LIBRO ADOTTATO

G.M. PIACENTINI CATTANEO: **MATEMATICA DISCRETA**, ed. ZANICHELLI

LIBRI CONSIGLIATI

A. FACCHINI: **ALGEBRA E MATEMATICA DISCRETA**, ed. ZANICHELLI

M.G. BIANCHI, A. GILLIO: **INTRODUZIONE ALLA MATEMATICA DISCRETA**, ed. McGRAW-HILL

L. DI MARTINO, M.C. TAMBURINI: **APPUNTI DI ALGEBRA**, ed. CLUED

INSIEMI NUMERICI

$$\mathbb{N} = \{0, 1, 2, 3, 4, \dots, \}$$

insieme dei numeri naturali

$$\mathbb{Z} = \{\dots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \dots\}$$

insieme dei numeri relativi

$\mathbb{Q}$ è l'insieme dei numeri della forma $\frac{p}{q}$,

dove p e q sono numeri relativi e q è diverso da 0; $\mathbb{Q}$ si dice insieme dei numeri razionali

con il simbolo $\mathbb{R}$ indicheremo l'insieme dei numeri reali e definiremo anche l'insieme $\mathbb{C}$ dei numeri complessi.

SIMBOLI FONDAMENTALI

Il simbolo di appartenenza di un oggetto ad un insieme è:

$$" \in "$$

si legge: "appartiene" oppure "è elemento di". Ad esempio:

$$3 \in \mathbb{N}, \quad -1 \in \mathbb{Z}, \quad \frac{5}{3} \in \mathbb{Q}, \quad -\sqrt{5} \in \mathbb{R}$$

I simboli di inclusione sono: $\begin{cases} \subset \\ \subseteq \end{cases}$

il primo indica l'inclusione stretta o propria (che può essere anche scritta come $\subsetneq$) tra insiemi e si legge: "è incluso (oppure è contenuto) propriamente o strettamente" o anche "è sottoinsieme proprio", il secondo si legge "è incluso (o uguale)" oppure "è contenuto (o uguale)". Esempi: $\mathbb{N} \subset \mathbb{Z}$, $\mathbb{Z} \subset \mathbb{Q}$.

Definizione 1 *Si dice che due insiemi A e B sono uguali, e si scrive $A = B$, se essi hanno gli stessi elementi.*

È chiaro, quindi, che $A = B$ se e soltanto se $A \subseteq B$ e $B \subseteq A$.

osservazione 2 Quali che siano gli insiemi A, B, C si ha:

1. $A \subseteq A$

2. se $A \subseteq B$ e $B \subseteq A$ allora $A = B$

3. se $A \subseteq B$ e $B \subseteq C$ allora $A \subseteq C$

Naturalmente abbiamo le negazioni:

"non appartiene": $\notin$

esempi: $-3 \notin \mathbb{N}, \quad \frac{1}{3} \notin \mathbb{Z}, \quad \pi \notin \mathbb{Q}$

"non è contenuto": $\not\subseteq$

esempi: $\mathbb{Z} \not\subseteq \mathbb{N}, \quad \mathbb{R} \not\subseteq \mathbb{Q}.$

Insieme vuoto: $\emptyset$

è l'insieme che non ha elementi. Si osservi che esso è sottoinsieme di qualunque insieme.

Si può assegnare un insieme enumerando i suoi elementi (nel caso questo sia possibile), oppure tramite una proprietà caratteristica, ovvero una proprietà che verificano tutti e soli gli elementi dell'insieme che si vuole definire. Si scrive:

$$A = \{x \in U \mid \mathcal{P}(x)\} \text{ oppure } A = \{x \in U \ : \ \mathcal{P}(x)\}$$

Esempi: $\{x \in \mathbb{Z} \mid x > -3\}$, $\{3n \mid n \in \mathbb{N}\}$.

quantificatori: $\begin{cases} \forall & \text{quantificatore universale} \\ \exists & \text{quantificatore esistenziale} \end{cases}$

il primo si legge "per ogni", il secondo si legge "esiste".

Si usa anche il simbolo

$$\exists|$$

che vuol dire "esiste ed è unico".

