, il grafico di id_X è la *diagonale* $\{(x, x) \mid x \in X\}$. Come accennavamo, le funzioni identità “non fanno niente” nemmeno se le componiamo:

Proposizione 3.27. Per ogni $f: X \rightarrow Y$ abbiamo che

1. $\text{id}_Y \circ f = f$, e che
2. $f \circ \text{id}_X = f$.

Dimostrazione. Esercizio. □

3.3 Come fare le cose al contrario

Nella definizione di funzione accoppiamo ad ogni elemento del dominio esattamente un elemento del codominio. La situazione è tutt'altro che simmetrica: un elemento del codominio può non essere stato accoppiato a niente, o può essere stato accoppiato a più elementi del dominio.

Data una funzione f , è possibile quindi chiedersi se sia possibile “tornare indietro” rispetto a f . In altre parole, so che un elemento di $\text{codom}(f)$ è della forma $f(x)$ per un qualche x , è possibile risalire a un unico tale x ? Se vogliamo farlo per tutti gli elementi del codominio, essenzialmente stiamo cercando un'*inversa sinistra* di f .

Abbiamo anche la domanda duale, cioè se esiste un'*inversa destra*: dato $y \in \text{codom}(f)$, è possibile trovare un elemento $x \in \text{dom}(f)$ tale che $y = f(x)$? È possibile farlo per tutti gli elementi del codominio? Ci stiamo chiedendo se c'è un “andare avanti” rispetto al quale f “torni indietro”.

Definizione 3.28. Siano $f: X \rightarrow Y$ e $g: Y \rightarrow X$.

1. g è un'*inversa sinistra* di f sse $g \circ f = \text{id}_X$
2. g è un'*inversa destra* di f sse $f \circ g = \text{id}_Y$
3. g è un'*inversa* di f sse è sia una sua inversa destra che una sua inversa sinistra.

Proposizione 3.29. Ogni funzione ha al più un'inversa.

Dimostrazione. Sia $f: X \rightarrow Y$ una funzione, e siano $g_1, g_2: Y \rightarrow X$ due inverse di f . Allora

$$g_1 = g_1 \circ \text{id}_Y = g_1 \circ f \circ g_2 = \text{id}_X \circ g_2 = g_2 \quad \square$$

Esercizio 3.30. Sia f una funzione che ha sia un'inversa sinistra g_1 che un'inversa destra g_2 . Allora $g_1 = g_2$, e in particolare f ha una sola inversa sinistra e una sola inversa destra.

Suggerimento. Vedi Suggerimento 4. $\square$

Notazione 3.31. Se f ha un'inversa, la si denota f^{-1} .

“Ma come, per $f: X \rightarrow Y$, non avevamo detto che $f^{-1}: Y \rightarrow \mathcal{P}(X)$ manda un punto nella sua fibra? È forse un altro abuso di notazione?”. Vi vedo sul pezzo, complimenti.

Osservazione 3.32. Se f ha un'inversa sinistra g , allora f è un'inversa destra di g . Una funzione $f: X \rightarrow Y$ ha un'inversa sinistra se e solo se è l'inversa destra di qualche funzione: in entrambi i casi stiamo dicendo che esiste $g: Y \rightarrow X$ tale che $g \circ f = \text{id}_X$. Analogamente, una funzione ha un'inversa destra se e solo se è un'inversa sinistra.

Vediamo subito che, in generale, possono non esserci inverse destre, se ci sono possono non essere uniche, e le stesse cose valgono per le inverse sinistre.

Esercizio 3.33. Sia $f: \mathbb{N} \rightarrow \mathbb{N}$ una funzione costante. Allora f non ha né inverse destre né inverse sinistre.

Esercizio 3.34. La funzione successore $s: \mathbb{N} \rightarrow \mathbb{N}$ definita da $s(n) := n + 1$ ha più di un'inversa sinistra, e non ha inverse destre.

Definizione 3.35. La funzione *parte intera inferiore* (o *floor*) $\mathbb{R} \rightarrow \mathbb{Z}$ manda un numero reale x nell'intero $y \in \mathbb{Z}$ più grande tale che $y \leq x$, denotato con $\lfloor x \rfloor$.⁸

Esercizio 3.36. La funzione $f: \mathbb{N} \rightarrow \mathbb{N}$ definita da $f(n) := \lfloor n/2 \rfloor$ ha più di un'inversa destra, e non ha inverse sinistre.

Definizione 3.37. Una funzione $f: X \rightarrow Y$ è *iniettiva* (o *ingettiva*) sse $\forall x_0, x_1 \in X$ $f(x_0) = f(x_1) \Rightarrow x_0 = x_1$.

Quindi, f è iniettiva se e solo se ogni suo output proviene da un solo input. Possiamo vederla da un altro punto di vista girando l'implicazione: è equivalente dire che $\forall x_0, x_1 \in X$ $x_0 \neq x_1 \Rightarrow f(x_0) \neq f(x_1)$, cioè che f manda input diversi in output diversi. In un certo senso, f non perde informazione: è possibile risalire a x partendo da $f(x)$.

Esempio 3.38. 1. Se X ha almeno due elementi, nessuna funzione costante con dominio X è iniettiva.

2. La funzione successore $\mathbb{N} \rightarrow \mathbb{N}$ è iniettiva.

⁸C'è anche una funzione *parte intera superiore* o (*ceiling*) $\lceil x \rceil$, l'intero y più piccolo tale che $y \geq x$.

3. La funzione $\mathbb{N} \rightarrow \mathbb{N}$ definita da $x \mapsto 2x$ è iniettiva.
4. La funzione $\mathbb{N} \rightarrow \mathbb{N}$ che scambia ogni numero pari col successivo dispari, cioè quella che, per ogni $k \in \mathbb{N}$, manda $2k \mapsto 2k+1$ e $2k+1 \mapsto 2k$, è iniettiva.
5. La funzione $\mathbb{N} \rightarrow \mathbb{N}$ definita da $x \mapsto |x-10|$ non è iniettiva.

Osservazione 3.39. Una funzione è iniettiva se e solo se ogni sua fibra ha al più un elemento.

Proposizione 3.40. Siano $X \neq \emptyset$ e $f: X \rightarrow Y$. Allora f ha un'inversa sinistra se e solo se f è iniettiva. Inoltre, se $X = \emptyset$ e f ha un'inversa sinistra, allora f è iniettiva.

Dimostrazione. Supponiamo che f abbia un'inversa sinistra, chiamiamola g , e siano $x_0, x_1 \in X$ tali che $f(x_0) = f(x_1)$. Dobbiamo mostrare che $x_0 = x_1$. Applicando g a entrambi i membri dell'uguaglianza $f(x_0) = f(x_1)$ otteniamo $g(f(x_0)) = g(f(x_1))$. Dato che $g \circ f = \text{id}_X$, abbiamo $x_0 = g(f(x_0)) = g(f(x_1)) = x_1$, come desiderato. Dato che non abbiamo mai usato l'ipotesi $X \neq \emptyset$, la parte "inoltre" della proposizione è dimostrata.

Viceversa, sia f iniettiva. L'idea per costruire un'inversa sinistra g (che deve necessariamente avere dominio Y e codominio X) è di rimandare ogni elemento di $\text{im}(f)$ in quello da cui proviene, e mandare quelli non raggiunti da f in un elemento di X qualunque. Dato che $X \neq \emptyset$, ha un qualche elemento; fissiamone uno e chiamiamolo a . Dato un elemento $y \in Y$, abbiamo due casi:

1. $y \in \text{im}(f)$. In altre parole, esiste $x \in X$ tale che $y = f(x)$. Dato che f è iniettiva, questo x è unico. Per questi y , definiamo allora $g(y)$ proprio come questo x .
2. $y \notin \text{im}(f)$. In questo caso, definiamo $g(y) = a$.

In altre parole, stiamo dando la seguente *definizione per casi*:

$$g(y) := \begin{cases} \text{l'unico elemento di } f^{-1}(y) & \text{se } f^{-1}(y) \neq \emptyset \\ a & \text{altrimenti} \end{cases}$$

Per verificare che g è un'inversa sinistra di f osserviamo che, *per costruzione*, per ogni $x \in X$ abbiamo $g(f(x)) = x = \text{id}_X(x)$. Ma questo vuol dire esattamente che $g \circ f = \text{id}_X$, dato che mostra l'uguaglianza dei loro grafici, mentre dominio e codominio sono entrambi X per entrambe le funzioni. $\square$

Corollario 3.41. La composizione di due funzioni iniettive è iniettiva.

Dimostrazione. È un buon esercizio dimostrare questa cosa direttamente dalle definizioni, ma vediamo un altro argomento.

Siano $f: X \rightarrow Y$ e $g: Y \rightarrow Z$. Se $X \neq \emptyset$ e $Y \neq \emptyset$, allora per la Proposizione 3.40 f e g hanno delle inverse sinistre, diciamo f_ℓ e g_ℓ rispettivamente. Allora abbiamo che

$$f_\ell \circ g_\ell \circ g \circ f = f_\ell \circ \text{id}_Y \circ f = f_\ell \circ f = \text{id}_X$$

e quindi $f_\ell \circ g_\ell$ è un'inversa sinistra di $g \circ f$, e concludiamo per la Proposizione 3.40.

Per il caso in cui uno fra X e Y è vuoto, osserviamo che, per ogni insieme A , esiste esattamente una funzione $\emptyset \rightarrow A$, che è iniettiva (esercizio), ed esiste una funzione $A \rightarrow \emptyset$ se e solo se $A = \emptyset$. Se X è vuoto, allora $g \circ f$ è l'unica funzione $\emptyset \rightarrow Z$, che abbiamo detto essere iniettiva. Se Y è vuoto, allora anche X è vuoto per quanto detto poco fa, e quindi siamo nel caso precedente. $\square$

Esercizio 3.42. Cosa succede alla Proposizione 3.40 nel caso in cui X sia vuoto? Dipende da Y ?

“Ma invece per avere un’inversa destra?” Grazie per averlo chiesto.

Definizione 3.43. Una funzione $f: X \rightarrow Y$ è *suriettiva* (o *surgettiva*) sse $\forall y \in Y \exists x \in X f(x) = y$.

Esempio 3.44. 1. Se Y ha almeno due elementi, nessuna funzione costante con codominio Y è surgettiva.

2. La funzione successore $\mathbb{N} \rightarrow \mathbb{N}$ non è surgettiva.

3. La funzione $\mathbb{N} \rightarrow \mathbb{N}$ definita da $x \mapsto 2x$ non è surgettiva.

4. La funzione $\mathbb{N} \rightarrow \mathbb{N}$ che scambia ogni numero pari col successivo dispari è surgettiva.

5. La funzione $\mathbb{N} \rightarrow \mathbb{N}$ definita da $|x - 10|$ è surgettiva.

Esercizio 3.45. Dare un esempio di funzione non iniettiva, non surgettiva, e non costante.

Esercizio 3.46. Le seguenti sono equivalenti per una funzione $f: X \rightarrow Y$ con $Y \neq \emptyset$.

1. f è surgettiva.

2. $\text{im}(f) = \text{codom}(f)$.

3. Ogni fibra di f è non vuota (in altre parole, ha almeno un elemento).

Osservazione 3.47. In particolare, ogni funzione si può “far diventare” surgettiva restringendone il codominio: per ogni $f: X \rightarrow Y$, la funzione $g: X \rightarrow \text{im}(f)$ con $\Gamma_g := \Gamma_f$ è surgettiva.

Proposizione 3.48. Una funzione ha un’inversa destra se e solo se è surgettiva.

Dimostrazione. Sia $f: X \rightarrow Y$ una funzione con inversa destra g . Dato un qualunque $y \in Y$, abbiamo

$$y = \text{id}_Y(y) = f \circ g(y) = f(g(y))$$

e quindi $g(y) \in f^{-1}(y)$.

Viceversa, supponiamo che f sia surgettiva. Dato che, per ogni $y \in Y$, la fibra $f^{-1}(y)$ è non vuota, possiamo definire $g(y)$ ponendola uguale a un elemento qualunque scelto da $f^{-1}(y)$. Ora $f \circ g$ ha dominio e codominio Y e, per costruzione, qualunque sia $y \in Y$ abbiamo $f \circ g(y) = f(g(y)) = y = \text{id}_Y(y)$. $\square$

Corollario 3.49. La composizione di funzioni surgettive è surgettiva.

Dimostrazione. Esercizio. □

Corollario 3.50. Per ogni X, Y insiemi non vuoti, esiste una funzione iniettiva $X \rightarrow Y$ se e solo se ne esiste una surgettiva $Y \rightarrow X$.

Dimostrazione. Per le Proposizioni 3.40 e 3.48 e l'Osservazione 3.32. (Esercizio: scrivere l'argomento per intero) □

La prossima domanda naturale è quella di *caratterizzare* le funzioni che hanno un'inversa. Un'inversa è, per definizione, sia un'inversa destra che un'inversa sinistra, e quindi tali funzioni devono essere necessariamente sia iniettive che surgettive per le Proposizioni 3.40 e 3.48. Diamo un nome a queste funzioni.

Definizione 3.51. Una funzione è *biiettiva* (o *bigettiva*, o *una bigezione*, o *biunivoca*) sse è sia iniettiva che surgettiva.

Abbiamo detto sopra che la bigettività è una condizione *necessaria* per ammettere un'inversa. Ora, a priori, potrebbe succedere che qualche funzione bigettiva f ammetta un'inversa sinistra g e un'inversa destra h , ma che per ogni tali g, h si abbia $g \neq h$. In realtà questo non succede mai⁹, e stiamo per dimostrare che la bigettività è condizione *necessaria e sufficiente* per ammettere un'inversa. In sostanza, questo è dovuto all'associatività della composizione.

Corollario 3.52. Una funzione ha un'inversa se e solo se è bigettiva.

Dimostrazione. Sia f una funzione con inversa g . Dato che g è un'inversa sinistra, f è iniettiva per la Proposizione 3.40; e dato che g è un'inversa destra, f è surgettiva per la Proposizione 3.48.

Viceversa, se $f: X \rightarrow Y$ è bigettiva allora ha un'inversa sinistra g_1 e un'inversa destra g_2 . Per l'Esercizio 3.30 $g_1 = g_2$, e quindi questa funzione è l'inversa di f . □

Osservazione 3.53. 1. Una funzione $f: X \rightarrow Y$ è bigettiva se e solo se, per ogni $y \in Y$, esiste un unico $x \in X$ tale che $f(x) = y$. L'inversa di f non ha altra scelta che mandare y nell'unico x da cui proviene.

2. Notiamo la simmetria col fatto che, per definizione, un sottoinsieme $\Gamma \subseteq X \times Y$ è il grafico di una funzione se e solo se, per ogni $x \in X$ esiste un unico $y \in Y$ tale che $(x, y) \in \Gamma$.

Esercizio 3.54. Se f è bigettiva allora anche f^{-1} è bigettiva.

Esempio 3.55. L'inversa della funzione successore $s: \mathbb{N} \rightarrow \mathbb{N} \setminus \{0\}$ è la funzione che manda $n \mapsto n - 1$. Dominio e codominio non ve li dico perché, per essere l'inversa di s , la scelta è forzata.

Esempio 3.56. Sia $f: \mathbb{N} \rightarrow \mathbb{N}$ la funzione che scambia ogni pari col successivo dispari. Allora $f^{-1} = f$, o in altre parole $f \circ f = \text{id}_{\mathbb{N}}$.

Esempio 3.57. Sia $f: \mathbb{N} \rightarrow \mathbb{N}$ la funzione che mappa

$$3k \mapsto 3k + 1 \quad 3k + 1 \mapsto 3k + 2 \quad 3k + 2 \mapsto 3k$$

Allora $f^3 = \text{id}_{\mathbb{N}}$, o in altre parole $f^{-1} = f^2$.

⁹E anzi, vedi Esercizio 3.30.

Proposizione 3.58. Se f e g sono funzioni bigettive, allora $g \circ f$ è bigettiva e la sua inversa è $f^{-1} \circ g^{-1}$.

Ovviamente, nell'enunciato sopra si sottointende che $g \circ f$ abbia senso, cioè che $\text{dom } g = \text{codom}(f)$.

Dimostrazione. La prima parte dell'enunciato segue dai Corollari 3.41 e 3.49. Per la seconda parte basta calcolare

$$\begin{aligned} f^{-1} \circ g^{-1} \circ g \circ f &= f^{-1} \circ \text{id}_{\text{dom } g} \circ f \\ &= \text{id}_{\text{dom } f} = g \circ \text{id}_{\text{dom } f} \circ g^{-1} = g \circ f \circ f^{-1} \circ g^{-1} \quad \square \end{aligned}$$

Il fatto che l'inversa di $g \circ f$ sia $f^{-1} \circ g^{-1}$, invece di $g^{-1} \circ f^{-1}$, è meno strano di quanto possa sembrare: se ci si mette prima i calzini e poi le scarpe, per togliersi tutto bisogna togliersi prima le scarpe e poi i calzini. Inoltre, $g^{-1} \circ f^{-1}$ può non avere nemmeno senso, perché non sta scritto da nessuna parte che $\text{codom}(f^{-1}) = \text{dom}(f)$ sia uguale a $\text{dom}(g^{-1}) = \text{codom}(g)$.

Esempio 3.59. Sia $\mathbb{Q}$ l'insieme dei numeri razionali (che dovrete già conoscere, ma ci torniamo). Se f e g sono le funzioni $\mathbb{Q} \rightarrow \mathbb{Q}$ definite da $f(x) = x + 1$ e $g(x) = 2x$, allora $(g \circ f)(x) = 2(x + 1)$ e $(g \circ f)^{-1}(x) = (f^{-1} \circ g^{-1})(x) = (x/2) - 1$.

Esercizio 3.60. Nell'Esempio 3.59, verificare che quella indicata come $(g \circ f)^{-1}$ è effettivamente l'inversa (sinistra e destra!) di $g \circ f$. Calcolare $g^{-1} \circ f^{-1}$ e verificare che (nonostante la composizione abbia senso perché qui sono tutte funzioni $\mathbb{Q} \rightarrow \mathbb{Q}$) $g^{-1} \circ f^{-1}$ non è l'inversa di $g \circ f$.

3.4 Esercizi

Esercizio 3.61. Quali di questi sono grafici di funzioni, per un'opportuna scelta di dominio e codominio? In altre parole, per quali di questi insiemi Γ esistono X e Y tali che (X, Y, Γ) è una funzione?

