Lezione 3.
Il Principio d'Induzione

Il primo insieme notevole cui siamo interessati è quello dei numeri naturali, cioè

$$\mathbb{N} = \{\ 1, 2, 3, 4, \ldots, n, n+1, \ldots\ \}.$$

Talvolta considereremo anche $\mathbb{N}_0 = \mathbb{N} \cup \{\ 0\ \}$. Spesso conviene pensare a $\mathbb{N}$ e $\mathbb{N}_0$ come sottoinsiemi dell'insieme dei numeri interi

$$\mathbb{Z} = \{\ 0, \pm 1, \pm 2, \pm 3, \pm 4, \ldots, \pm n, \pm(n+1), \ldots\ \mid n \in \mathbb{N}\ \}.$$

Nel seguito indicheremo con I_n l'insieme dei primi numeri naturali, cioè

$$I_n = \{\ 1, 2, 3, 4, \ldots, n\ \} \subseteq \mathbb{N}.$$

Per esempio

$$I_1 = \{\ 1\ \}, \qquad I_2 = \{\ 1, 2\ \}, \qquad I_3 = \{\ 1, 2, 3\ \}.$$

Ricordiamo che in $\mathbb{N}$ sono definite un'operazione di somma e una di moltiplicazione tali che:

- $n + m = m + n$ per ogni $n, m \in \mathbb{N}$;
- $(n + m) + k = m + (n + k)$ per ogni $n, m, k \in \mathbb{N}$;
- $nm = mn$ per ogni $n, m \in \mathbb{N}$;
- $(nm)k = m(nk)$ per ogni $n, m, k \in \mathbb{N}$;
- $(n + m)k = nk + mk$ per ogni $n, m, k \in \mathbb{N}$.

Tali operazioni di somma e prodotto sono compatibili con l'ordinamento totale naturale definito su $\mathbb{N}$.

Esiste una teoria assiomatica (la cosiddetta *assiomatica di Peano*) che permette di individuare univocamente l'insieme $\mathbb{N}$, le operazioni di somma e prodotto definite in esso, nonché la relazione d'ordine.

Uno degli assiomi di Peano è il seguente *Principio di induzione*: esso è un primo strumento importante legato a $\mathbb{N}$.

Assioma 3.2 (Principio di induzione nella forma di Peano)**.** *Sia $S \subseteq \mathbb{N}$ tale che $1 \in S$. Se per ogni $n \in S$ anche $n + 1 \in S$, allora $S = \mathbb{N}$.*

Normalmente il Principio di induzione viene utilizzato per dimostrare degli enunciati che dipendono da un numero naturale (o intero): in tal caso si usa la seguente forma.

Assioma 3.3 (Principio di induzione)**.** *Sia $P(k)$ una proprietà che dipende da $k \in \mathbb{N}$. Se*

1. *$P(1)$ è vera;*
2. *per ogni $n \geq 1$, il fatto che $P(n)$ sia vera implica che $P(n+1)$ è vera;*

allora $P(k)$ è vera per ogni $k \in \mathbb{N}$.

Osservazione 3.3. *Talvolta il Principio di induzione viene formulato come segue. Sia $P(k)$ una proprietà che dipende da $k \in \mathbb{N}$. Se*

1. *esiste $n_0 \in \mathbb{Z}$ tale che $P(n_0)$ è vera;*
2. *per ogni $n \geq n_0$, il fatto che $P(n)$ sia vera implica che $P(n+1)$ è vera;*

allora $P(k)$ è vera per ogni $k \in \mathbb{Z}$, $k \geq n_0$.

Diamo alcuni esempi di applicazione del Principio d'induzione.

Esempio 3.13. Dimostriamo per induzione che $I_n \approx I_m$ se e solo se $n = m$.

Chiaramente, se $n = m$, l'applicazione identità su I_n è biiettiva, dunque $I_n \approx I_m$.

Viceversa sia $I_n \approx I_m$ e supponiamo che $n \leq m$. Se $n = 1$ e $\varphi\colon I_1 \to I_m$ è biiettiva, allora è anche suriettiva: pertanto $m = 1$. Supponiamo vera la tesi per un fissato $n \geq 1$ e verifichiamola per $n+1$. Sia $\varphi\colon I_{n+1} \to I_m$ biiettiva e sia $u = \varphi(n+1) \in I_m$. L'applicazione

$$\begin{aligned} \tau\colon I_m &\longrightarrow I_m \\ k &\longrightarrow \begin{cases} k & \text{se } k \neq u, m, \\ u & \text{se } k = m, \\ m & \text{se } k = u \end{cases} \end{aligned}$$

è biiettiva, sicché anche $\tau \circ \varphi\colon I_{n+1} \to I_m$ lo è. Poiché

$$\tau \circ \varphi(n+1) = \tau(u) = m,$$

segue che $\varphi_{|I_n}$ è una biiezione da I_n su I_{m-1}, quindi per ipotesi induttiva $n = m - 1$ ovvero $n + 1 = m$.