Esempi:

$$(\forall n \in \mathbb{N})\ (3n \in \mathbb{N})$$

Sia $\mathbf{P}$ l'insieme dei numeri pari. Allora si può scrivere

$$\mathbf{P} = \{n \in \mathbb{Z} \mid \exists m \in \mathbb{Z} \text{ tale che } n = 2m\}.$$

L'insieme $\mathbf{D}$ dei numeri dispari può essere scritto come

$$\mathbf{D} = \{n \in \mathbb{Z} \mid \exists h \in \mathbb{Z} \text{ tale che } n = 2h + 1\}.$$

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

$$(\forall A \text{ insieme})(\emptyset \subseteq A)$$

Connettivi logici

congiunzione: $\wedge$ che si legge "e"

disgiunzione: $\vee$ che si legge "o".

Esempi: $(8 \in \mathbf{P}) \wedge (8$ è divisibile per $4)$

sia $n \in \mathbb{Z}$ allora: $(n \in \mathbf{P}) \vee (n \in \mathbf{D})$.

Definizione 3 *Dati due insiemi A e B si definiscono l'unione $A \cup B$ e l'intersezione $A \cap B$ come segue:*

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

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

Si osserva subito che per ogni insieme A

$$A \cup \emptyset = A \quad A \cap \emptyset = \emptyset$$

e che se $A \subseteq B$ allora si ha

$$A \cup B = B \quad A \cap B = A.$$

1. $(A \cup B) \cup C = A \cup (B \cup C)$ proprietà associativa dell'unione

2. $(A \cap B) \cap C = A \cap (B \cap C)$ proprietà associativa dell'intersezione

3. $A \cup B = B \cup A$ proprietà commutativa dell'unione

4. $A \cap B = B \cap A$ proprietà commutativa dell'intersezione

5. $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

6. $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

5. proprietà distributive dell'intersezione rispetto all'unione,
6. proprietà distributive dell'unione rispetto all'intersezione.

Definizione 4 *Sia A insieme e $B \subseteq A$ si definisce il complementare di B rispetto ad A:*

$$\complement_A(B) = \{x \in A \mid x \notin B\}.$$

Si ha ovviamente:

$$\complement_A(A) = \emptyset; \quad \complement_A(\emptyset) = A; \quad B \cup \complement_A(B) = A; \quad B \cap \complement_A(B) = \emptyset$$

Si dimostrano le LEGGI DI DE MORGAN:

$$\complement_A(B \cup C) = \complement_A(B) \cap \complement_A(C); \quad \complement_A(B \cap C) = \complement_A(B) \cup \complement_A(C)$$

Definizione 5 *L'insieme:*

$$A \setminus B = \{x \in A \mid x \notin B\}$$

si dice insieme differenza tra l'insieme A e l'insieme B

Definizione 6 *Sia A un insieme. Si dice insieme delle parti di* A *e si indica con* $\mathcal{P}(A)$ *l'insieme formato da tutti i sottoinsiemi di* A*. In simboli:*

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

È ovvio che $A \in \mathcal{P}(A)$, $\emptyset \in \mathcal{P}(A)$, se $X \in \mathcal{P}(A)$, $Y \in \mathcal{P}(A)$, allora $X \cup Y \in \mathcal{P}(A)$ e $X \cap Y \in \mathcal{P}(A)$.

Definizione 7 *Siano* A *e* B *insiemi. Si definisce il prodotto cartesiano:*

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

Naturalmente si ha: $A \times \emptyset = \emptyset \times A = \emptyset$.

Definizione 8 *Siano* A *e* B *insiemi. Si dice relazione tra* A *e* B *un qualunque sottoinsieme del prodotto cartesiano.*

Sia A un insieme ed $\mathcal{R}$ una relazione tra gli elementi di A, cioè $\mathcal{R} \subseteq A \times A$.

Definizione 9 *Si dice che $\mathcal{R}$ è riflessiva se è verificata la sequente condizione:*

$$(\forall a \in A)\ ((a, a) \in \mathcal{R}).$$

osservazione 10 Ovviamente, perchè $\mathcal{R}$ non sia riflessiva basta che esista un solo elemento $x \in A$ tale che $(x, x) \notin A$.