1. $\{(x, y) \in \mathbb{N}^2 \mid x = 5\}$
2. $\{(x, y) \in \mathbb{N}^2 \mid y = 5\}$
3. $\{(x, y) \in \mathbb{N}^2 \mid x = 2y\}$
4. $\{(x, y) \in \mathbb{N}^2 \mid y = 2x\}$
5. $\{y \in \mathbb{N} \mid \exists x \, x = 2y\}$
6. $\{x \in \mathbb{N} \mid \exists y \, y = 2x\}$
7. $\emptyset$
8. $\{1\}$
9. $\{(1, 2)\}$
10. $\{\{(1, 2)\}\}$
11. $\{(x, y) \in \mathbb{N} \mid x = x\}$

12. $\{(x, y) \in \mathbb{N} \mid y = y\}$
13. $\{(x, y) \in \mathbb{N} \mid x = y\}$
14. $\{(x, y) \in \mathbb{N} \mid x \neq y\}$
15. $\{(x, y) \in \mathbb{N} \mid \top\}$
16. $\{(x, y) \in \mathbb{N} \mid \perp\}$
17. $\{(x, y) \in \mathbb{N}^2 \mid \exists k \in \mathbb{N} (x = 2k \wedge y = 2k + 1) \vee (x = 2k + 1 \wedge y = 2k)\}$
18. $\{(x, y) \in \mathbb{N}^2 \mid \exists k \in \mathbb{N} (x = 2k \wedge y = 2k + 1) \wedge (x = 2k + 1 \wedge y = 2k)\}$
19. $\{(x, y) \in \mathbb{N}^2 \mid \exists k \in \mathbb{N} (x = 2k \wedge y = 2k + 1) \Rightarrow (x = 2k + 1 \wedge y = 2k)\}$
20. $\{(x, y) \in \mathbb{N}^2 \mid \exists k \in \mathbb{N} (x = 2k \wedge y = 2k + 1)\}$
21. $\{(x, y) \in \mathbb{N}^2 \mid \exists k \in \mathbb{N} (x = 2k + 1 \wedge y = 2k)\}$
22. $\{(x, y) \in \mathbb{N}^2 \mid \exists k \in \mathbb{N} (x = 2k \vee y = 2k + 1)\}$
23. $\{(x, y) \in \mathbb{N}^2 \mid \exists k \in \mathbb{N} (x = 2k + 1 \vee y = 2k)\}$

Esercizio 3.62. Siano X un insieme, I un altro insieme, e per ogni $i \in I$, sia dato un sottoinsieme $A_i \subseteq X$.

1. Chi è $\{x \in X \mid x \in \bigcup_{i \in \emptyset} A_i\}$?
2. Chi è $\{x \in X \mid x \in \bigcap_{i \in \emptyset} A_i\}$?

Esercizio 3.63. Esattamente uno fra i seguenti enunciati è falso. Trovarlo, fornire un controesempio, e dimostrare gli altri tre. Nell'enunciato falso c'è comunque qualche relazione fra LHS e RHS?

1. $\forall X, Y \forall f: X \rightarrow Y \forall A, B \subseteq X (f(A) \cup f(B) = f(A \cup B))$
2. $\forall X, Y \forall f: X \rightarrow Y \forall A, B \subseteq X (f(A) \cap f(B) = f(A \cap B))$
3. $\forall X, Y \forall f: X \rightarrow Y \forall A, B \subseteq Y (f^{-1}(A) \cup f^{-1}(B) = f^{-1}(A \cup B))$
4. $\forall X, Y \forall f: X \rightarrow Y \forall A, B \subseteq Y (f^{-1}(A) \cap f^{-1}(B) = f^{-1}(A \cap B))$

Esercizio 3.64. Fra gli insiemi nell'Esercizio 3.61 che sono grafici di funzioni:

1. Ha senso dire se sono grafici di funzioni iniettive? Se sì, quali lo sono?
2. Ha senso dire se sono grafici di funzioni surgettive? Se sì, quali lo sono?
3. Ha senso dire se sono grafici di funzioni bigettive? Se sì, quali lo sono?
4. Quali coppie ordinate di questi insiemi ammettono scelte di codomini che le rendono componibili? Per tali coppie, fissare delle tali scelte e calcolare la composizione.

Esercizio 3.65. Siano $f: X \rightarrow Y$ e $g: Y \rightarrow Z$.

1. Supponiamo che $g \circ f$ sia iniettiva. La funzione f deve essere per forza iniettiva? La funzione g ?

2. Supponiamo che $g \circ f$ sia surgettiva. La funzione f deve essere per forza surgettiva? La funzione g ?
3. Supponiamo che $g \circ f$ sia bigettiva. La funzione f deve essere per forza bigettiva? La funzione g ?

Esercizio 3.66. Chi è $\Gamma_{g \circ f}$, in termini di Γ_f e Γ_g ? Per esempio, trovare un [qualcosa] e una formula $\varphi(x, z, \Gamma_f, \Gamma_g)$ da sostituire in

$$\Gamma_{g \circ f} = \{(x, z) \in [\text{qualcosa}] \mid \varphi(x, z, \Gamma_f, \Gamma_g)\}$$

Esercizio 3.67. Siano X, Y non vuoti, $f: X \rightarrow Y$ e $g: Y \rightarrow X$. Vero o falso?

1. Se f è costante allora $g \circ f$ è costante.
2. Se g è costante allora $g \circ f$ è costante.
3. Se $g \circ f$ è costante allora f è costante.
4. Se $g \circ f$ è costante allora g è costante.
5. Se $g \circ f$ è costante allora f è costante e g è costante.
6. Se $g \circ f$ è costante allora f è costante o g è costante.
7. Stesse domande di sopra con l'ipotesi aggiuntiva che $X = Y$.
8. Stesse domande di sopra con le ipotesi aggiuntive che $X = Y$ e $f = g$.

Esercizio 3.68. Sia Y un insieme. Quante funzioni ci sono $\emptyset \rightarrow Y$? Quali di queste sono iniettive? Surgettive? Dipende da Y ?

Esercizio 3.69. Sia $f: \mathbb{N} \rightarrow \mathbb{N}$ la funzione

$$f(x) := \left\lfloor \frac{2x^2 + 1}{3} \right\rfloor$$

Calcolare $f^{-1}(\{n \in \mathbb{N} \mid n \leq 10\})$.

Esercizio 3.70. Dire quali di queste funzioni hanno inverse destre, quali hanno inverse sinistre, e in entrambi i casi esibirne una se esiste (e se non esiste, dimostrarlo¹⁰).

1. $f_1: \mathbb{N} \rightarrow \mathbb{N}$ $f_1(x) = \begin{cases} 3 & \text{se } x = 1 \\ 1 & \text{se } x = 3 \\ x & \text{altrimenti} \end{cases}$
2. $f_2: \mathbb{N} \rightarrow \mathbb{N}$ $f_2(x) = \begin{cases} x + 1 & \text{se } x \text{ è pari} \\ x - 1 & \text{se } x \text{ è dispari} \end{cases}$
3. $f_3: \mathbb{N} \rightarrow \mathbb{N}$ $f_3(x) = \begin{cases} x + 2 & \text{se } x \text{ è pari} \\ x - 2 & \text{se } x \geq 3 \text{ è dispari} \\ 0 & \text{se } x = 1 \end{cases}$

¹⁰Altro genere di cose che d'ora in avanti non starò a scrivere ogni volta.

$$4. f_4: \mathbb{N} \rightarrow \mathbb{N} \quad f_4(x) = \begin{cases} x+2 & \text{se } x \text{ è pari} \\ x-2 & \text{se } x \geq 3 \text{ è dispari} \\ 1 & \text{se } x = 1 \end{cases}$$

$$5. f_5: \mathbb{N} \rightarrow \mathbb{N} \quad f_5(x) = \begin{cases} x+2 & \text{se } x \text{ è pari} \\ x-2 & \text{se } x \geq 5 \text{ è dispari} \\ 1 & \text{se } x = 1 \\ 0 & \text{se } x = 3 \end{cases}$$

$$6. f_6: \mathbb{N} \rightarrow \mathbb{N}^2 \quad f_6(x) = (20x, 35x)$$

$$7. f_7: \mathbb{N} \rightarrow \mathbb{N}^2 \quad f_7(x) = (20x, 5)$$

$$8. f_8: \mathbb{N} \rightarrow \mathbb{N}^2 \quad f_8(x) = (5, 5x)$$

$$9. f_9: \mathbb{N} \rightarrow \mathbb{N}^2 \quad f_9(x) = (20x, (8x+12)^7 + 2^{2^x})$$

$$10. f_{10}: \mathbb{N}^2 \rightarrow \mathbb{N} \quad f_{10}(x, y) = x + y.$$

Capitolo 4

Relazioni

In matematica (e nella vita in generale) è molto frequente parlare di relazioni fra oggetti: questo è più piccolo di quello, queste due cose hanno lo stesso colore, questa persona è figlia di queste altre due, eccetera.

Ora, alcune relazioni hanno delle proprietà che altre non hanno. Per esempio, la relazione “ha stretto la mano a” sull’insieme delle persone ha la proprietà che se A ha stretto la mano a B allora anche B ha stretto la mano ad A , mentre questo non è vero, per esempio, per la relazione “essere minore di” sui numeri naturali o, per rimanere sull’insieme delle persone, per la relazione “essere figlio di”.

In questo capitolo vediamo cos’è una relazione in matematica, e alcune proprietà importanti che una data relazione può avere o meno.

4.1 Mettere le cose in relazione

Nello specificare una funzione (oltre a dare dominio e codominio), specifichiamo semplicemente quale output corrisponde a quale input. Alla stessa maniera, nello specificare una relazione diciamo semplicemente cosa è in relazione in con cosa:

Definizione 4.1.

1. Una *relazione n -aria* R è una tupla¹ $(X_1, \dots, X_n, \Gamma_R)$ tale che $X_1, \dots, X_n$ sono insiemi e $\Gamma_R \subseteq X_1 \times \dots \times X_n$.
2. Se $(x_1, \dots, x_n) \in \Gamma_R$ diciamo che Γ_R è *vera* su $(x_1, \dots, x_n)$. Altrimenti, diciamo che è *falsa* su $(x_1, \dots, x_n)$.
3. Γ_R si chiama *grafico* di R .
4. Se tutti gli X_i sono uguali a un certo X , diciamo che R è una relazione *n -aria su X* .
5. Se $R = (X, Y, \Gamma_R)$ è una relazione binaria, X e Y si chiamano *dominio* e *codominio* di R , e si indicano rispettivamente con $\text{dom}(R)$ e $\text{codom}(R)$.

¹Cioè una k -upla ordinata per qualche k . In questo caso, $k = n + 1$.

Nel seguito, considereremo quasi esclusivamente relazioni binarie (X, Y, Γ_R) con $X = Y$. Inoltre, scriveremo cose come $x \leq y$ invece di $(x, y) \in \Gamma_{\leq}$. Stipuliamo quindi quanto segue.

Notazione 4.2.

1. Se $R = (X_1, \dots, X_n, \Gamma_R)$ è una relazione, invece di $(x_1, \dots, x_n) \in \Gamma_R$ scriviamo $R(x_1, \dots, x_n)$.
2. Se R è una relazione binaria, invece di $R(x, y)$ scriviamo anche $x R y$.
3. Salvo avviso contrario, con “relazione” intenderemo “relazione binaria con dominio uguale al codominio”, e invece di scrivere $R = (X, X, \Gamma_R)$ scriveremo (X, R) .

Possiamo anche pensare a (X, R) come a una struttura nel linguaggio con un simbolo per R , cosa che tornerà comoda nelle prossime sezioni.² Ed è anche comune, quando dominio e codominio sono chiari dal contesto, identificare una relazione con il suo grafico e parlare e.g. de “la relazione $\emptyset$ ” invece che de “la relazione con grafico $\emptyset$ ”.

Esempio 4.3. 1. La relazione $V = (X, Y, \Gamma_V)$ “ha visitato”, dove X è l’insieme delle persone, Y l’insieme delle città, e $x V y$ sse x è stato almeno una volta a y .

2. Per ogni fissato $n \geq 1$ possiamo considerare la relazione su $\mathbb{N}$ denotata $x \equiv y \pmod{n}$, che si legge “ x è congruo a y modulo n ”, e che è vera sse il resto della divisione di x per n è uguale a quello della divisione di y per n . Per esempio, per $n = 2$, abbiamo $x \equiv y \pmod{2}$ se e solo se x e y sono entrambi pari o entrambi dispari.
3. Dato un insieme X , possiamo considerare la relazione $\subseteq$ su $\mathcal{P}(X)$, o la relazione $\supseteq$, o la relazione $\subsetneq$, o la relazione “ A è disgiunto da B ” che è vera sse $A \cap B = \emptyset$.
4. Prendete gli insiemi X, Y che vi pare e il sottoinsieme $\Gamma \subseteq X \times Y$ che vi pare. Potete pensarlo come relazione, dove x è in relazione con y sse $(x, y) \in \Gamma$.
5. In particolare, fra ogni X e Y abbiamo la relazione con grafico $\emptyset \subseteq X \times Y$ e quella con grafico $X \times Y$, rispettivamente falsa su tutte le coppie (x, y) e vera su tutte le coppie (x, y) .
6. Possiamo pensare al grafico Γ_f di una funzione $f: X \rightarrow Y$ come a una relazione fra X e Y . In altre parole, tutte le funzioni sono relazioni binarie fra il loro dominio e il loro codominio.
7. “ x e y sono i genitori di z ” è una relazione ternaria sull’insieme delle persone.
8. Su $\{x \in \mathbb{N} \mid 1 \leq x \leq 12\}$, la relazione ternaria “procedendo in senso orario sull’orologio e partendo da x si incontra prima y e poi z ”.

²E quando dicevamo che una struttura può essere pensata come un database, e che questo è più di analogia, è perché una maniera di implementare i database è proprio tramite strutture con tante relazioni.

9. Sull'insieme delle persone, “ a e b si sono conosciuti prima di c e d ” è una relazione quaternaria.
10. Sull'insieme delle persone, “ $x_0, \dots, x_{10}$ hanno giocato a calcio nella stessa squadra, con x_0 come portiere” è una relazione 11-aria.
11. La relazione “ n è il numero di un biglietto per il film f alle ore h del giorno g al cinema c intestato alla persona p ” è una relazione 6-aria il cui grafico è incluso in³

$$\mathbb{N} \times \text{Films} \times \text{Orari} \times \text{Giorni} \times \text{Cinema} \times \text{Persone}$$

12. Se volete rimuginare su cos'è una relazione 0-aria, vi lascio come indizio/esercizio: X^n è in biezione con (e può essere pensato come) l'insieme delle funzioni $\{0, 1, \dots, n-1\} \rightarrow X$.

Mentre i grafici delle funzioni devono avere delle specifiche proprietà per essere chiamati tali, i grafici delle relazioni possono fare quello che gli pare. Ad esempio, per la relazione $\subseteq$ su $\mathcal{P}(\mathbb{N})$ non esiste nessun A tale che $\mathbb{N} \subseteq A$, ed esiste più di un A tale che $\{1, 2, 3\} \subseteq A$.

Definizione 4.4. Se $R \subseteq X \times Y$ è una relazione, la sua *inversa* è la relazione $R^{-1} \subseteq Y \times X$ definita da

$$y R^{-1} x \iff x R y$$

Esercizio 4.5. Per ogni relazione R abbiamo che $(R^{-1})^{-1} = R$.

Esempio 4.6. Guardiamo le inverse delle relazioni binarie nell'Esempio 4.3.

1. L'inversa di “ha visitato” è “è stata visitata da”.
2. L'inversa della congruenza modulo n è sé stessa.
3. Per qualunque insieme X , l'inversa della relazione $\subseteq$ su $\mathcal{P}(X)$ è la relazione $\supseteq$, l'inversa di $\supseteq$ è [vedi Esercizio 4.5], l'inversa di $\subsetneq$ è $\supsetneq$, l'inversa di “essere disgiunto” è sé stessa.
4. Chiaramente, qualunque relazione binaria può essere invertita.
5. L'inversa di $\emptyset$ è sé stessa, l'inversa di $X \times Y$ è $Y \times X$. In particolare, se $X = Y$ questa relazione è l'inversa di sé stessa.
6. L'inversa di Γ_f , è $f^{-1}(y) \ni x$. Che in un certo senso è la stessa cosa di $f(x) = y$, ma stiamo scambiando dominio e codominio. Come visto nella Sezione 3.3, notiamo che Γ_f^{-1} è il grafico di una funzione $Y \rightarrow X$ se e solo se f è bigettiva. In altre parole, se prendiamo una funzione f e la consideriamo come relazione, la sua inversa è una funzione se e solo se f è bigettiva.

Esercizio 4.7. Se $f: X \rightarrow Y$, allora Γ_f^{-1} è il grafico di qualche funzione (non per forza $Y \rightarrow X$) se e solo se f è iniettiva.

³Il che sperabilmente dovrebbe rendere più chiaro il perché dicevo che strutture e database sono parenti.

4.2 Prima, dopo, nessuna delle due, o entrambe

Tantissime delle relazioni usate in matematica sono relazioni di un tipo speciale; in buona sostanza, sono quelle che ci permettono di confrontare le cose.

Definizione 4.8. Una relazione $(X, \sqsubseteq)$ è un *preordine* sse è

1. *riflessiva*, cioè $\forall x \in X \ x \sqsubseteq x$, e
2. *transitiva*, cioè $\forall x, y, z \in X \ ((x \sqsubseteq y) \wedge (y \sqsubseteq z)) \Rightarrow x \sqsubseteq z$.

Esempio 4.9.

1. L'usuale ordine $\leq$ di $\mathbb{N}$ è un preordine.
2. Per ogni insieme X , l'inclusione $\subseteq$ è un preordine su $\mathcal{P}(X)$. La riflessività è la Proposizione 1.12, e la transitività è un (facile) esercizio.
3. Sull'insieme delle stringhe, “ x è un prefisso di y ” è un preordine.⁴
4. Sull'insieme delle stringhe, “ x è sottostringa di y ” è un preordine.⁵
5. Sull'insieme dei partecipanti ad un torneo, “ y ha totalizzato almeno tanti punti quanto x ” è un preordine.
6. Fissiamo un gioco a due giocatori. Sull'insieme dei partecipanti ad un torneo, “ y ha vinto contro x ” *non* è un preordine. Intanto fallisce la riflessività, dato che nessuno gioca (e quindi in particolare nessuno vince) con sé stesso. Ma anche se guardiamo “ y ha vinto contro x oppure $x = y$ ”, forzando la riflessività, otteniamo una relazione che non è necessariamente un preordine, cioè esistono tornei in cui non lo è. Questo perché, chiaramente, è possibile avere tornei con una situazione “carta-forbici-sasso” dove x vince contro y che vince contro z che vince contro x , e quindi in tali tornei la transitività fallisce.
7. In un filesystem, “il path di x è un prefisso del path di y ” è un preordine.
8. Sull'insieme delle persone, “ x abita almeno tanto a nord quanto y ” è un preordine.
9. Sull'insieme delle persone, “ x abita almeno tanto a sud quanto y ” è un preordine.
10. Sull'insieme delle persone, “ x abita ad al più 10km da y ” *non* è un preordine, perché non è transitivo.
11. Sull'insieme delle persone, “ x abita nella stessa città di y ” è un preordine.
12. Su $\mathbb{N}$, la relazione “ x e y hanno lo stesso resto quando divisi per 7” è un preordine.
13. Su ogni insieme X , la relazione $=$ è un preordine.

⁴ x è un prefisso di y sse esiste una stringa z tale che y è la concatenazione xz . Insomma, “prefisso” vuol dire “pezzo iniziale”.

⁵ x è una sottostringa di y sse esistono stringhe z e t tali che $y = txz$.

