# Fondamenti di Informatica

Gualtiero Volpe
gualtiero.volpe@unige.it

1

# 1. Elementi di matematica discreta

2

# 1.1 Teoria degli insiemi

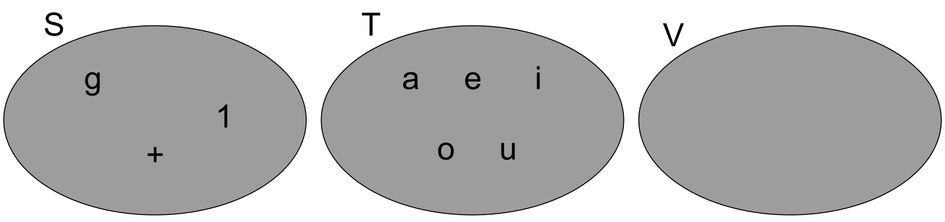
C. Delizia, P. Longobardi, M. Maj, C. Nicotera.
Matetica Discreta, McGraw-Hill. Capitolo 1.

3

## Insiemi

Con il termine insieme si intende una collezione di oggetti, detti elementi dell'insieme.

Esempio: S = {g, 1, +}
T = {$x$ : $x$ è una vocale}
V = $\emptyset$ insieme vuoto



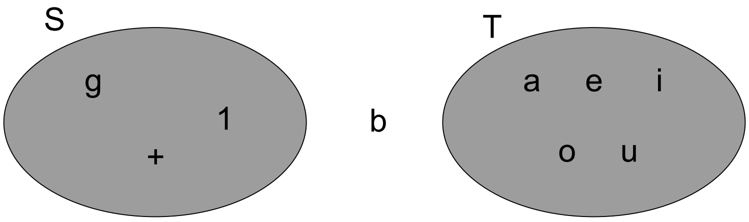

Diagrammi di Venn

4

## Appartenenza ad un insieme

- Per indicare che un elemento $x$ appartiene all'insieme A si scrive: $x \in A$.
- Per indicare che un elemento $y$ non appartiene all'insieme B si scrive: $y \notin B$.

Esempio: $g \in S$, $a \in T$
$b \notin T$, $b \notin S$
$U = \{m\}$ insieme singolo, $m \in U$




5

## Insiemi numerici notevoli

- $\mathbf{N}_0 = \{0, 1, 2, 3, \ldots\}$, insieme dei numeri naturali
- $\mathbf{N} = \{1, 2, 3, \ldots\}$
  insieme dei numeri naturali diversi da zero
- $\mathbf{N}_p$ o $2\mathbf{N}_0$, insieme dei numeri naturali pari
- $\mathbf{N}_d$, insieme dei numeri naturali dispari
- $\mathbf{Z} = \{0, 1, -1, 2, -2, \ldots\}$, insieme dei numeri interi
- $\mathbf{Q}$, insieme dei numeri razionali
- $\mathbf{R}$, insieme dei numeri reali
- $\mathbf{C}$, insieme dei numeri complessi

6

# Ordine o cardinalità di un insieme

- Si definisce ordine o cardinalità di un insieme il numero dei suoi elementi.
- L'ordine di un insieme A si denota con |A|.

Esempio: |S| = 3
|T| = 5
|V| = 0
|U| = 1

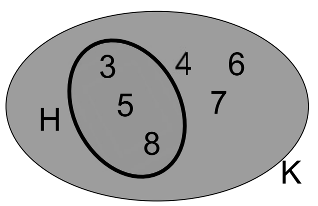
- Un insieme il cui ordine è un numero finito è detto insieme finito.
- Un insieme non finito è detto insieme infinito.

7

# Sottoinsiemi

- Un insieme A è contenuto (o incluso) in un insieme B (è sottoinsieme di B) se e soltanto se ogni elemento di A è elemento di B.
- Se A è contenuto in B si scrive $A \subseteq B$.
- Si scrive anche $B \supseteq A$ (B contiene A).

Esempio: H = {3, 5, 8}, K = {3, 4, 5, 6, 7, 8}
$H \subseteq K$, ma $K \nsubseteq H$ (K non contiene H)




$A \subseteq B := \forall x \in A, x \in B$

8

# Sottoinsiemi

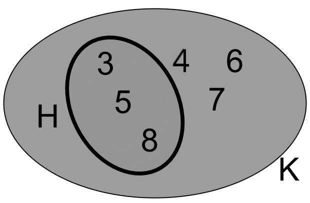
- Qualunque sia l'insieme A:
  - $\varnothing \subseteq A$
  - $A \subseteq A$
  - $\{x\} \subseteq A$ per ogni $x \in A$
- Inoltre, dati gli insiemi A, B e C:
  - Se $A \subseteq B$ e $B \subseteq C$, allora $A \subseteq C$
    (proprietà transitiva dell'inclusione)

9

# Sottoinsiemi

- Un insieme A è contenuto strettamente (o incluso strettamente) in un insieme B se A è contenuto in B, ma è distinto da B.
- In altre parole A è contenuto strettamente in B se ogni elemento di A è elemento di B ed esiste almeno un elemento di B che non è elemento di A.
- Se A è contenuto strettamente in B si scrive $A \subset B$.

Esempio: $H = \{3, 5, 8\}$, $K = \{3, 4, 5, 6, 7, 8\}$
$H \subseteq K$ e, in particolare, $H \subset K$.




$A \subset B := A \subseteq B, A \neq B$

10

# Insieme potenza

- L'insieme delle parti o insieme potenza di un insieme A, denotato con $\mathcal{P}(A)$, è l'insieme costituito da tutti e soli i sottoinsiemi di A.

$$\mathcal{P}(A) := \{X : X \subseteq A\}$$

- Per qualunque insieme A, $\varnothing \in \mathcal{P}(A)$, $A \in \mathcal{P}(A)$ e $\{x\} \in \mathcal{P}(A)$ per ogni $x \in A$.
Inoltre per ogni insieme A, si ha $\mathcal{P}(A) \neq \varnothing$.

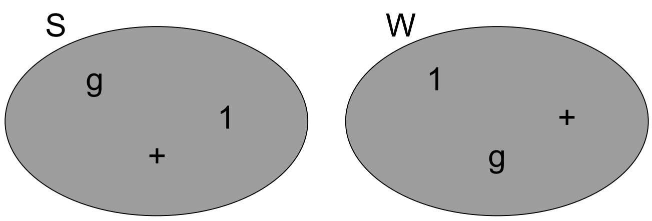
Esempio: Dato H = {3, 5, 8},
$\mathcal{P}(H) = \{\varnothing, \{3\}, \{5\}, \{8\}, \{3, 5\}, \{3, 8\}, \{5, 8\}, \{3, 5, 8\}\}$.

11

# Uguaglianza tra insiemi

- Due insiemi A e B sono detti uguali (A = B) se e soltanto se hanno gli stessi elementi, cioè $x \in A$ se e soltanto se $x \in B$.

Esempio: se S = {g, 1, +} e W = {+, g, 1}, S = W.




$$A = B := x \in A \Leftrightarrow x \in B$$

12

## Uguaglianza tra insiemi

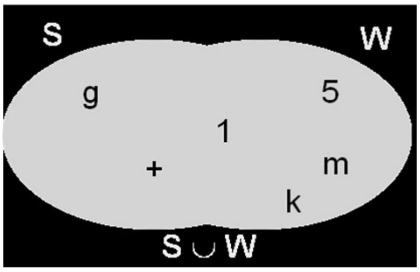
- Dati gli insiemi A e B:
  - A = B se e soltanto se $A \subseteq B$ e $B \subseteq A$
  - $A \neq B$ se e soltanto se $A \nsubseteq B$ o $B \nsubseteq A$
- Dati gli insiemi A, B e C,
  - se A = B e B = C, allora A = C
    (proprietà transitiva dell'uguaglianza)

13

## Unione di insiemi

- Siano A e B insiemi, si definisce unione di A e B l'insieme i cui elementi sono tutti e soli gli elementi appartenenti ad A o a B.
- L'unione di A e B si denota con $A \cup B$.

