

## notazioni standard

- $a \in A$  indica che  $a$  *é un elemento* dell'insieme  $A$ ;
- $a \notin A$  indica che  $a$  *non é un elemento* dell'insieme  $A$ ;
- $\emptyset :=$  *insieme vuoto*.
- $A \subseteq B, B \supseteq A \Leftrightarrow A$  é *sottoinsieme* di  $B$ ;
- $A \subset B, B \supset A \Leftrightarrow A$  é sottoinsieme di  $B$  e non é uguale a  $B$ ;  
cioé  $A$  é un *sottoinsieme proprio* di  $B$ ;
- $A \cup B := \{x : x \in A \text{ o } x \in B\}$   
(*unione* degli insiemi  $A$  e  $B$ );
- $A \cap B := \{x : x \in A \text{ e } x \in B\}$   
(*intersezione* degli insiemi  $A$  e  $B$ );
- $A \setminus B := \{x : x \in A \text{ e } x \notin B\}$   
(*differenza* degli insiemi  $A$  e  $B$ );
- $A \times B := \{(a, b) : a \in A, b \in B\}$   
(*prodotto cartesiano* degli insiemi  $A$  e  $B$ ).

## simboli standard

- $N_o$  := insieme dei numeri naturali (compreso lo zero);
- $N$  := insieme dei numeri naturali diversi da zero;
- $Z$  := insieme dei numeri interi (relativi);
- $Q$  := insieme dei numeri razionali;
- $R$  := insieme dei numeri reali;
- $C$  := insieme dei numeri complessi;
- $A^* := A \setminus \{0\}$ ,  $A = Z, Q, R, C$ ;
- $A[x]$  := insieme dei polinomi nell'indeterminata  $x$  a coefficienti in  $A$ ,  $A = N_o, Z, Q, R, C$ ;
- $M_{m,n}(A)$  := insieme delle matrici di tipo  $m \times n$  ad elementi in  $A$ ,  $A = N_o, Z, Q, R, C$ ;
- $M_n(A)$  := insieme delle matrici quadrate d'ordine  $n$  ad elementi in  $A$ ,  $A = N_o, Z, Q, R, C$ ;
- $P(S)$  := insieme delle parti di un insieme non vuoto  $S$ ;
- $Perm(S)$  := insieme delle permutazioni su un insieme non vuoto  $S$ .

## notazioni per le funzioni

- $A \rightarrow B$  indica che é assegnata una **funzione**, o **applicazione**, tra gli insiemi  $A$  (**dominio** o **insieme di definizione**) e  $B$  (**codominio**)
- $f : A \rightarrow B$ , o  $A \xrightarrow{f} B$ , o  $x \in A \rightarrow f(x) \in B$ , indica che é assegnata una **funzione  $f$**  tra gli insiemi  $A$  e  $B$ . Il simbolo  $f(x)$  denota il **corrispondente**, o **immagine**, dell'elemento  $x$  nella funzione  $f$ .
- Assegnati una funzione  $f : A \rightarrow B$ , un sottoinsieme  $X$  di  $A$  ed uno  $Y$  di  $B$ , si pone

$$f(X) = \{y \in B : y = f(x), \text{ per qualche } x \in X\}$$

( **immagine di  $X$  in  $f$**  )

$$f^{-1}(Y) = \{x \in A : f(x) \in Y\}$$

( **controimmagine di  $Y$  in  $f$**  )

- Assegnate le funzioni  $f : A \rightarrow B$  e  $g : B \rightarrow C$ ,  $g \circ f$  indica la **funzione composta**, o **composizione**, di  $f$  e  $g$ , cioé

$$g \circ f : x \in A \rightarrow g(f(x)) \in C.$$

Nel seguito porremo quasi sempre  $fg := g \circ f$ , cioé

$$(fg)(x) = g(f(x)), \text{ per ogni } x \in A.$$


## proprietá fondamentali di $\mathbb{Z}$

1.  $a + b$  e  $ab$  sono elementi di  $\mathbb{Z}$ .
2.  $a + b = b + a$  e  $ab = ba$ .
3.  $(a + b) + c = a + (b + c)$  e  $(ab)c = a(bc)$ .
4. Esiste un elemento 0 (lo **zero**) tale che  $a + 0 = a$ . Esiste un elemento 1 (l' **unitá**) tale che  $a1 = a$ .
5.  $a(b + c) = ab + ac$ .
6. Per ogni  $a$  esiste un elemento  $-a$  (l' **opposto** di  $a$ ) tale che  $a + (-a) = 0$ .
7.  $a \neq 0$  e  $ab = ac \Rightarrow b = c$ .
8. La relazione  $\leq$  é d' **ordine totale** in  $\mathbb{Z}$ .
9.  $a \leq b \Rightarrow a + c \leq b + c$ .
10.  $a \leq b$  e  $0 \leq c \Rightarrow ac \leq bc$ .
11. **principio di induzione** Sia  $S$  un insieme di elementi di  $\mathbb{Z}$  e  $h$  un elemento di  $S$ . Se vale la proprietá

