

# RAGIONAMENTO MATEMATICO

Lo scopo del capitolo è quello di esemplificare l'uso della Logica Matematica, della formalizzazione e delle regole di prova, (capitolo ??) in pratica. Affronteremo il problema di dimostrare teoremi matematici in due contesti esemplificativi: gli *insiemi* (vedi Sezione ??) e l'*aritmetica*. Questi esempi hanno lo scopo di spiegare la relazione tra le dimostrazioni formali e quelle standard che non sono scritte in modo completamente formale. Infatti,

1. hanno un livello di dettaglio minore rispetto alle dimostrazioni formali, dato che alcuni passaggi ovvi e soprattutto le loro giustificazioni sono omesse o sottintese.
2. usano il linguaggio naturale (ma con un chiaro significato logico);
3. sono scritte in linguaggio naturale ma con un significato non ambiguo.

L'osservazione fondamentale è che le dimostrazioni matematiche, anche se scritte ad un altro livello di dettaglio, seguono lo stesso schema delle dimostrazioni formali e sono basate sulle regole di inferenza e sui metodi di prova formali. La conoscenza di questi metodi ci permette quindi di capire come leggere e scrivere dimostrazioni matematiche con minore dettaglio, individuando quali passaggi sono critici e devono necessariamente essere giustificati, e quali possono invece essere omessi.

Prima di affrontare questi esempi è necessario fare una premessa. È chiaro che dimostrare una proprietà, formalizzata per esempio da una formula  $A$ , degli insiemi o dell'aritmetica, non vuol dire dimostrare che  $A$  è valida, ovvero che  $A$  è vera in ogni possibile interpretazione. Quello che vogliamo dimostrare è che  $A$  è vera rispetto ad una *interpretazione specifica*, il cui dominio è il dominio di interesse ed in cui i simboli hanno un significato preciso. Per esempio, nel caso dell'aritmetica il dominio di interesse è  $\mathcal{Z}$  ed i simboli  $+$ ,  $\times$ ,  $\leq$ ,  $\dots$  hanno l'ovvio significato e soddisfano le proprietà standard. Dato che le regole di inferenza sono corrette per ogni interpretazione, sono corrette per l'interpretazione specifica che stiamo considerando.

## 1 Dimostrazioni in Domini Specifici: Insiemi

Andiamo a fare degli esempi nel contesto degli insiemi, assumendo quindi che il *dominio di interesse*, sia quello degli insiemi e degli elementi degli insiemi e che  $\in$  abbia l'ovvio significato. Per non appesantire la notazione useremo

semplicemente le lettere minuscole per indicare oggetti dell'universo, le lettere maiuscole per indicare insiemi di oggetti.

Riprendiamo i concetti (insiemi, unione, intersezione, differenza, ecc.) della Sezione ?? e vediamo come possono essere formalizzati in Logica Predicativa.

Le usuali operazioni tra insiemi non sono altro che dei simboli di funzione  $\cap$ ,  $\cup$  ed  $-$  che sono definiti dalle seguenti formule

- **Unione**

$$A \cup B = \{a \mid a \in A \vee a \in B\}$$

- **Intersezione**

$$A \cap B = \{a \mid a \in A \wedge a \in B\}$$

- **Differenza**

$$A - B = \{a \mid a \in A \wedge a \notin B\}$$

Le usuali relazioni tra insiemi *uguaglianza* e *sottoinsieme* sono dei simboli di predicato  $=$  ed  $\subseteq$  che soddisfano le seguenti formule:

$$\forall A, B (A = B \leftrightarrow \forall x (x \in A \leftrightarrow x \in B))$$

$$\forall A, B (A \subseteq B \leftrightarrow \forall x (x \in A \rightarrow x \in B))$$

Introduciamo anche un simbolo di costante  $\emptyset$  per rappresentare l'insieme *vuoto* definito come segue<sup>1</sup>

$$(\forall x. x \notin \emptyset)$$

Chiamiamo la teoria formata dalle formule precedenti *Ins* e vediamo come si dimostrano *in modo formale* alcuni semplici proprietà (alcune già viste nella Sezione ??).

**Esempio 1.1** *Consideriamo la seguente proprietà:* “Siano  $A$  e  $B$  due insiemi ed  $a$  un elemento dell'universo. Se  $a \in A$  ed  $a \in B$ , allora  $a \in (A \cap B)$ ”

*Per dimostrarla formalmente bisogna*

1. *tradurre in formule l'enunciato del teorema;*
2. *dimostrare che la formula corrispondente al testo del teorema segue dalla teoria Ins.*

*Il testo del teorema si può formalizzare come*

$$\forall A, B (\forall x (x \in A \wedge x \in B \rightarrow x \in (A \cap B))).$$

*Proviamo quindi che*

$$Ins \vdash \forall A, B (\forall x (x \in A \wedge x \in B \rightarrow x \in (A \cap B))).$$

---

<sup>1</sup>o equivalentemente  $\neg \exists x (x \in \emptyset)$ .

1.  $x \in A \wedge x \in B$  (Premessa\*<sup>2</sup>)
2.  $x \in A \cap B$  (Def. di  $\cap$  da 1.)
3.  $x \in A \wedge x \in B \rightarrow x \in A \cap B$  (imp)
4.  $\forall A, B (\forall x (x \in A \wedge x \in B \rightarrow x \in (A \cap B)))$  ( $\forall$ -G da 3.)

La dimostrazione è abbastanza lunga, nonostante la proprietà sia ovvia. Omettendo i dettagli inutili possiamo dare una versione della dimostrazione semi-formale, ma convincente, in cui i passaggi irrilevanti sono omessi e/o raggruppati in un unico passaggio.