Definizione 11 *Si dice che $\mathcal{R}$ è antiriflessiva se è verificata la sequente condizione:*

$$(\forall a \in A)\ ((a, a) \notin \mathcal{R}).$$

Esempi Delle relazioni sull'insieme $A = \{\alpha, \beta, \gamma\}$

$$\mathcal{R}_1 = \{(\alpha,\alpha),(\beta,\beta),(\gamma,\gamma),(\alpha,\beta),(\alpha,\gamma)\}$$

$$\mathcal{R}_2 = \{(\alpha,\alpha),(\beta,\beta),(\alpha,\beta),(\beta,\gamma)\}$$

$$\mathcal{R}_3 = \{(\alpha,\beta),(\beta,\alpha),(\gamma,\beta),(\beta,\gamma),(\gamma,\gamma)\}$$

$$\mathcal{R}_4 = \{(\alpha,\beta),(\beta,\alpha),(\alpha,\gamma)\}$$

$$\mathcal{R}_5 = \{(\alpha,\alpha),(\beta,\beta),(\gamma,\gamma),(\alpha,\beta),(\beta,\alpha)\}$$

sono riflessive $\mathcal{R}_1$ e $\mathcal{R}_5$, è antiriflessiva $\mathcal{R}_4$ mentre $\mathcal{R}_2$ e $\mathcal{R}_3$ non sono riflessive (ne' antiriflessive).

Definizione 12 *Si dice che* $\mathcal{R}$ *è* <u>*simmetrica*</u> *se è verificata la sequente condizione:*

$$(\forall a, b \in A) \text{ (se } (a, b) \in \mathcal{R} \text{ allora } (b, a) \in \mathcal{R}).$$

osservazione 13 Naturalmente è sufficiente che esista una sola coppia $(x, y) \in \mathcal{R}$, $x \neq y$, tale che $(y, x) \notin \mathcal{R}$ perchè $\mathcal{R}$ non sia simmetrica.

Definizione 14 *Si dice che* $\mathcal{R}$ *è* <u>*antisimmetrica*</u> *se è verificata la sequente condizione:*

$$(\forall a, b \in A) \text{ (se } ((a, b) \in \mathcal{R} \ \wedge (b, a) \in \mathcal{R}) \text{ allora } a = b).$$

Esempi Si ha: $\mathcal{R}_1$ e $\mathcal{R}_2$ sono antisimmetriche, $\mathcal{R}_3$ e $\mathcal{R}_5$ sono simmetriche, $\mathcal{R}_4$ non è simmetrica ne' antisimmetrica.

Definizione 15 *Si dice che $\mathcal{R}$ è transitiva se è verificata la seguente condizione:*

$$(\forall a, b, c \in A) \text{ (se } ((a, b) \in \mathcal{R} \ \wedge (b, c) \in \mathcal{R}) \text{ allora } (a, c) \in \mathcal{R}).$$

osservazione 16 Anche in questo caso è sufficiente che esistano $(x, y),\ (y, z) \in \mathcal{R}$ tali che $(x, z) \notin \mathcal{R}$ perchè $\mathcal{R}$ non sia transitiva.

Esempi Si ha: $\mathcal{R}_1$ e $\mathcal{R}_5$ sono transitive, $\mathcal{R}_2$, $\mathcal{R}_3$ e $\mathcal{R}_4$ non lo sono.

osservazione 17 Si osservi che spesso si usa la notazione $a\mathcal{R}b$ in luogo di $(a, b) \in \mathcal{R}$.

Definizione 18 *Si dice che* $\mathcal{R}$ *è* *una relazione d'ordine* *se è* **riflessiva, antisimmetrica e transitiva**. *La coppia ordinata* $(A, \mathcal{R})$ *(ovvero l'insieme* A *munito della relazione d'ordine) si chiama insieme ordinato.*

Esempio 19 $\mathcal{R}_1$ *è d'ordine.*

Esempio 20 Sia X un insieme. Allora la relazione " $\subseteq$ " è una relazione d'ordine su $\mathcal{P}(X)$. Infatti dall'osservazione 2 si ha che per ogni A, B, C sottoinsiemi di X

1. $A \subseteq A$

2. se $A \subseteq B$ e $B \subseteq A$ allora $A = B$

3. se $A \subseteq B$ e $B \subseteq C$ allora $A \subseteq C$

Esempio 21 L'ordinamento naturale " $\leq$ " sull'insieme $\mathbb{Z}$ dei numeri relativi è la relazione definita come segue:

$\forall m, n \in \mathbb{Z}$, si dice che $m \leq n$ se e solo se $\exists h \in \mathbb{N}$ tale che $n = m+h$.