14. Su ogni insieme X , la relazione X^2 è un preordine.
15. Su ogni insieme $X \neq \emptyset$, la relazione $\emptyset$ non è un preordine perché non è riflessiva.⁶

Notiamo che i preordini in questo esempio “si comportano” in maniera abbastanza eterogenea. Ad esempio, se $n \neq m$ sono due numeri naturali distinti, allora esattamente una fra $n \leq m$ e $m \leq n$ è vera. Invece, per esempio, in $(\mathcal{P}(\mathbb{N}), \subseteq)$ esistono elementi *incomparabili*, cioè degli A, B tali che $A \not\subseteq B$ e $B \not\subseteq A$, e nel punto 9 ci sono persone distinte che abitano alla stessa latitudine.

Gli ultimi preordini in questo esempio hanno chiaramente un “sapore” diverso da quelli più in alto nella lista, e a primo impatto potrebbe addirittura fare strano chiamarli “preordini”. Ci torniamo nella prossima sezione, ma intanto:

Definizione 4.10. Una relazione $(X, \sqsubseteq)$ è un *ordine parziale* sse è un preordine e inoltre è *antisimmetrico*, cioè soddisfa:

$$\forall x, y \in X ((x \sqsubseteq y) \wedge (y \sqsubseteq x)) \Rightarrow x = y$$

Esempio 4.11. Nell'Esempio 4.9:

1. Tutti gli esempi di cose che non sono preordini non sono—a maggior ragione—ordini parziali.
2. Il punto 2 è un ordine parziale per il Corollario 1.13. Per un esempio, vedi Figura 4.1.
3. Il punto 3 è un ordine parziale: le stringhe hanno lunghezza finita, e se x è un prefisso di y e y è un prefisso di x allora x e y devono necessariamente coincidere.
4. Il punto 9 non è un ordine parziale, perché esistono persone diverse che abitano alla stessa latitudine.
5. Se il filesystem ha link simbolici, il punto 7 non è un ordine parziale!
6. Il punto 12 non è un ordine parziale perché $7 \cdot 0 + 3 = 1 \neq 10 = 7 \cdot 1 + 3$.

Vi lascio il piacere di esaminare gli altri esempi:

Esercizio 4.12. Trovare tutti e soli gli ordini parziali fra le relazioni dell'Esempio 4.9.

Diamo ora un nome alla proprietà che abbiamo usato per distinguere $(\mathbb{N}, \leq)$ da $(\mathcal{P}(\mathbb{N}), \subseteq)$.

Definizione 4.13. Una relazione $(X, \sqsubseteq)$ è un *preordine lineare* sse è un preordine e inoltre soddisfa:

$$\forall x, y \in X (x \sqsubseteq y) \vee (y \sqsubseteq x)$$

Un *ordine lineare* è un ordine parziale che è anche un preordine lineare.

⁶Su $X = \emptyset$, è invece un preordine (esercizio).

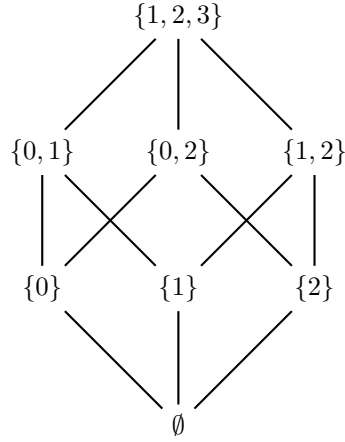


Figura 4.1: *Diagramma di Hasse* dell'ordine parziale $(\mathcal{P}(\{0, 1, 2\}), \subseteq)$.

In altre parole, un ordine lineare è un ordine parziale dove tutte le coppie di elementi sono comparabili: come suggerisce il nome “lineare”, è una maniera per mettere in fila gli elementi del suo dominio. Nel caso di un preordine lineare ammettiamo anche punti del dominio “a pari merito”.

Esercizio 4.14. 1. Trovare tutti e soli i preordini lineari fra le relazioni dell'Esempio 4.9.

2. Trovare tutti e soli gli ordini lineari fra le relazioni dell'Esempio 4.9.

Notazione 4.15. I seguenti sono sinonimi della terminologia introdotta in questa sezione.

1. Un preordine si può anche chiamare *quasi-ordine*.
2. Un ordine parziale si può anche chiamare *poset* (abbreviazione per *partially ordered set*).
3. Un ordine lineare si può anche chiamare *ordine totale*. In particolare, per definizione tutti gli ordini totali sono ordini parziali, anche se la terminologia sembrerebbe suggerire il contrario.⁷

4.3 Perdere informazione (e vivere felici)

Con tutti questi alberi non riesco a vedere la foresta!

Less is more.

Capita spesso di trovarsi ad affrontare problemi dove la soluzione è ovvia se si buttano a mare abbastanza distrattori. Una maniera matematica per sbarazzarsi di informazione inutile e concentrarsi su quello che ci interessa veramente è fare un *quoziente* per una *relazione d'equivalenza*.

⁷Nella terminologia matematica, purtroppo, questo genere di cose succede più frequentemente di quanto potrebbe piacerci.

Definizione 4.16. Una relazione E su X è una *relazione d'equivalenza* sse è e un preordine e inoltre è *simmetrica*, cioè

$$\forall x, y \in X (x E y \Rightarrow y E x)$$

Fra i simboli usati spesso per denotare una qualche relazione d'equivalenza troviamo E , $\sim$, $\equiv$.

Esempio 4.17. Nell'Esempio 4.9:

1. La relazione $\subseteq$ nel punto 2, con $X = \mathbb{N}$, *non* è una relazione d'equivalenza: per esempio $\{1\} \subseteq \{1, 2\}$ ma $\{1, 2\} \not\subseteq \{1\}$.
2. La relazione del punto 9 *non* è una relazione d'equivalenza dato che, ad esempio, Napoli è più a sud di Bari (ed entrambe le città hanno almeno un abitante).
3. La relazione del punto 11 è una relazione d'equivalenza.
4. La relazione del punto 12 è una relazione d'equivalenza.

Esercizio 4.18. Trovare tutte e sole le relazioni d'equivalenza fra le relazioni dell'Esempio 4.9.

Se fate l'esercizio, vi renderete conto che le relazioni che sono sia ordini parziali che d'equivalenza scarseggiano. Questa non è una peculiarità di quell'elenco:

Proposizione 4.19. Su un insieme X , l'unica relazione che è riflessiva, simmetrica e antisimmetrica è l'uguaglianza.

Dimostrazione. Sia (X, R) una relazione che è sia un ordine parziale che una relazione d'equivalenza. Per mostrare che R coincide con $=$ dobbiamo mostrare che

$$\forall x, y \in X (x R y \Leftrightarrow x = y) \quad (4.1)$$

Per ipotesi R è riflessiva, e quindi l'implicazione $\Leftarrow$ nella (4.1) è vera. Per l'altra implicazione, siano $x, y \in X$ arbitrari e supponiamo che $x R y$. Dato che R è simmetrica abbiamo $y R x$. Quindi $x R y$ e $y R x$, e dato che R è antisimmetrica ne segue che $x = y$. $\square$

Corollario 4.20. Sia (X, R) una relazione. Se R è sia un ordine parziale che una relazione di equivalenza, allora R è l'uguaglianza $=$.

L'altra cosa di cui potreste esservi resi conto facendo l'Esercizio 4.18 è che quelle che erano relazioni d'equivalenza tendevano ad essere robe del tipo “avere qualcosa in comune”, o un po' più precisamente suonavano come “ x e y hanno lo stesso z ”. Anche questo è un fatto generale, che ora svisceriamo. Iniziamo notando che *tutte* le relazioni della forma “avere lo stesso z ” sono relazioni d'equivalenza. In breve, il punto è che questo “qualcosa” è una funzione di x , e riflessività, simmetria e transitività vengono “ereditate” dall'uguaglianza. Più in dettaglio:

Lemma 4.21. Sia $f: X \rightarrow Y$ una funzione. Definiamo E_f come la relazione binaria su X data da

$$x_0 E_f x_1 \iff f(x_0) = f(x_1)$$

Allora E_f è una relazione d'equivalenza.

Dimostrazione. Dobbiamo verificare tre cose.

Riflessività. Chiaramente $f(x_0) = f(x_0)$, e quindi $x_0 E_f x_0$.

Simmetria. Analogamente, deriva dal fatto che $f(x_0) = f(x_1)$ implica $f(x_1) = f(x_0)$.

Transitività. Segue facilmente dal fatto che se $f(x_0) = f(x_1)$ e $f(x_1) = f(x_2)$ allora $f(x_0) = f(x_2)$. $\square$

La cosa più interessante è che *tutte* le relazioni d'equivalenza sono di questa forma. In breve, l'idea è più semplice/tautologica di quanto uno si possa aspettare: la “cosa che hanno in comune” due cose equivalenti è... essere equivalenti alle stesse cose, o meglio ancora “le cose a cui sono equivalenti”. Ma facciamo le cose con calma e introduciamo un po' di terminologia.

Definizione 4.22. Sia (X, E) una relazione d'equivalenza.

1. Per $x \in X$, la *classe d'equivalenza di x modulo E* è $\{y \in X \mid y E x\}$, e si denota con x/E o con $[x]_E$, o anche $[x]$ se E è chiara dal contesto.
2. Il *quoziente* di X per E è $X/E := \{x/E \mid x \in X\}$.
3. La *proiezione al quoziente* $\pi_E: X \rightarrow X/E$ è la funzione $\pi_E(x) := x/E$.

In sostanza, fare un quoziente per una relazione d'equivalenza vuol dire smettere di distinguere certe cose, un po' come se avessimo gli occhiali appannati. In altre parole, una relazione d'equivalenza è “una maniera di identificare le cose”, in un certo senso una maniera di “inciccionire” l'uguaglianza.

Lo facciamo con delle relazioni d'equivalenza, e non con delle relazioni qualunque, perché se una relazione vogliamo usarla per “non distinguere le cose” allora:

1. sarà meglio non distinguere x da x ; quindi una tale relazione vogliamo che sia riflessiva;
2. se non distinguiamo x da y , non vogliamo distinguere nemmeno y da x , e quindi la vogliamo simmetrica; e
3. se non distinguiamo x da y né y da z , allora non dobbiamo distinguere nemmeno x da z , quindi la vogliamo transitiva.

Tutto questo si concretizza nei fatti che stiamo per vedere.

Lemma 4.23. Sia (X, E) una relazione d'equivalenza. Per ogni $x, y \in X$, le seguenti sono equivalenti.

1. $x E y$

$$2. x/E = y/E$$

$$3. \pi_E(x) = \pi_E(y)$$

Dimostrazione. Vediamo che $1 \Rightarrow 2$. Assumiamo che $x E y$ e dimostriamo $x/E = y/E$ per doppia inclusione. Se $z \in x/E$, per definizione $z E x$. Dato che E è transitiva, abbiamo $z E y$, e quindi $z \in y/E$, il che dimostra $x/E \subseteq y/E$. Dato che $x E y$ e E è simmetrica abbiamo $y E x$, e dato che x, y erano arbitrari il paragrafo precedente ci dà $y/E \subseteq x/E$, come desiderato.

L'implicazione $2 \Rightarrow 3$ è ovvia per definizione di π_E .

Per dimostrare $3 \Rightarrow 1$ siano x, y tali che $\pi_E(x) = \pi_E(y)$. Segue immediatamente dalle definizioni che questo vuol dire che $\forall z \in X (z E x \Leftrightarrow z E y)$. Dato che E è simmetrica, ne segue che $\forall z \in X (x E z \Leftrightarrow z E y)$. Quindi per concludere basta trovare un qualche $z \in X$ tale che $x E z$, e questo z farà da “ponte” per transitività, e potremo concludere che $x E y$. Ma dato che E è riflessiva, possiamo prendere $z := x$. $\square$

Insomma, il “qualcosa” che hanno in comune due cose equivalenti è la loro immagine nel quoziente. Equivalentemente, l'insieme delle cose a cui sono equivalenti. Ne segue che dare una relazione d'equivalenza è in un certo senso la stessa cosa di dare una funzione surgettiva. O quasi, in realtà una funzione surgettiva ha un po' più informazione di una relazione d'equivalenza (ci torniamo).

Teorema 4.24. Sia $X \neq \emptyset$ un insieme nonvuoto. Per ogni insieme Y e ogni funzione surgettiva $f: X \rightarrow Y$, denotiamo con E_f la relazione E_f definita da $x E_f y \Leftrightarrow f(x) = f(y)$. Allora:

1. Per ogni relazione d'equivalenza E su X ,
 - (a) la funzione $\pi_E: X \rightarrow X/E$ è surgettiva, e
 - (b) $E_{\pi_E} = E$.
2. Per ogni $f: X \rightarrow Y$ surgettiva:
 - (a) E_f è una relazione d'equivalenza,
 - (b) le classi di equivalenza di E_f sono esattamente le fibre di f , e
 - (c) esiste una bigezione $g: X/E_f \rightarrow Y$ tale che $f = g \circ \pi_{E_f}$ (vedi Figura 4.2).

La prima parte del teorema ci sta dicendo che ogni proiezione al quoziente è una funzione surgettiva, e che se usiamo questa funzione per definire una relazione d'equivalenza ritroviamo quella di partenza.

La seconda parte ci sta dicendo: come tutte le funzioni, quelle surgettive inducono una relazione d'equivalenza. Ma se f è surgettiva, possiamo quasi recuperarla dalla relazione d'equivalenza che induce, a meno di “rietichettare” Y . Insomma, non è letteralmente vero che “ogni funzione bigettiva è una proiezione al quoziente”, ma quasi: ogni funzione bigettiva è una proiezione al quoziente a meno di una bigezione del codominio con un altro insieme.

Detto in un'altra maniera, una funzione surgettiva contiene più informazione della relazione d'equivalenza che induce: dà in un certo senso “un nome” a ogni classe d'equivalenza. In un certo senso, dare una relazione di equivalenza è come dare “una funzione surgettiva su un insieme di punti anonimi”.

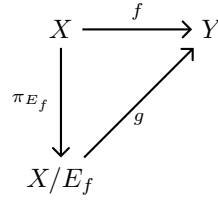


Figura 4.2: Le funzioni nel Teorema 4.24. Questo diagramma *commuta*, cioè non importa che giro facciamo seguendo le frecce, la funzione è la stessa: $f = g \circ \pi_{E_f}$.

Dimostrazione. Dimostriamo i punti della conclusione uno alla volta.

1a Se $A \in X/E$, per definizione esiste $x \in X$ tale che $A = x/E$, e quindi $A = \pi_E(x)$.

1b Per ogni $x, y \in X$ abbiamo,

$$x E_{\pi_E} y \Leftrightarrow \pi_E(x) = \pi_E(y) \Leftrightarrow x E y$$

2a Per il Lemma 4.21.

2b Sia A una classe di equivalenza di E_f , quindi della forma x/E_f per qualche $x \in X$. Per definizione, $y E_f x \Leftrightarrow f(y) = f(x) \Leftrightarrow y \in f^{-1}(f(x))$, e quindi x/E_f è la fibra di f in $f(x)$. Viceversa, dato $y \in Y$, per surgettività la fibra $f^{-1}(y)$ è non vuota, e dato un qualunque suo elemento x si mostra che $f^{-1}(y)$ è la classe di equivalenza di x (esercizio).

2c È più facile definire l'inversa di g , quindi definiamo $h: Y \rightarrow X/E_f$ come $h(y) = f^{-1}(y)$. Questa è una bigezione per il punto 2b appena dimostrato. Se poniamo $g := h^{-1}$, allora far vedere che $f = g \circ \pi_{E_f}$ è equivalente a far vedere che $h \circ f = \pi_{E_f}$. Ma $h \circ f(x) = h(f(x)) = f^{-1}(f(x))$, e come mostrato nel punto 2b sopra questo coincide con $x/E_f = \pi_{E_f}(x)$. $\square$

Un altro concetto che è “la stessa cosa” delle relazioni d'equivalenza—questa volta per davvero, senza bisogno di “a meno di”—è quello di fare un insieme “a pezzi”.

Definizione 4.25. Una *partizione* di un insieme X è una famiglia⁸ $\mathcal{P} \subseteq \mathcal{P}(X)$ di sottoinsiemi di X tali che

1. ogni $A \in \mathcal{P}$ è nonvuoto,
2. gli elementi di $\mathcal{P}$ sono a due a due disgiunti, cioè se $A, B \in \mathcal{P}$ e $A \neq B$ allora $A \cap B = \emptyset$, e
3. l'unione di $\mathcal{P}$ è X , cioè $\bigcup_{A \in \mathcal{P}} A = X$.

Osservazione 4.26. In altre parole, $\mathcal{P} \subseteq \mathcal{P}(X)$ è una partizione di X se e solo se:

⁸Una *famiglia* è un insieme i cui elementi sono tutti insiemi (tipicamente sottoinsiemi di un insieme fissato).

$\mathbb{N}$	0	1	2	3	4
	5	6	7	8	9
	10	11	12	13	14
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

Figura 4.3: Partizione di $\mathbb{N}$ in classi di resto modulo 5.

1. ogni $A \in \mathcal{P}$ contiene un qualche $x \in X$,
2. ogni $x \in X$ appartiene ad al più un $A \in \mathcal{P}$, e
3. ogni $x \in X$ appartiene ad almeno un $A \in \mathcal{P}$.

Insomma, una partizione di X è una famiglia di sottoinsiemi non vuoti di X tale che ogni $x \in X$ appartiene ad esattamente un elemento della famiglia.

Esempio 4.27.

1. Sia G l'insieme dei giorni g del calendario (bisestile), e per ogni tale g sia C_g l'insieme delle persone che sono nate il giorno g di qualche anno. Allora $\{C_g \mid g \in G\}$ è una partizione dell'insieme delle persone.
2. L'insieme degli iscritti a Informatica all'Università di Bari nell'anno accademico 2026/2027 è partizionato con la partizione $\{\text{"A-D"}, \text{"E-M"}, \text{"N-Z"}\}$ a seconda dell'iniziale del cognome. La *partizione* qui è la famiglia di questi tre insiemi, anche se su Esse3 si parla della "partizione" E-M.
3. Denotiamo con $2\mathbb{N}$ l'insieme dei numeri naturali pari e con $2\mathbb{N}+1$ l'insieme dei dispari. Allora $\{2\mathbb{N}, 2\mathbb{N}+1\}$ è una partizione di $\mathbb{N}$.
4. Più in generale, se $n \in \mathbb{N} \setminus \{0\}$ e, per $0 \leq k < n$ naturale, denotiamo con $n\mathbb{N}+k$ l'insieme dei numeri naturali il cui resto nella divisione per n è k , allora $\{n\mathbb{N}+k \mid 0 \leq k < n\}$ è una partizione di $\mathbb{N}$. Vedi Figura 4.3.
5. $\{3\mathbb{N}, 3\mathbb{N}+1\}$ *non* è una partizione di $\mathbb{N}$ perché 2 non appartiene a nessun elemento della famiglia, e quindi l'unione della stessa non è tutto $\mathbb{N}$.
6. $\{2\mathbb{N}, 2\mathbb{N}+1, 3\mathbb{N}\}$ *non* è una partizione di $\mathbb{N}$, perché i suoi elementi non sono a due a due disgiunti. Ad esempio, $6 \in 2\mathbb{N} \cap 3\mathbb{N}$.
7. L'insieme vuoto non ha partizioni, dato che tutti gli elementi di una partizione di X sono sottoinsiemi non vuoti di X .

Proposizione 4.28. Siano $X \neq \emptyset$ e $f: X \rightarrow Y$ una qualunque funzione. Allora $\{f^{-1}(y) \mid y \in Y\}$ è una partizione di X se e solo se f è surgettiva.