Esempio: S = {g, 1, +}, W = {1, +, 5, m, k}
$S \cup W$ = {g, 1, +, 5, m, k}




$A \cup B := \{x : x \in A \text{ o } x \in B\}$

14

# Unione di insiemi

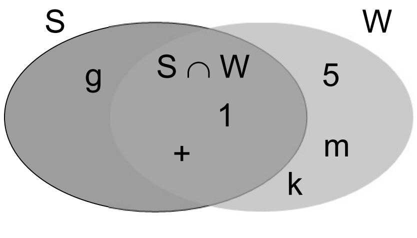
- Dati gli insiemi A, B, C e D:
  - $A \subseteq A \cup B$ e $B \subseteq A \cup B$
  - $A \cup B = B \cup A$
    proprietà commutativa dell'unione
  - $(A \cup B) \cup C = A \cup (B \cup C)$
    proprietà associativa dell'unione
  - $A \cup \varnothing = \varnothing \cup A$
    $\varnothing$ elemento neutro per l'unione
  - $A \cup A = A$
    proprietà iterativa dell'unione
  - $A \subseteq B$ se e soltanto se $A \cup B = B$
  - se $A \subseteq B$ e $C \subseteq D$ allora $A \cup C \subseteq B \cup D$

15

# Intersezione di insiemi

- Siano A e B insiemi, si definisce intersezione di A e B l'insieme i cui elementi sono tutti e soli gli elementi appartenenti sia ad A che a B.
- L'intersezione di A e B si denota con $A \cap B$.

Esempio: $S = \{g, 1, +\}$, $W = \{+, 5, m, 1, k\}$
$S \cap W = \{1, +\}$




$A \cap B := \{x : x \in A \text{ e } x \in B\}$

16

# Intersezione di insiemi

- Dati gli insiemi A, B, C e D:
  - $A \cap B \subseteq A$ e $A \cap B \subseteq B$
  - $A \cap B = B \cap A$
    proprietà commutativa dell'intersezione
  - $(A \cap B) \cap C = A \cap (B \cap C)$
    proprietà associativa dell'intersezione
  - $A \cap A = A$
    proprietà iterativa dell'intersezione
  - $A \subseteq B$ se e soltanto se $A \cap B = A$
  - se $A \subseteq B$ e $C \subseteq D$ allora $A \cap C \subseteq B \cap D$
  - Se A e B sono tali che $A \cap B = \emptyset$, allora A e B si dicono insiemi disgiunti

17

# Proprietà di unione e intersezione

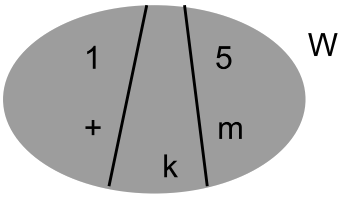
- Dati gli insiemi A, B e C:
  - $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
    $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$
    proprietà distributiva dell'unione rispetto all'intersezione
  - $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
    $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$
    proprietà distributiva dell'intersezione rispetto all'unione
  - $A \cup (A \cap B) = A = A \cap (A \cup B)$
    leggi di assorbimento

18

## Partizione di un insieme

- Sia A un insieme non vuoto e $F \subseteq \mathcal{P}$(A) un insieme di sottoinsiemi di A. Si dice che *F* è una partizione di A se ogni elemento di *F* è un sottoinsieme non vuoto di A, gli elementi di *F* sono a due a due disgiunti e la loro unione è A.

Esempio: W = {+, 5, m, 1, k}
*F* = {{1, +}, {k}, {5, m}} è una partizione di W.




*F* partizione di A :=

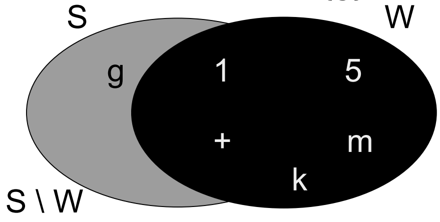
$$\begin{cases} X \neq \emptyset, \forall X \in F \\ X, Y \in F, X \neq Y \Rightarrow X \cap Y = \emptyset \\ \bigcup_{X \in F} X = A \end{cases}$$

19

## Complemento di insiemi

- Siano A e B insiemi, si definisce complemento di B rispetto ad A (o differenza tra A e B) l'insieme costituito da tutti e soli gli elementi di A che non appartengono a B.
- Il complemento di B rispetto ad A si denota con A \ B.

Esempio: S = {g, 1, +}, W = {+, 5, m, 1, k}
S \ W = {g}, W \ S = {5, m, k}.




A \ B := {$x$ : $x \in$ A e $x \notin$ B}

20

## Complemento di insiemi

- Dati gli insiemi A e B:
  - NON vale la proprietà commutativa
  - NON vale la proprietà associativa
  - $A \setminus B \subseteq A$
  - $A \setminus \emptyset = A$
  - $\emptyset \setminus A = \emptyset$
  - $A \setminus A = \emptyset$
  - $A \cap (B \setminus A) = \emptyset$
  - $A \setminus B = A \setminus (A \cap B)$
  - $A \setminus B = A$ se e soltanto se $A \cap B = \emptyset$
  - $A \setminus B = \emptyset$ se e soltanto se $A \subseteq B$

21

## Complemento di insiemi

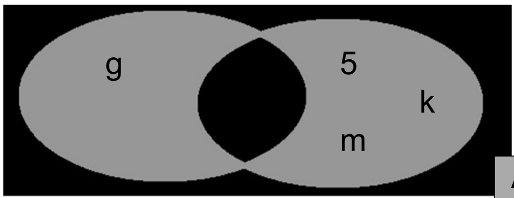
- Dati gli insiemi A, B e C:
  - $(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$
    proprietà distributiva a destra del complemento rispetto all'unione
  - $(A \cap B) \setminus C = (A \setminus C) \cap (B \setminus C)$
    proprietà distributiva a destra del complemento rispetto all'intersezione
  - $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$
    $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$
    formule di De Morgan

22

## Unione disgiunta di insiemi

- Siano A e B insiemi, si definisce unione disgiunta (o differenza simmetrica) di A e B l'insieme costituito dagli elementi che appartengono all'unione di A e B, ma non appartengono alla loro intersezione.
- L'unione disgiunta si denota con $A \dot\cup B$ o con $A \Delta B$.

Esempio: S = {g, 1, +}, W = {+, 5, m, 1, k}
S Δ W = {g, 5, m, k}




S Δ W

$A \Delta B := (A \cup B) \setminus (A \cap B)$

23

## Unione disgiunta di insiemi

- Dati gli insiemi A, B e C:
  - $A \Delta B = B \Delta A$
    proprietà commutativa dell'unione disgiunta
  - $(A \Delta B) \Delta C = A \Delta (B \Delta C)$
    proprietà associativa dell'unione disgiunta
  - $A \Delta \emptyset = A$
    $\emptyset$ elemento neutro dell'unione disgiunta
  - $A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)$
    $(A \Delta B) \cap C = (A \cap C) \Delta (B \cap C)$
    distributività dell'intersezione rispetto all'unione disgiunta
  - $A \Delta A = \emptyset$
  - $A \Delta B = (A \setminus B) \cup (B \setminus A)$

24

## Prodotto cartesiano di insiemi

- Con ($x$, $y$) si denota la coppia (ordinata) di prima coordinata $x$ e seconda coordinata $y$.
- Per convenzione:
  ($x$, $y$) = ($x'$, $y'$) se e soltanto se $x = x'$ e $y = y'$.
- Siano A e B insiemi, si definisce prodotto cartesiano di A e B l'insieme costituito da tutte le coppie aventi per prima coordinata un elemento di A e per seconda coordinata un elemento di B.
- Il prodotto cartesiano di A e B si denota con A × B.

$$A \times B := \{(x, y) : x \in A, y \in B\}$$

Esempio: S = {g, 1, +}, W = {+, 5, m, 1, k}

S × W = {(g, +), (g, 5), (g, m), (g, 1), (g, k), (1, +), (1, 5), (1, m), (1, 1), (1, k), (+, +), (+, 5), (+, m), (+, 1), (+, k)}

25

## Prodotto cartesiano di insiemi

- Dati gli insiemi A, B e C:
  - $(A \cup B) \times C = (A \times C) \cup (B \times C)$
    proprietà distributiva a destra del prodotto cartesiano rispetto all'unione
  - $(A \cap B) \times C = (A \times C) \cap (B \times C)$
    proprietà distributiva a destra del prodotto cartesiano rispetto all'intersezione
  - $(A \setminus B) \times C = (A \times C) \setminus (B \times C)$
    proprietà distributiva a destra del prodotto cartesiano rispetto al complemento