1.  $x \in A \wedge x \in B$  (Premessa)
2.  $x \in A \cap B$  (Def. di  $\cap$  da 1.)

La dimostrazione semi-formale segue lo stesso schema e gli stessi passaggi logici di quella formale omettendo solo dettagli che sono ovvi: 3. ovvero la introduzione di  $\rightarrow$  (si sa che  $A \models B$  equivale a  $\models A \rightarrow B$ ); 4. ovvero  $\forall$ -G (dato che nella dimostrazione gli elementi considerati sono generici.)

Questa prova scritta a parole ha il livello di dettaglio in cui normalmente vengono scritte le dimostrazioni matematiche. Notate che la struttura del ragionamento logico resta la stessa. Assumiamo  $a \in A$  ed  $a \in B$ . Dalla Def. di  $\cap$  abbiamo  $a \in A \cap B$ .

Vediamo la versione semi-formale di alcune dimostrazioni viste nella Sezione ?? e diamone una dimostrazione nello stile dell'Esempio 1.1. Consideriamo per esempio la proprietà distributiva (Teorema ??) :

*Siano  $A, B$  e  $C$  insiemi. Abbiamo  $(A \cup B) \cap (A \cup C) = A \cup (B \cap C)$ .*

Dobbiamo fare vedere che

$$Ins \vdash \forall A, B, C ((A \cup B) \cap (A \cup C) = A \cup (B \cap C)).$$

La prova è una sequenza di equivalenze:

1.  $A \cup (B \cap C) = \{a \mid a \in A \vee (a \in B \wedge a \in C)\}$  (Def. di  $\cap$  ed  $\cup$ )
2.  $\{a \mid a \in A \vee (a \in B \wedge a \in C)\} = \{a \mid (a \in A \vee a \in B) \wedge (a \in A \vee a \in C)\}$   
(Proprietà distributiva di  $\wedge$  e  $\vee$ )
3.  $\{a \mid (a \in A \vee a \in B) \wedge (a \in A \vee a \in C)\} = (A \cup B) \cap (A \cup C)$  (Def. di  $\cap$  ed  $\cup$ )

Dato che i passaggi sono tutte equivalenze i due insiemi sono uguali. Confrontate questa dimostrazione del Teorema ?? con quella informale della Sezione ?. È evidente che lo *schema logico seguito* è lo stesso. Solo che nella Sezione ?? abbiamo dovuto giustificare l'uso della proprietà distributiva (passaggio 2.), ovvero spiegare che nel caso specifico vale la proprietà distributiva. Ora la prova è semplificata dal fatto che sappiamo che questa proprietà vale in generale.

<sup>2</sup>dove  $x$  ed  $A, B$  sono un oggetto ed insiemi generici.

## 1.1 Esercizi

**Esercizio 1.2** *Dimostrare in modo formale il seguente teorema*

Siano  $A$ ,  $B$ , e  $C$  insiemi. Se  $A \subseteq C$  e  $B \subseteq C$ , allora  $(A \cup B) \subseteq C$ .

*Tradotto in formule dimostriamo*

$$\text{Ins} \vdash \forall A, B, C ((A \subseteq C \wedge B \subseteq C) \rightarrow ((A \cup B) \subseteq C)).$$

1.  $A \subseteq C \wedge B \subseteq C$  (Premessa)
2.  $x \in A \cup B$  (Premessa)
3.  $x \in A \vee x \in B$  (Def. di  $\cup$  da 2.)
4.  $x \in A$  (Premessa per la regola per casi)
5.  $A \subseteq C$  (da 1.)
6.  $x \in C$  (M.P. da 4. e 5.)
7.  $x \in B$  (Premessa per la regola per casi)
8.  $B \subseteq C$  (da 1.)
9.  $x \in C$  (M.P. da 7. e 8.)
10.  $x \in C$  (Per casi da 9. cancella 4. e 7.)
11.  $x \in A \cup B \rightarrow x \in C$  (IMP cancella 2.)
12.  $(A \cup B) \subseteq C$  (Def. di  $\subseteq$  da 11.)
13.  $(A \subseteq C \wedge B \subseteq C) \rightarrow ((A \cup B) \subseteq C)$ . (IMP cancella 1.)

**Esercizio 1.3** *Dimostrare in modo formale il seguente teorema: Siano  $A$ ,  $B$  e  $C$  insiemi. Se  $A \subseteq B$  e  $B \subseteq C$  allora  $A \subseteq C$ .*

**Esercizio 1.4** *Dimostrare in modo formale il seguente teorema*

Siano  $A$ ,  $B$ ,  $C$  e  $D$  insiemi. Se  $A \subseteq C$  e  $B \subseteq D$  e  $D \cap C = \emptyset$ , allora  $A \cap B = \emptyset$ .

*Bisogna dimostrare che*

$$\text{Ins} \vdash \forall A, B, C, D ((A \subseteq C \wedge B \subseteq D \wedge D \cap C = \emptyset) \rightarrow A \cap B = \emptyset).$$

1.  $A \subseteq C \wedge B \subseteq D \wedge D \cap C = \emptyset$  (Premessa dell'implica)
2.  $A \cap B \neq \emptyset$  (premessa, negazione della conclusione)
3.  $\exists x \in (A \cap B)$  (Def. di  $\emptyset$  da 2.)
4.  $a \in (A \cap B)$  ( $\exists$ -I da 3.)