Dimostrazione. Per ogni f come nelle ipotesi, abbiamo che

- $\bigcup_{y \in Y} f^{-1}(y) = X$, per l'Esempio 3.12.1 e l'Esercizio 3.15 (se non avete fatto l'esercizio è un buon momento per farlo; in sostanza, è vero per definizione di funzione).

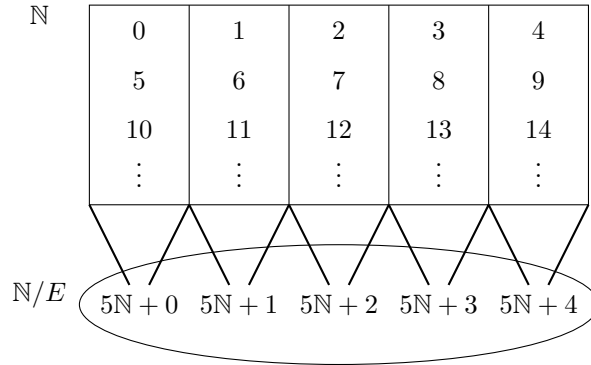


Figura 4.4: Partizione di $\mathbb{N}$ in classi di resto modulo 5 e relativa proiezione al quoziente per la relazione di equivalenza E indotta.

- Se $y_0, y_1 \in Y$ e $y_0 \neq y_1$, allora per definizione di funzione $f^{-1}(y_0) \cap f^{-1}(y_1) = \emptyset$.

Per definizione di partizione, ne segue che $\{f^{-1}(y) \mid y \in Y\}$ è una partizione di X se e solo se non esiste nessun $y \in Y$ tale che $f^{-1}(y) = \emptyset$. Ma questo è equivalente alla surgettività di f per l'Esercizio 3.46 (che, di nuovo, è un buon momento per fare, se non l'avete già fatto) e il fatto che, dato che $X \neq \emptyset$ ed esiste una funzione $X \rightarrow Y$ (proprio f), dobbiamo avere anche che $Y \neq \emptyset$ (esercizio). $\square$

Lemma 4.29. Se $X \neq \emptyset$ e E è una relazione d'equivalenza su X , allora X/E è una partizione di X .

Dimostrazione. Consideriamo la proiezioni al quoziente $\pi_E: X \rightarrow X/E$. Per il Teorema 4.24 π_E è surgettiva. Concludiamo per la Proposizione 4.28. $\square$

Vedi Figura 4.4 per un esempio.

Lemma 4.30. Se $\mathcal{P}$ è una partizione di X , allora la relazione

$$e(\mathcal{P}) := \{(x, y) \in X^2 \mid \exists A \in \mathcal{P} \ x \in A \wedge y \in A\}$$

è una relazione d'equivalenza.

Dimostrazione. Per l'Osservazione 4.26, ogni $x \in X$ appartiene a un qualche $A \in \mathcal{P}$. Ne segue che $e(\mathcal{P})$ è riflessiva. La simmetria segue direttamente dalla definizione di $e(\mathcal{P})$ (e, se volete, il fatto che $\wedge$ è commutativa). Per la transitività, siano $A, B \in \mathcal{P}$ tali che $x \in A \wedge y \in A \wedge y \in B \wedge z \in B$. Se mostriamo che $A = B$, allora possiamo prendere questo come testimone dell'esistenziale che mostra che $x e(\mathcal{P}) z$. Ma per ipotesi $y \in A \cap B$, quindi $A \cap B \neq \emptyset$, e quindi $A = B$ per definizione di partizione. $\square$

Definizione 4.31. Sia $X \neq \emptyset$.

1. Denotiamo con $\text{Partizioni}(X)$ l'insieme delle partizioni di X .
2. Denotiamo con $\text{EqRel}(X)$ l'insieme delle relazioni di equivalenza su X .

3. Definiamo $e: \text{Partizioni}(X) \rightarrow \text{EqRel}(X)$ come la funzione che manda una partizione $\mathcal{P}$ nella relazione d'equivalenza

$$e(\mathcal{P}) := \{(x, y) \in X^2 \mid \exists A \in \mathcal{P} \ x \in A \wedge y \in A\}$$

4. Definiamo $p: \text{EqRel}(X) \rightarrow \text{Partizioni}(X)$ come la funzione che manda una relazione d'equivalenza E nella partizione X/E .

Teorema 4.32. Sia $X \neq \emptyset$ un insieme non vuoto. Allora $e: \text{Partizioni}(X) \rightarrow \text{EqRel}(X)$ e $p: \text{EqRel}(X) \rightarrow \text{Partizioni}(X)$ sono bigezioni, e sono una l'inversa dell'altra.

Dimostrazione. Per il Corollario 3.52 basta mostrare che queste due funzioni sono una l'inversa dell'altra, cioè che per ogni partizione $\mathcal{P}$ di X abbiamo $p(e(\mathcal{P})) = \mathcal{P}$ e per ogni relazione d'equivalenza E su X abbiamo $e(p(E)) = E$.

Per la prima parte abbiamo, per definizione di e e p , che per ogni $x, y \in X$

$$\begin{aligned} x \ e(p(E)) \ y &\Leftrightarrow \exists A \in p(E) \ (x \in A \wedge y \in A) \\ &\Leftrightarrow \exists A \in X/E \ (x \in A \wedge y \in A) \\ &\Leftrightarrow \exists A \in X/E \ \pi_E(x) = A = \pi_E(y) \\ &\Leftrightarrow x \ E \ y \end{aligned}$$

dove nella penultima equivalenza abbiamo usato che c'è un unico elemento di X/E a cui appartiene x , cioè la sua classe di equivalenza $x/E = \pi_E(x)$.

Per la seconda parte notiamo che segue facilmente dalla definizione di $e(\mathcal{P})$ che le sue classi di equivalenza sono proprio gli elementi di $\mathcal{P}$. Ma allora, per ogni $A \in \mathcal{P}(X)$,

$$A \in p(e(\mathcal{P})) \iff A \in X/e(\mathcal{P}) \iff A \in \mathcal{P}$$

e quindi $p(e(\mathcal{P})) = \mathcal{P}$ per estensionalità. $\square$

4.4 Portarsi appresso una relazione

Un concetto di importanza cruciale in matematica è quello di “funzione che conserva le relazioni”. Fra le altre cose, permette di dire quando due strutture “fanno le stesse cose”, e di parlare di *simmetrie* di una struttura.

Definizione 4.33. Siano (X, R) e (Y, S) due relazioni binarie. Un *omomorfismo* $(X, R) \rightarrow (Y, S)$ è una funzione $f: X \rightarrow Y$ tale che

$$\forall x_0, x_1 \in X \ (x_0 \ R \ x_1) \implies (f(x_0) \ S \ f(x_1))$$

A parole, un omomorfismo è una funzione che manda coppie in relazione in coppie in relazione, o che *preserva* le relazioni.

Esempio 4.34.

1. La funzione identità sull'insieme delle persone è un omomorfismo dalla relazione “ha scritto un messaggio a” alla relazione “ha comunicato con”.
2. Sia X un insieme di sassi. La funzione da $(\mathcal{P}(X), \subseteq)$ a $(\mathbb{R}, \leq)$ che manda un sottoinsieme di X nel suo peso in kg è un omomorfismo.

3. Una funzione $f: (X, \leq) \rightarrow (Y, \leq)$ ⁹ fra due ordini parziali è, per definizione, un omomorfismo se e solo se è (debolmente) crescente, cioè sse $\forall x_0, x_1 \in X \ x_0 \leq x_1 \Rightarrow f(x_0) \leq f(x_1)$. Quindi, per esempio, la funzione $\mathbb{N} \rightarrow \mathbb{N}$ data da $n \mapsto n^2 + n$ è un *endomorfismo* di $(\mathbb{N}, \leq)$, cioè un omomorfismo da $(\mathbb{N}, \leq)$ in sé stesso.
4. Un altro esempio è la funzione $n \mapsto \lfloor n/10 \rfloor$ da $(\mathbb{N}, \leq)$ a $(\mathbb{N}, \leq)$, per lo stesso motivo.
5. Siano P l'insieme delle persone ed F il sottoinsieme delle persone di sesso femminile, entrambi equipaggiati con la relazione “ x discende da y ”. La funzione $F \rightarrow F$ che mappa ogni x in sua madre è un omomorfismo. La funzione $P \rightarrow F$ che mappa ogni x in sua madre no, perché ad esempio mio padre è un mio antenato ma mia nonna paterna non è antenata di mia madre.
6. Scriviamo $\mathbb{N}_{>0}$ come abbreviazione per $\mathbb{N} \setminus \{0\}$, e denotiamo con $x \mid y$ la relazione “ x divide y ”, cioè $\exists z (x \cdot z = y)$. L'identità $\text{id}_{\mathbb{N}_{>0}}: \mathbb{N}_{>0} \rightarrow \mathbb{N}_{>0}$ è un omomorfismo $(\mathbb{N}_{>0}, \mid) \rightarrow (\mathbb{N}_{>0}, \leq)$. Tuttavia, *non* è un omomorfismo $(\mathbb{N}_{>0}, \leq) \rightarrow (\mathbb{N}_{>0}, \mid)$, perché ad esempio $2 \leq 3$ ma $2 \nmid 3$.
7. Fissiamo $n \in \mathbb{N}$ e sia $X = \{x \in \mathbb{N} \mid x < n\}$. La funzione $(\mathcal{P}(X), \subseteq) \rightarrow (X, \leq)$ che manda un sottoinsieme $A \subseteq X$ nel numero dei suoi elementi è un omomorfismo: se $A \subseteq B$ allora B ha almeno tanti elementi quanto A .
8. Per ogni relazione d'equivalenza (X, E) , la proiezione al quoziente è un omomorfismo $(X, E) \rightarrow (X/E, =)$.

Alcuni omomorfismi hanno la proprietà che la loro immagine è una “copia” della struttura di partenza. Questi omomorfismi si meritano un nome.

Definizione 4.35. Siano (X, R) e (Y, S) due relazioni binarie. Un *embedding* $(X, R) \rightarrow (Y, S)$ è una funzione iniettiva $f: X \rightarrow Y$ tale che

$$\forall x_0, x_1 \in X \ x_0 R x_1 \iff f(x_0) S f(x_1)$$

Osservazione 4.36. Non tutti gli omomorfismi iniettivi sono embedding: *non* è vero che, per ogni omomorfismo $f: (X, R) \rightarrow (Y, S)$, se $f(x_0) S f(x_1)$ allora $x_0 R x_1$. Nemmeno se assumiamo anche che f è iniettiva.

Esercizio 4.37. Verificare l'Osservazione 4.36 trovando degli esempi.

Suggerimento. Vedi Suggerimento 6. □

Esercizio 4.38. Quali sono gli embedding fra due ordini parziali?

Definizione 4.39. Siano (X, R) e (Y, S) due relazioni binarie. Un *isomorfismo* $f: (X, R) \rightarrow (Y, S)$ è un omomorfismo bigettivo la cui inversa è un omomorfismo. Sse esiste un isomorfismo fra (X, R) e (Y, S) scriviamo $(X, R) \cong (Y, S)$ e diciamo che queste strutture sono *isomorfe*.

Esercizio 4.40. Una funzione fra due relazioni binarie è un isomorfismo se e solo se è un embedding bigettivo.

⁹Stiamo scrivendo $\leq$ sia per l'ordine di X che per l'ordine di Y , ma ovviamente queste sono in generale due relazioni diverse.

Due strutture isomorfe “fanno le stesse cose”. Vediamo qualche esempio.

Esempio 4.41.

1. Sia $\mathbb{N}$ l'insieme dei numeri naturali ma ogni numero è stato dipinto di blu.¹⁰ Sia $\leq$ la relazione su $\mathbb{N}$ che vi aspettate. Allora la funzione che manda n in n è un isomorfismo $(\mathbb{N}, \leq) \rightarrow (\mathbb{N}, \leq)$.
2. La funzione successore $s: (\mathbb{N}, \leq) \rightarrow (\mathbb{N} \setminus \{0\}, \leq)$ è un isomorfismo.
3. La funzione successore $s: (\mathbb{N}, \leq) \rightarrow (\mathbb{N}, \leq)$ è un embedding che non è un isomorfismo.
4. La funzione identità nell'Esempio 4.34.6 *non* è un isomorfismo.
5. L'alfabeto (inglese) A , con l'ordine alfabetico, è isomorfo a $\{n \in \mathbb{N} \mid n < 26\}$. In questo caso, esiste un unico isomorfismo $A \rightarrow \{n \in \mathbb{N} \mid n < 26\}$.
6. L'isomorfismo f del punto precedente *induce* un isomorfismo $(\mathcal{P}(A), \subseteq) \rightarrow (\mathcal{P}(\{n \in \mathbb{N} \mid n < 26\}), \subseteq)$ definito da $X \mapsto f(X) = \{f(x) \mid x \in X\}$. Invece di f però avremmo potuto prendere una qualunque bigezione $A \rightarrow X$ (esercizio).
7. Se $(X, \sqsubseteq)$ è un ordine lineare e $(X, \sqsubseteq) \cong (Y, \sqsubseteq)$, allora anche Y è un ordine lineare (esercizio). Quindi, per esempio, $(\mathcal{P}(\{0, 1\}), \subseteq)$ *non* è isomorfo a $(\{0, 1, 2, 3\}, \leq)$, anche se i due hanno lo stesso numero di elementi.
8. $(\mathbb{N}, \leq)$ e $(\mathbb{Z}, \leq)$ sono due ordini lineari *non* isomorfi: il primo ha un minimo, il secondo no, e se ci fosse un isomorfismo $f: (\mathbb{N}, \leq) \rightarrow (\mathbb{Z}, \leq)$ allora $f(0)$ sarebbe l'inesistente minimo di $\mathbb{Z}$ (esercizio).
9. $(X, =)$ e $(Y, =)$ sono isomorfi se e solo se esiste una bigezione $X \rightarrow Y$.
10. Se (X, E) è una relazione d'equivalenza, e $f: (X, E) \rightarrow (Y, F)$ è un isomorfismo, e per esempio $x \in X$ è tale che x/E ha 1435 elementi, allora $f(x)/F$ ha 1435 elementi. E se il quoziente X/E ha 12 elementi, allora Y/F ha anche lui 12 elementi.

Esercizio 4.42.

1. Ogni funzione identità da una struttura in sé stessa è un isomorfismo.
2. L'inversa di un isomorfismo è un isomorfismo.
3. La composizione di due isomorfismi è un isomorfismo.
4. Sia $\mathcal{X}$ un insieme di strutture, ognuna con una relazione binaria (e niente altro). Allora $(\mathcal{X}, \cong)$ è una relazione d'equivalenza.

Per dimostrare che due strutture sono isomorfe, la maniera “standard” è di esibire un isomorfismo. Per dimostrare che due strutture *non* sono isomorfe, controllare tutte le funzioni fra di loro di solito non è praticabile, e bisogna trovare una qualche proprietà preservata dagli isomorfismi (un *invariante*) vera in una struttura e falsa nell'altra. Questo è esattamente quello che abbiamo fatto sopra nell'Esempio 4.41.8.

¹⁰Nota per chi stesse guardando una copia in bianco e nero o non riesca a vedere i colori per altro motivo: alcuni simboli in questo esempio sono colorati di blu.

4.5 Esercizi

Esercizio 4.43. Scrivere esplicitamente (nel senso di: elencarne tutti gli elementi) il grafico della relazione $\leq$ su $\{0, 1, 2\}$.

Esercizio 4.44. Una relazione binaria R è simmetrica sse $R = R^{-1}$.

Definizione 4.45. Se R è una relazione fra X e Y e S è una relazione fra Y e Z , la *composizione* $S \circ R$ è la relazione fra X e Z definita da $(S \circ R)(x, z)$ sse $\exists y \in Y \ R(x, y) \wedge S(y, z)$.

Esercizio 4.46. Una relazione binaria R è transitiva se e solo se $\Gamma_{R \circ R} \subseteq \Gamma_R$.

Esercizio 4.47. Se R è un preordine (rispettivamente, un ordine parziale), allora R^{-1} è un preordine (rispettivamente, un ordine parziale).

Esercizio 4.48. Che proprietà hanno queste relazioni binarie su $\{0, 1, 2\}$ (simmetria, transitività...)? Che relazioni sono (poset, equivalenza...)?

1. $\{(0, 1), (0, 2), (1, 2)\}$
2. $\{(0, 1), (1, 0), (1, 2)\}$
3. $\{(0, 0), (0, 1), (1, 0), (1, 1)\}$
4. $\{(0, 0), (0, 1), (1, 0), (1, 1), (2, 2)\}$
5. $\{(0, 0), (0, 1), (1, 0), (1, 1), (1, 2), (2, 2)\}$
6. $\{(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2), (2, 2)\}$
7. $\{0, 1, 2\}^2$
8. $\emptyset$

Esercizio 4.49. Sia $(X, \leq)$ un preordine.

1. La relazione $E(x, y) \iff x \leq y \wedge y \leq x$ è una relazione d'equivalenza.
2. Sul quoziente X/E , la relazione $\leq_E$ definita da $x/E \leq_E y/E \iff x \leq y$ è ben definita¹¹ ed è un ordine parziale.
3. $(X/E, \leq_E)$ è lineare se e solo se $(X, \leq)$ è lineare.
4. La proiezione al quoziente $\pi_E: X \rightarrow X/E$ è un omomorfismo.

Esercizio 4.50. Il seguente argomento è sbagliato: “ogni relazione transitiva e simmetrica è riflessiva: infatti da $x \sqsubseteq y$ segue $y \sqsubseteq x$ per riflessività, e quindi $x \sqsubseteq y \sqsubseteq x$ dà per transitività che $x \sqsubseteq x$ ”. Infatti, l'enunciato che l'argomento vorrebbe dimostrare è falso. Trovare

1. l'errore nell'argomento, e
2. un controesempio all'enunciato.

Definizione 4.51. Sia R la relazione su $\mathbb{N}$ definita da: $R(x, y)$ sse $\exists z \ x + z = y$. Dire che tipo di relazione è R .

¹¹Ci torniamo più avanti. Per ora ignorate pure questo punto.

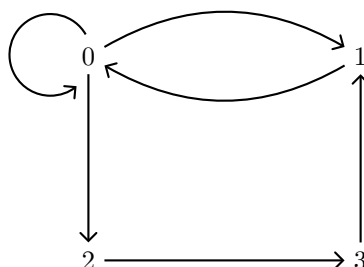


Figura 4.5: Un esempio di digrafo.

Esercizio 4.52. Fissiamo insiemi X, Y e consideriamo l'insieme $\{f: X \rightarrow Z \mid Z \subseteq Y \wedge \text{im}(f) = Z\}$ delle funzioni surgettive da X a un qualche sottoinsieme di Y . Su questo insieme, definiamo $f E g$ sse esiste una bigezione $h: \text{codom}(f) \rightarrow \text{codom}(g)$ tale che $g = h \circ f$. Dimostrare che E è una relazione d'equivalenza.

Suggerimento. Vedi Suggerimento 5. □

Altre classi di relazioni binarie.