26

## Prodotto cartesiano di insiemi

- Dati gli insiemi A, B e C:
  - $A \times (B \cup C) = (A \times B) \cup (A \times C)$
    proprietà distributiva a sinistra del prodotto cartesiano rispetto all'unione
  - $A \times (B \cap C) = (A \times B) \cap (A \times C)$
    proprietà distributiva a sinistra del prodotto cartesiano rispetto all'intersezione
  - $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$
    proprietà distributiva a sinistra del prodotto cartesiano rispetto al complemento

27

## Prodotto cartesiano di insiemi

- Dati gli insiemi A e B:
  - $\emptyset \times A = A \times \emptyset = \emptyset$
  - $|A \times B| = |A| \cdot |B| = |B \times A|$
  - se $A \times B = B \times A$, allora $A = \emptyset$ o $B = \emptyset$ o $A = B$
- Dati gli insiemi A, B, C e D:
  - Se $A \times B = C \times D$ allora $A = C$ e $B = D$
- Il sottoinsieme di $A \times A$ costituito da tutte e sole le coppie di coordinate uguali è denotato con $\Delta_A$ ed è detto diagonale di A.
  Esempio: $S = \{g, 1, +\}$, $\Delta_s = \{(g, g), (1, 1), (+, +)\}$.

28

## Prodotto cartesiano di insiemi

- Se $A_1, A_2, \ldots, A_n$ ($n \geq 2$) sono insiemi, allora $(x_1, x_2, \ldots x_n)$ con $x_1 \in A_1$, $x_2 \in A_2, \ldots x_n \in A_n$ si dice n-upla
- Il prodotto cartesiano $A_1 \times A_2 \times \ldots \times A_n$ si definisce come l'insieme di tutte e sole le n-uple $(x_1, x_2, \ldots x_n)$ con $x_1 \in A_1$, $x_2 \in A_2, \ldots x_n \in A_n$
- Se $A_1 = A_2 = \ldots = A_n = A$, il prodotto cartesiano $A_1 \times A_2 \times \ldots \times A_n = A \times \ldots \times A$ (*n* volte) viene detto prodotto cartesiano di *n* copie di A e denotato con $A^n$

$$A^n := \underbrace{A \times A \times \ldots \times A}_{n \text{ volte}} := \{(x_1, x_2, \ldots x_n) : x_1, x_2, \ldots x_n \in A\}$$

29

# 1.2 Relazioni e funzioni

C. Delizia, P. Longobardi, M. Maj, C. Nicotera.
Matetica Discreta, McGraw-Hill. Capitolo 2.

30

## Relazioni tra insiemi

- Siano A e B insiemi. Un sottoinsieme $\mathcal{R}$ di A × B è detto relazione o corrispondenza tra A e B.
- Se $x \in$ A e $y \in$ B sono tali che $(x, y) \in \mathcal{R}$, si scrive $x \mathcal{R} y$ e si dice che $x$ è nella relazione $\mathcal{R}$ con $y$ o che $y$ è corrispondente in $\mathcal{R}$ di $x$.

Esempio: S = {g, 1, +}, W = {+, 5, m, 1, k}
Sono esempi di relazione tra S e W:
$\mathcal{R}_1$ = {(g, 5), (g, 1)}
$\mathcal{R}_2$ = {(1, 5), (1, 1)}
$\mathcal{R}_3$ = {(g, m), (g, k), (1, 5), (1, 1)}

31

## Relazioni tra insiemi

- Spesso per assegnare una relazione si precisa una proprietà che individua un sottoinsieme di A × B
  Esempio: sono relazioni in $\mathbf{N}_0 \times \mathbf{Z}$:
  $x \mathcal{R}_4 y \Leftrightarrow x = y$
  $x \mathcal{R}_5 y \Leftrightarrow x = y^2$
  $x \mathcal{R}_6 y \Leftrightarrow y^3 = x$.

- Se A e B sono insiemi finiti non vuoti, esiste un numero finito di relazioni tra A e B e tale numero è $|\mathcal{P}(A \times B)| = 2^{|A \times B|} = 2^{|A|\cdot|B|}$.
  Esempio: il numero di relazioni in S × W è $2^{3\cdot5} = 2^{15} = 32768$.

32

# Relazione vuota e piena

- Siano A e B insiemi. Ponendo $\mathcal{R}_0 = \emptyset$ si individua la relazione vuota tra A e B e si ha che $x \not\mathcal{R}_0 y$, per ogni $x \in$ A e $y \in$ B.
- Ponendo invece $\mathcal{R}_t$ = A × B si ottiene la relazione totale (o piena) tra A e B e si ha che $x \mathcal{R}_t y$, per ogni $x \in$ A e $y \in$ B.
- Ovviamente $\mathcal{R}_0 = \mathcal{R}_t$ se e solo se A = $\emptyset$ oppure B = $\emptyset$. Inoltre, se A = $\emptyset$ oppure B = $\emptyset$, allora A × B = $\emptyset$ e $\mathcal{R}_0$ è l'unica relazione esistente tra A e B.

33

# Relazione opposta

- Se $\mathcal{R}$ è una relazione tra gli insiemi A e B, si definisce relazione opposta (o inversa) di $\mathcal{R}$ (denotata con $\mathcal{R}^{op}$) la relazione tra B e A definita come $\mathcal{R}^{op} = \{(y, x) : (x, y) \in \mathcal{R}\}$.
- Esempio: Considerati gli insiemi S = {g, 1, +}, W = {+, 5, m, 1, k} e la relazione $\mathcal{R}_7$ = {(g, m), (g, k), (g, 5)}, la relazione $\mathcal{R}_8$ = {(m, g), (k, g), (5, g)} è relazione opposta di $\mathcal{R}_7$.
- Esempio: le relazioni in $\mathbf{N}_0 \times \mathbf{Z}$ $x \mathcal{R}_9 y \Leftrightarrow x = y^2$ e $x \mathcal{R}_{10} y \Leftrightarrow x^2 = y$ sono l'una l'opposta dell'altra.

34

# Relazione indotta

- Se A, B, C e D sono insiemi tali che $C \subseteq A$ e $D \subseteq B$, considerata una qualunque relazione $\mathcal{R}$ tra A e B, la relazione $\mathcal{R} \cap (C \times D)$ tra C e D è detta relazione indotta da $\mathcal{R}$ su C e D e denotata con $\mathcal{R}_{|C \times D}$
- Esempio: Considerati gli insiemi
  $S = \{g, 1, +\}$, $W = \{+, 5, m, 1, k\}$ e i sottoinsiemi
  $X = \{g\} \subseteq S$ e $Y = \{m, k\} \subseteq W$, si ha che
  $X \times Y = \{(g, m), (g, k)\}$.
  Data la relazione $\mathcal{R}_7$ su $S \times W$ definita come
  $\mathcal{R}_7 = \{(g, m), (g, k), (g, 5)\}$,
  la relazione indotta da $\mathcal{R}_7$ su $X \times Y$ è
  $\mathcal{R}_{7|X \times Y} = \mathcal{R}_7 \cap (X \times Y) = \{(g, m), (g, k)\}$.