$$h \leq k, \quad k \in S \Rightarrow k + 1 \in S,$$

allora  $S$  contiene tutti gli interi maggiori o uguali ad  $h$ .

## alcune proprietà di $\mathbb{Z}$

**DEFINIZIONE 1** L'intero  $a + (-b)$  si denota con  $a - b$  e si chiama *differenza* fra  $a$  e  $b$ . L'operazione che ad ogni coppia di interi  $(a, b)$  associa la loro differenza  $a - b$  prende il nome di *sottrazione*. 

Valgono le seguenti proprietà:


- $a + b = a \Rightarrow b = 0$ .
- $ab = a, a \neq 0 \Rightarrow b = 1$ .
- $a - (-b) = a + b$ .
- $a0 = 0$ .
- $a, b > 0$  o  $a, b < 0 \Leftrightarrow ab > 0$ .
- $a, b$  uno positivo e l'altro negativo  $\Leftrightarrow ab < 0$ .
- $ab = 0 \Rightarrow a = 0$  oppure  $b = 0$ .
- $a \leq b \Rightarrow -b \leq -a$ .
- $0 \leq a^2$ .
- $a \leq a + 1$ .


## principio di buon ordinamento

**PROPOSIZIONE 2 (principio di buon ordinamento)** *Ogni sottoinsieme non vuoto  $X$  di  $Z$  che sia inferiormente limitato possiede l'elemento minimo.*

**DIM.** L'insieme  $S$  degli interi  $a$  tali che  $a \leq x$ , per ogni  $x \in X$ , é non vuoto perché  $X$  é inferiormente limitato. Si deve, dunque, provare che  $S$  contiene un elemento di  $X$ . Nell'ipotesi contraria, cioè  $S \cap X = \emptyset$ , detto  $h$  un elemento di  $S$ , risulta

$$h \leq k \quad , \quad k \in S \quad \Rightarrow \quad k + 1 \in S,$$

ed  $S$ , per il principio d'induzione, contiene tutti gli interi maggiori o uguali ad  $h$  e, quindi,  $X$ . Ciò é evidentemente assurdo e l'asserto é così provato. 

**OSSERVAZIONE 3** Se negli assiomi che definiscono  $Z$  si sostituisce il principio di induzione con quello di buon ordinamento, é facile provare che quest'ultimo implica il primo. I due principi, dunque, sono equivalenti. 

## Varianti del principio di induzione

**TEOREMA 4** Sia  $S$  un sottoinsieme di  $N_0$  con le seguenti proprietà:

$$(i) \quad 0 \in S \quad e \quad (ii) \quad k \in S \Rightarrow k + 1 \in S.$$

Allora risulta  $S = N_0$ .

**TEOREMA 5** Sia  $P(k)$  una proposizione definita per ogni intero  $k \geq h$ . Se  $P(h)$  è vera e se

$$P(k) \text{ vera con } k \geq h \Rightarrow P(k + 1) \text{ vera,}$$

allora  $P(k)$  è vera per ogni  $k \geq h$ .

## dimostrazione per induzione

**OSSERVAZIONE 6** L'ultima versione del principio di induzione fornisce un importante metodo di dimostrazione: la *dimostrazione per induzione*. In alcuni casi, questo permette di ridurre soltanto a due un numero non finito di prove da effettuare: se vogliamo provare che tutte le proposizioni (in numero non finito)  $P(n)$  sono vere per ogni  $n \geq h$ , basta dimostrare soltanto che:

- $P(h)$  è vera;
- se  $P(n)$  è vera per  $n > h$ , allora  $P(n + 1)$  è vera.