Definizione 4.53. Una relazione (X, E) è

1. un *grafo diretto semplice*¹² (o anche solo *digrafo*) sempre,
2. un *grafo diretto semplice senza loop* se è *irriflessiva*, cioè $\forall x \in X \neg(x E x)$,
3. un *grafo semplice* sse è simmetrica,
4. un *grafo semplice senza loop* (o anche solo *grafo*) sse è irriflessiva e simmetrica,
5. un *torneo* sse è irriflessiva e $\forall x, y \in X (x \neq y) \Rightarrow ((x E y) \vee (y E x))$,
6. un *ordine parziale stretto* sse è irriflessiva, transitiva, e *asimmetrica*: $\forall x, y (x E y) \Rightarrow \neg(y E x)$ (notare la differenza con “antisimmetrica”),
7. un *ordine lineare stretto* sse è un ordine parziale stretto e un torneo.

Disegnare le cose come digrafi è, a volte, una buona maniera di rappresentare delle relazioni. Un esempio è in Figura 4.5.

Quando si disegna un grafo, che è simmetrico per definizione, invece di disegnare i due archi nelle due direzioni fra ogni coppia di vertici, se ne disegna uno solo senza frecce. Vedi ad esempio Figura 4.6.

Esercizio 4.54.

1. Trovare un isomorfismo fra il grafi delle Figure 4.5 e 4.7.
2. Quanti isomorfismi ci sono fra quei due grafi?

¹²Il “semplice” sopra vuol dire che da un *vertice* $x \in X$ a un altro vertice $y \in X$ c'è al massimo un *arco* $(x, y) \in E$ (ma ci può essere anche $(y, x) \in E$). Ad esempio, questo è un digrafo semplice. È possibile parlare anche di grafi o digrafi con più archi fra gli stessi vertici, ma vanno codificati in maniera diversa (il grafico di una relazione è un insieme, i suoi elementi ci possono appartenere solo 0 o 1 volta!).

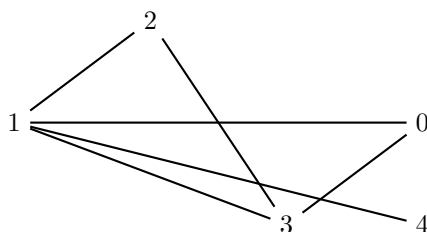


Figura 4.6: Un esempio di grafo.

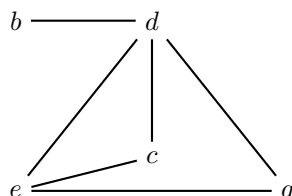


Figura 4.7: Un grafo isomorfo a quello della Figura 4.6.

3. Quanti isomorfismi ci sono da uno di quei due grafi in sé stesso?

Un isomorfismo fra una struttura e sé stessa si chiama *automorfismo*, e può essere pensato come una simmetria della struttura.

Esercizio 4.55.

1. Se $(X, \sqsubseteq)$ è un ordine parziale e definiamo $x \sqsubset y$ sse $(x \sqsubseteq y) \wedge (x \neq y)$, allora $(X, \sqsubset)$ è un ordine parziale stretto.
2. Se $(X, \prec)$ è un ordine parziale stretto e definiamo $x \preceq y$ sse $(x \prec y) \vee (x = y)$, allora $(X, \preceq)$ è un ordine parziale.

Esercizio 4.56. Sia E un torneo su X .

1. Dimostrare che E è un ordine lineare stretto se e solo se non esistono $x, y, z \in X$ tali $x E y$, $y E z$ e $z E x$.
2. Dedurre che, se in un torneo non esistono giocatori x_0, x_1, x_2 tali che x_0 batte x_1 che batte x_2 che batte x_0 , allora per ogni $n \geq 2$ non esistono giocatori $y_0, \dots, y_n$ tali che y_n batte y_0 e per ogni $i < n$ il giocatore y_i batte y_{i+1} .

Esercizio 4.57. La proiezione al quoziente $X \rightarrow X/E$ è un isomorfismo se e solo se E è l'uguaglianza $=$.

Esercizio 4.58. Siano (X, E) e (Y, F) due relazioni di equivalenza. Allora $(X, E) \cong (Y, F)$ se e solo se esistono:

1. una bigezione $f: X/E \rightarrow Y/F$, e
2. per ogni $A \in X/E$, una bigezione $\{x \in X \mid x \in A\} \rightarrow \{y \in Y \mid y \in f(A)\}$.

Capitolo 5

Costruire nuovi numeri

5.1 Voglio poter sottrarre quello che mi pare!

Come dicevamo qualche pagina indietro, l'insieme $\mathbb{N}$ dei numeri naturali lo prendiamo per buono. Prendiamo per buone anche le usuali operazioni $+$ e $\cdot$ su $\mathbb{N}$, la relazione $\leq$, e le loro proprietà di base (associatività, commutatività, distributività di $\cdot$ su $+$) (ma per le curiose c'è la Sezione 5.5). Dati loro però, vediamo come si fa a costruire l'insieme $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ dei numeri interi.

L'idea di base è: in $\mathbb{N}$, “la sottrazione non si può sempre fare”: esistono delle coppie $(a, b) \in \mathbb{N}^2$ tali che $\neg \exists c \in \mathbb{N} \ a = b + c$, per esempio $(0, 1)$, o più in generale tutte le coppie (a, b) con $a < b$. Per avere una struttura più grande di $\mathbb{N}$ dove “la sottrazione si può fare”, un'idea può essere aggiungere a $\mathbb{N}$ un tale c per ogni coppia (a, b) . Per non saper né leggere né scrivere, come c potremmo per esempio prendere proprio la coppia (a, b) è “pensarla” come $a - b$. Il problema è che, facendo così, stiamo aggiungendo troppe cose: per esempio stiamo aggiungendo una “copia” di -1 per la coppia $(0, 1)$ e una per la coppia $(1, 2)$.

L'idea è quindi di identificare tali coppie tramite una relazione di equivalenza: se vogliamo “pensare” la coppia (a, b) come il numero $a - b$ allora dobbiamo “pensare” che (a, b) e (c, d) siano uguali quando $a - b = c - d$. Quest'idea l'avete già vista a scuola con le frazioni, dove $\frac{1}{2}$ e $\frac{2}{4}$ sono lo stesso numero (ci torniamo). Ora, $a - b$ e $c - d$ però appunto “non si possono fare” e quindi scrivere $a - b = c - d$ non ha ancora senso. Ma basta spostare le cose:

Lemma 5.1. La relazione $\sim$ su $\mathbb{N}^2$ definita da $(a, b) \sim (c, d) \iff a + d = c + b$ è una relazione d'equivalenza.

Dimostrazione. Controllare la riflessività vuol dire controllare che $a + b = a + b$ e ci siamo. La simmetria segue dalla commutatività del $+$. Per la transitività, se $(a, b) \sim (c, d)$ e $(c, d) \sim (e, f)$ allora $a + d = c + b$ e $c + f = e + d$, e dobbiamo dimostrare che $(a, b) \sim (e, f)$, cioè $a + f = e + b$. Sommando membro a membro le uguaglianze date dalle ipotesi otteniamo

$$a + d + c + f = c + b + e + d$$

che per commutatività è equivalente a $a + f + c + d = e + b + c + d$. Concludiamo usando il fatto che, nei numeri naturali è vero che $\forall x, y, z (x + z = y + z \Rightarrow x = y)$ (esercizio, vedi Suggerimento 8). $\square$

Definizione 5.2. L'insieme $\mathbb{Z}$ dei *numeri interi* è il quoziente di $\mathbb{N}^2$ per la relazione d'equivalenza $(a, b) \sim (c, d) \iff a + d = c + b$.

Ci sono ancora delle cose da fare:

1. Questo è un quoziente di $\mathbb{N}^2$, ma avevamo detto che volevamo qualcosa che contenesse $\mathbb{N}$.
2. Poi dobbiamo definire $+$, $\cdot$, $\leq$ su $\mathbb{Z}$ in qualche maniera.
3. Dobbiamo far vedere che effettivamente in $\mathbb{Z}$ “la sottrazione si può sempre fare”.

Per fare queste cose iniziamo a fissare un po' di notazione. Un elemento di $\mathbb{Z}$ è la classe di equivalenza di qualche (a, b) . Per il momento, denotiamolo come $[(a, b)]$. Notiamo che la coppia (a, b) non è unica (di nuovo, esattamente come ci sono frazioni diverse che rappresentano lo stesso numero), perché la classe di equivalenza $[(a, b)]$ ha più di un elemento: ad esempio, $[(a, b)] = [(a + 1, b + 1)]$.

Per il punto 1, la soluzione è trovare una “copia” sensata di $\mathbb{N}$ in $\mathbb{Z}$ e *identificare* $\mathbb{N}$ con questa copia. Questo è facile: basta definire la funzione $\mathbb{N} \rightarrow \mathbb{Z}$ che manda $n \mapsto [(n, 0)]$, seguendo l'idea intuitiva che $[(a, b)]$ dovrebbe essere $a - b$. Notiamo che questa funzione è iniettiva, perché

$$[(n, 0)] = [(m, 0)] \iff (n, 0) \sim (m, 0) \iff n + 0 = m + 0 \iff n = m$$

e ha quindi senso pensare all'immagine di questa funzione come a una copia di $\mathbb{N}$. Diciamo che *identifichiamo* $\mathbb{N}$ con la sua immagine tramite questa funzione per dire che ora se parliamo di $\mathbb{N}$ stiamo in realtà pensando a questa immagine, per cui per esempio possiamo scrivere $\mathbb{N} \subseteq \mathbb{Z}$. In realtà, a volte ci riferiremo ancora al “vecchio” $\mathbb{N}$; ad esempio quando stiamo scrivendo qualche elemento di $\mathbb{Z}$ come $[(a, b)]$, pensiamo ad a, b come elementi del vecchio $\mathbb{N}$.

Vediamo ora come definire $+$ su $\mathbb{Z}$. Notiamo che vogliamo una definizione compatibile con il $+$ che la copia di $\mathbb{N}$ che abbiamo trovato in $\mathbb{Z}$ “si porta appresso”. Se $[(a, b)]$ deve stare per $a - b$, perché le cose tornino dobbiamo avere che $(a - b) + (c - d) = (a + c) - (b + d)$. Tendendo questo a mente, diamo la seguente

Definizione 5.3. La *somma* $+$ su $\mathbb{Z}$ è definita da

$$[(a, b)] + [(c, d)] = [(a + c, b + d)]$$

C'è però un problema: la definizione sopra, a guardarla molto attentamente *potrebbe non avere senso* e bisogna assicurarsi che questo non succeda, cioè che sia una *buona definizione*.

Il problema in sostanza è il seguente. Supponiamo che vi dica “diciamo che un numero razionale a/b è *bello* sse il suo numeratore a è pari”. Da questa definizione seguirebbe che $1/2$ non è bello, ma che $2/4$ è bello. Chiaramente, questo non ha senso, perché $1/2$ e $2/4$ sono due nomi per lo stesso numero.

Il problema è che la “definizione” che ho dato *non* è una *buona definizione*: per definirvi una proprietà di un elemento $[x]$ di un quoziente—quindi, di una

classe di equivalenza—ho usato una proprietà di un suo specifico *rappresentante* (cioè elemento) x , *ma questa proprietà è vera su alcuni rappresentanti e falsa su altri*. Insomma, se definisco una proprietà di $[x]$ in termini di una proprietà di x , perché le cose abbiano senso, se $[x] = [y]$ allora questa proprietà deve valere per x se e solo se vale per y . Questa proprietà deve *passare al quoziente*. Stessa cosa per le funzioni: ad esempio, probabilmente alle superiori vi hanno definito l'esponenziazione con esponenti razionali come $a^{\frac{b}{c}} := \sqrt[c]{a^b}$, ma vi hanno detto che questo ha senso solo per $a \geq 0$. Il motivo è, che per esempio, $1/3 = 2/6$. Ma quindi $(-1)^{\frac{1}{3}} = (-1)^{\frac{2}{6}}$ dovrebbe fare $\sqrt[3]{-1} = -1$ oppure $\sqrt[6]{(-1)^2} = 1$?

Tornando agli interi, nella Definizione 5.3 abbiamo definito la somma di $[(a, b)]$ e $[(c, d)]$ usando a, b, c, d . Ma chi mi dice che se cambio (a, b) con una coppia equivalente, e (c, d) con una coppia equivalente, il risultato è lo stesso? Beh, dimostriamolo.

Lemma 5.4. La Definizione 5.3 è una buona definizione, cioè non dipende dalla scelta di rappresentanti (a, b) e (c, d) per le classi di equivalenza $[(a, b)]$ e $[(c, d)]$ rispettivamente.

Dimostrazione. Dobbiamo dimostrare che, se $(a, b) \sim (a', b')$ e $(c, d) \sim (c', d')$, allora $[(a + c, b + d)] = [(a' + c', b' + d')]$, cioè $(a + c, b + d) \sim (a' + c', b' + d')$. Per definizione di $\sim$, abbiamo $a + b' = b + a'$ e $c + d' = d + c'$. Ma allora

$$a + c + b' + d' = (a + b') + (c + d') = (b + a') + (d + c') = a' + c' + b + d$$

che per definizione vuol dire che $(a + c, b + d) \sim (a' + c', b' + d')$. $\square$

Esercizio 5.5. Dimostrare che la somma appena definita su $\mathbb{Z}$ è associativa e commutativa, e che $\forall x \in \mathbb{Z} \ x + 0 = x$.

Ora, avevamo detto che identifichiamo $\mathbb{N}$ con un certo sottoinsieme di $\mathbb{Z}$. Abbiamo fatto questo per trovare un'estensione di $\mathbb{N}$ dove la somma avesse certe proprietà. Per non barare, dobbiamo vedere che il $+$ sulla copia di $\mathbb{N}$ che abbiamo trovato dentro $\mathbb{Z}$ “funziona come” il solito $+$ su $\mathbb{N}$. Questo è facile, ma approfittiamone per introdurre della terminologia. Che in realtà abbiamo già introdotto: come si può parlare di omomorfismi fra strutture con relazioni, si può parlare di omomorfismi fra strutture con operazioni.

Definizione 5.6. Siano $(M, +_M)$ e $(N, +_N)$ due strutture nel linguaggio con una singola operazione binaria $+$. Una funzione $f: M \rightarrow N$ è un *omomorfismo* sse

$$\forall a, b \in M \ f(a +_M b) = f(a) +_N f(b)$$

In altre parole dire che f è un omomorfismo vuol dire che: non importa se

- prima sommiamo a e b dentro M e poi gli applichiamo f , oppure
- prima applichiamo f ad a e b poi sommiamo i risultati dentro N ,

il risultato è lo stesso.

Osservazione 5.7. In questo caso, un omomorfismo iniettivo è automaticamente un embedding, nel senso che se la formula $a + b = c$ è vera in arrivo (cioè $f(a) + f(b) = f(c)$) allora è vera anche in partenza (cioè $a + b = c$) (esercizio).

Osservazione 5.8. La funzione $n \mapsto [(n, 0)]$ definita sopra non solo è iniettiva, ma è anche un omomorfismo per il $+$. Infatti, scrivendo $+\mathbb{N}$ e $+\mathbb{Z}$ per distinguere l'operazione $+$ di $\mathbb{N}$ data da quella su $\mathbb{Z}$ appena costruita,

$$[(n +_{\mathbb{N}} m, 0)] = [(n, 0)] +_{\mathbb{Z}} [(m, 0)]$$

Quindi effettivamente non stiamo barando, e abbiamo costruito una struttura più grande di $(\mathbb{N}, +)$ con un'estensione del $+$. Vediamo ora che in questa struttura “la sottrazione si può fare”.

Proposizione 5.9. Per ogni $x \in \mathbb{Z}$ esiste $y \in \mathbb{Z}$ tale che $x + y = 0$. Inoltre, tale y è unico.

Dimostrazione. Per dimostrare l'esistenza, prendiamo $x \in \mathbb{Z}$ e, scegliendo un rappresentante, scriviamolo come $x = [(a, b)]$. Definiamo $y := [(b, a)]$. Allora

$$x + y = [(a, b)] + [(b, a)] = [(a + b, b + a)] = [(0, 0)]$$

come desiderato.

Per dimostrare l'unicità, supponiamo che y' sia tale che $x + y' = 0$. Allora, sommando y a entrambi i membri, troviamo $y + x + y' = y$, e dato che $y + x = 0$ abbiamo $y' = y$. $\square$

Notazione 5.10. Per $x \in \mathbb{Z}$, l'unico $y \in \mathbb{Z}$ tale che $x + y = 0$ si denota con $-x$. Scriviamo $x - y$ come abbreviazione per $x + (-y)$.

Quindi $\mathbb{Z}$ effettivamente è un'estensione di $\mathbb{N}$ dove ogni elemento ha un inverso additivo. Ma convinciamoci del fatto che, come promesso, abbiamo $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$.

Lemma 5.11. Per ogni $x \in \mathbb{Z}$ abbiamo $-(-x) = x$.

Dimostrazione. La conclusione vuol dire che l'inverso additivo di $-x$ è x , cioè che se aggiungiamo x a $-x$ otteniamo 0. Ma questo è vero per definizione di $-x$. $\square$

Proposizione 5.12. Se $x \in \mathbb{Z} \setminus \{0\}$, allora esattamente uno fra x e $-x$ è in $\mathbb{N}$.

Dimostrazione. Se x e $-x$ sono entrambi in $\mathbb{N}$, allora abbiamo un elemento di $\mathbb{N}$ con un inverso additivo. In $\mathbb{N}$, l'unico tale elemento è 0.

Vediamo ora che almeno uno vi appartiene. Se $x = [(a, b)]$ allora $-x = [(b, a)]$. Dire che $[(a, b)]$ è in $\mathbb{N} \subseteq \mathbb{Z}$ vuol dire che esiste $n \in \mathbb{N}$ (nella “copia” originale, non in quella in $\mathbb{Z}$) tale che $[(a, b)] = [(n, 0)]$, cioè tale che $a + 0 = b + n$. Abbiamo tre casi. Se $a > b$, un tale n esiste. Se invece $a < b$, allora esiste n tale che $a + n = b + 0$, e quindi $[(b, a)] \in \mathbb{N}$. E se $a = b$ allora $[(a, b)] = 0$ e non c'è niente da dimostrare. $\square$

Definizione 5.13. Definiamo la relazione $\leq$ su $\mathbb{Z}$ come: $x \leq y$ sse $y - x \in \mathbb{N}$.

Esercizio 5.14. Dimostrare che:

1. $(\mathbb{Z}, \leq)$ è un ordine lineare.
2. $\forall x, y, z \in \mathbb{Z} (x \leq y) \Rightarrow (x + z) \leq (y + z)$.

Le stesse cose che abbiamo fatto per la somma le possiamo fare anche per il prodotto. Teniamo in mente che pensiamo a $[(a, b)]$ come ad $a - b$. Pensando a cosa succede calcolando $(a - b)(c - d)$, diamo la seguente

Definizione 5.15. Siano $x = [(a, b)]$ e $y = [(c, d)]$ numeri interi. Il *prodotto* $x \cdot y$, o anche xy , è il numero intero $[(ac + bd, bc + ad)]$.