Si verifica che " $\leq$ " è una relazione d'ordine su $\mathbb{Z}$.

Definizione 22 *Siano $m, n \in \mathbb{Z}$, $m \neq 0$. Si dice che m divide oppure è un divisore di n (ovvero che n è un multiplo di m) e si scrive*

$$m \mid n$$

se esiste $h \in \mathbb{Z}$ tale che $n = mh$.

Si osserva subito che un qualunque numero intero divide 0.

Esempio 23 La relazione "$|$ " sull'insieme $\mathbb{N}^* := \mathbb{N} \setminus \{0\}$ dei numeri naturali non nulli è una relazione d'ordine.

Esempio 24 Per ogni $n \in \mathbb{N}^*$ si indica con $\mathcal{D}_n$ l'insieme dei divisori di n. Di particolare interesse è la relazione d'ordine "$|$ " indotta sull'insieme $\mathcal{D}_n$.

Definizione 25 *Sia $(A, \leq)$ un insieme ordinato, X un sottoinsieme di A, $x_0 \in X$. Si dice che x_0 è minimo di X se:*

$$\forall x \in X \ x_0 \leq x.$$

Si dice che x_0 è massimo di X se

$$\forall x \in X \ x \leq x_0.$$

Proposizione 26 *Sia $(A, \leq)$ un insieme ordinato, X un sottoinsieme di A. Se esiste un massimo (o un minimo) di X, esso è unico.*

Dimostrazione Siano, infatti, x_0 e x_1 due massimi di X. Allora, poichè x_0 è massimo e $x_1 \in X$, si ha $x_1 \leq x_0$ e, scambiando i ruoli di x_0 e x_1, si ha $x_0 \leq x_1$. Per la proprietà antisimmetrica delle relazioni d'ordine deve essere $x_0 = x_1$. (Analoga la dimostrazione dell'unicità del minimo.)

È quindi lecito scrivere $x_0 = min(X)$ se x_0 è il minimo (che si dice anche il più piccolo elemento) di X, oppure $x_0 = max(X)$ se x_0 è il massimo (che si dice anche il più grande elemento) di X.

Esempi

1. considerato l'insieme ordinato $(A, \mathcal{R}_1)$, dove $A = \{\alpha, \beta, \gamma\}$ e

$$\mathcal{R}_1 = \{(\alpha, \alpha), (\beta, \beta), (\gamma, \gamma), (\alpha, \beta), (\alpha, \gamma)\}.$$

   Si ha $\alpha = min(A)$ ma non esiste il massimo di A

2. 0=$min(\mathbb{N})$, ma non esiste il massimo considerando su $\mathbb{N}$ la relazione d'ordine " $\leq$ " naturale

3. $1 = min(\mathbb{N}^*)$ ma non esiste il massimo considerando su $\mathbb{N}^*$ la relazione d'ordine "$|$"

4. considerando il sottoinsieme $X = \{2, 3, 9, 18\}$ come sottoinsieme dell'insieme ordinato $(\mathbb{N}^*, |)$, esiste $max(X) = 18$ ma non esiste il minimo di X

5. considerando l'insieme ordinato $(D_n, |)$ si ha $min(D_n) = 1$, $max(D_n) = n$

Definizione 27 *Sia $(A, \leq)$ un insieme ordinato, $A \subseteq X$. Un elemento $y \in A$ si dice <u>minorante</u> di X se*

$$(\forall x \in X)(y \leq x).$$

Se X è dotato di minoranti si dice minorato o limitato inferiormente.

Definizione 28 *Sia $(A, \leq)$ un insieme ordinato, X un sottoinsieme di A, minorato, $\alpha \in A$. Si dice che α è <u>estremo inferiore di</u> X se è il più grande dei minoranti.*

In altri termini α è estremo inferiore di se verifica le seguenti condizioni:

1. $(\forall x \in X)\ (\alpha \leq x)$

2. $\forall\ \beta \in A$ tale che $(\forall x \in X)\ (\beta \leq x)$ si ha $\beta \leq \alpha$.

Si vede che se esiste un estremo inferiore, esso è unico, per cui è lecito scrivere $\alpha = inf(X)$. Inoltre, se $inf(X) \in X$, allora $inf(X) = min(X)$.