5.  $a \in A \wedge a \in B$  (Def. di  $\cap$ )
6.  $a \in A$  (and-elim)
7.  $a \in B$  (and-elim)
8.  $A \subseteq C$  (da 1.)
9.  $a \in C$  (modus ponens da 6. e 8.)
10.  $B \subseteq D$  (da 1.)
11.  $a \in D$  (modus ponens da 7. e 10.)
12.  $a \in C \wedge a \in D$  (and-intro)
13.  $a \in C \cap D$  (Def. di  $\cap$ )
14.  $\exists x(x \in C \cap D)$  ( $\exists$ -G)
15.  $D \cap C = \emptyset$
16.  $\perp$  (contradiction da 14. e 15.)
17.  $A \cap B = \emptyset$  (regola dell'assurdo cancella 2.)
18.  $((A \subseteq C \wedge B \subseteq D \wedge D \cap C = \emptyset) \rightarrow A \cap B = \emptyset)$  (IMP cancella 1.).

**Esercizio 1.5** Dimostrare in modo formale il seguente teorema

Siano  $A, B, C$  insiemi. Se  $A \subseteq B$  ed  $A \cap C = \emptyset$ , allora  $A \subseteq B - C$ .

Bisogna dimostrare che

$$Ins \vdash \forall A, B, C ((A \subseteq B \wedge A \cap C = \emptyset \rightarrow A \subseteq (B - C)).$$

1.  $A \subseteq B \wedge A \cap C = \emptyset$  (Premessa)
2.  $A \subseteq B$  (Da 1.)
3.  $A \cap C = \emptyset$  (Da 1.)
4.  $x \in A$  (Premessa)
5.  $x \in B$  (modus ponens da 4. e 2.)
6.  $A \cap C = \emptyset$  (da 1.)
7.  $x \notin C$  (da 4. e 6.)
8.  $x \in B \wedge x \notin C$  (and intro)
9.  $x \in B - C$  (Def. di  $-$ )
10.  $x \in A \rightarrow x \in B - C$  (IMP)
11.  $A \subseteq (B - C)$  (Def. di  $\subseteq$ )
12.  $A \subseteq B \wedge A \cap C = \emptyset \rightarrow A \subseteq (B - C)$  (IMP)

## 2 Dimostrazioni in Domini Specifici: Aritmetica

In questa lezione ci occuperemo di aritmetica, ovvero degli interi con le note operazioni e di alcune proprietà di base. Nel caso in cui si vogliano dimostrare asserti rispetto ad una certa interpretazione si potranno usare come assiomi (premesse) le proprietà note del dominio di riferimento. Per esempio lavorando rispetto ai numeri interi si utilizzeranno tipicamente le proprietà associativa, commutativa, distributiva etc. di somma e prodotto.

Dati due interi  $a$  e  $b$  con  $a \neq 0$ , diciamo che  $a$  divide  $b$  sse  $\exists c(b = a \times c)$ . In tal caso  $a$  è detto un *fattore* di  $b$  e  $b$  è detto un *multiplo* di  $a$ . Si utilizza la notazione  $a \setminus b$  per dire che  $a$  divide  $b$  ( $a$  è un *divisore* di  $b$ ).

Vediamo delle semplici proprietà della divisibilità.

**Lemma 2.1** *Siano  $a, b$  e  $c$  interi.*

1. Se  $a \setminus b$  e  $a \setminus c$ , allora  $a \setminus (b + c)$ ;
2. Se  $a \setminus b$  e  $b \setminus c$ , allora  $a \setminus c$ ;
3. Se  $a \setminus b$ , allora per ogni  $c$  abbiamo  $a \setminus (b \times c)$ .

**Prova:** Diamo una dimostrazione semi-formale della proprietà 1) del Lemma 2.1. Le altre sono lasciate come esercizio.

Assumiamo che  $a \setminus b$  e  $a \setminus c$  dove  $a, b$  e  $c$  sono dei generici interi. Dalla Def. di divisibilità abbiamo che  $b = a \times p$  e  $c = a \times q$  per qualche intero  $p$  e  $q$ . Quindi sostituendo  $b + c = (a \times p) + (a \times q)$ . Inoltre per la proprietà distributiva,  $(a \times p) + (a \times q) = a \times (p + q)$ . Quindi  $b + c = a \times (p + q)$  per qualche  $p$  e  $q$ . Dalla Def. di  $\setminus$  abbiamo  $a \setminus (b + c)$ .  $\square$

**Nota**[Prova Formale] Notate che gli assiomi della dimostrazione formale sono la definizione di  $\setminus$  e le ben note proprietà delle operazioni tra interi. Notate inoltre che la versione formale della proprietà è

$$\forall a, b, c (a \setminus b \wedge a \setminus c \rightarrow a \setminus (b + c)).$$

La versione formale della prova è analoga a quella informale in cui alcuni passaggi sono semplicemente omissi o sottintesi (come la generalizzazione e l'esplicita prova di  $\rightarrow$ ).

1.  $a \setminus b \wedge a \setminus c$  (Premessa)
2.  $a \setminus b$
3.  $\exists p(b = a \times p)$  (Def. di  $\setminus$ )
4.  $a \setminus c$
5.  $\exists q(c = a \times q)$  (Def. di  $\setminus$ )
6.  $b + c = (a \times p) + (a \times q)$  (*equivalence*)
7.  $(a \times p) + (a \times q) = a \times (p + q)$  (Proprietà distributiva)

8.  $b + c = a \times (p + q)$  (*equivalence*)
9.  $\exists h(b + c = a \times h)$  ( $\exists$ -G)
10.  $a \setminus (b + c)$  (Def. di  $\setminus$ )
11.  $a \setminus b \wedge a \setminus c \rightarrow a \setminus (b + c)$  (metodo di prova dell'implica)
12.  $\forall a, b, c(a \setminus b \wedge a \setminus c \rightarrow a \setminus (b + c))$  ( $\forall$ -G)

Il più grande intero che divide due numeri interi è noto come il *massimo comun divisore*. Dato un insieme di interi  $A \in \wp(\mathbb{Z})$  diciamo che  $A$  ha un massimo (resp. minimo) sse esiste  $c \in A$  tale che per ogni  $d \in A$ ,  $d \leq c$  (resp.  $c \leq d$ ). Si usano  $\max(A)$  e  $\min(A)$  per indicare il massimo ed il minimo dell'insieme  $A$ <sup>3</sup>.

