

Nota La parte delle dispense che va dall'Esame 4.1 p. 12 (incluso) fino a tutta pagina 19 non verrà fatta e quindi non verrà chiesta all'esame.]

L'ASSIOMA DI BUON ORDINAMENTO

DFF. 7.2 Sia X un insieme e sia \leq un ordinamento su X . Consideriamo A un sottinsieme di X . Diciamo che un elemento z di A è un minimo di A se $z \leq x$ per ogni $x \in A$. Se ciò è verificato, allora scriviamo $z = \min(A)$.

OSSERVAZIONE Se z è un minimo di A , allora tale minimo è unico. Infatti, se esistesse $z' \in A$ t.c. $z' \leq x \quad \forall x \in A$, allora $z' \leq z \leq z' \stackrel{\text{ASSUM.}}{\Rightarrow} z = z'$

DFT. 7.3 Un ordinamento totale \leq su un dato insieme X si dice essere un BUON ORDINAMENTO di X se ogni sottinsieme non vuoto di (X, \leq) ammette minimo. Se ciò è verificato, allora (X, \leq) si dice INSIEME BEN ORDINATO.

TEOREMA 7.4 (BUON ORDINAMENTO DEI NUMERI NATURALI)

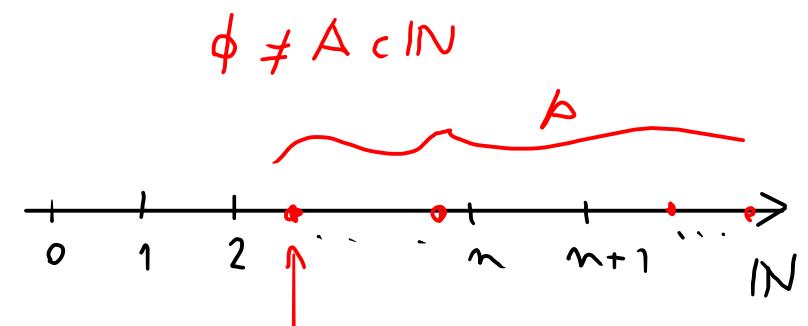
(\mathbb{N}, \leq) è un insieme ben ordinato, dove \leq è l'ordinamento usuale su \mathbb{N} (ovvero, dati $n, m \in \mathbb{N}$, $n \leq m$ se $\exists k \in \mathbb{N}$ t.c. $n+k=m$).]

DISC. Dobbiamo provare che se un sottinsieme

A di \mathbb{N} non possiede minimo allora $A = \emptyset$.

Sia A un sottinsieme di \mathbb{N} senza minimo.

Definiamo $B := \mathbb{N} \setminus A$. Dobbiamo provare che $B = \mathbb{N}$, ovvero che $A = \emptyset$.



Dimostrazione per induzione su $n \in \mathbb{N}$ che vale ciò che segue:

$$\forall n \in \mathbb{N}, \quad \underbrace{\{0, 1, \dots, n\}}_{P(n)} \subset B.$$

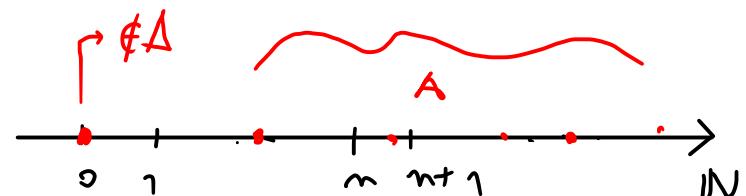
Osserviamo, se ciò è vero, allora $n \in \{0, 1, \dots, n\} \subset B \Rightarrow n \in B$ $\forall n \in \mathbb{N} \Rightarrow B = \mathbb{N}$.

(BASSE INDUT.) $n=0$ Dobbiamo provare che $\{0\} \subset B$, ovvero $0 \in B$.