## dimostrazione per induzione


**ESEMPIO 7** *Provare che, per ogni intero non negativo  $n$ , l'intero  $2^{2^n} - 1$  é divisibile per 3.*

**SOLUZIONE** L'asserto é banalmente vero per  $n = 0$ . Denotiamo con  $S$  l'insieme di tutti gli interi non negativi  $k$  tali che  $2^{2^k} - 1$  sia divisibile per 3; ovviamente  $0 \in S$ .

Ora, se assumiamo che un intero  $n$  appartenga ad  $S$ , abbiamo

$$2^{2^{(n+1)}} - 1 = 4 \cdot 2^{2^n} - 1 = 4 \cdot 2^{2^n} - 4 + 3 = 4(2^{2^n} - 1) + 3,$$

da cui ricaviamo che  $2^{2^{(n+1)}} - 1$  é divisibile per 3 e cioè  $n+1 \in S$ .

Il principio di induzione assicura, allora, che  $S = N_0$ ; cioè che il nostro asserto é vero. 

## dimostrazione per induzione

**ESERCIZIO** 8 Supponiamo di giocare a poker avendo a disposizione solo fiches da 5 e 8 euro. E' facile rendersi conto che in queste condizioni non é possibile fare puntate di

1, 2, 3, 4, 6, 7, 9, 11, 12, 14, 17, 19, 22, 27

euro. Provare che é possibile fare puntate di  $n$  euro, per ogni  $n > 27$ .

**SOLUZIONE** Basta provare che ogni intero  $n > 27$  puó scriversi nella forma  $a5 + b8$ , con  $a, b$  interi positivi. Ovviamente  $28 = 4 \cdot 5 + 1 \cdot 8$  é di questo tipo.


Supponiamo ora che un intero  $n > 28$  sia del tipo  $n = a5 + b8$  e osserviamo che  $a$  e  $b$  non possono essere entrambi minori di 3. Allora abbiamo:

$$a \geq 3 \Rightarrow$$

$n + 1 = (a5 + b8) + (-3 \cdot 5 + 2 \cdot 8) = (a - 3)5 + (b + 2)8$ ,  
cioé  $n + 1$  é del tipo desiderato;

$$b \geq 3 \Rightarrow$$

$n + 1 = (a5 + b8) + (5 \cdot 5 - 3 \cdot 8) = (a + 5)5 + (b - 3)8$   
e anche in questo caso  $n + 1$  é del tipo desiderato.

Il principio di induzione assicura, allora, che il nostro asserto é vero. 

## dimostrazione per induzione

**ESERCIZIO 9 (formula di de Moivre)** *Provare che, per ogni intero non negativo  $n$  e per ogni numero reale  $\theta$ , risulta*

$$(\cos \theta + i \operatorname{sen} \theta)^n = \cos n\theta + i \operatorname{sen} n\theta,$$

ove  $i = \sqrt{-1}$  é l'unitá immaginaria del campo complesso.

**SOLUZIONE** L'asserto é vero per  $n = 0$ . Se supponiamo che sia vero per un intero  $n > 0$ , abbiamo:

$$\begin{aligned}(\cos \theta + i \operatorname{sen} \theta)^{n+1} &= (\cos \theta + i \operatorname{sen} \theta)^n (\cos \theta + i \operatorname{sen} \theta) \\ &= (\cos n\theta + i \operatorname{sen} n\theta) (\cos \theta + i \operatorname{sen} \theta) \\ &= \cos n\theta \cos \theta - \operatorname{sen} n\theta \operatorname{sen} \theta + i (\operatorname{sen} n\theta \cos \theta + \operatorname{sen} \theta \cos n\theta) \\ &= \cos (n+1)\theta + i \operatorname{sen} (n+1)\theta.\end{aligned}$$

Allora l'asserto segue dal principio di induzione.



## divisione euclidea

**TEOREMA 10 (divisione euclidea)** Siano  $a, b$  interi con  $b > 0$ . Allora esiste un'unica coppia di interi  $(q, r)$  per cui risulta  $a = bq + r$  e  $0 \leq r < b$ .

**DIM.** • L'insieme  $X = \{n \geq 0 : a = bm + n \text{ con } m \in \mathbb{Z}\}$  é non vuoto perché:

$$a = b0 + a \Rightarrow a \in X, \text{ se } a \geq 0;$$

$$a = ba + (1 - b)a \Rightarrow (1 - b)a \in X, \text{ se } a < 0.$$

• Il principio di buon ordinamento assicura l'esistenza del minimo  $r$  di  $X$  e quindi esiste  $q$  tale che  $a = bq + r$ .