Esercizio 5.16. Dimostrare che:

1. La Definizione 5.15 è una buona definizione.
2. Il prodotto appena definito su $\mathbb{Z}$ è associativo e commutativo, e $\forall x \in \mathbb{Z} \ x \cdot 1 = x$.
3. In $\mathbb{Z}$, il prodotto distribuisce sulla somma.
4. Se $a \geq 0$ e $b \geq 0$ allora $ab \geq 0$.

Complimenti, mettendo insieme tutte le proprietà di $+, \cdot, \leq$ che abbiamo visto, avete dimostrato che $(\mathbb{Z}, +, \cdot, \leq)$ è un *anello ordinato commutativo con unità*. Ci torneremo più avanti.

Esercizio 5.17. Dimostrare le seguenti.

1. Il $\cdot$ su $\mathbb{Z}$ estende quello su $\mathbb{N}$. In altre parole, l'inclusione $\mathbb{N} \rightarrow \mathbb{Z}$ è un omomorfismo anche per il prodotto (e quindi un embedding, dato che è iniettiva).
2. Il $\leq$ su $\mathbb{Z}$ estende quello su $\mathbb{N}$. In altre parole, l'inclusione $\mathbb{N} \rightarrow \mathbb{Z}$ è un embedding di ordini lineari.

Già che ci siamo, dimostriamo anche la cosiddetta “regola dei segni”. Dove con “dimostriamo” intendo “dimostrate”.

Esercizio 5.18. Dimostrare che, per ogni $a, b \in \mathbb{Z}$, abbiamo $(-a) \cdot b = -(a \cdot b)$ e $(-a) \cdot (-b) = ab$.

Suggerimento. Vedi Suggerimento 7. □

5.2 Voglio poter dividere per quello che mi pare!

Beh, per zero no.

Ma a parte quello, in $\mathbb{Z}$ non esiste nessun x tale che $x \cdot 2 = 1$, e vorremmo passare a una struttura dove invece un tale x esiste (non solo per 2). Come sapete dalle scuole elementari, la soluzione è “fare le frazioni”.

Notoriamente, il denominatore di una frazione non può essere zero, alcune frazioni denotano lo stesso numero, e le frazioni si sommano e moltiplicano in una certa maniera. Ma facciamo le cose per bene. O meglio, fate, dato che questa sezione sarà sostanzialmente un lungo esercizio guidato.

Rappresentiamo le frazioni usando le coppie ordinate, dove la prima coordinata è il numeratore e la seconda è il denominatore.

Definizione 5.19. L'insieme $\mathbb{Q}$ dei *numeri razionali* è il quoziente di $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ per la relazione d'equivalenza definita da

$$(a, b) \sim (c, d) \iff ad = cb$$

Equipaggiamo $\mathbb{Q}$ con le operazioni $+$ e $\cdot$, e la relazione $\leq$, definite come segue.

$$\begin{aligned} [(a, b)] + [(c, d)] &:= [(ad + bc, bd)] \\ [(a, b)] \cdot [(c, d)] &:= [(ac, bd)] \\ [(a, b)] \leq [(c, d)] &\iff (bc - ad)bd \geq 0 \end{aligned}$$

Abbiamo fatto le cose davvero per bene? Non ancora. Abbiamo preso per buone un po' di proprietà, che vanno dimostrate. Le idee per fare queste dimostrazioni sono simili a quelle usate per fare le analoghe verifiche che abbiamo fatto per $\mathbb{Z}$, e le lascio a voi nel prossimo esercizio.

Come sapete dalle elementari, la classe di equivalenza $[(a, b)]$ si denota a/b , o $\frac{a}{b}$. Sentitevi libere di usare questa notazione già nell'esercizio (o di non farlo se la cosa vi crea confusione). In ogni caso, dopo l'esercizio la useremo liberamente.

Esercizio 5.20. Dimostrare che, nella Definizione 5.19:

1. La $\sim$ è una relazione d'equivalenza.
2. Il $+$ è ben definito.
3. Il $\cdot$ è ben definito.
4. Il $\leq$ è ben definito, cioè se $[(a', b')] \sim [(a, b)]$ e $[(c', d')] \sim [(c, d)]$ allora $(bc - ad)bd \geq 0$ se e solo se $(b'c' - a'd')b'd' \geq 0$.

Inoltre, è bene verificare che le usuali proprietà di $+$, $\cdot$, $\leq$ valgano, che effettivamente in $\mathbb{Q}$ “la divisione si può fare”, e che $\mathbb{Z}$ si embedda in $\mathbb{Q}$ come ci aspettiamo. Anche queste verifiche sono un buon esercizio.

Definizione 5.21. Indichiamo l'elemento $\frac{0}{1} \in \mathbb{Q}$ con 0 , e l'elemento $\frac{1}{1} \in \mathbb{Q}$ con 1 . Inoltre, definiamo la funzione $-: \mathbb{Q} \rightarrow \mathbb{Q}$ come $-(\frac{a}{b}) := \frac{-a}{b}$.

Esercizio 5.22. Dimostrare che in $\mathbb{Q}$ valgono le seguenti.

1. Il $+$ è associativo.
2. Lo 0 è l'*elemento neutro* per la somma, cioè $\forall a \in \mathbb{Q} (a + 0 = a = 0 + a)$.
3. La funzione $-$ restituisce l'*inverso additivo* del suo argomento, cioè $\forall a \in \mathbb{Q} (a + (-a) = 0 = (-a) + a)$.
4. Il $+$ è commutativo.

Complimenti, avete dimostrato che $(\mathbb{Q}, +, 0, -)$ è un *gruppo abeliano*.¹

5. Il $\cdot$ distribuisce sul $+$.
6. Il $\cdot$ è associativo.

¹Se avete fatto i punti nell'ordine dato e vi siete fermati prima, quello che avete portato a casa è, nell'ordine, un *semigrupp*o, un *monoide*, o un *gruppo*.

7. L'1 è l'elemento neutro per il prodotto (sotto-esercizio: capire cosa vuol dire prendendo ispirazione dalla somma).
8. Il $\cdot$ è commutativo.
9. Se $\frac{a}{b} \in \mathbb{Q} \setminus \{0\}$, allora $\frac{b}{a}$ è l'inverso moltiplicativo di $\frac{a}{b}$ (sotto-esercizio: capire cosa vuol dire prendendo ispirazione dalla somma).

Complimenti, avete dimostrato che $(\mathbb{Q}, +, 0, -, \cdot, 1)$ è un *campo*.²

10. $\leq$ è un ordine lineare.
11. $\forall x, y, z \in \mathbb{Q} (x \leq y) \Rightarrow (x + z) \leq (y + z)$.
12. $\forall x, y \in \mathbb{Q} ((x \geq 0) \wedge (y \geq 0)) \Rightarrow (x \cdot y \geq 0)$.

Complimenti, avete dimostrato che $(\mathbb{Q}, +, 0, -, \cdot, 1, \leq)$ è un *campo ordinato*.

Le seguenti proprietà si possono dimostrare come corollario delle precedenti.³

Esercizio 5.23.

1. Dimostrare che l'elemento neutro della somma è unico, cioè che se $0_{\spadesuit}$ è tale che $a + 0_{\spadesuit} = a = 0_{\spadesuit} + a$ allora $0_{\spadesuit} = 0$.
2. Dimostrare che l'inverso additivo è unico, cioè che, per ogni a , se b e c sono tali che $a + b = 0 = b + a$ e $a + c = 0 = c + a$ allora $c = b$.
3. Dimostrare le cose analoghe per il prodotto invece della somma (e 1 invece di 0, e $\frac{1}{a}$ invece di $-a$, ovviamente) su $\mathbb{Q} \setminus \{0\}$.
4. Dimostrare che per ogni $a \in \mathbb{Q}$ si ha $a \cdot 0 = 0$. (Vedi Suggerimento 9)
5. Dimostrare che 0 non ha un inverso moltiplicativo.

Esercizio 5.24. Dimostrare che la mappa $\mathbb{Z} \rightarrow \mathbb{Q}$ definita da $a \mapsto \frac{a}{1}$ è un embedding per il $+$, per il $\cdot$ e per il $\leq$.

Come avevamo identificato $\mathbb{N}$ con un sottoinsieme di $\mathbb{Z}$, possiamo quindi identificare $\mathbb{Z}$ con un sottoinsieme di $\mathbb{Q}$ (e quindi, di conseguenza, anche $\mathbb{N}$ con un sottoinsieme di $\mathbb{Q}$, componendo le due identificazioni).

Esercizio 5.25. Per ogni $a, b \in \mathbb{Q}$, se $ab = 0$ allora $a = 0$ oppure $b = 0$.

Suggerimento. Vedi Suggerimento 10. □

Gli elementi di una classe di equivalenza sono, per definizione, tutti equivalenti, ma per alcune relazioni d'equivalenza può accadere che alcuni siano "più equivalenti degli altri". Per esempio, $\frac{3}{2} = \frac{6}{4}$, ma a scuola avete imparato a "ridurre le frazioni ai minimi termini", che sostanzialmente vuol dire trovare un *rappresentante canonico* per la classe di equivalenza, sostanzialmente un elemento "più bello degli altri". Non è infrequente ragionare per rappresentanti canonici: d'altra parte pensare a "quel numero che se lo moltiplichi per 2 fa 3"

²Qui il bottino parziale per chi si è fermata al punto 6 è un *anello*, e i punti dopo fanno guadagnare un *anello con unità* e un *anello commutativo con unità*.

³E usano solo loro, non usano davvero che stiamo lavorando su $\mathbb{Q}$. Ci torniamo.

è più facile di pensare a “l’insieme di tutte le coppie ordinate (a, b) di interi tali che il doppio di a è il triplo di b ”.

Ragionare così non è necessariamente sbagliato, ma bisogna stare attenti a non dare accidentalmente cose che non sono buone definizioni. In altre parole, bisogna stare attenti a non dimenticarsi che lo stesso numero può essere rappresentato in più modi, e che se usiamo una rappresentazione di un numero per definire qualcosa bisogna controllare che, se scegliamo un’altra rappresentazione per lo stesso numero, la definizione che stiamo dando non cambia.

5.3 Voglio dividere e tenermi il resto!

Più avanti lavoreremo parecchio in $\mathbb{Z}$. Iniziamo a tornarci brevemente per dimostrare una sua proprietà fondamentale, che sostanzialmente conoscete già dalle elementari. Ancora prima di introdurre $\mathbb{Q}$, in $\mathbb{Z}$ avremmo potuto “fare la divisione” tenendoci però un *resto*. Per dimostrare questa cosa, usiamo una variante del principio di induzione.

Teorema 5.26 (Principio di induzione forte). Sia $A \subseteq \mathbb{N}$. Se A soddisfa

$$0 \in A \wedge \forall n \in \mathbb{N} ((\forall x \leq n (x \in A)) \Rightarrow n + 1 \in A)$$

allora $A = \mathbb{N}$.

La differenza col principio di induzione già visto è che, nell’usare il principio di induzione, nel passo induttivo potevamo assumere solo $n \in A$. Qui invece possiamo assumere che tutti i numeri fino ad n sono in A , che in alcune dimostrazioni torna comodo.

Notiamo che il principio di induzione forte implica il principio di induzione (esercizio), e qui stiamo dicendo che vale l’altra implicazione. Quindi, a dispetto del nome, i due principi sono equivalenti, e l’induzione forte è solo apparentemente più forte.

Dimostrazione. Dato un insieme A , sia B l’insieme

$$B := \{n \in \mathbb{N} \mid \forall x \leq n (x \in A)\}$$

Dato che il principio di induzione vale per tutti i sottoinsiemi di $\mathbb{N}$, vale anche per B , quindi abbiamo

$$(0 \in B \wedge \forall n \in \mathbb{N} (n \in B \Rightarrow n + 1 \in B)) \Rightarrow \forall n \in \mathbb{N} (n \in B)$$

che, usando la definizione di B , vuol dire che

$$\begin{aligned} \left((\forall x \leq 0 (x \in A) \wedge \forall n \in \mathbb{N} ((\forall x \leq n (x \in A)) \Rightarrow (\forall x \leq n + 1 (x \in A)))) \right) \\ \Rightarrow \forall n \in \mathbb{N} \forall x \leq n (x \in A) \end{aligned} \quad (5.1)$$

Ma l’unico $x \leq 0$ è 0, quindi $\forall x \leq 0 (x \in A)$ è equivalente a $0 \in A$. Inoltre

$$(\forall x \leq n (x \in A)) \Rightarrow (\forall x \leq n + 1 (x \in A))$$

è equivalente a

$$(\forall x \leq n (x \in A)) \Rightarrow n + 1 \in A$$

perché se già sappiamo che tutti i numeri fino a n sono in A , allora dire che $n+1$ è in A o dire che tutti i numeri fino a $n+1$ sono in A è la stessa cosa. Infine, la formula $\forall n \in \mathbb{N} \forall x \leq n (x \in A)$ dice che, per ogni $n \in \mathbb{N}$, tutti i numeri fino a n sono in A . Ma dato che lo stiamo dicendo per ogni n , e che non importa quante volte diciamo che un numero sta in A , questa è la stessa cosa che dire $\forall n \in \mathbb{N} (n \in A)$. Usando queste tre cose scopriamo che la (5.1) è equivalente a

$$\left(0 \in A \wedge \forall n \in \mathbb{N} ((\forall x \leq n (x \in A)) \Rightarrow (n+1 \in A))\right) \Rightarrow \forall n \in \mathbb{N} (n \in A)$$

e abbiamo la conclusione. $\square$

La variante del principio di induzione che ci serve è un'altra (che però dimostreremo usando quella sopra), che usa il concetto di *minimo*.

Definizione 5.27. Sia $(P, \sqsubseteq)$ un poset. Un elemento $m \in P$ è

1. il *minimo* di P sse $\forall p \in P (m \sqsubseteq p)$, ed è
2. il *massimo* di P sse $\forall p \in P (m \sqsupseteq p)$.

Osservazione 5.28.

1. Un poset non ha necessariamente un minimo, né necessariamente un massimo. Ad esempio, $(\mathbb{N}, \leq)$ ha minimo ma non ha massimo, $(\mathbb{N}, \geq)$ (quindi $\mathbb{N}$ con l'ordine al contrario) ha massimo ma non ha minimo, e $\mathbb{Z}$ non ha nessuno dei due.
2. Però, se un minimo esiste allora è unico, e se un massimo esiste allora è unico (esercizio).
3. Se $(P, \sqsubseteq)$ è un poset e $A \subseteq P$, allora A ha una struttura di poset “ereditata” da P , il cui grafico è la *restrizione* $\Gamma_{\sqsubseteq} \cap A \times A$. In particolare ha senso parlare del minimo e del massimo di un sottoinsieme. Questi possono tranquillamente non esistere, anche se P ce li ha: ad esempio, se P è $\{x \in \mathbb{Q} \mid 0 \leq x \leq 1\}$, questo ha sia massimo che minimo, ma il suo sottoinsieme $\{x \in \mathbb{Q} \mid 0 < x < 1\}$ non ha nessuno dei due.
4. Se però m è il minimo di P , e $m \in A \subseteq P$, allora m è il minimo di A (esercizio). Analogamente con “minimo” sostituito da “massimo”.
5. Al contrario, può succedere che un poset P non abbia minimo ma un suo sottoinsieme sì, e idem per il massimo. Per esempio, basta prendere $(\mathbb{Q}, \leq)$ e il suo sottoinsieme $\{x \in \mathbb{Q} \mid 0 \leq x \leq 1\}$, o più banalmente $\{0\} \subseteq \mathbb{Q}$.

Teorema 5.29 (Principio del minimo). L'ordine lineare $(\mathbb{N}, \leq)$ è un *buon ordine*, cioè ogni sottoinsieme non vuoto di $\mathbb{N}$ ha un minimo.

Dimostrazione. Sia $B \subseteq \mathbb{N}$ un sottoinsieme di $\mathbb{N}$ che non ha minimo. Dobbiamo mostrare che $B = \emptyset$.

Per farlo, usiamo il principio di induzione forte per far vedere che $\forall n \in \mathbb{N} (n \notin B)$ (se volete, stiamo applicando il Teorema 5.26 ad $A := B^c$). Dato che 0 è il minimo di $\mathbb{N}$, abbiamo $0 \notin B$, perché altrimenti 0 sarebbe il minimo di B , che stiamo supponendo non esistere. Se ora $\forall x \leq n (n \notin B)$, allora anche $n+1 \notin B$, perché altrimenti $n+1$ sarebbe il minimo di B . $\square$

Definizione 5.30. La funzione *valore assoluto* $|\cdot|: \mathbb{Q} \rightarrow \mathbb{Q}$ è definita da

$$|a| := \begin{cases} a & \text{se } a \geq 0 \\ -a & \text{se } a < 0 \end{cases}$$

Teorema 5.31 (Divisione euclidea). Siano $a, b \in \mathbb{Z}$ con $b \neq 0$. Allora esiste un'unica coppia $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tale che $r < |b|$ e $a = bq + r$.

Dimostrazione. Dimostriamo prima l'unicità. Supponiamo che

$$bq' + r' = a = bq + r$$

con $r < |b|$ e $r' < |b|$. Allora $b(q' - q) = r - r'$. Il LHS $b(q' - q)$ è un multiplo di b , e dato che è uguale a $r - r'$ anche questo è un multiplo di b . Ma da $0 \leq r < |b|$ e $0 \leq r' < |b|$ segue che $-b < r - r' < b$, e l'unico multiplo di b che soddisfa queste disuguaglianze è 0. Quindi $r = r'$, per cui $b(q' - q) = 0$ e siccome $b \neq 0$ ne segue che $q' = q$.

Per dimostrare l'esistenza, quello che facciamo è in sostanza osservare che l'algoritmo per la divisione che avete imparato a scuola termina sempre. Dato che se $a = qb + r$ allora $a = (-q)(-b) + r$ (per l'Esercizio 5.18), il caso generale segue dal caso $b > 0$, e quindi possiamo assumere che $b > 0$ senza perdita di generalità.

Iniziamo notando che esistono $q_0 \in \mathbb{Z}$ e $r_0 \in \mathbb{N}$ tali che $a = q_0b + r_0$ (senza la richiesta $r_0 < |b|$); questo è vero perché se $a \geq 0$ basta prendere $q_0 = 0$ e $r = a$, e se $a < 0$ basta prendere $q_0 = a$ e $r_0 = a(1 - b)$, che appartiene a $\mathbb{N}$ (cioè, è non negativo) perché stiamo assumendo $a < 0$ e $b > 0$ (e quindi $b \geq 1$ perché $b \in \mathbb{Z}$, e quindi $1 - b \leq 0$, e applichiamo l'Esercizio 5.22.12).

Quindi una qualche coppia $(q', r') \in \mathbb{Z} \times \mathbb{N}$ tale che $a = bq' + r'$ esiste. In altre parole, l'insieme $\{r' \in \mathbb{N} \mid \exists q' \in \mathbb{Z} \ a = bq' + r'\}$ è non vuoto. Quindi, per il Teorema 5.29, ha un minimo. Concludiamo facendo vedere che, se r è il minimo di questo insieme, allora $r < |b|$, che è la stessa cosa di $r < b$ perché stiamo assumendo $b > 0$. Infatti, se così non fosse, potremmo scrivere $r = b + r'$ per qualche $r' \in \mathbb{N}$. Ma allora da $a = qb + r = qb + b + r'$ segue che $a = (q+1)b + r'$, quindi $((q+1), r')$ è un'altra coppia come sopra ma con $r' < r$ (dato che $r - r' = b \in \mathbb{N}$), contro la minimalità di r . $\square$

Notazione 5.32. Se a, b, q, r sono come nel teorema precedente, q ed r si chiamano rispettivamente il *quoziente* e il *resto* della divisione di a per b .