La tesi è dunque dimostrata per induzione.

Esempio 3.14. Dimostriamo per induzione che se $x_1, \ldots, x_n, y_1, \ldots, y_m \in \mathbb{N}$, allora

$$\left(\sum_{i=1}^{n} x_i\right)\left(\sum_{j=1}^{m} y_j\right) = \sum_{i=1}^{n}\left(\sum_{j=1}^{m} x_i y_j\right) :$$

tale uguaglianza è detta *proprietà distributiva generalizzata della somma rispetto all'addizione*.

Sia $n = 1$. Se $m = 1$ non c'è nula da dimostrare, mentre per $m = 2$ è l'usuale regola distributiva

$$x_1(y_1 + y_2) = x_1y_1 + x_1y_2.$$

Supponiamo che sia verificata per m, cioè

$$x_1 \left(\sum_{j=1}^{m} y_j \right) = \sum_{j=1}^{m} x_1 y_j.$$

Risulta

$$x_1 \left(\sum_{j=1}^{m+1} y_j \right) = x_1 \left(\left(\sum_{j=1}^{m} y_j \right) + y_{m+1} \right).$$

Utilizzando la formula per $m = 2$ e, poi, l'ipotesi induttiva, otteniamo

$$x_1 \left(\sum_{j=1}^{m+1} y_j \right) = x_1 \left(\sum_{j=1}^{m} y_j \right) + x_1 y_{m+1} = x_1 \sum_{j=1}^{m} y_j + x_1 y_{m+1} = \sum_{j=1}^{m} x_1 y_j.$$

Ciò dimostra l'uguaglianza per $n = 1$ e ogni $m \in \mathbb{N}$.

Supponiamo che l'uguaglianza sia vera per un certo n e per ogni $m \in \mathbb{N}$: dimostriamola per $n + 1$ e per ogni $m \in \mathbb{N}$. Si ha

$$\left(\sum_{i=1}^{n+1} x_i \right) \left(\sum_{j=1}^{m} y_j \right) = \left(\sum_{i=1}^{n} \left(\sum_{j=1}^{m} x_i y_j \right) + x_{n+1} \right) \left(\sum_{j=1}^{m} y_j \right).$$

La proprietà distributiva ordinaria implica allora

$$\left(\sum_{i=1}^{n+1} x_i \right) \left(\sum_{j=1}^{m} y_j \right) = \left(\sum_{i=1}^{n} x_i \right) \left(\sum_{j=1}^{m} y_j \right) + x_{n+1} \left(\sum_{j=1}^{m} y_j \right).$$

Per l'ipotesi induttiva e per la proprietà generalizzata per $n = 1$ abbiamo allora

$$\left(\sum_{i=1}^{n+1} x_i \right) \left(\sum_{j=1}^{m} y_j \right) = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} x_i y_j \right) + \sum_{j=1}^{m} x_{n+1} y_j = \sum_{i=1}^{n+1} \left(\sum_{j=1}^{m} x_i y_j \right).$$

La tesi è dunque dimostrata per induzione.

Esempio 3.15. Dimostriamo per induzione la formula del binomio di Newton: se $a, b, n \in \mathbb{N}$ allora

$$(a + b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i},$$

ove per $1 \leq i \leq n - 1$

$$\binom{n}{0} = \binom{n}{n} = 1, \qquad \binom{n}{i} = \frac{n!}{i!(n-i)!}.$$

L'uguaglianza è banalmente vera se $n = 1$. Supponiamola vera per un certo $n \geq 1$ e dimostriamola per $n + 1$. Per ipotesi induttiva isulta

$$\begin{aligned}(a+b)^{n+1} &= (a+b)^n(a+b) = \\ &= \left(\sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}\right)(a+b) = \\ &= \sum_{i=0}^{n} \binom{n}{i} a^{i+1} b^{n-i} + \sum_{i=0}^{n} \binom{n}{i} a^i b^{n+1-i}.\end{aligned}$$

Si ha

$$\sum_{i=0}^{n} \binom{n}{i} a^{i+1} b^{n-i} = \sum_{i=1}^{n+1} \binom{n}{i-1} a^i b^{n+1-i},$$

dunque

$$\begin{aligned}(a+b)^{n+1} &= a^{n+1} + \sum_{i=1}^{n} \binom{n}{i-1} a^i b^{n+1-i} + \sum_{i=1}^{n} \binom{n}{i} a^i b^{n+1-i} + b^{n+1} = \\ &= a^{n+1} + \sum_{i=1}^{n} \left(\binom{n}{i-1} + \binom{n}{i}\right) a^i b^{n+1-i} + b^{n+1}.\end{aligned}$$