35

# Relazione binaria

- Una relazione tra insiemi A e B con A = B è detta anche relazione binaria in A.
- Esempio: la diagonale $\Delta_A$ è una relazione binaria in A. Tale relazione è anche detta identità di A o uguaglianza in A ed è denotata con $id_A$ o $1_A$

$$\boxed{x\ (id_A)\ y \Leftrightarrow x = y}$$

36

## Proprietà delle relazioni binarie

- Sia A un insieme. Una relazione binaria $\mathcal{R}$ in A è detta
  - riflessiva, se ogni $x \in$ A è in relazione con se stesso:

    $\mathcal{R}$ riflessiva := $x \mathcal{R} x \ \forall x \in$ A
  - simmetrica se con $x, y \in$ A da $x \mathcal{R} y$ segue $y \mathcal{R} x$:

    $\mathcal{R}$ simmetrica := ($x \mathcal{R} y \Rightarrow y \mathcal{R} x$)
  - asimmetrica se con $x, y \in$ A da $x \mathcal{R} y$ e $y \mathcal{R} x$ segue $x = y$ (o anche da $x \mathcal{R} y$ e $x \neq y$ segue $y \not\mathcal{R} x$):

    $\mathcal{R}$ asimmetrica := (($x \mathcal{R} y$ e $y \mathcal{R} x$) $\Rightarrow x = y$)
  - transitiva se con $x, y, z \in$ A da $x \mathcal{R} y$ e $y \mathcal{R} z$ segue $x \mathcal{R} z$:

    $\mathcal{R}$ transitiva := (($x \mathcal{R} y$ e $y \mathcal{R} z$) $\Rightarrow x \mathcal{R} z$)

37

## Proprietà delle relazioni binarie

- Esempio. Sia S = {g, 1, +} e si considerino:

  $\mathcal{R}_{11}$ = {(g, 1)}
  $\mathcal{R}_{12}$ = {(g, 1), (1, g), (g, g)}
  $\mathcal{R}_{13}$ = {(g, 1), (1, g), (g, g), (1, 1)}
  $\mathcal{R}_{14}$ = {(g, g), (1, 1), (+, +), (g, 1)}
  $\mathcal{R}_{15}$ = {(g, g), (1, 1), (+, +), (g, 1), (1, g)}

  si ha che:

  $\mathcal{R}_{11}$ non è riflessiva, è asimmetrica
  $\mathcal{R}_{12}$ non è riflessiva, è simmetrica, non è transitiva
  $\mathcal{R}_{13}$ non è riflessiva, è simmetrica, è transitiva
  $\mathcal{R}_{14}$ è riflessiva, è asimmetrica, è transitiva
  $\mathcal{R}_{15}$ è riflessiva, è simmetrica, è transitiva

38

## Relazioni binarie

- Rispetto alle proprietà di riflessività, simmetria e transitività le relazioni indotte conservano le proprietà delle relazioni originali.

- Tipologie significative di relazioni binarie tra insiemi sono:
  - Le relazioni di equivalenza
  - Le relazioni d'ordine

39

## Relazioni di equivalenza

- Una relazione binaria $\mathcal{R}$ in un insieme A è detta relazione di equivalenza se è:
  - riflessiva
  - simmetrica
  - transitiva

- Esempio: dato S = {g, 1, +},
  $\mathcal{R}$ = {(g, g), (1, 1), (+, +), (g, 1), (1, g)}
  è una relazione di equivalenza.

40

# Classi di equivalenza

- Sia A un insieme non vuoto e $\mathcal{R}$ una relazione di equivalenza in A. Se $x \in$ A, si dice classe di equivalenza di $x$ modulo $\mathcal{R}$ il sottoinsieme di A costituito da tutti e soli gli elementi che sono in relazione con $x$ attraverso $\mathcal{R}$.
- La classe di equivalenza di x si denota con $[x]_{\mathcal{R}}$ (o più semplicemente con $[x]$). Si parla anche di classe di equivalenza rappresentata da $x$.

$$[x]_{\mathcal{R}} := \{s \in A : s\, \mathcal{R}\, x\}$$

- Esempio: dato S = {g, 1, +} e la relazione di equivalenza $\mathcal{R}$ = {(g, g), (1, 1), (+, +), (g, 1), (1, g)}, la classe di equivalenza di g $\in$ S è [g] = {g, 1}.

41

# Insieme quoziente

- L'insieme delle classi di equivalenza di A modulo $\mathcal{R}$ viene detto insieme quoziente di A modulo $\mathcal{R}$ e viene denotato con A / $\mathcal{R}$.

$$A / \mathcal{R} := \{[x]_{\mathcal{R}} : x \in A\}$$

- Esempio: dato S = {g, 1, +} e la relazione di equivalenza $\mathcal{R}$ = {(g, g), (1, 1), (+, +), (g, 1), (1, g)}, le classi di equivalenza di S modulo $\mathcal{R}$ sono [g] = {g, 1}; [1] = {1, g} = [g], [+] = {+}. Quindi, l'insieme quoziente di S modulo $\mathcal{R}$ è dato da: S / $\mathcal{R}$ = {[g], [1], [+]} = {{g, 1}, {+}}.

42

# Teorema fondamentale delle relazioni di equivalenza

- Teorema fondamentale delle relazioni di equivalenza
  Sia A un insieme non vuoto. Allora:
  - Se $\mathcal{R}$ è una relazione di equivalenza in A, l'insieme quoziente A / $\mathcal{R}$ è una partizione di A.
  - Se *F* è una partizione di A, esiste una ed una sola relazione di equivalenza $\mathcal{R}_F$ tale che $F$ = A / $\mathcal{R}_F$

43

# Relazioni d'ordine

- Una relazione binaria $\mathcal{R}$ in un insieme A è detta relazione d'ordine se è:
  - riflessiva,
  - asimmetrica
  - transitiva
- Spesso si preferisce denotare una relazione d'ordine con ≤ ($x \leq y := x\ \mathcal{R}\ y$) e si dice *x* minore o uguale di *y*.
- Equivalentemente si può scrivere $y \geq x$ e si dice *y* maggiore o uguale di *x*.
- Esempi: dato S = {g, 1, +}, $\mathcal{R}$ = {(g, g), (1, 1), (+, +), (g, 1)} è una relazione d'ordine.
  Gli ordini usuali in $\mathbf{N}_0$ e **Z** sono relazioni d'ordine.

44

# Insiemi ordinati

- La coppia (A, ≤) con A insieme e ≤ relazione d'ordine in A è detta insieme ordinato o parzialmente ordinato.
- Esempi di insiemi ordinati: ($\mathbf{N}_0$, usuale), (**Z**, usuale), ($\mathcal{P}$(T), $\subseteq$) con T insieme arbitrario.
- Sia (A, ≤) un insieme ordinato. Elementi $x$ e $y$ in A sono detti confrontabili se si ha $x \leq y$ oppure $y \leq x$.
- Ogni elemento è confrontabile con se stesso e si ha contemporaneamente $x \leq y$ e $y \leq x$ se e solo se $x = y$.
- Un insieme ordinato (A, ≤) tale che x e y sono confrontabili per ogni $x, y \in$ A è detto insieme totalmente ordinato o catena.
- Esempi di insieme totalmente ordinati: ($\mathbf{N}_0$, usuale), (**Z**, usuale), non lo è ($\mathcal{P}$(T), $\subseteq$).

45

# Insiemi ordinati

- Se (A, ≤) è un insieme ordinato, con $x, y \in$ A si dice che x è minore strettamente di y, ponendo:

$$x < y := x \leq y \text{ e } x \neq y$$

- Si dice anche che y è maggiore strettamente di x e si scrive y > x per indicare che x < y.
- Se (A, ≤) è un insieme ordinato e X $\subseteq$ A, la relazione indotta da ≤ in X è una relazione d'ordine e (X, ≤) è un insieme ordinato.

46

## Minimo e massimo

- Sia (A, ≤) un insieme ordinato.
  Un elemento $a \in$ A è detto minimo di A e si denota con min A, se è confrontabile con ogni elemento di A e risulta $a \leq x$ per ogni $x \in$ A.

$$a = \min A := a \leq x \quad \forall x \in A$$

- Analogamente, un elemento $b \in$ A è detto massimo di A e si denota con max A, se è confrontabile con ogni elemento di A e risulta $x \leq b$ per ogni $x \in$ A.

$$b = \max A := x \leq b \ \forall x \in A$$

- Sia (A, ≤) un insieme ordinato. Si dimostra che se gli elementi min A e max A esistono, sono unici.

47

## Minimo e massimo

- Esempio:
  - dato S = {g, 1, +} e la relazione d'ordine $\mathcal{R}_1$ = {(g, g), (1, 1), (+, +), (g, 1)}, in (S, $\mathcal{R}_1$) non esiste né massimo né minimo.
  - dato S = {g, 1, +} e la relazione d'ordine $\mathcal{R}_2$ = {(g, g), (1, 1), (+, +), (g, 1), (1, +), (g, +)}, in (S, $\mathcal{R}_2$) g è minimo e + è massimo.