Osserviamo $0 \notin A$, altrimenti $0 = \min(A)$ ma

A non possiede il minimo per ipotesi. Dunque,

$$0 \notin A \Rightarrow 0 \in \mathbb{N} \setminus A = B \Rightarrow \{0\} \subset B.$$



(PASSO INDUTT.) $n \Rightarrow n+1$ Assumiamo che $\{0, 1, \dots, n\} \subset B$ per qualche $n \in \mathbb{N}$ (ip. ind.). Dobbiamo dimostrare che $\{0, 1, \dots, n, n+1\} \subset B$, ovvero $n+1 \in B$.

Per ip. ind., $\{0, 1, \dots, n\} \cap A = \emptyset$ dunque

$A \subset \{n+1, n+2, \dots\}$. Segue che

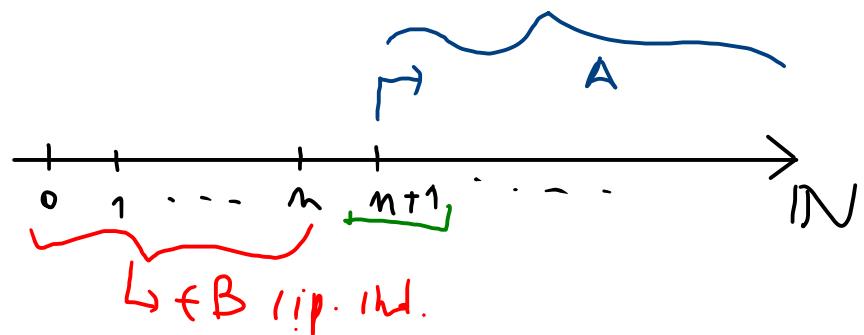
$n+1 \notin A$, altrimenti $n+1 = \min(A)$, che

è impossibile per ipotesi (A non ha minimo). Dunque:

$$n+1 \notin A \Leftrightarrow n+1 \in \mathbb{N} \setminus A = B \Rightarrow \{0, 1, \dots, n, n+1\} \subset B.$$

Il passo induttivo è stato fatto. Dunque grazie al princ. di induz. (d'1^a forma), vale che

$$\{0, 1, \dots, n\} \subset B \text{ per } \forall n \in \mathbb{N} \Rightarrow B = \mathbb{N}.$$



PRINCIPIO DI INDUT. D. 2^a FORMA

Teorema 7.5 Sia $\{P(m)\}_{m \in \mathbb{N}}$ una famiglia di proposizioni indicate su \mathbb{N} .

Supponiamo che valgano le seguenti due proprietà:

(1) (Base dell'indut.) $P(0)$ è vera.

(2) (Passo Indut.) Per ogni $n > 0$, se $P(k)$ è vera per ogni $k \in \mathbb{N}$ t.r. $0 \leq k < n$,
allora $P(n)$ è vera.

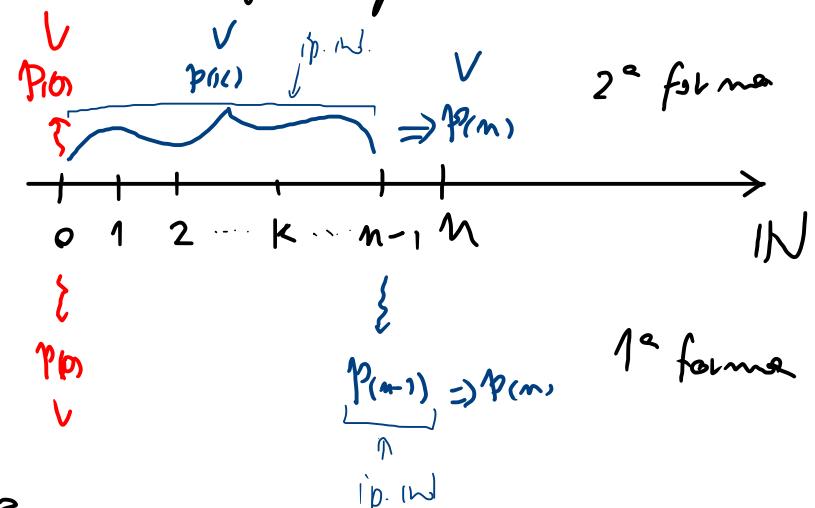
Allora $P(n)$ è vera $\forall n \in \mathbb{N}$.