Si ha

$$\begin{aligned}\binom{n}{i-1} + \binom{n}{i} &= \frac{n!}{(i-1)!(n+1-i)!} + \frac{n!}{i!(n-i)!} = \\ &= \frac{n!}{(i-1)!(n-i)!}\left(\frac{1}{n+1-i} + \frac{1}{i}\right) = \\ &= \frac{n!}{(i-1)!(n-i)!}\frac{n+1}{i(n+1-i)} = \frac{(n+1)!}{i!(n+1-i)!} = \binom{n+1}{i}.\end{aligned}$$

Pertanto

$$(a+b)^{n+1} = a^{n+1} + \sum_{i=1}^{n} \binom{n+1}{i} a^i b^{n+1-i} + b^{n+1} = \sum_{i=0}^{n+1} \binom{n+1}{i} a^i b^{n+1-i}.$$

La tesi è dunque dimostrata per induzione.

Osservazione 3.4. *La formula di Newton ha come conseguenza interessante che $\mathscr{P}(I_n)$ ha 2^n elementi. Infatti $\mathscr{P}(I_n)$ contiene un solo sottoinsieme di I_n con 0 elementi (cioè $\emptyset$); n sottoinsiemi di I_n con un solo elemento; in generale $\binom{n}{i}$ sottoinsiemi con i elementi.*

Quindi $\mathscr{P}(X)$ contiene in totale

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

sottoinsiemi di I_n. Questo è uno dei motivi per cui talvolta si scrive anche 2^X in luogo di $\mathscr{P}(X)$.

Un altro motivo è che ogni sottoinsieme $Y \subseteq X$ individua ed è individuato univocamente dalla sua funzione indicatrice

$$\begin{aligned} 1_Y \colon X &\longrightarrow \{\ 0,1\ \} \\ x &\longrightarrow \begin{cases} 0 & \text{se } x \notin Y, \\ 1 & \text{se } x \in Y. \end{cases} \end{aligned}$$

Poiché l'insieme delle funzioni da X a $\{\ 0,1\ \}$, allora $\mathscr{P}(X) = \{\ 0,1\ \}^X$.

La formulazione data del Principio d'induzione viene anche detta *Principio di induzione in forma debole* per distinguerla dalla seguente che ha, apparentemente, delle ipotesi più restrittive: in realtà si può dimostrare che le due formulazioni sono, di fatto, equivalenti.

Assioma 3.4 (Principio di induzione in forma forte)**.** *Sia $P(k)$ una proprietà che dipende da $k \in \mathbb{N}$. Se*

1. *$P(1)$ è vera;*
2. *per ogni $n \geq 1$, il fatto che $P(m)$ sia vera per ogni $m \leq n$ implica che $P(n+1)$ è vera;*

allora $P(k)$ è vera per ogni $k \in \mathbb{N}$.

Esempio 3.16. Ricordiamo che dati $a, b \in \mathbb{N}_0$ diciamo che a è multiplo di b se esiste $c \in \mathbb{N}_0$ tale che $a = bc$. Se a è multiplo di b si dice anche che b divide a, ovvero che b è un divisore di a: 1 e a sono divisori di a, detti banali, mentre ogni altro eventuale divisore si dice proprio.

Un numero $p \in \mathbb{N}_0$ si dice primo se non ha divisori propri, cioè i suoi unici divisori sono 1 e p: convenzionalmente 1 non viene considerato primo.

Dimostriamo per induzione (forte) che ogni $n \in \mathbb{N} \setminus \{\ 1\ \}$ si scrive come prodotto finito di numeri primi. Se $n = 2$ questo è ovvio, visto che 2 è primo.

Supponiamo che la tesi sia vera per ogni $m \leq n$ e dimostriamola per $n+1$. Se $n+1$ è primo non c'è nulla da dimostrare, sicché possiamo supporre che $n+1$ abbia un divisore proprio a con $1 < a < n+1$. Allora esiste b tale che $n+1 = ab$: è facile verificare che $1 < b < n+1$. Poiché $1 < a, b \leq n$ segue che ciascuno di essi si scrive come prodotto di un numero finito di primi, diciamo

$$a = \prod_{i=1}^{u} p_i, \qquad b = \prod_{j=1}^{v} q_i.$$

Allora

$$n+1 = \prod_{i=1}^{u} p_i \prod_{j=1}^{v} q_i.$$

La tesi è dunque dimostrata per induzione (forte).