- Esempio:
  - In ($\mathbf{N}_0$, usuale) 0 è minimo e non esiste massimo.
  - In (**Z**, usuale) non esiste né massimo né minimo.
  - In ($\mathcal{P}$(T), $\subseteq$), $\emptyset$ è minimo e T è massimo.

48

# Insiemi ben ordinati

- Un insieme ordinato (A, ≤) è detto ben ordinato (e dice anche che ≤ è un buon ordine), se ogni sottoinsieme non vuoto di A, con la relazione d'ordine indotta, ammette minimo.

A ben ordinato := $\forall X \subseteq A, X \neq \emptyset, \exists \min X$

- Esempio: ($\mathbf{N}_0$, usuale) è ben ordinato.
- Ogni insieme ben ordinato è totalmente ordinato.
- Esistono insiemi totalmente ordinati, ma non ben ordinati, come ad esempio (**Z**, usuale).

49

# Minimali e massimali

- Un elemento *c* di un insieme ordinato (A, ≤) è detto minimale se non esistono in A elementi strettamente minori di *c*.
- Analogamente, un elemento *d* di un insieme ordinato (A, ≤) è detto massimale se non esistono in A elementi strettamente maggiori di *d*.
- Se un insieme ordinato ha minimo, questo è l'unico elemento minimale. Un insieme ordinato può avere più elementi minimali, ma non ammettere minimo. Analoga proprietà vale per il massimo.

50

# Minimali e massimali

- Un insieme può non avere minimali (massimali).
- Esempio: si consideri l'insieme C = {2, 3, 4, 5, 6} e la relazione d'ordine $x \mathcal{R}_d y \Leftrightarrow x$ divide $y$. Applicando $\mathcal{R}_d$ si ha che $2 \leq 4$, $2 \leq 6$, $3 \leq 6$. Dunque:
  – 2, 3 e 5 sono minimali in (C, $\mathcal{R}_d$)
  – 4, 5 e 6 sono massimali in (C, $\mathcal{R}_d$)
  – In (C, $\mathcal{R}_d$) non esiste minimo
  – In (C, $\mathcal{R}_d$) non esiste massimo

51

# Minoranti e maggioranti

- Sia (A, ≤) un insieme ordinato e X un sottoinsieme non vuoto di A. Un elemento $v$ di A è detto minorante di X in A se è confrontabile con ogni elemento di X e risulta minore o uguale di ogni $x \in X$.

$v$ minorante di X in A := $v \leq x \ \forall x \in X$

- Un elemento $w$ di A è detto maggiorante di X in A se è confrontabile con ogni elemento di X e risulta maggiore o uguale di ogni $x \in X$.

$w$ maggiorante di X in A := $x \leq w \ \forall x \in X$

- Se A ha minimo (massimo), tale elemento risulta minorante (maggiorante) di qualunque $X \subseteq A$, $X \neq \emptyset$.

52

# Minoranti e maggioranti

- Un sottoinsieme non vuoto di un insieme ordinato può non avere minoranti (maggioranti), averne uno solo, averne un numero finito o un numero infinito.
- Esempio: il sottoinsieme $2\mathbf{N}_0$ di ($\mathbf{N}_0$, usuale) ha in $\mathbf{N}_0$ un solo minorante (lo zero) e nessun maggiorante; il sottoinsieme $2\mathbf{N}_0$ di ($\mathbf{Z}$, usuale) ha infiniti minoranti in $\mathbf{Z}$ e nessun maggiorante; in ($\mathcal{P}$(T), $\subseteq$) con T = {a, b, c}, il sottoinsieme {{a}, {b}} ha come minorante solo $\varnothing$ e come maggioranti {a, b} e T.
- Se il sottoinsieme X $\subseteq$ A ha minoranti, è non vuoto l'insieme M = {*v* $\in$ A : v è minorante di X}.
- Se il sottoinsieme X $\subseteq$ A ha maggioranti, è non vuoto l'insieme N = {*w* $\in$ A : w è maggiorante di X}.

53

# Estremo inferiore e superiore

- Ordinato l'insieme M $\subseteq$ A con la relazione indotta, se esiste il massimo di M questo viene detto estremo inferiore di X in A e denotato con inf X.

$$k = \inf X := \begin{cases} k \le x \quad \forall x \in X \\ s \le x \ \forall x \in X \Rightarrow s \le k \end{cases}$$

- Ordinato l'insieme N $\subseteq$ A con la relazione indotta, se esiste il minimo di N questo viene detto estremo superiore di X in A e denotato con sup X.

$$h = \sup X := \begin{cases} x \le h \quad \forall x \in X \\ x \le s \ \forall x \in X \Rightarrow h \le s \end{cases}$$

54

# Estremo inferiore e superiore

- Esempio: si consideri l'insieme K = {3, 6, 12, 18, 36} e la relazione d'ordine $x \mathcal{R}_d y \Leftrightarrow x$ divide $y$. Applicando $\mathcal{R}_d$ si ha che $3 \leq 6$, $3 \leq 12$, $3 \leq 18$, $3 \leq 36$, $6 \leq 12$, $6 \leq 18$, $6 \leq 36$, $12 \leq 36$, $18 \leq 36$. Preso il sottoinsieme X = {12, 18} $\subseteq$ K si ha che:
  – M = {3, 6} è l'insieme dei minoranti di X
  – N = {36} è l'insieme dei maggioranti di X
  – inf X = 6
  – sup X = 36
  – non esiste min X
  – non esiste max X

55

# Funzioni

- Siano A e B insiemi. Una relazione $\mathcal{R}$ tra A e B tale che per ogni elemento $x$ di A esiste uno e uno solo elemento corrispondente in B è detta applicazione o funzione di A in B.

$\mathcal{R}$ funzione di A in B := $\forall x \in A\ \exists!\ y \in B : x \mathcal{R} y$

- Si scrive anche: $\mathcal{R} : x \in A \to \mathcal{R}(x) \in B$

Esempio: sono funzioni:

$$\mathcal{R}_{16} : x \in \mathbf{N}_0 \to 3 - x \in \mathbf{Z}$$

$$\mathcal{R}_{17} : x \in \mathbf{N}_0 \to x^2 \in \mathbf{N}_0$$

Non è una funzione: $x \mathcal{R}_{18} y \Leftrightarrow x + 2 < y$

56

# Funzioni

- Una funzione $\mathcal{R}$ è un sottoinsieme di A × B.
- Una relazione tra A e B che sia una funzione di solito è indicata con una lettera minuscola: *f* (da "funzione"), *g*, *h*, … e si usa la notazione $f : A \to B$.

- L'insieme A è detto il dominio della funzione *f*.
- L'insieme B è detto il codominio della funzione *f*.
- L'unico elemento $y \in B$ corrispondente di $x \in A$ attraverso *f* è detto l'immagine di *x* mediante *f* ed è denotato con $f(x)$.

57

# Funzioni

- Esempio: siano S = {g, 1, +}, W = {+, 5, m, 1, k} e $f : S \to W$ tale che $f(g) = m$, $f(1) = 5$ e $f(+) = +$. Si ha:
  – S è il dominio di *f*;
  – W è il codominio di *f*;
  – m è l'immagine di g mediante *f*; 5 è l'immagine di 1 mediante *f* e + è l'immagine di + mediante *f*.

- Una funzione di dominio $\mathbf{N}$ o $\mathbf{N}_0$ e codominio B è detta una successione di elementi di B. Per le successioni spesso si usa la notazione $a_n$, $n \in \mathbf{N}_0$

58

# Funzioni

- Se A è l'insieme vuoto esiste solo la relazione vuota tra A e un qualunque insieme B. Tale relazione è anche una funzione, la funzione vuota.
- Se invece B è vuoto, non esistono funzioni tra A e B.
- Una funzione $f : A \rightarrow B$ per la quale esiste un dato elemento $c \in B$ tale che $f(x) = c$ per ogni $x \in A$ è detta costante o costantemente uguale a $c$. Esempio: $f : \mathbf{R} \rightarrow \mathbf{N}_0$, $f(x) = 5$ per ogni $x \in \mathbf{R}$.
- Se A e B sono insiemi finiti con B non vuoto:
  – Il numero di funzioni constanti tra A e B è $|B|$
  – Il numero di funzioni tra A e B è $|B|^{|A|}$
  – L'insieme delle funzioni di A in B si denota con $\mathbf{B^A}$

59

# Funzioni

- Se A = B, la funzione $id_A : x \in A \rightarrow x \in A$ è detta funzione identica.
- Se $X \subseteq A$, la funzione $imm_X : x \in X \rightarrow x \in A$ è detta immersione di X in A.
- Sia $f : A \rightarrow B$ una funzione. Se $X \subseteq A$, l'insieme costituito dalle immagini in $f$ degli elementi di X è detto immagine di X in $f$ ed è denotato con $f(X)$.
- Sia $f : A \rightarrow B$ una funzione. Se $Y \subseteq B$, l'insieme costituito dagli elementi di A la cui immagine appartiene a Y è detto controimmagine di Y in f ed è denotato con $f^{-1}(Y)$.