Notiamo che esistono insiemi di interi che non hanno il massimo, mentre ogni insieme di interi ha un minimo (Principio del Buon Ordinamento ??).

Possiamo quindi definire il massimo comun divisore come

$$\text{mcd}(a, b) = \max(D(a) \cap D(b))$$

dove  $D(n) = \{x \mid x \setminus n\}$  è l'insieme dei divisori di  $n$ . Notate che l'insieme dei divisori di  $n$  ammette un massimo perchè è finito.

Consideriamo il problema di volere calcolare il massimo comun divisore di due interi  $a$  e  $b$ . Un modo banale consiste nel calcolare  $D(a)$  e  $D(b)$  e trovare l'elemento massimo della intersezione.

Per esempio, per  $a = 24$  e  $b = 36$  abbiamo

$$D(24) = \{1, 2, 3, 4, 6, 8, 12, 24\}$$

$$D(36) = \{1, 2, 3, 4, 6, 8, 12, 36\}$$

Quindi  $\text{mcd}(24, 36) = 12$ .

Un metodo più efficiente per calcolare il massimo comun divisore è il ben noto *Algoritmo di Euclide* che è basato sulla seguente proprietà.

**Teorema 2.2** *Sia  $a = b \times q + r$  dove  $a, b, q$  ed  $r$  sono interi. Allora  $\text{mcd}(a, b) = \text{mcd}(b, r)$ .*

**Prova:** Per dimostrare  $\text{mcd}(a, b) = \text{mcd}(b, r)$  dimostriamo una proprietà più forte, ovvero  $D(a) \cap D(b) = D(b) \cap D(r)$ .

Per fare vedere  $D(a) \cap D(b) = D(b) \cap D(r)$  dalla Proposizione ?? basta fare vedere che  $D(a) \cap D(b) \subseteq D(b) \cap D(r)$  e che  $D(b) \cap D(r) \subseteq D(a) \cap D(b)$ .

1. Per mostrare  $D(a) \cap D(b) \subseteq D(b) \cap D(r)$  facciamo vedere che se  $x \in D(a) \cap D(b)$  allora  $x \in D(b) \cap D(r)$ . Assumiamo quindi che  $x \in D(a) \cap D(b)$  e deriviamo che  $x \in D(b) \cap D(r)$ . Per Def. di  $\cap$ ,  $x \in D(a) \cap D(b)$  vuol dire che  $x \in D(a)$  ed  $x \in D(b)$ .

---

<sup>3</sup>In formule  $\max(A) = c \leftrightarrow c \in A \wedge \forall d(d \in A \rightarrow d \leq c)$

Notiamo che dal Lemma 2.1 dato che  $x \in D(b)$  abbiamo  $x \in D(b \times q)$ . Inoltre dato che  $x \in D(b \times q)$  ed  $x \in D(a)$  abbiamo  $x \in D(a - b \times q)$

Dalla premessa  $a = b \times q + r$  abbiamo quindi  $x \in D(r)$  (nota che  $r = a - (b \times q)$ ). Quindi  $x \in D(b)$  ed  $x \in D(r)$  e per Def. di  $\cap$ ,  $x \in D(b) \cap D(r)$ .

2. Analogo a sopra.

□

Il Teorema 2.2 suggerisce un algoritmo per calcolare il massimo comun divisore tra due interi. Ricordiamo che dati due interi positivi  $a$  e  $b$ , esistono due unici interi  $q$  ed  $r$ , con  $0 \leq r < b$ , tali che  $a = b \times q + r$ . Gli elementi  $q$  ed  $r$  sono detti rispettivamente il *quoziente* ed il *resto* della divisione di  $a$  per  $b$ . Notate che se il resto della divisione è zero, vuol dire che  $b$  è un fattore di  $a$ .

L'idea dell'algoritmo di Euclide è semplice. Siano  $a$  e  $b$  due interi positivi di cui vogliamo calcolare il massimo comun divisore. Dividiamo  $a$  per  $b$ , ottenendo per qualche  $q$  ed  $0 \leq r < b$

$$a = b \times q + r.$$

Se il resto è zero allora  $b \mid a$  e quindi il massimo comun divisore è  $b$  (ovviamente  $b \mid b$  ed è il massimo divisore di  $b$ ).

Se il resto è diverso da zero, allora dal Teorema 2.2 sappiamo che  $mcd(a, b) = mcd(b, r)$ . Quindi ripetiamo lo stesso procedimento per  $b$  ed  $r$ . Quando troviamo il resto zero abbiamo trovato il massimo comun divisore<sup>4</sup>.

Per esempio usiamo l'algoritmo di Euclide per calcolare  $mcd(287, 91)$ . Abbiamo

1. Dividiamo 287 per 91,  $287 = 91 \times 3 + 14$ . Siccome il resto è diverso da zero procediamo con 91 e 14;
2. Dividiamo 91 per 14,  $91 = 14 \times 6 + 7$ . Siccome il resto è diverso da zero procediamo con 14 e 7;
3. Dividiamo 14 per 7,  $14 = 7 \times 2$ . Abbiamo trovato il resto zero!