Vale un risultato analogo anche per ogni intero diverso da 0 e ± 1 definendo come numeri primi in $\mathbb{Z}$ i numeri positivi privi di divisori propri. In tal caso, ogni $x \in \mathbb{Z}$ si può scrivere come il prodotto di ± 1 per un numero finito di numeri primi.

Verificheremo in seguito che tale scomposizione è anche unica a meno dell'ordine dei fattori.

Il Principio di induzione implica il seguente *Principio di buon ordinamento*.

Proposizione 3.6 (Principio di buon ordinamento)**.** *Ogni sottoinsieme non vuoto $S \subseteq \mathbb{N}$ ha un primo elemento.*

Dimostrazione. Sia $S \subseteq \mathbb{N}$ un insieme privo di un primo elemento: dimostriamo che $S = \emptyset$, verificando per induzione (forte) che $\mathbb{N} \setminus S = \mathbb{N}$. Infatti $1 \notin S$, altrimenti 1 sarebbe un primo elemento, poiché non esistono numeri naturali più piccoli di 1. Supponiamo che $I_n \subseteq \mathbb{N} \setminus S$: se $n+1 \notin \mathbb{N} \setminus S$ allora $n+1 \in S$, dunque $n+1$ sarebbe un primo elemento di S visto che S non contiene elementi minori. □

Osservazione 3.5. *In realtà si può dimostrare che il Principio del buon ordinamento implica il Principio di induzione.*

Sia $S \subseteq \mathbb{N}$ contenente 1 e tale che se contiene n allora contiene anche $n+1$: vogliamo dimostrare che $S = \mathbb{N}$, cioè che $\mathbb{N} \setminus S = \emptyset$.

Supponiamo che $\mathbb{N} \setminus S \neq \emptyset$ e sia m il suo primo elemento: poiché $1 \in S$ segue che $1 \notin \mathbb{N} \setminus S$, sicché $m > 1$. Per definizione di m si ha $m-1 \in S$: per la definizione di S allora $m = (m-1)+1 \in S$, una contraddizione. Deduciamo che $S = \mathbb{N}$.

Chiaramente il Principio del buon ordinamento vale anche per ogni sottoinsieme di $\mathbb{Z}$ avente un primo elemento, per esempio $\mathbb{N}_0$.

Esempio 3.17. In $\mathbb{N}_0$ vale *l'Algoritmo euclideo di divisione*, cioè per ogni $a \in \mathbb{N}_0$ e $b \in \mathbb{N}$ esistono unici $q, r \in \mathbb{N}_0$ (detti rispettivamente quoziente e resto) con $0 \leq r \leq b$ tali che $a = qb + r$. In particolare b è divisore di a se e solo se il resto della divisione intera di a per b è 0.

Infatti sia

$$S = \{\ a - qb \mid q \in \mathbb{N}_0\ \} \subseteq \mathbb{N}_0.$$

S è non vuoto, perché $a = a - 0b \in S$. Sia r il primo elemento di S, sicché $a = qb + r$: si noti che $0 \leq r$. Inoltre se fosse $r \geq b$ avremmo che $0 \leq r - b = a - (q+1)b \in S$, dunque S conterrebbe un elemento più piccolo di r, contraddicendone la definizione.

Sia anche $a = q'b + r'$ per qualche r' con $0 \leq r' < b$ e supponiamo che $q' < q$: allora $aq + r = aq' + r'$ implica

$$b \leq b(q - q') = r' - r < b,$$

dunque $r = r'$, $q = q'$.

La stessa dimostrazione si può estendere a qualsiasi coppia $a, b \in \mathbb{Z}$ con $b \neq 0$. Infatti basta verificare che

$$S = \{\ a - qb \mid q \in \mathbb{Z}\ \} \cap \mathbb{N}_0 \neq \emptyset.$$

Se $a \geq 0$ questo è ovvio. Se $a < 0$ e $b > 0$, scelto $q = a$ risulta $a - qb = -a(b-1) \geq 0$. Se $a < 0$ e $b < 0$, scelto $q = -a$ risulta $a - qb = -a(-b-1) \geq 0$.

Osservazione 3.6. *È interessante osservare che quanto dimostrato sopra insieme all'esempio 3.17 implica anche che i numeri primi (in $\mathbb{N}$ o $\mathbb{Z}$) sono infiniti. Infatti supponiamo che esistano un numero finito di primi, diciamo $p_1, \ldots, p_t$ e consideriamo*

$$q = 1 + \prod_{i=1}^{t} p_i \neq 1 :$$

allora $q \neq p_i$, perché $q > p_i$. Inoltre q ha una scomposizione in numeri primi per quanto visto sopra, ma nessuno dei p_i è un suo fattore, perché il resto della divisione intera di q per p_i è sempre $1 \neq 0$.

Quindi deve esistere un altro numero primo diverso dai precedenti, una contraddizione.