DIM. Sia $A := \{m \in \mathbb{N} \mid P(m) \text{ è falso}\}$.

Dobbiamo provare che $A = \emptyset$. Supponiamo per esempio

che $A \neq \emptyset$. Grazie al teorema di buon ordinamento di \mathbb{N} , A ha un minimo m .

Osserviamo che $m \in A \Rightarrow P(m)$ è falso. Da (1), segue $m \neq 0$.



Dunque, se $k \in \mathbb{N}$ t.c. $0 \leq k < m = \min(A)$,

allora $k \notin A$, ovvero $P(k)$ è vera. Da (2),

segue che $P(m)$ è vera, che è impossibile.

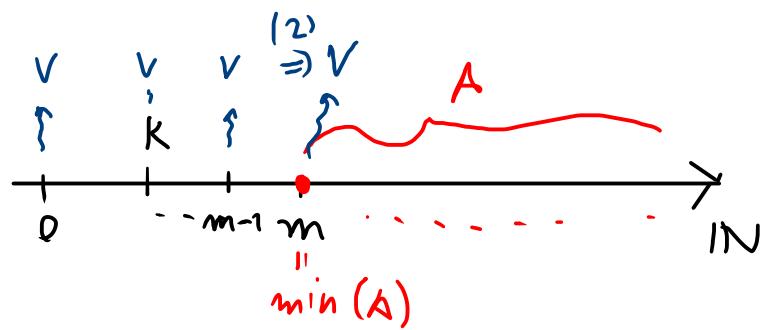
Segue che $A = \emptyset$, ovvero $P(m)$ è vera $\forall m \in \mathbb{N}$. \square

LA DIVISIONE EUCLIDEA

Assumiamo di conoscere l'insieme $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, \dots, n, \dots\}$ dei numeri interi.

TEOREMA (ESISTENZA ED UNICITÀ DELLA DIVISIONE EUCLIDEA SU \mathbb{Z}) Siano $m, m_0 \in \mathbb{Z}$ t.c.

$m \neq 0$. Allora esistono, e sono unici, $q, r \in \mathbb{Z}$ t.c. $\begin{cases} m = qm_0 + r \\ 0 \leq r < |m| \end{cases}$ (q si dice QUOTIENTE
di m per m_0)
Inoltre, $q, r \in \mathbb{N}$ se $m, m_0 \in \mathbb{N}$.



DIM. ESISTENZA DI q e r

$m \neq$ fissato

Assumiamo che $n, m \in \mathbb{N}$, $\underline{m > 0}$. Procediamo per induz. d. 2^e forme su $m \in \mathbb{N}$.

(BASE INDUT.) $n=0$ è suff. parre $q:=0, r:=0$; infatti vale:

$$\left\{ \begin{array}{l} n=0 = \overset{0}{\underset{\parallel}{q}} \cdot m + \overset{0}{\underset{\parallel}{r}} \quad \text{VERA} \\ 0 \leq r < m \\ \overset{||}{0} \end{array} \right.$$

Dunque se $m=0$, per esistono: $q=r:=0$.

(PASSO INDUTTIVO) $(\forall k < n) \Rightarrow n \sqrt{\text{Assumiamo l'esistenza di un quoziente e d. un resto}}$

per la divisione di n : $k \in \mathbb{Z}$ t. c. $0 \leq k < n$ (ip. Ind.). Dobbiamo provare l'esistenza

di un quoz. e d. resto della divisione di n per m . Se $\underline{n < m}$, allora $q:=0$ e $r:=n$, vale:

$$\left\{ \begin{array}{l} n = \overset{0}{\underset{\parallel}{q}} \cdot m + \overset{n}{\underset{\parallel}{r}} \quad \text{VERA} \\ 0 \leq \overset{m}{\underset{\parallel}{r}} < m \quad \text{VERA} \end{array} \right.$$

Supponiamo che $n \geq m$. Poniamo $k := n - m$. OSSERVARE che: $0 \leq k < m$. Per ip. ind.