Abbiamo  $mcd(14, 7) = 7$ . Dal Teorema 2.2,  $7 = mcd(14, 7) = mcd(91, 14) = mcd(287, 91)$ .

### 3 Induzione

Supponiamo di volere provare sul dominio degli *interi positivi*<sup>5</sup>  $\mathcal{Z}^+$  un asserto del tipo  $\forall n P(n)$  dove  $P(n)$  è un asserto matematico dipendente dal valore della variabile  $n$ .

Consideriamo per esempio di volere dimostrare che per ogni intero positivo  $n$

“La somma dei primi  $n$  numeri dispari è uguale ad  $n^2$ ”.

---

<sup>4</sup>La procedura termina in quanto i resti ottenuti in successione sono decrescenti.

<sup>5</sup>O analogamente sul dominio dei numeri naturali  $\mathcal{N}$ .

Abbiamo

$$\begin{aligned}n = 1 & \quad 1^2 = 1 \\n = 2 & \quad 2^2 = 1 + 3 = 4 \\n = 3 & \quad 3^2 = 1 + 3 + 5 = 9 \\& \dots\end{aligned}$$

La proprietà sembra essere vera, ma l'abbiamo verificata fino ad  $n = 3$  e quindi non possiamo concludere che valga per ogni  $n$ . Potremmo sempre trovare un *controesempio*, ovvero un valore di  $n$  per cui la proprietà non vale. Per provarla dovremmo dimostrarla per  $n$  generico, ma questo è un po' difficile.

Come vedremo il dominio degli interi positivi o dei naturali gode di proprietà che ci permettono di applicare un metodo di dimostrazione molto conosciuto e potente, il *Principio di Induzione*.

Un asserto  $\forall n P(n)$  vale se valgono

**Caso Base**  $P(1)$ <sup>6</sup>

**Caso Induttivo**  $\forall x(P(n) \rightarrow P(n+1))$ .

**Nota** Notate che il caso induttivo non richiede di dimostrare  $P(n)$  per un  $n$  generico, ma per il ben noto significato di  $\rightarrow$ , richiede di dimostrare  $P(n+1)$  assumendo che  $P(n)$  valga.

Facciamo una prova per induzione della proprietà vista in precedenza che in modo più formale si può scrivere come

$$P(n) \leftrightarrow (1 + 3 + 5 \dots + (2n - 1) = n^2)$$

utilizzando il fatto che l'ennesimo numero dispari è  $2n - 1$ .

Dimostriamo quindi  $\forall n P(n)$  sul dominio degli interi positivi:

**Caso Base** Bisogna mostrare che vale  $P(1)$ . Abbiamo già visto che  $1^2 = 1$ .

**Caso Induttivo** Bisogna mostrare  $\forall n(P(n) \rightarrow P(n+1))$ , ovvero che  $P(n+1)$  segue da  $P(n)$  per un  $n$  generico.

Assumiamo che  $P(n)$  valga ovvero che

$$(1 + 3 + 5 \dots + (2n - 1) = n^2).$$

Dobbiamo derivare la validità di  $P(n+1)$  ovvero che  $1 + 3 + 5 \dots + (2n - 1) + (2(n+1) - 1) = (n+1)^2$ . Consideriamo  $1 + 3 + 5 \dots + (2n - 1) + (2(n+1) - 1)$  e sostituiamo l'ipotesi. Abbiamo applicando ben note proprietà algebriche,

$$1 + 3 + 5 \dots + (2n - 1) + (2(n+1) - 1) = n^2 + (2(n+1) - 1) = n^2 + 2n - 1 = (n+1)^2.$$

---

<sup>6</sup>La proprietà per  $n = 0$ .

**Nota**[Perchè l'induzione è un metodo di prova corretto sul dominio degli interi positivi (o dei naturali)?]

La validità del Principio di Induzione è basata su alcune proprietà specifiche del dominio degli interi positivi (Principio del Buon Ordinamento). Dato un insieme  $A \in \wp(\mathcal{Z}^+)$  definiamo il *minimo* di  $A$  come segue:  $\min(A) = a$ , tale che  $a \in A$  e  $a \leq b$  per ogni  $b \in A$ .

1. Per ogni  $A \in \wp(\mathcal{Z}^+)$ ,  $\min(A)$  è definito. In particolare abbiamo  $1 = \min(\mathcal{Z}^+)$ .
2. Per ogni intero  $n \neq 1$  esiste  $n - 1$  tale che  $n - 1 < n$ .

La correttezza del principio di induzione è analoga a quello di validità delle regole di inferenza e dei metodi di prova visti nella Sezioni ?? e ?? con la differenza che qui abbiamo un dominio particolare che gode delle proprietà 1) e 2) di sopra. Quindi facciamo vedere che se valgono sia  $P(1)$  che  $\forall n(P(n) \rightarrow P(n + 1))$  allora vale anche  $\forall nP(n)$ .

Facciamolo vedere per assurdo, assumiamo quindi che  $\forall nP(n)$  non valga. Questo equivale a dire che esiste un valore di  $n$  per cui  $P(n)$  è falso. Abbiamo quindi

$$S = \{n \in \mathcal{Z}^+ \mid P(n) \text{ è falso}\} \neq \emptyset.$$

Dato che  $S \in \wp(\mathcal{Z}^+)$ , sappiamo dal Principio del Buon Ordinamento che esiste  $a$  tale che  $a = \min(S)$  per cui  $P(a)$  è falso.

Dato che  $P(1)$  vale per ipotesi e  $P(a)$  è falso, allora  $a \neq 1$ . Quindi dalla seconda proprietà degli interi di sopra, abbiamo che  $a - 1$  è definito ed  $a - 1 < a$ .