Questo è un buon punto per lasciarvi un esercizio (e il Suggerimento 11).

Esercizio 5.33. Dimostrare che $(\mathbb{N}, 0, s)$ è l'unica struttura che soddisfa gli assiomi di Peano a meno di isomorfismo, cioè che se $(M, 0_M, s_M)$ è un'altra struttura che li soddisfa allora esiste una bigezione $f: M \rightarrow \mathbb{N}$ tale che $f \circ s_M = s \circ f$ (cioè $\forall m \in M \ f(s_M(n)) = s(f(n))$).

E già che ci siamo:

Esercizio 5.34. Dimostrare che $\{x \in \mathbb{Q} \mid 0 \leq x \leq 1\}$ non è un buon ordine.

5.4 Voglio fare i conti sull'orologio!

Sono le 3 di notte e, in preda all'insonnia, guardo l'orologio e mi chiedo che ora sarà fra 123489761235789451393761952 ore (non mi interessa di che giorno). Il conto da fare non è particolarmente mostruoso: ogni 24 ore saranno di nuovo le 3 di notte, e dato che non interessa sapere che giorno sarà, mi basta sapere qual è il resto della divisione di $3 + 123489761235789451393761952$ per 24.

Insonnia a parte, quest'idea di fare i conti con i resti è molto più potente di quanto possa sembrare a prima vista,⁴ e si merita delle strutture tutte sue.

Definizione 5.35. Sia $n \in \mathbb{N} \setminus \{0\}$. Definiamo $\mathbb{Z}/n\mathbb{Z}$ (“zeta modulo ennezeta”) come il quoziente di $\mathbb{Z}$ per la relazione d'equivalenza $x - y \in n\mathbb{Z}$, cioè $\exists k \in \mathbb{Z} \ x - y = nk$. Equipaggiamo $\mathbb{Z}/n\mathbb{Z}$ con le operazioni

$$\begin{aligned}[a] + [b] &:= [a + b] \\ [a] \cdot [b] &:= [ab]\end{aligned}$$

Notazione 5.36. 1. La relazione d'equivalenza sopra si denota anche con $x \equiv y \pmod{n}$, o $x \equiv_n y$, e le sue classi di equivalenza sono chiamate *classi di resto*. Sì, è la stessa relazione dell'Esempio 4.3.2 ma definita in maniera diversa (esercizio; vedi Suggerimento 14).

2. Un'altra notazione⁵ per $\mathbb{Z}/n\mathbb{Z}$ è $\mathbb{Z}_n$.

3. Il resto della divisione di a per n (se volete, il rappresentante canonico della sua classe d'equivalenza) a volte si denota con $a \bmod n$.

Esercizio 5.37. Dimostrare

1. che quella sopra è effettivamente una relazione d'equivalenza,
2. che le operazioni $+$ e $\cdot$ su $\mathbb{Z}/n\mathbb{Z}$ sono ben definite, e
3. che la proiezione al quoziente $\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ è un omomorfismo sia per il $+$ che per il $\cdot$.

Soluzione parziale. Mostriamo che il $+$ è ben definito. Supponiamo che $a \equiv c \pmod{n}$ e che $b \equiv d \pmod{n}$. Per definizione, esistono $k, \ell \in \mathbb{Z}$ tali che $a - c = kn$ e $b - d = \ell n$. Ma allora $a + b - (c + d) = kn + \ell n = (k + \ell)n$ e quindi $a + b \equiv c + d \pmod{n}$. $\square$

Torneremo su queste strutture più avanti. Ma come prima applicazione, vediamo come usarle per dimostrare qualcosa che forse avete visto a scuola.

Proposizione 5.38. Un numero $n \in \mathbb{N}$ è divisibile per 3 se e solo se, quando scritto in base 10, la somma delle sue cifre è divisibile per 3.

In matematica a volte succede una cosa buffa: è più facile dimostrare una cosa più forte, da cui l'obiettivo originale segue come corollario. Questo è uno di quei casi. Dimostriamo quindi la seguente proposizione, di cui la precedente è il caso particolare dove la classe di congruenza è quella di 0.

⁴Ad esempio, ci si fanno protocolli crittografici come RSA.

⁵... che all'autore di queste note non piace perché ha anche un altro significato...

Proposizione 5.39. Per calcolare la classe di resto modulo 3 di un arbitrario $n \in \mathbb{N}$ basta scriverlo in base 10, calcolare le classi di resto delle cifre di questa scrittura, e sommarle (in $\mathbb{Z}/3\mathbb{Z}$).

Dimostrazione. Scrivere un numero n in base 10 vuol dire trovare dei numeri naturali $a_0, \dots, a_k$ tutti fra 0 e 9 tali che

$$n = \sum_{i=0}^k a_i 10^i$$

Consideriamo la proiezione al quoziente $\mathbb{Z} \rightarrow \mathbb{Z}/3\mathbb{Z}$. Per l'Esercizio 5.37 questa è un omomorfismo. Da $[cd] = [c][d]$ segue per induzione che⁶ $[c^i] = [c]^i$, e quindi

$$[n] = \left[\sum_{i=0}^k a_i 10^i \right] = \sum_{i=0}^k [a_i][10]^i$$

dove la somma più a sinistra è calcolata in $\mathbb{N}$ (o in $\mathbb{Z}$) e quella a destra in $\mathbb{Z}/3\mathbb{Z}$. Ora, $10 = 9 + 1$ e quindi $[10] = [1]$, quindi

$$\sum_{i=0}^k [a_i][10]^i = \sum_{i=0}^k [a_i][1]^i = \sum_{i=0}^k [a_i]$$

ma il fatto che il RHS è uguale a $[n]$ è la conclusione. $\square$

Con la stessa idea si possono dimostrare un bel po' di *criteri di congruenza* simili a quello di sopra.

Esercizio 5.40. Dare un criterio di congruenza per 5 dalla scrittura in base 16.

Suggerimento. Vedi Suggerimento 12. $\square$

Esercizio 5.41. Dimostrare il criterio di congruenza modulo 11. Se non ve lo ricordate, ricavatevelo usando le idee sopra.

Suggerimento. Vedi Suggerimento 13. $\square$

5.5 Digressione: voglio costruire altri numeri!

Abbiamo visto le costruzioni di $\mathbb{Z}$ e $\mathbb{Q}$ per fare pratica con le relazioni di equivalenza, ma potrebbe esservi venuta la voglia di sapere come si costruiscono altre strutture numeriche, come $\mathbb{N}$ o $\mathbb{R}$, (e magari pure $\mathbb{C}$). Questo esula dagli argomenti di questo corso, ma tanto questa è una sezione “Digressione”.

Abbiamo già parlato della costruzione di $\mathbb{N}$ nella Sezione 1.5, ma non vi ho detto come si definiscono $+$ e $\cdot$. In breve, si definisce il $+$ usando il successore s come

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

cioè $n + (m+1) := (n+m)+1$ (da pensarsi induttivamente in m). Analogamente, si definisce il $\cdot$ usando il $+$ come

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

⁶Qui $[c]^i$ vuol dire “il prodotto di $[c]$ con sé stesso i volte”. Su $\mathbb{Z}/n\mathbb{Z}$ non è definita un'operazione “esponenziale”.

cioè $n \cdot (m+1) := n \cdot m + n$. Poi si dimostrano per induzione associatività, commutatività, distributività. E se avete fatto gli esercizi sapete come si definisce il $\leq$ partendo dal successore. Se volete fare i dettagli, e nel mentre imparare un linguaggio di programmazione che sta diventando abbastanza popolare ($L\exists\forall N$), il tutto gamificato, vi raccomando [BP].

La costruzione di $\mathbb{R}$ è un po' più complicata. O meglio, le costruzioni di $\mathbb{R}$, dato che ce ne sono almeno due abbastanza popolari, quella con i *tagli di Dedekind*, dove un numero reale è un sottoinsieme di $\mathbb{Q}$ di un certo tipo, e quella con le *successioni di Cauchy*, dove un numero reale è una classe di equivalenza di una certa relazione d'equivalenza su un certo insieme di funzioni $\mathbb{N} \rightarrow \mathbb{Q}$. Le due costruzioni “fanno le stesse cose” nel senso che entrambe restituiscono un *campo ordinato completo*, e di campi ordinati completi ce n'è uno solo a meno di isomorfismo. Qui “campo ordinato” vi ho detto cosa vuol dire più su, e “completo” vuol dire che *ogni insieme superiormente limitato ha un sup*, cioè un *minimo dei maggioranti*, cioè che

$$\begin{aligned} \forall A \subseteq \mathbb{R} \left((\exists x \in \mathbb{R} \forall a \in A \ x \geq a) \right. \\ \left. \Rightarrow (\exists x \in \mathbb{R} \forall a \in A \forall z \in \mathbb{R} ((\forall a \in A \ z \geq a) \Rightarrow z \geq x)) \right) \end{aligned}$$

ma di questa cosa vi preoccuperete a dovere nel corso di analisi.

L'insieme dei numeri complessi $\mathbb{C}$ poi viene identificato con $\mathbb{R}^2$, con le operazioni $(a, b) + (c, d) := (a + c, b + d)$ e $(a, b) \cdot (c, d) := (ac - bd, ad + bc)$. Qui “si possono fare sempre le radici quadrate” (e molto, molto di più), e per esempio $(0, 1)$ e $(0, -1)$ sono le due radici quadrate di -1 .

La storia non finisce qui, e i matematici di strutture numeriche ne hanno definite tante, come ad esempio i *razionali p-adici* $\mathbb{Q}_p$, dove p è un primo, che sono una specie di “interi in base p ma con infinite cifre *prima* della virgola”, o i *quaternioni* $\mathbb{H}$, o i numeri *surreali* $\mathbf{No} \dots$

In ogni caso, se avete letto fin qui vi meritate un memino, vedi Figura 5.1.

	Counting numbers, haha $\mathbb{N} = \{1, 2, 3, \dots\}$
	Just two natural numbers! $\mathbb{Z} = \{a - b \mid a, b \in \mathbb{N}\}$
	Just two integers! $\mathbb{Q} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0 \right\}$
	The limits of infinite convergent Cauchy sequences of rational numbers $\mathbb{R} = \left\{ \lim_{n \rightarrow \infty} a(n) \mid a : \mathbb{N} \rightarrow \mathbb{Q}, \forall \varepsilon > 0. \exists N \in \mathbb{N}. \forall n > N. a(n) - a(N) < \varepsilon \right\}$
	Just two real numbers! $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$

Figura 5.1: Per apprezzare appieno questo meme vi tocca aspettare il corso di analisi, ma intanto ora sapete che è un po' impreciso perché c'è da fare anche dei quozienti. Notare che, a differenza delle convenzioni che adottiamo in questo corso, per l'autore di questo meme $0 \notin \mathbb{N}$.

Capitolo 6

Successioni e ricorsione

6.1 Numeri in fila

Definizione 6.1. Una *successione* è una funzione con dominio $\mathbb{N}$. Una *successione di elementi di X* è una funzione $\mathbb{N} \rightarrow X$.

Quindi, ad esempio, una successione di numeri razionali è una funzione $\mathbb{N} \rightarrow \mathbb{Q}$. Di solito, quando una funzione $\mathbb{N} \rightarrow X$ la chiamiamo “successione” è perché stiamo pensando a degli elementi di X “elencati uno dopo l’altro”. Questa è una differenza più psicologica che matematica, ma è comunque abbastanza da far sì che si usi spesso la stessa notazione che si usa per le tuple:¹

Notazione 6.2. Se $a: \mathbb{N} \rightarrow X$ è una successione, l’elemento $a(n)$ si denota anche con a_n . La successione a si denota anche con $(a_n)_{n \in \mathbb{N}}$, o con $(a_n \mid n \in \mathbb{N})$, o con $\{a_n\}_{n \in \mathbb{N}}$.

Osservazione 6.3. Il dominio $\mathbb{N}$ lo pensiamo come insieme di *indici*. A volte torna comodo indicizzare su un altro insieme, per esempio prendere come dominio di una successione $\mathbb{N} \setminus \{0\}$ invece di $\mathbb{N}$. Insomma, partire con a_1 invece che con a_0 . O partire da a_{-1} , o da $a_7, \dots$. A volte si chiama “successione” anche qualcosa di indicizzato su un ordine lineare non isomorfo ad $\mathbb{N}$, per esempio un sottoinsieme finito di $\mathbb{N}$, oppure $\mathbb{Z}$. Comunque, di default, le nostre successioni saranno indicizzate su $\mathbb{N}$.

Esempio 6.4. Qualche esempio di successione.

1. La successione $(a_n)_{n \in \mathbb{N}}$ definita da $a_n := n$. Se la pensiamo come funzione $\mathbb{N} \rightarrow \mathbb{N}$, è l’identità.
2. La successione $(b_n)_{n \in \mathbb{N}}$ che vale costantemente 42 (cioè $\forall n \in \mathbb{N} \, b_n = 42$).
3. La successione dei numeri naturali dispari $c_n := 2n + 1$, che possiamo denotare anche con $(2n + 1)_{n \in \mathbb{N}}$.
4. La successione $d_n := (n \bmod 5)$ i cui primi termini sono

$0, 1, 2, 3, 4, 0, 1, 2, 3, 4, 0, 1, 2, 3, 4, \dots$

¹Vedi anche Esempio 4.3.12.

5. La successione $e_n := 2^n$ delle potenze di 2, che inizia con

$$1, 2, 4, 8, 16, 32, 64, \dots$$

6. La successione di numeri razionali $f_n := (-1)^n/n^2$. (Esercizio: scriverne qualche termine, che ne so, i primi 9).
7. C'è un'intera enciclopedia online di esempi [Oei].

6.2 Saltare la fila

Sopra abbiamo definito una successione dando una *formula chiusa*: una qualche espressione che ci permette, per ogni n , di calcolare a_n direttamente. Ad esempio, anche senza calcolare tutti i valori precedenti, si vede subito che $a_{12} = 12$, che $c_{101} = 203$, o che $f_{20} = 1/400$.

Un'altra maniera per definire una successione è *per ricorrenza* (o *ricorsione*). Essenzialmente, si specificano un po' di valori $a_0, \dots, a_k$ per un qualche k , e poi si dice chi è a_{n+1} in funzione dei valori precedenti. Questo genere di definizione tende a comparire spesso “in natura”², ma ha lo svantaggio che, almeno usando solo la definizione, per calcolare a_n bisogna calcolarsi tutti gli a_i precedenti. Ci torniamo, ma prima vediamo qualche esempio.

Esempio 6.5. Fissati due interi $b, d \in \mathbb{Z}$ possiamo definire per ricorrenza la *progressione aritmetica*

$$\begin{cases} a_0 = b \\ a_{n+1} = a_n + d \end{cases}$$

Insomma, partiamo da b e ad ogni passo sommiamo lo stesso numero d . Qual è una formula chiusa per a_n ?

Soluzione. Dopo n passi abbiamo sommato a b per n volte il numero d , quindi sembra ragionevole aspettarsi che una formula chiusa sia

$$a_n = b + nd \tag{6.1}$$

Dimostriamo per induzione che effettivamente questa funziona.

Per il passo base, abbiamo che $a_0 = b$ per definizione, mentre il RHS della (6.1) è uguale a $b + 0 \cdot d = b$. Quindi il passo base è ok.

Per il passo induttivo, assumiamo che la (6.1) valga per n , e mostriamo che vale per $n + 1$. Per definizione di $(a_n)_{n \in \mathbb{N}}$ il LHS per $n + 1$ è

$$a_{n+1} = a_n + d$$

e se usiamo l'ipotesi induttiva

$$a_{n+1} = a_n + d = b + nd + d$$

ma il RHS di quest'ultima, raccogliendo, è uguale a $b + (n + 1)d$, cioè il RHS della (6.1) per $n + 1$. $\square$

²Nel senso di “salta fuori facilmente quando si provano a risolvere certi problemi”, non nel senso di “si trova fra piante e animali”. Cioè, non necessariamente, ma a volte sì, per esempio fra poco parleremo di conigli.

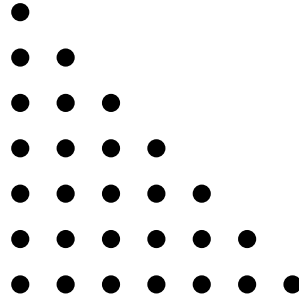


Figura 6.1: Il numero di pallini in questa figura è il settimo numero triangolare $7(7+1)/2 = 28$. Contemplare questa figura abbastanza a lungo dovrebbe farvi venire in mente una dimostrazione alternativa della Proposizione 2.46. Altrimenti, vedi Suggerimento 15.

Esercizio 6.6. Fissati due razionali $b, d \in \mathbb{Q}$ possiamo definire per ricorrenza la *progressione geometrica*

$$\begin{cases} a_0 = b \\ a_{n+1} = a_n \cdot d \end{cases}$$

Dimostrare che una formula chiusa per questa successione è $a_n = b \cdot d^n$.

Esempio 6.7. La successione dei *numeri triangolari* è definita da

$$\begin{cases} a_0 = 0 \\ a_{n+1} = a_n + (n+1) \end{cases}$$

Come sappiamo dalla Proposizione 2.46, una formula chiusa è $a_n = n(n+1)/2$. Il nome “numeri triangolari” viene dal fatto che, ad esempio, a_7 è uguale al numero di pallini in Figura 6.1.

Nello studiare un qualche problema è facile imbattersi in successioni definite per ricorrenza, perché magari il problema che stiamo studiando si presta bene a descrivere quello che succede in un certo momento in termini di quello che è successo poco prima (vedi Esempio 6.8 ed Esercizio 6.24).

Tuttavia, se le definizioni per ricorrenza sono comode da dare, possono essere parecchio scomode da calcolare. Per esempio, se $(a_n)_{n \in \mathbb{N}}$ è definita per ricorrenza, calcolare, che ne so, $a_{12038752893}$ usando direttamente la definizione può essere computazionalmente dispendioso, perché richiede di calcolare 12038752894 valori della successione.

A questo punto dovrebbe essere chiaro che avere una formula chiusa per una successione è parecchio utile, non fosse altro che per poterne calcolare un qualche termine in breve tempo. Per non parlare del fatto che tende a rendere più facile capire come la successione si comporta. Ad esempio, prima di sapere la formula chiusa per la somma dei naturali fino a n , avreste mai detto che cresce circa quanto n^2 ? O avreste mai detto che il suo quadrato è uguale a... la somma dei cubi fino a n^3 ? (Esercizio 6.18)³

Trovare formule chiuse per una successione tende a non essere facilissimo. Alcune sono più o meno “visibili ad occhio” (tipo quella dell’Esempio 6.5), a

³Vedi [Wiki] per dimostrazioni alternative e rappresentazioni grafiche.

volte si può provare a indovinarne una calcolando ed osservando i primi termini della successione, e ci sono dei trucchi standard che a volte funzionano (ma che non vedremo in questo corso). Ma in generale il problema di trovare una formula chiusa è difficile, anche se la ricorrenza è facile: vedi Esempio 6.10 per un caso famoso aperto dal 1937.