60

# Funzioni

- Esempio: sia S = {g, 1, +}. $id_S : x \in S \rightarrow x \in S$ è tale che $id_S$ (g) = g, $id_S(1) = 1$, $id_S(+) = +$.
- Esempio: sia S = {g, 1, +} e X = {g, +} $\subseteq$ S. $imm_X : x \in X \rightarrow x \in S$ è tale che $imm_X$ (g) = g e $imm_X$ (+) = +.
- Esempio: siano S = {g, 1, +}, W = {+, 5, m, 1, k} e $f$ : S $\rightarrow$ W tale che $f$(g) = m, $f$(1) = 5 e $f$(+) = +.
  - Dato X = {g, +} $\subseteq$ S, l'immagine di X in $f$ è data da $f$(X) = {m, +}
  - Dato Y = {m, 5} $\subseteq$ W, la controimmagine di Y in $f$ è data da $f^{-1}$(Y) = {g, 1}.

61

# Funzioni

- Una funzione $f$ : A $\rightarrow$ B è detta iniettiva se è tale che elementi distinti in A hanno immagine distinta in B.

$f$ : A $\rightarrow$ B iniettiva := $x_1, x_2 \in A, x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$

- Una funzione $f$ : A $\rightarrow$ B è detta suriettiva se l'immagine di $f$ coincide con B.

$f$ : A $\rightarrow$ B suriettiva := $f$(A) = B ovvero $\forall y \in B, \exists x \in A : y = f(x)$

- Una funzione $f$ : A $\rightarrow$ B è detta biettiva (o biezione o corrispondenza biunivoca) se è sia iniettiva che suriettiva.

62

# Funzioni

- Esempio: $f : x \in \mathbf{Z} \rightarrow x^2 \in \mathbf{N}_0$ non è una funzione iniettiva, infatti ad esempio $f(-1) = f(1) = 1$.
  Invece la funzione $g : x \in \mathbf{N}_0 \rightarrow 2x \in 2\mathbf{N}_0$ è una funzione iniettiva.
- Esempio: $f : x \in \mathbf{Z} \rightarrow x^2 \in \mathbf{N}_0$ non è una funzione suriettiva, infatti ad esempio esiste $2 \in \mathbf{N}_0$ tale che non esiste alcun $x \in \mathbf{Z}$ per il quale risulti $x^2 = 2$.
  Invece la funzione $g : x \in \mathbf{N}_0 \rightarrow 2x \in 2\mathbf{N}_0$ è una funzione suriettiva.
- Esempio: la funzione $g : x \in \mathbf{N}_0 \rightarrow 2x \in 2\mathbf{N}_0$
  è sia iniettiva che suriettiva: è quindi una funzione biettiva.

63

# Funzioni

- Sia $f : A \rightarrow B$ una funzione biettiva. Si può allora definire una funzione di B in A che associa ad ogni elemento di B l'unico elemento di A di cui l'elemento di B è immagine secondo $f$. Tale funzione è detta funzione inversa di $f$ ed è denotata con $f^{-1}$.
  Esempio: data $g : x \in \mathbf{N}_0 \rightarrow 2x \in 2\mathbf{N}_0$
  si ha $g^{-1} : y \in 2\mathbf{N}_0 \rightarrow y / 2 \in \mathbf{N}_0$

$$f^{-1} : B \rightarrow A := y \rightarrow x \in A : f(x) = y$$

- Nel caso in cui la funzione inversa di una funzione biettiva $f : A \rightarrow B$ corrisponda con $f$ stessa, allora $f$ si dice un'involuzione di A.
  Esempio: $f : x \in \mathbf{Z} \rightarrow -x \in \mathbf{Z}$ è un'involuzione di $\mathbf{Z}$.

64

# 1.3 Introduzione alle strutture algebriche

C. Delizia, P. Longobardi, M. Maj, C. Nicotera.
Matematica Discreta, McGraw-Hill. Capitolo 4.

65

## Operazioni interne

- Sia A un insieme. Una funzione $\perp : A \times A \to A$ è detta operazione interna (o legge interna) di A.
- L'immagine mediante $\perp$ della coppia $(x, y)$ è di solito denotata con il simbolo $x \perp y$ e detta composto di $x$ e $y$ in $\perp$.
- Si usa il simbolo $(A, \perp)$ per indicare l'insieme A dotato dell'operazione interna $\perp$.
- Esempio: l'addizione e la moltiplicazione usuali in $\mathbf{N}_0$, $\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$ e $\mathbf{R}$ sono operazioni interne nei rispettivi insiemi; la sottrazione usuale non è un'operazione interna in $\mathbf{N}_0$ e $\mathbf{N}$.

66

# Tabella di moltiplicazione

- Se A è un insieme finito dotato di un'operazione interna $\perp$, è possibile rappresentare tale operazione mediante una tabella, la cosiddetta tabella di moltiplicazione di (A, $\perp$).

| $\perp$ | $x_1$ | $x_2$ | … | $x_n$ |
|---|---|---|---|---|
| $x_1$ | $x_1 \perp x_1$ | $x_1 \perp x_2$ | … | $x_1 \perp x_n$ |
| $x_2$ | $x_2 \perp x_1$ | $x_2 \perp x_2$ | … | $x_2 \perp x_n$ |
| $\vdots$ | $\vdots$ | $\vdots$ | | $\vdots$ |
| $x_n$ | $x_n \perp x_1$ | $x_n \perp x_2$ | … | $x_n \perp x_n$ |

67

# Proprietà delle operazioni

- Sia A un insieme e $\perp$ un'operazione interna in A.
  - Elementi $x, y \in$ A sono detti permutabili in (A, $\perp$) se si ha $x \perp y = y \perp x$.
  - L'operazione $\perp$ è detta commutativa se $x$ e $y$ sono permutabili per ogni $x, y \in$ A, cioè se si ha $x \perp y = y \perp x$ per ogni $(x, y) \in$ A $\times$ A.
  - L'operazione $\perp$ è detta associativa se si ha $(x \perp y) \perp z = x \perp (y \perp z)$ per ogni $x, y, z \in$ A.
- Esempio: le usuali operazioni di somma e prodotto in $\mathbf{N}_0$, in **N**, in **Z**, in **Q** e in **R** sono sia commutative che associative; la sottrazione in **Z** non è commutativa né associativa.

68

# Proprietà delle operazioni

- Sia A un insieme e siano $\perp$ e $\top$ due operazioni interne di A.
  - Si dice che $\top$ è distributiva a sinistra rispetto a $\perp$ se $x \top (y \perp z) = (x \top y) \perp (x \top z)$.
  - Si dice che $\top$ è distributiva a destra rispetto a $\perp$ se $(x \perp y) \top z = (x \top z) \perp (y \top z)$.
  - L'operazione $\top$ è detta distributiva rispetto a $\perp$ se lo è a destra e a sinistra.
- Esempio: il prodotto usuale in **N** (o in $\mathbf{N}_0$, in **Z**, in **Q**, in **R**) è distributivo rispetto alla somma usuale. La somma, invece, non lo è rispetto al prodotto.

69

# Elemento neutro

- Sia A un insieme e $\perp$ un'operazione interna di A. Un elemento $e \in$ A è detto neutro rispetto a $\perp$ se si ha $e \perp x = x = x \perp e$ per ogni $x \in$ A.
- In particolare, un elemento neutro è permutabile con ogni elemento di A.
- Esempio:
  - In $(\mathbf{N}_0, +)$, il numero 0 è elemento neutro; in $(\mathbf{N}_0, \cdot)$, il numero 1 è elemento neutro.
  - Se V è un insieme, l'insieme vuoto è elemento neutro in $(\mathcal{P}(V), \cup)$, mentre l'insieme V è elemento neutro in $(\mathcal{P}(V), \cap)$.