Dato che  $a = \min(S)$  allora  $a - 1 \notin S$ . Quindi dalla Def. di  $S$ ,  $P(a - 1)$  vale.

Sappiamo che  $\forall n(P(n) \rightarrow P(n + 1))$  vale per ipotesi. Allora da  $P(a - 1)$  deriviamo (per modus ponens)  $P(a - 1 + 1) = P(a)$ . Abbiamo ottenuto una contraddizione dato che  $a \in S$ , ovvero  $P(a)$  è falso.

### 3.0.1 Esercizi

**Esercizio 3.1** *Si dimostri che per ogni intero positivo  $n$  si ha  $2 \mid (n^2 + n)$ .*

*Per induzione mostriamo che  $n^2 + n$  è multiplo di 2 (e.g.  $n^2 + n$  è divisibile per 2).*

**Caso Base** *Per  $n = 1$  abbiamo  $n^2 + n = 1 + 1 = 2$  e 2 è multiplo di 2.*

**Caso Induttivo** *Assumiamo che  $n^2 + n$  sia multiplo di 2 e facciamo vedere che  $(n + 1)^2 + (n + 1)$  è multiplo di 2. Abbiamo*

$$(n + 1)^2 + (n + 1) = (n^2 + 2n + 1) + (n + 1) = (n^2 + n) + (2n + 2).$$

*Per ipotesi induttiva  $n^2 + n$  è multiplo di 2. Inoltre  $(2n + 2)$  è ovviamente multiplo di 2. Concludiamo che  $(n^2 + n) + (2n + 2)$  è multiplo di 2 perchè somma di due multipli di 2.*

A volte può essere difficile definire un oggetto matematico (una sequenza, un insieme, una funzione etc.) in modo esplicito. È più agevole poterlo definire in termini di se stesso, ovvero in modo *ricorsivo-induttivo*.

In particolare una sequenza  $a_0, a_1, \dots, a_n, \dots$  si può definire in modo ricorsivo dandone i termini base e specificando una regola che permetta di trovare i termini successivi a partire da quelli prima<sup>7</sup>. Per esempio la sequenza delle potenze di 2 ( $a_n = 2^n$ ) si può definire in modo ricorsivo come

$$a_0 = 1$$

$$a_{n+1} = 2 \times a_n$$

Analogamente il fattoriale  $!n$  si può definire come

$$!0 = 1$$

$$!(n+1) = (n+1) \times !n.$$

**Esercizio 3.2 (Induzione)** *Dimostrare che  $2^n < !n$  per ogni intero  $n$  con  $n \geq 4$ .*

**Caso Base** *Bisogna mostrare che  $2^4 < !4$ . Abbiamo  $2^4 = 16$  e  $!4 = 4 \times 3 \times 2 \times 1 = 24$ .*

**Caso Induttivo** *Assumiamo l'ipotesi induttiva,*

$$2^n < !n \text{ dove } n \text{ è un intero con } n \geq 4$$

*e mostriamo che*

$$2^{(n+1)} < !(n+1).$$

*Dato che  $2^n < !n$  (per ipotesi induttiva) moltiplicando entrambe le parti per 2 abbiamo  $2 \times 2^n < 2 \times !n$ , ovvero  $2^{(n+1)} < 2 \times !n$ .*

*Dato che  $n \geq 4$ , abbiamo  $n+1 > 2$  e quindi  $2 \times !n < (n+1) \times !n$ . Dalla Def. di fattoriale sappiamo che  $!(n+1) = (n+1) \times !n$ . Quindi sostituendo abbiamo  $2 \times !n < !(n+1)$ .*

*Quindi per la proprietà transitiva di  $<$ , abbiamo*

$$2^{(n+1)} < 2 \times !n < !(n+1).$$

Una sequenza di numeri interi molto famosa è quella dei *Numeri di Fibonacci* che sono definiti induttivamente come segue.

$$f_0 = 0$$

$$f_1 = 1$$

$$f_n = f_{n-1} + f_{n-2}$$

---

<sup>7</sup>Lo stesso procedimento è alla base delle definizioni ricorsive di insiemi, funzioni etc. la cui trattazione esula dagli scopi del corso.

Abbiamo quindi

$$f_2 = f_1 + f_0 = 1$$

$$f_3 = f_2 + f_1 = 1 + 1 = 2$$

$$f_4 = f_3 + f_2 = 1 + 2 = 3$$

$$f_5 = f_4 + f_3 = 2 + 3 = 5$$

...

**Esercizio 3.3 (Induzione)** *Dimostrare che per ogni intero positivo  $n$*

$$\sum_{i=1}^n f_i^2 = f_n \times f_{n+1}.$$

**Caso Base** *Bisogna mostrare che la proprietà vale per  $n = 1$ . Abbiamo  $f_1^2 = 1 = f_1 \times f_2 = 1 \times 1$ .*

**Caso Induttivo** *Assumendo l'ipotesi induttiva*

$$\sum_{i=1}^n f_i^2 = f_n \times f_{n+1}$$

*mostriamo che*

$$\sum_{i=1}^{(n+1)} f_i^2 = f_{n+1} \times f_{n+2}.$$

*Abbiamo*

$$\sum_{i=1}^{(n+1)} f_i^2 = \sum_{i=1}^n f_i^2 + f_{n+1}^2.$$

*Dall'ipotesi induttiva*

$$\sum_{i=1}^{(n+1)} f_i^2 = (f_n \times f_{n+1}) + f_{n+1}^2$$

*Abbiamo per le ben note proprietà di  $\times$ ,*

$$(f_n \times f_{n+1}) + f_{n+1}^2 = f_{n+1} \times (f_n + f_{n+1}).$$

*Dalla Def. di Fibonacci  $f_{n+2} = f_{n+1} + f_n$ . Quindi sostituendo*

$$\sum_{i=1}^{(n+1)} f_i^2 = f_{n+1} \times f_{n+2}.$$

**Nota 3.4 (Numeri di Fibonacci)** *La successione di Fibonacci è interessante perchè è la soluzione al seguente problema. Supponiamo di avere una coppia di conigli (di sesso) diverso su un'isola. Supponendo che la legge di riproduzione dei conigli sia la seguente: dopo i due mesi di età ogni coppia "produce" un'altra coppia ogni mese. Quante coppie di conigli si trovano sull'isola dopo  $n$  mesi?*