$\exists q, r \in \mathbb{N}$ t.c.

$$\begin{cases} k = qm + r \\ 0 \leq r < m \end{cases}$$

Vale: $n = k + m = qm + r + m = (q+1)m + r$. Poi da

$$\begin{cases} n = (q+1)m + r \\ 0 \leq r < m \end{cases}, \text{ il passo indutt.}$$

è stato fatto. Dunque grazie al principio d'induz. di 2^a forma, \exists sempre q e r delle divisioni di n per m con $n, m \in \mathbb{N}$, $m > 0$.

Supponiamo che $n < 0$ e $m > 0$. Grazie alle parti precedenti, $\exists q, r \in \mathbb{N}$ t.c.

$$\begin{cases} -n = qm + r \\ 0 \leq r < m \end{cases}$$

Vale: $-n = qm + r \Rightarrow n = -qm - r = (-q)m - r$. Se $r = 0$, allora

$$\begin{cases} n = (-q)m + 0 \\ 0 \leq 0 < m \end{cases}$$

Supp. che $r > 0$, ovvero $0 < r < m \Leftrightarrow 0 < m - r < m$. Vale:

$$n = (-q)m - r = \boxed{(-q)m} - \boxed{m + m - r} = (-q - 1)m + (m - r).$$

Poiché $\begin{cases} n = (-q - 1)m + (m - r) \\ 0 \leq m - r < m \end{cases}$, $-q - 1$ è il quoziente della divisione di n per m e $m - r$ è il resto della stessa divisione.

Supponiamo infine che $m < 0$. Dato $n \in \mathbb{Z}$, grazie ai due casi precedenti, $\exists q, r \in \mathbb{Z}$

t.c. $\begin{cases} \underline{n = q(-m)} + r = \underline{(-q)m + r} \\ \underline{0 \leq r < -m} = \underline{|m|} = \underline{|-m|} \end{cases}$.

Dunque $-q$ è il quoziente della divisione di n per m e r è il resto della stessa divisione.

UNICITÀ: Siano $n, m \in \mathbb{Z}$ con $m \neq 0$. Siano $q, q', r, r' \in \mathbb{Z}$ t.c.

$$\begin{cases} \boxed{n = qm + r} \\ 0 \leq r < |m| \end{cases} \quad \text{e} \quad \begin{cases} \boxed{n = q'm + r'} \\ 0 \leq r' < |m| \end{cases}$$

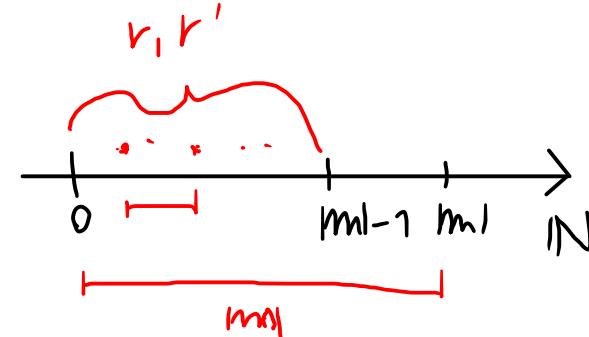
$$\begin{aligned} qm + r &= q'm + r' \\ qm - q'm &= r' - r \end{aligned} \quad \left\{ \begin{array}{l} |q - q'| |m| = |r' - r| \\ qm - q'm = r' - r \Leftrightarrow (q - q')m = r' - r \end{array} \right.$$

$$\Rightarrow \frac{|q-q'|}{|m|} = |r'-r| < \frac{1}{|m|}$$



$$|q-q'| < 1 \Rightarrow \underline{q=q'}$$

$$\Rightarrow \begin{array}{l} n = \cancel{q'm+r} \\ || \\ q'm+r' = \cancel{q'm+r'} \end{array} \quad \left. \begin{array}{l} \\ \\ \end{array} \right\} \Rightarrow \underline{r=r'} \quad \text{by}$$



ESERCIZIO Eseguire le seguenti divisioni di n per m :

- (1) $n=16, m=5.$
- (2) $n=-16, m=5$
- (3) $n=16, m=-5$
- (4) $n=-16, m=\underline{-5.}$