70

# Elemento simmetrico

- Sia (A, $\perp$) dotato di elemento neutro *e* e sia $x \in$ A. Un elemento $x'$ $\in$ A è detto simmetrico di *x* se si ha $x \perp x' = e = x' \perp x$.
- *x* è detto simmetrizzabile se è dotato di simmetrico.
- Esempio:
  - In ($\mathbf{N}_0$, +), il numero 0 è l'unico elemento simmetrizzabile; in ($\mathbf{N}_0$, $\cdot$), il numero 1 è l'unico elemento simmetrizzabile.
  - In (**Z**, +) ogni $x \in \mathbf{Z}$ ha come simmetrico $-x$.
  - In (**Q**, $\cdot$) ogni elemento $m/n \neq 0$ ha come simmetrico il numero $n/m$.

71

# Notazione additiva e moltiplicativa

- Quando l'operazione interna $\perp$ è denotata con + è adottata la cosiddetta notazione additiva. In tal caso:
  - L'elemento neutro, se esiste, è indicato con 0.
  - Se l'operazione in A è associativa e l'elemento $x \in$ A è simmetrizzabile, il suo unico simmetrico è indicato con il simbolo $-x$ ed è detto opposto di *x*.
- Quando l'operazione interna $\perp$ è denotata con $\cdot$ è adottata la cosiddetta notazione moltipicativa e si ha:
  - L'elemento neutro, se esiste, è indicato con 1.
  - Se l'operazione in A è associativa e l'elemento $x \in$ A è simmetrizzabile, il suo unico simmetrico è indicato con il simbolo $x^{-1}$ ed è detto inverso di *x*.

72

# Operazione esterna

- Siano A e Ω insiemi. Una funzione $\star : \Omega \times A \to A$ è detta operazione esterna di A con dominio di operatori in Ω (o anche con operatori in Ω).
- Gli elementi di Ω vengono di solito denotati con lettere greche e sono detti anche scalari.
- L'immagine mediante $\star$ della coppia $(\alpha, x)$ è spesso denotata con $\alpha \star x$ e detta composto di α e x in $\star$.
- Esempio: $\star_1 : (\alpha, x) \in \mathbf{Q} \times \mathbf{R} \to \alpha \cdot x \in \mathbf{R}$ è un operazione esterna di **R** con operatori in **Q**;
  $\star_2 : (\alpha, x) \in \mathbf{R} \times \mathbf{R} \to \alpha \cdot x \in \mathbf{R}$ è un operazione esterna di **R** con operatori in **R**;
  $\star_3 : (\alpha, (x, y)) \in \mathbf{R} \times \mathbf{R}^2 \to (\alpha \cdot x, \alpha \cdot y) \in \mathbf{R}^2$ è un operazione esterna di $\mathbf{R}^2$ con operatori in **R**.

73

# Strutture algebriche

- Un insieme A dotato di una o più operazioni interne o esterne è detto struttura algebrica.
- Se l'operazione è unica allora A è detto struttura algebrica semplice.
- Esempio:
  $(\mathbf{Z}, +, \cdot)$, $(\mathbf{R}, +, \star_1)$, $(\mathcal{P}(S), \cup, \cap, \setminus)$
  sono strutture algebriche;
  $(\mathbf{N}_0, +)$ è una struttura algebrica semplice.

74

## Semigruppi, monoidi e gruppi

- La struttura (A, ⊥), con ⊥ operazione interna, è detta:
  - semigruppo se ⊥ è associativa;
  - monoide se ⊥ è associativa e, inoltre, è dotata di elemento neutro;
  - gruppo se ⊥ è associativa, dotata di elemento neutro e ogni elemento di A è simmetrizzabile;
  - gruppo abeliano se è un gruppo e, inoltre, l'operazione ⊥ è commutativa.
- Esempio:
  (**N**, +) è un semigruppo, ma non è un monoide
  ($\mathbf{N}_0$, +) è un monoide, ma non è un gruppo
  (**Z**, +) è un gruppo abeliano

75

## Anelli

- La struttura (A, ⊥, ⊤), con ⊥ e ⊤ operazioni interne, è detta anello se (A, ⊥) è un gruppo abeliano e ⊤ è associativa ed è distributiva rispetto a ⊥.
  - Se esiste anche l'elemento neutro rispetto a T, l'anello è detto unitario.
  - Se inoltre ⊤ è commutativa, l'anello è detto commutativo.
- Esempio: (**Z**, +, ·) è un anello commutativo unitario; ($\mathcal{P}$(S), $\dot\cup$, ∩) è un anello commutativo unitario.

76

# Corpi e campi

- Un anello unitario (A, $\perp$, $\top$) è detto corpo se ha più di un elemento e ogni elemento distinto dall'elemento neutro è simmetrizzabile rispetto a $\top$.
- Se (A, $\perp$, $\top$) è un corpo ed inoltre $\top$ è commutativa, allora (A, $\perp$, $\top$) è detto campo.
- Esempio: ($\mathbf{Q}$, +, $\cdot$) e ($\mathbf{R}$, +, $\cdot$) sono campi.

77

# Omomorfismi

- Siano (A, $\perp$) e (B, $\top$) strutture algebriche con un'operazione interna:
  - Una funzione $f : A \to B$ è detta omomorfismo di (A, $\perp$) in (B, $\top$) se si ha $f(x \perp y) = f(x) \top f(y)$ per ogni $x, y \in A$.
  - Un omomorfismo iniettivo è detto monomorfismo.
  - Un omomorfismo suriettivo è detto epimorfismo.
  - Un omomorfismo biettivo è detto isomorfismo.
  - Un omomorfismo di una struttura (A, $\perp$) in se stessa è detto endomorfismo (o automorfismo).
- Esempio: $g : n \in \mathbf{N}_0 \to 2^n \in \mathbf{N}$ è un monomorfismo di ($\mathbf{N}_0$, +) in ($\mathbf{N}$, $\cdot$).

78

# 1.4 Elementi di calcolo combinatorio

C. Delizia, P. Longobardi, M. Maj, C. Nicotera.
Matetica Discreta, McGraw-Hill. Capitolo 3.

79

## Principio di addizione e di inclusione-esclusione

- Principio di addizione: siano A e B due insiemi finiti disgiunti. Allora $|A \cup B| = |A| + |B|$.
- Sia A un insieme finito.
  - Se $C \subseteq A$, allora $|A \setminus C| = |A| - |C|$.
  - Se B è un insieme qualunque, allora si ha che $|A \setminus B| = |A| - |A \cap B|$.
- Principio di inclusione-esclusione: siano A e B due insiemi finiti. Si ha che $|A \cup B| = |A| + |B| - |A \cap B|$.
- Esempio: i numeri naturali positivi minori di 31 e divisibili per 2 o per 3 sono 20.

80

# Principio di moltiplicazione

- Principio di moltiplicazione: siano A e B due insiemi finiti. Allora $|A \times B| = |A| \cdot |B|$.
- Più in generale, siano $A_1, A_2, \ldots, A_k$ insiemi finiti con $k \geq 2$. Si ha $|A_1 \times A_2 \times \ldots \times A_k| = |A_1| \cdot |A_2| \cdot \ldots \cdot |A_k|$.
- Nota. Il principio di moltiplicazione può essere interpretato in questo modo: se $E_1, \ldots E_k$ sono eventi indipendenti tali che ci siano $n_1$ possibilità per $E_1$, $n_2$ possibilità per $E_2$, …, $n_k$ possibilità per $E_k$, allora il numero di possibilità per la sequenza $E_1E_2\ldots E_k$ è $n_1 \cdot n_2 \cdot \ldots \cdot n_k$. Da ciò deriva:
  - Sia A un insieme finito. Allora $|\mathcal{P}(A)| = 2^{|A|}$.
  - Siano A e B insiemi finiti. Allora l'insieme $B^A$ delle funzioni di A in B ha cardinalità $|B|^{|A|}$.