*La soluzione è  $C_n = f_n$ :*

$$C_1 = 1$$

$$C_2 = 1$$

$$C_3 = 1 + 1 = 2 \quad \text{La prima coppia produce un'altra coppia}$$

$$C_4 = 2 + 1 = 3 \quad \text{La prima coppia produce un'altra coppia}$$

$$C_5 = 3 + 1 + 1 = 5 \quad \text{La prima e la seconda coppia producono un'altra coppia}$$

...

Abbiamo visto il *Principio di Induzione* e lo abbiamo applicato per provare proprietà sul dominio degli interi positivi (o dei naturali). Mostremo alcuni esempi che ci faranno capire come l'importanza del principio di induzione va ben oltre alla prova di proprietà specifiche nel dominio degli interi positivi. Infatti il principio di induzione si può applicare in ogni dominio analogo a  $\mathcal{Z}^+$ , che soddisfa il principio del buon ordinamento.

Vediamo per esempio l'utilizzo dell'induzione per provare due semplici proprietà sugli insiemi del tipo  $\forall n P(n)$  dove  $n \in \mathcal{Z}^+$ .

Consideriamo per esempio una importante proprietà degli insiemi vista nella Sezione ?? (Proposizione ??):

$$\overline{A \cap B} = \bar{A} \cup \bar{B}$$

dove  $\bar{A} = U - A$  e  $\bar{B} = U - B$  rispetto all'universo  $U$ . Utilizzando l'induzione si può fare vedere che la proprietà si può generalizzare alle famiglie di insiemi. Sia  $A_1, \dots, A_n$  una famiglia di insiemi con  $n \geq 2$  ed  $n \in \mathcal{N}$ ,

$$\overline{\bigcap_{i=1}^n A_i} = \bigcup_{i=1}^n \bar{A}_i.$$

La proprietà di sopra è infatti del tipo  $\forall n P(n)$ , dove  $P(n)$  dipende dal valore del numero naturale  $n$  è proprio,

$$\forall A_1, \dots, A_n \left( \overline{\bigcap_{i=1}^n A_i} = \bigcup_{i=1}^n \bar{A}_i \right).$$

Per dimostrarla possiamo usare l'induzione mostrando che

**Caso Base**  $P(2)$  vale, ovvero la proprietà vale per tutte le famiglie formate da due insiemi <sup>8</sup>;

**Caso Induttivo** se la proprietà vale per tutte le famiglie formate da  $n$  insiemi, allora vale per tutte le famiglie formate da  $n + 1$  insiemi.

**Caso Base** Per  $n = 2$  si tratta di fare vedere che

$$\overline{A \cap B} = \bar{A} \cup \bar{B}.$$

Facciamo vedere che  $\overline{A \cap B} \subseteq \bar{A} \cup \bar{B}$  e  $\bar{A} \cup \bar{B} \subseteq \overline{A \cap B}$ .

1. Consideriamo  $x \in \overline{A \cap B}$ . Dalla Def. di complemento, abbiamo  $x \in U$  ed  $x \notin A \cap B$ . Inoltre se  $x \notin A \cap B$  ci sono due casi: o  $x \notin A$  o  $x \notin B$  <sup>9</sup>.

Nel primo caso, dato che  $x \notin A$  ed  $x \in U$ , allora dalla Def. di complemento segue  $x \in \bar{A}$ . Dato che  $x \in \bar{A}$ , allora dalla Def. di  $\cup$  segue  $x \in \bar{A} \cup \bar{B}$ . Nel secondo caso, dato che  $x \notin B$  ed  $x \in U$ , allora dalla Def. di complemento segue  $x \in \bar{B}$ . Dato che  $x \in \bar{B}$ , allora dalla Def. di  $\cup$  segue  $x \in \bar{A} \cup \bar{B}$ .

Quindi possiamo concludere (dal ragionamento per casi) che  $x \in \bar{A} \cup \bar{B}$ . Dalla Def. di  $\subseteq$  otteniamo  $\overline{A \cap B} \subseteq \bar{A} \cup \bar{B}$ .

2. Consideriamo  $x \in \bar{A} \cup \bar{B}$ . Dalla Def. di  $\cup$  abbiamo due casi: o  $x \in \bar{A}$  o  $x \in \bar{B}$ .

Nel primo caso  $x \in \bar{A}$  vuol dire per Def. di complemento che  $x \in U$  e  $x \notin A$ . Dato che  $x \notin A$  segue dalla Def. di  $\cap$  che  $x \notin A \cap B$ . Nel secondo caso  $x \in \bar{B}$  vuol dire per Def. di complemento che  $x \in U$  e  $x \notin B$ . Dato che  $x \notin B$  segue dalla Def. di  $\cap$  che  $x \notin A \cap B$ .

Quindi possiamo concludere dal ragionamento per casi che  $x \in U$  and  $x \notin A \cap B$ . Dalla Def. di complemento abbiamo  $x \in \overline{A \cap B}$ . Dalla Def. di  $\subseteq$  otteniamo  $\bar{A} \cup \bar{B} \subseteq \overline{A \cap B}$ .