Dall'ultima uguaglianza abbiamo  $a = b(q+1) + (r-b)$  e, essendo  $r - b < r$ , deve essere  $r - b < 0$  e cioè  $r < b$ .

• Sia  $(q', r')$  una coppia di interi tale che  $a = bq' + r'$  e  $0 \leq r' < b$  e supponiamo  $q' < q$ . Allora é  $q - q' \geq 1$  e abbiamo


$$r' = a - bq' = (a - bq) + b(q - q') \geq r + b \Rightarrow r' \geq b,$$

il che é assurdo.

Invertendo i ruoli di  $q$  e  $q'$  si vede che non puó essere  $q < q'$  e cosí abbiamo  $r = r'$  e  $q = q'$ . 

**DEFINIZIONE 11** La funzione  $|\cdot| : a \in \mathbb{Z} \rightarrow |a| \in \mathbb{N}_0$  definita da

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

si chiama **valore assoluto**. L'intero  $|a|$  si chiama *valore assoluto* di  $a$ . 

## divisione euclidea

**TEOREMA 12 (divisione euclidea in  $Z$ )** Siano  $a, b$  interi con  $b \neq 0$ . Allora esiste un'unica coppia di interi  $(q, r)$  per cui risulta  $a = bq + r$  e  $0 \leq r < |b|$ .

**OSSERVAZIONE 13** Sia  $a \geq 2$  un fissato intero e consideriamo un arbitrario intero  $n > 0$ . Applicando ripetutamente la divisione euclidea, possiamo scrivere in un unico modo:

$$\begin{aligned}n &= aq_0 + r_0, \\q_0 &= aq_1 + r_1, \\q_1 &= aq_2 + r_2, \\&\dots \\q_{m-2} &= aq_{m-1} + r_{m-1}, \\q_{m-1} &= aq_m + r_m, \quad q_m = 0,\end{aligned}$$

ove gli  $r_j$  sono interi non negativi minori di  $a$ . Eliminando i quozienti  $q_j$  dalle precedenti relazioni, otteniamo:

$$\begin{aligned}n &= aq_0 + r_0 = a(aq_1 + r_1) + r_0 \\&= a^2q_1 + r_1a + r_0 = a^2(aq_2 + r_2) + r_1a + r_0 = \dots \\&= r_ma^m + r_{m-1}a^{m-1} + \dots + r_2a^2 + r_1a + r_0.\end{aligned}$$



**OSSERVAZIONE 14** La funzione

$$\nu_a : n \rightarrow (r_m, r_{m-1}, \dots, r_1, r_0)$$

tra  $N$  e le successioni finite di interi non negativi minori di  $a$  é biunivoca.



**DEFINIZIONE 15** Sia

$$n = r_m a^m + r_{m-1} a^{m-1} + \dots + r_2 a^2 + r_1 a + r_0, \quad \text{con } 0 \leq r_j < a.$$

La scrittura

$$(r_m r_{m-1} \dots r_2 r_1 r_0)_a$$

prende il nome di **rappresentazione in base  $a$  di  $n$** .



**OSSERVAZIONE 16** Naturalmente la definizione precedente presuppone che si sia fissato un insieme di  $a$  simboli, detti *cifre*, per rappresentare tutti gli interi maggiori o uguali a zero e minori di  $a$ .



**DEFINIZIONE 17** La funzione che ad ogni intero positivo associa la successione delle cifre che lo rappresentano in base  $a$  si chiama **sistema di numerazione in base  $a$** .



**OSSERVAZIONE 18** I sistemi di numerazione piú in uso sono i seguenti:

- Il sistema in base *dieci* o *decimale*, le cui cifre sono nell'ordine: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9.
- Il sistema in base *due* o *binario*, le cui cifre sono nell'ordine: 0=zero, 1=uno.
- Il sistema in base *otto*, le cui cifre sono nell'ordine: 0, 1, 2, 3, 4, 5, 6, 7.
- *Il sistema in base sedici* o *esagesimale*: le cui cifre da zero a nove sono quelle decimali e le rimanenti sono: A:=dieci, B:=undici, C:=dodici, D:=tredici, E:=quattordici, F:=quindici.



**ESEMPIO 19**  $(109)_{dieci} = (1101101)_{due} = (6D)_{sedici}$ .



**ESEMPIO 20**  $a = (10)_a$ , per ogni intero  $a > 1$ .