81

# Fattoriale

- Sia $n$ un numero naturale positivo.
  Il prodotto $1 \cdot 2 \cdot \ldots \cdot n$ è detto fattoriale di $n$ e denotato con il simbolo $n!$
- Si pone inoltre $0! := 1$.
- Nota: questo equivale a porre con $n \in \mathbf{N}_0$
  $0! := 1$ e induttivamente $(n + 1)! := n! \cdot (n + 1)$.
- Esempio:
  $1! = 1$
  $2! = 1 \cdot 2 = 2$
  $3! = 1 \cdot 2 \cdot 3 = 6$
  $4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24$
  $5! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120$

82

# Permutazioni

- Sia X un insieme finito. Una funzione biettiva di X in X è detta permutazione (o sostituzione) di X.
- L'insieme delle permutazioni di X è di solito denotato con $\mathbf{S}_X$.
- Sia X un insieme finito. Se $|X| = n$, si ha $|\mathbf{S}_X| = n!$
- Esempio: le permutazioni di un qualunque insieme di cardinalità 2 sono 2, di cardinalità 3 sono 6, di cardinalità 4 sono 24.
- Esempio: volendo contare in quanti modi si possono allineare 3 dischetti di diverso colore, basta determinare il numero delle permutazioni di un insieme di cardinalità 3. Pertanto ci sono 6 possibili allineamenti.

83

# Permutazioni con ripetizioni

- Si considerino $k$ oggetti $a_1$, $a_2$, …, $a_k$ a due a due distinti ($k \geq 1$), sia $n = n_1 + n_2 + \ldots n_k$ con ogni $n_i \geq 1$, e siano $b_1$, $b_2 \ldots b_n$ $n$ oggetti.
- Una n-upla ($b_1$, $b_2 \ldots b_n$) in cui $a_1$ compare $n_1$ volte, $a_2$ compare $n_2$ volte, …, $a_k$ compare $n_k$ volte, è denotata con il simbolo $b_1 \ldots b_n$ ed è detta permutazione con ripetizioni dei $k$ oggetti $a_1$, $a_2$, …, $a_k$ in cui $a_1$ si ripete $n_1$ volte, $a_2$ si ripete $n_2$ volte, …, $a_k$ si ripete $n_k$ volte.
- Esempio: 1131733739 è una permutazione con ripetizioni dei 4 numeri 1, 3, 7, 9, in cui 1 si ripete 3 volte, 3 si ripete 4 volte, 7 si ripete 2 volte e 9 si ripete una volta.

84

# Permutazioni con ripetizione

- Siano *k, $n_1$*, $n_2$, … $n_k$ numeri naturali positivi e si ponga $n = n_1 + n_2 + \dots n_k$.
  Allora il numero delle permutazioni con ripetizione dei *k* oggetti $a_1$, $a_2$, …, $a_k$ in cui $a_1$ si ripete $n_1$ volte, $a_2$ si ripete $n_2$ volte, …, $a_k$ si ripete $n_k$ è dato da:

*numero di permutazioni* := $\dfrac{n!}{n_1! \cdot n_2! \cdot \ldots \cdot n_k!}$

- Esempio: il numero di permutazioni con ripetizione dei 4 numeri 1, 3, 7, 9, in cui 1 si ripete 3 volte, 3 si ripete 4 volte, 7 si ripete 2 volte e 9 si ripete una volta è 10! / (3! · 4! · 2! · 1!) = 12600.

85

# Disposizioni

- Siano *n* e *h* numeri naturali positivi. Il numero $d_{n,h}$ delle disposizioni di *n* elementi su *h* posti è definito come segue:

$$d_{n,h} := \begin{cases} 0 & \text{se } h > n \\ n(n-1)\ldots(n-(h-1)) & \text{se } h \le n \end{cases}$$

- Per $h \le n$, $d_{n,h}$ è pertanto calcolato come il prodotto dei primi *h* numeri presi in ordine decrescente a partire da *n*. Questo equivale a scrivere:

$$d_{n,h} = \frac{n!}{(n-h)!} \quad \text{se } h \le n$$

86

# Disposizioni

- Esempio: le parole non necessariamente di senso compiuto che si possono scrivere con 4 lettere distinte scelte nell'insieme {A, C, D, E, I, S, O} sono $d_{7,4} = 7 \cdot 6 \cdot 5 \cdot 4 = 840$.
- Esempio: si ha una possibilità su 1680 di indovinare l'ordine esatto di arrivo dei primi 4 classificati in una gara cui partecipano 8 concorrenti. Infatti $d_{8,4} = 1680$.
- Il numero di funzioni iniettive di un insieme di cardinalità *h* in un insieme di cardinalità *n*, con $h$, $n > 0$ è $d_{n,h}$.
- Esempio: il numero delle funzioni iniettive di A = {a, b, c, d, e} in B= {9, 10, 11, 12, 13, 14, 15, 16} è $d_{8,5} = 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 = 6720$.

87

# Disposizioni con ripetizione

- Disporre su *h* posti oggetti scelti tra *n*, permettendo ripetizioni, equivale a definire una funzione di un insieme di cardinalità *h* nell'insieme costituito dagli *n* oggetti. Il numero di tali funzioni è $n^h$.
- Quindi: il numero di disposizioni con ripetizione di *n* oggetti su *h* posti è $n^h$.
- Esempio: i numeri naturali positivi costituiti da 4 cifre dispari non necessariamente distinte sono $5^4 = 625$.
- Esempio: nel gioco Mastermind le sequenze di 4 colori non necessariamente distinti scelti tra 6 colori sono $6^4 = 1296$.

88

# Combinazioni

- Siano $n$ e $h$ numeri naturali con $0 < h \leq n$. Il numero $c_{n,h}$ delle combinazioni semplici di $n$ elementi ad $h$ ad $h$ è definito come:

$$c_{n,h} := \frac{d_{n,h}}{h!} = \frac{n(n-1)...(n-h+1)}{h!}$$

- Si pone inoltre per ogni $n \in \mathbf{N}_0$, $c_{n,0} := 1$.
- Esempio: il numero di terni che si possono giocare al Lotto sono quanti le combinazioni di 90 elementi a 3 a 3, ossia $c_{90,3} = (90 \cdot 89 \cdot 88) / 3! = 117480$.
- Esempio: il numero di bouquet distinti che si possono comporre con 7 fiori presi 5 a 5 è $c_{7,5} = 21$.

89

# Combinazioni

- Si noti che $c_{n,n} = n! / n! = 1 = c_{n,0}$
- Inoltre con $0 < h \leq n$ si ha che:

$$c_{n,h} = \frac{d_{n,h}}{h!} = \frac{n!/(n-h)!}{h!} = \frac{n!}{h!(n-h)!}$$

- $c_{n,h}$ è sempre un numero intero.
- Se $n$ e $h$ sono numeri interi, con $0 < h \leq n$, il numero dei sottoinsiemi di cardinalità $h$ di un insieme di cardinalità $n$ è $c_{n,h}$.

90

# Coefficienti binomiali

- A volte, invece di usare il simbolo $c_{n,h}$ il numero di combinazioni semplici di *n* elementi ad *h* ad *h* si denota con il coefficiente binomiale *n* su *h*:

$$c_{n,h} = \binom{n}{h} = \frac{n(n-1)...(n-h+1)}{h!} = \frac{n!}{h!(n-h)!}$$

- Se *n* e *h* sono numeri interi, con $0 < h \leq n$, si ha che:

$$\binom{n}{h} = \binom{n}{n-h} \text{ e inoltre } \binom{n}{h-1} + \binom{n}{h} = \binom{n+1}{h}$$

91

# Combinazioni con ripetizione

- Volendo contare in quanti modi è possibile scegliere *h* oggetti, *non necessariamente distinti*, tra *n* possibilità, tale numero – detto numero di combinazioni con ripetizione di *h* oggetti tra *n* – è:

$$c^r_{n,h} = \frac{(n+h-1)!}{h!\,(n-1)!}$$

- Esempio: al mercato sono disponibili mele, pere, banane, arance e kiwi. Volendo acquistare due frutti non necessariamente diversi si hanno tante scelte quante sono le combinazioni con ripetizione di 2 oggetti tra 5: (2 + 5 – 1)! / (2! · 4!) = 15.

92