**Caso induttivo** Facciamo vedere che, assumendo

$$\overline{\bigcap_{i=1}^n A_i} = \bigcup_{i=1}^n \bar{A}_i$$

vale

$$\overline{\bigcap_{i=1}^{n+1} A_i} = \bigcup_{i=1}^{n+1} \bar{A}_i.$$

Abbiamo sostituendo l'*ipotesi induttiva*,

$$\bigcup_{i=1}^{n+1} \bar{A}_i = \left( \bigcup_{i=1}^n \bar{A}_i \right) \cup \bar{A}_{n+1} = \overline{\left( \bigcap_{i=1}^n A_i \right) \cup A_{n+1}}.$$

<sup>8</sup>Notate che l'induzione parte da  $n = 2$  perchè  $\cap$  e  $\cup$  richiedono almeno due argomenti.

<sup>9</sup>ricordate che  $\neg(x \in A \cap B) \equiv \neg(x \in A \wedge x \in B) \equiv x \notin A \vee x \notin B$ .

Inoltre per la proprietà dimostrata nel caso base,

$$\overline{\left(\bigcap_{i=1}^n A_i\right) \cup A_{n+1}} = \overline{\left(\bigcap_{i=1}^n A_i\right)} \cap A_{n+1}.$$

Il seguente esercizio si può dimostrare in modo simile.

**Esercizio 3.5** *Dimostrare che*

$$\overline{\bigcup_{i=1}^n A_i} = \bigcap_{i=1}^n \bar{A}_i.$$

Vediamo ora un altro esempio. Sia  $A$  un insieme finito<sup>10</sup>. Diciamo che  $A$  ha *cardinalità*  $n$  ( $|A| = n$ ), con  $n \in \mathcal{N}$ , sse  $A$  ha  $n$  elementi.

Per esempio l'insieme  $A = \{a, b, c\}$  ha cardinalità 3, mentre  $\emptyset$  ha cardinalità 0. Consideriamo l'insieme delle parti di  $A$ . Abbiamo

$$\wp(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, A\}.$$

Notiamo che  $|\wp(A)| = 8 = 2^3$ .

Questa relazione tra cardinalità di  $A$  e cardinalità di  $\wp(A)$  vale più in generale, cioè per ogni cardinalità.

**Teorema 3.6** *Sia  $A$  un insieme tale che  $|A| = n$ . Allora  $|\wp(A)| = 2^n$ .*

La proprietà del Teorema 3.6 è una proprietà del tipo  $\forall n P(n)$  dove  $P(n)$  dipende dal valore del numero naturale  $n$ , cioè dalla cardinalità dell'insieme  $A$ . Formalmente potremmo scrivere  $P(n)$  come

$$\forall A (|A| = n \rightarrow |\wp(A)| = 2^n).$$

Dato che la cardinalità è un numero naturale, possiamo usare l'induzione per dimostrare il Teorema, facendo vedere che

**Caso Base** la proprietà vale per tutti gli insiemi di cardinalità 0;

**Caso Induttivo** se la proprietà vale per tutti gli insiemi di cardinalità  $n$  allora la proprietà vale per tutti quelli di cardinalità  $n + 1$ .

**Prova:** **Caso Base** Mostriamo  $P(0)$ , ovvero

$$\forall A (|A| = 0 \rightarrow |\wp(A)| = 2^0 = 1).$$

Consideriamo quindi un generico  $A$  tale che  $|A| = 0$ <sup>11</sup>. Notiamo che  $A$  non può che essere l'insieme vuoto  $\emptyset$ . Dato che l'insieme vuoto ha come sottoinsieme solo se stesso, abbiamo  $\wp(\emptyset) = \{\emptyset\}$ . Quindi  $|\wp(\emptyset)| = 1$ .

<sup>10</sup>Nelle prossime lezioni vedremo come estendere il concetto di cardinalità ad insiemi infiniti.

<sup>11</sup>Notate che stiamo assumendo la premessa dell'implicazione che dobbiamo provare.

**Caso Induttivo** Dobbiamo mostrare che vale  $\forall A(|A| = n + 1 \rightarrow |\wp(A)| = 2^{n+1})$  assumendo che  $\forall B(|B| = n \rightarrow |\wp(B)| = 2^n)$ .

Consideriamo quindi un generico  $A$  tale che  $|A| = n + 1$ <sup>12</sup>. Notiamo che deve esistere un insieme  $C$  con  $|C| = n$  ed elemento dell'universo  $a$  tale che  $A = C \cup \{a\}$ . Quindi  $C \subset A$  e  $\wp(C) \subset \wp(A)$ . Ma possiamo dire anche qualcosa di più. Dato che  $A = C \cup \{a\}$  abbiamo che

1. ogni  $X \in \wp(A)$  è tale che  $X \in \wp(C)$  o  $X = Y \cup \{a\}$  dove  $Y \in \wp(C)$ ;
2. per ogni  $Y \in \wp(C)$  sia  $Y \in \wp(A)$  che  $Y \cup \{a\} \in \wp(A)$ .

In altre parole ogni sottoinsieme  $Y$  di  $C$  produce esattamente due sottoinsiemi di  $A$ ,  $Y$  ed  $Y \cup \{a\}$ . Quindi,  $|\wp(A)| = 2 \times |\wp(C)|$ . Per *ipotesi induttiva* abbiamo  $|\wp(C)| = 2^n$ . Quindi sostituendo

$$|\wp(A)| = 2 \times 2^n = 2^{n+1}.$$

□

---

<sup>12</sup>Notate che stiamo assumendo la premessa dell'implicazione che dobbiamo provare.