In compenso (come forse vi aspettate ricordando la dimostrazione della Proposizione 2.46), verificare che una formula chiusa per una successione è effettivamente corretta è molte volte un esercizio che si fa per induzione.⁴

Esempio 6.8 (Numeri di Fibonacci). Il mese 0 decido che voglio comprare dei conigli. Anzi, ne voglio comprare una coppia. Ci rimugino per tutto il mese, e il mese 1 vado in un negozio e mi propongono di comprare una coppia di conigli immortali, in grado di riprodursi generando prole a sua volta immortale. Incurante delle conseguenze ambientali, li compro, un maschio e una femmina. Il negoziante allora mi spiega che: i conigli sono appena nati, e, da quando compiono due mesi, ogni mese generano un'altra coppia di conigli, sempre un maschio e una femmina. Questa nuova coppia, a sua volta, dal secondo mese dopo la nascita genera un altro maschio e un'altra femmina, eccetera.

Quante coppie di conigli ho al mese n ? Beh, il mese 2 sempre una, perché quella che ho comprato non è ancora fertile. Il mese 3 invece ho quelli che avevo prima, più una nuova coppia, quindi 2. Il mese 4 ho quelli che avevo prima, più un'altra coppia generata da quella che ho comprato (i loro figli non sono ancora fertili), quindi 3. Il mese 5 però ne ho 5: quelli che avevo il mese prima (che sono 3), più una nuova coppia per ogni coppia fertile, cioè ogni coppia di almeno 2 mesi, cioè tante nuove coppie quante ne avevo in totale due mesi prima (che erano 2).

Più in generale, il mese n ho tutte le coppie che avevo al mese $n-1$ (dato che sono immortali), più una nuova coppia per ogni vecchia coppia che ha almeno due mesi, cioè tante nuove coppie quante coppie avevo al mese $n-2$. Quindi il numero di coppie al mese n è dato dalla *successione di Fibonacci*, definita per ricorrenza come

$$\begin{cases} F_0 = 0 \\ F_1 = 1 \\ F_{n+2} = F_{n+1} + F_n \end{cases}$$

Esercizio 6.9. Calcolare i termini della successione di Fibonacci fino a F_{10} .

Ma quindi quante coppie di conigli ho al mese 20? Vedi Esercizio 6.22 per una formula chiusa.

Esempio 6.10. Per $k \in \mathbb{N}$ fissato, definiamo $c_{k,0} = k$ e

$$c_{k,n+1} = \begin{cases} c_{k,n}/2 & \text{se } c_{k,n} \text{ è pari} \\ 3c_{k,n} + 1 & \text{se } c_{k,n} \text{ è dispari} \end{cases}$$

Per esempio, i primi termini di $(c_{10,n})_{n \in \mathbb{N}}$ sono 10, 5, 16, 8, 4, 2, 1, 4, 2, 1... Sembra innocua, vero? Quanto mai sarà difficile trovare una formula chiusa? Prima di continuare a leggere, vi invito a scegliervi due o tre valori di k , per ognuno di questi, calcolare i primi valori di $c_{k,n}$.

⁴E che, molte volte, compare nelle tracce degli esami.

Come possiamo facilmente calcolare, se per un qualche n_0 abbiamo $c_{k,n_0} = 1$, allora da quel punto in poi la successione è destinata a “ciclare” fra 1, 4 e 2 per sempre. Se provate a calcolare i primi termini di $(c_{k,n})_{n \in \mathbb{N}}$ per qualche k , dovrete arrivare presto a un qualche n_0 tale che $c_{k,n_0} = 1$ (provate!). Se trovate un k per cui $a_{k,n}$ non è mai 1 (o avete sbagliato i conti⁵, o), avete refutato la *Congettura di Collatz*, che dice appunto che $\forall k \in \mathbb{N} \setminus \{0\} \exists n_0 \in \mathbb{N} (c_{k,n_0} = 1)$. Il fatto che si chiami *congettura* vuol dire che “ci si aspetta” che sia vero, ma nessuno è mai riuscito⁶ a dimostrarlo, né a refutarlo (cioè a dimostrare il contrario). Per saperne di più, vedi [Wika].

Esempio 6.11. Quanti sono gli ordini in cui si può trovare un mazzo di carte napoletane dopo averlo mischiato? E un mazzo di carte francesi? Un mazzo di carte francesi con anche i jolly? E se per sbaglio mescolo dentro anche quella carta coi punti del bridge che non è chiaro perché continuano a mettercela?

In generale, vogliamo capire quanti ordini sono possibili su un mazzo di n carte. Qui definire una successione per ricorrenza ci aiuta, perché nel fare questo conto ci riconduciamo ogni volta allo stesso conto ma con un numero più piccolo. Vediamo come, facendo due osservazioni cruciali:

1. Che mischi un mazzo di carte napoletane, o un mazzo di carte siciliane, o un mazzo di carte napoletane dove ho tolto il 6 di coppe e aggiunto la carta con le regole della scopa⁷, il risultato è lo stesso. Insomma, non mi interessa cosa c'è sulle carte, mi interessa solo che siano a due a due distinte.
2. Se mescolo un mazzo di 40 carte, ci sono 40 possibilità per la carta in cima al mazzo. Tolta quella, mi rimane un mazzo con una carta in meno, quindi di 39 carte, che può a sua volta essere in vari ordini.

Chiaramente, che la carta in cima fosse il 7 di denari, l'asso di bastoni, o qualunque altra carta, ai fini di sapere in quante maniere posso ordinare le altre 39 non cambia niente, come non cambiava niente fra usare le carte napoletane o le siciliane.

Quindi, per un mazzo di 40 carte, il numero degli ordini è 40 volte il numero di ordini di un mazzo di 39 carte: scelgo la prima carta, e poi scelgo come ordinare il resto del mazzo. E in quante maniere si può ordinare un mazzo di 39 carte? È lo stesso problema, *ma con un numero più piccolo*, per cui ha senso procedere ricorsivamente.

Invece di partire dal fondo, iniziamo con mazzi piccoli. Di maniere in cui mescolare un mazzo di 0 carte ce n'è una sola. Anche con 1 carta, la scelta è forzata. Con 2 carte, ho 2 maniere di scegliere la prima carta, e mi resta un mazzo di 1 carta, che come abbiamo detto si può ordinare in 1 maniera. Con 3 carte, ho 3 maniere di scegliere la prima, e poi mi rimane un mazzo di 2 carte, che abbiamo già visto potersi ordinare in 2 maniere. Quindi in totale abbiamo $3 \cdot 2 = 6$ maniere di ordinare un mazzo di 3 carte. Con 4 carte, similmente, ne abbiamo $4 \cdot 6 = 24$. Insomma, dovrete aver capito. La successione che conta questa cosa è abbastanza importante da meritarsi una notazione tutta sua:

⁵Cosa abbastanza probabile, dato che fino a $k = 2.36 \cdot 10^{21}$ è stato controllato che non ci sono esempi.

⁶Beh, o almeno non ce l'ha fatto sapere.

⁷Anche questa non è chiaro perché continuano a mettercela.

Definizione 6.12. La funzione *fattoriale*, denotata da $n!$, è definita ricorsivamente da

$$\begin{cases} 0! = 1 \\ (n+1)! = (n+1) \cdot n \end{cases}$$

Insomma, $n!$ è il prodotto di tutti i numeri da 1 a n , con la convenzione che il prodotto di 0 numeri è 1. Notiamo l'analogia con la Proposizione 2.46: lì stavamo sommando i numeri fino ad n , qui li stiamo moltiplicando. Per la cronaca, come lì c'era il simbolo di *sommatoria*, cioè la notazione

$$\sum_{i=1}^n i$$

per la somma dei numeri da 1 a n , c'è anche un simbolo di *produttoria* per il prodotto, e $n!$ si può denotare come

$$n! = \prod_{i=1}^n i$$

Ora, per lo stesso motivo per cui invece delle carte napoletane avremmo potuto usare le siciliane, possiamo chiaramente usare, invece di 40 carte, che ne so 40 biglie a due a due diverse o, per fare prima, direttamente i naturali da 1 a 40. O da 0 a 39. O da 102 a 141. E una maniera di esprimere l'ordine in cui metterli può essere espresso tramite la funzione che ci manda un numero nella sua posizione dopo aver mescolato, che può essere da 1 a 40. Questa funzione è bigettiva (esercizio). Viceversa, ogni funzione bigettiva da $\{n \in \mathbb{N} \mid 1 \leq n \leq 40\}$ ci dà un ordinamento dei numeri da 1 a 40: l'ordinamento⁸

$$f(1) < f(2) < f(3) < \dots < f(39) < f(40)$$

Ora, semplicemente osservando che il numero 40 non ha nulla di speciale nel paragrafo sopra, scopriamo di aver appena imparato a contare il numero di *permutazioni* di n elementi:

Definizione 6.13. Sia X un insieme. Una *permutazione* di X è una bigezione $X \rightarrow X$.

Teorema 6.14. Il numero di permutazioni di un insieme con n elementi è $n!$.

Dimostrazione. Sostanzialmente dimostrato sopra. Scrivere una dimostrazione come si deve è un buon esercizio. $\square$

Usando queste idee, possiamo contare molte altre cose. Se invece mischio *due* mazzi di carte napoletane, e quindi ora ogni carta appare due volte, quanti possibili ordini ci sono, senza distinguere le due copie della stessa carta? E quanti sono gli insiemi di 3 carte napoletane? E le giocate possibili al superenalotto? O, sempre al superenalotto, la probabilità di fare 3?⁹

⁸Stiamo usando anche che queste mappe, da ordinamenti a bigezioni e viceversa, sono una l'inversa dell'altra. Ci torniamo presto, per ora il punto di cui convincervi è che mettere 40 cose in ordine è la stessa cosa di dare una bigezione fra l'insieme di queste 40 cose e $\{1, 2, \dots, 40\}$.

⁹Spoiler: il superenalotto paga *molto* meno di quanto dovrebbe pagare per essere a *valore atteso* 0, cioè di quanto dovrebbe pagare perché, giocando tante volte, un giocatore in media non guadagni né perda niente. In altre parole, è un gioco *molto* redditizio per lo Stato. Se volete sapere esattamente *quanto* meno paga, è un buon esercizio da fare dopo il prossimo capitolo.

Prima di contare altro, però, vediamo di capire cosa vuol dire “contare”. E prima ancora, ~~facciam~~fatte un altro po’ di pratica con induzione e ricorsione.

6.3 Esercizi

Esercizio 6.15. Dare una definizione ricorsiva della successione $(a_n)_{n \in \mathbb{N}}$ il cui termine a_n è l’ n -esimo numero congruo a 3 modulo 5.

Esercizio 6.16. Dimostrare che la somma dei primi n numeri dispari è l’ n -esimo quadrato, cioè che

$$\sum_{i=0}^{n-1} (2i+1) = n^2$$

Esercizio 6.17. Dimostrare che $\sum_{i=0}^n i^2 = n(n+1)(2n+1)/6$.

Esercizio 6.18. Dimostrare che

$$\sum_{i=0}^n i^3 = \left(\frac{n(n+1)}{2} \right)^2$$

Esercizio 6.19 (Serie aritmetica). Fissiamo $b, d \in \mathbb{Z}$, e sia $a_n = b + nd$ la corrispondente progressione aritmetica (Esempio 6.5). Dimostrare che

$$\sum_{i=0}^n a_i = \frac{(2b + dn)(n+1)}{2} = \frac{(a_0 + a_n)(n+1)}{2}$$

Suggerimento. Vedi Suggerimento 16. □

Esercizio 6.20 (Serie geometrica). Fissiamo $b, d \in \mathbb{Q}$ e ricordiamo dall’Esercizio 6.6 che la relativa progressione geometrica ha come formula chiusa $a_n = bd^n$.

1. Calcolare $\sum_{i=0}^n a_i$ quando $d = 1$.
2. Per $d \neq 1$, dimostrare che

$$\sum_{i=0}^n a_i = \frac{b(d^{n+1} - 1)}{1 - d}$$

Esercizio 6.21. Dimostrare che la successione definita da

$$\begin{cases} a_0 = 0 \\ a_{n+1} = 2a_n + n \end{cases}$$

ha come formula chiusa $a_n = 2^n - n - 1$.

Esercizio 6.22 (Formula di Binet). Dimostrare che la seguente è una formula chiusa per la successione di Fibonacci.

$$F_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1 + \sqrt{5}}{2} \right)^n - \left(\frac{1 - \sqrt{5}}{2} \right)^n \right)$$

Suggerimento. Vedi Suggerimento 17. □

Esercizio 6.23 (Numeri di Pell). La successione dei *numeri di Pell* è definita dalla ricorrenza

$$\begin{cases} P_0 = 0 \\ P_1 = 1 \\ P_{n+2} = 2P_{n+1} + P_n \end{cases}$$

Dimostrare che una formula chiusa per questa successione è

$$P_n = \frac{(1 + \sqrt{2})^n - (1 - \sqrt{2})^n}{2\sqrt{2}}$$

Suggerimento. Vedi Suggerimento 18. □

Esercizio 6.24 (Fork bomb). Consideriamo il seguente programma bash:

```
fork() {
    fork | fork &
};
fork
```

che lancia due copie di sé stesso in parallelo (e fa piping dell'inesistente output di una copia nell'altra, in background).¹⁰ Supponiamo che il lancio delle due copie in parallelo richieda 1 millisecondo. Quanti processi sono stati lanciati dopo 1 secondo?¹¹ E se invece di 1 millisecondo la macchina ci mette 1 microsecondo?

Visto che siamo in tema di esercizi che si possono risolvere per induzione, e visto che probabilmente avete scritto i numeri naturali sempre (o quasi) in una qualche base (tipicamente 10), dimostriamo di non esserci persi nessun numero per strada.

Esercizio 6.25. Dimostrare che ogni numero ammette una scrittura in base 10, cioè che per ogni $n \in \mathbb{N}$ esistono $k \in \mathbb{N}$ e $a_0, \dots, a_k \in \{x \in \mathbb{N} \mid x < 10\}$ tali che

$$n = \sum_{i=0}^k a_i 10^i$$

Chiaramente, l'unica cosa che ha 10 di speciale è che gli umani hanno molto spesso 10 dita delle mani.¹²

Esercizio 6.26. Dimostrare che, per ogni $b \in \mathbb{N}$ tale che $b \geq 2$, ogni numero ammette una scrittura in base b , cioè che per ogni $n \in \mathbb{N}$ esistono $k \in \mathbb{N}$ e $a_0, \dots, a_k \in \{x \in \mathbb{N} \mid x < b\}$ tali che

$$n = \sum_{i=0}^k a_i b^i$$

¹⁰La maniera tradizionale (ma poco leggibile) di definire un programma equivalente a quello sopra in GNU bash è `:(){ :|:& };: (sì, in GNU bash ":" è un nome valido per una funzione).`

¹¹Assumete di stare usando un sistema operativo che non implementa salvaguardie contro questo genere di scherzoni e che abbia abbastanza risorse da sopravvivere per 1 secondo senza rallentare.

¹²I maya immagino guardassero anche le dita dei piedi [Wikif] e i sumeri... chiedevano aiuto a un po' di amici? [Wikik]

Suggerimenti

Quest'appendice contiene suggerimenti per gli esercizi, messi lontano dagli esercizi di riferimento per evitare spoiler involontari a chi non li volesse.

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

Suggerimento 2. 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.

Suggerimento 3. Scegliete un qualche insieme piccolo ma non troppo (boh, 7 elementi?) in $\mathbb{N}^2$, diciamo A , e calcolate chi è $\{x \mid \exists y (x, y) \in A\}$.

Suggerimento 4. Guardare bene l'argomento nella dimostrazione della Proposizione 3.29. Cosa usa esattamente? Per la parte "in particolare", usare ad esempio che g_1 è una *qualunque* inversa sinistra.

Suggerimento 5. Identità, inversa, composizione.

Suggerimento 6. Quanti esempi di omomorfismo conosci?

Suggerimento 7. Una maniera è usare la costruzione di $\mathbb{Z}$, ma si può fare anche usando solo le proprietà di base di $+$ e $\cdot$ (associatività, distributività...). Se riuscite a farlo nella seconda maniera meglio (perché l'avrete dimostrata automaticamente anche per altre strutture, ci torniamo).

Suggerimento 8. Induzione e iniettività del successore.

Suggerimento 9. $0 = 1 + (-1)$.

Suggerimento 10. Se $a \neq 0$ allora ha un inverso moltiplicativo.

Suggerimento 11. Per la funzione f non ci sono molte scelte: 0_M deve andare in 0, e se vogliamo $f \circ s_M = s \circ f \dots$. L'iniettività è facile. La surgettività vuol dire $\text{Im}(f) = M$. Cosa abbiamo dimostrato appena prima dell'esercizio?

Suggerimento 12. La dimostrazione prima l'abbiamo capita davvero?

Suggerimento 13. $10 \equiv -1 \pmod{11}$.

Suggerimento 14. Usate il Teorema 5.31.

Suggerimento 15. Fate quel disegno due volte e *riflettete*.

Suggerimento 16. Invece di fare per induzione, si può anche fare usando quello che sapete già.

Suggerimento 17. $(3 + \sqrt{5})/2 = ((1 + \sqrt{5})/2)^2$.

Suggerimento 18. Vedi Suggerimento [17](#).

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.
- [BP] Kevin Buzzard e Mohammad Pedramfar. *The natural numbers game*. https://cbirkbeck.github.io/natural_number_game/.
- [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).
- [Oei] *The on-line encyclopedia of integer sequences*. <https://oeis.org/>.
- [Wika] Wikipedia. *Collatz conjecture*. https://en.wikipedia.org/wiki/Collatz_conjecture.
- [Wikb] Wikipedia. *Cook-Levin theorem*. https://en.wikipedia.org/wiki/Cook%E2%80%93Levin_theorem#Consequences.
- [Wikc] Wikipedia. *First-order logic*. https://en.wikipedia.org/wiki/First-order_logic.
- [Wikd] Wikipedia. *Hilbert's program*. https://en.wikipedia.org/wiki/Hilbert's_program.

- [Wike] Wikipedia. *Logic gate*. https://en.wikipedia.org/wiki/Logic_gate.
- [Wikf] Wikipedia. *Maya numerals*. https://en.wikipedia.org/wiki/Maya_numerals.
- [Wikg] Wikipedia. *Model checking*. https://en.wikipedia.org/wiki/Model_checking.
- [Wikh] Wikipedia. *P versus NP problem*. https://en.wikipedia.org/wiki/P_versus_NP_problem.
- [Wiki] Wikipedia. *Russell's paradox*. https://en.wikipedia.org/wiki/Russell%27s_paradox.
- [Wikj] Wikipedia. *Schröder–Bernstein theorem*. https://en.wikipedia.org/wiki/Schr%C3%B6der%E2%80%93Bernstein_theorem.
- [Wikk] Wikipedia. *Sexagesimal*. <https://en.wikipedia.org/wiki/Sexagesimal>.
- [Wikl] Wikipedia. *Squared triangular number*. https://en.wikipedia.org/wiki/Squared_triangular_number.
- [Wikm] Wikipedia. *Zermelo–Fraenkel set theory*. https://en.wikipedia.org/wiki/Zermelo%E2%80%93Fraenkel_set_theory.