Definizione 29 *Sia $(A, \leq)$ un insieme ordinato, $A \subseteq X$. Un elemento $y \in A$ si dice maggiorante di X se*

$$(\forall x \in X)(x \leq y).$$

Se X è dotato di maggioranti si dice maggiorato o limitato superiormente.

Definizione 30 *Sia $(A, \leq)$ un insieme ordinato, X un sottoinsieme di A, maggiorato, $\alpha \in A$. Si dice che α è estremo superiore di X se è il più piccolo dei maggioranti.*

In altre parole α è estremo superiore verifica le seguenti condizioni:

1. $(\forall x \in X)\ (x \leq \alpha)$

2. $\forall\ \beta \in A$ tale che $(\forall x \in X)\ (x \leq \beta)$ si ha $\alpha \leq \beta$.

Si vede che se esiste un estremo superiore di X, esso è unico, per cui è lecito scrivere $\alpha = sup(X)$. Inoltre, se $sup(X) \in X$, allora $sup(X) = max(X)$.

osservazione 31 Nel caso $X = \{x, y\}$, $\alpha = sup(x, y)$ vuol dire

1. $x \leq \alpha,\ y \leq \alpha$

2. $\forall\ \beta \in A$ tale che $x \leq \beta,\ y \leq \beta$ si ha $\alpha \leq \beta$.

Analogamente $\alpha = inf(x, y)$ si scrive

1. $\alpha \leq x,\ \alpha \leq y$

2. $\forall\ \beta \in A$ tale che $\beta \leq x,\ \beta \leq y$ si ha $\beta \leq \alpha$.

Definizione 32 *Sia* $(A, \leq)$ *un insieme ordinato. Si dice che* " $\leq$ " *è una relazione di ordine totale ovvero che* $(A, \leq)$ *è totalmente ordinato se e soltanto se*

$$(\forall x, y \in A)\ (x \leq y \vee y \leq x).$$

Nel caso contrario, cioè se $\exists x, y$ *tali che* $x \not\leq y \wedge y \not\leq x$*, si dice che* " $\leq$ " *è una relazione di ordine parziale oppure che* $(A, \leq)$ *è parzialmente ordinato.*

Esempi Sono totalmente ordinati $(\mathbb{N}, \leq)$, $(\mathbb{Z}, \leq)$; sono parzialmente ordinati $(\mathbb{N}^*, |)$, $(D_n, |)$, $(\mathcal{P}(X), \subseteq)$, $(A, \mathcal{R}_1)$.

Definizione 33 *Siano A, B insiemi non vuoti, $\mathcal{R}$ una relazione tra elementi di A ed elementi di B. Si dice che $\mathcal{R}$ è una relazione funzionale se e soltanto se*

$$\forall a \in A \ \exists | b \in B \text{ tale che } (a,b) \in \mathcal{R}$$

Se $\mathcal{R}$ è una relazione funzionale tra A e B, la terna ordinata $f = (A, B, \mathcal{R})$ si dice applicazione o funzione tra A e B. A si dice dominio o insieme di partenza di f, B si dice insieme di arrivo di f. La relazione $\mathcal{R}$ si chiama grafico di f.

Quando ci si riferirà ad applicazioni, si supporrà implicitamente che l'insieme di partenza e l'insieme di arrivo siano non vuoti.

Esempi: Siano $A = \{1, 2, 3, 4\}$, $B = \{a, b, c, d, e\}$ allora

$$\mathcal{R} = \{(1, a), (2, b), (2, c), (3, d), (4, e)\}$$

non è funzionale,

$$\mathcal{R}' = \{(1, a), (2, a), (3, b), (4, c)\}$$

è funzionale

$$\mathcal{R}'' = \{(1, a), (2, b)(4, c)\}$$

non è funzionale.

D'ora in avanti si userà la notazione

$$f : A \to B$$

per indicare un'applicazione dall'insieme A all'insieme B. Se, inoltre, $\mathcal{R}_f$ è la relazione funzionale tale che $f = (A, B, \mathcal{R}_f)$, si porrà $b = f(a)$ se e solamente se $(a, b) \in \mathcal{R}_f$. In questo caso si dice che b è l'immagine di a mediante f o il valore assunto da f in a. Pertanto il grafico dell'applicazione f è:

$$\mathcal{R}_f = \{(a, f(a)) \mid a \in A\}.$$

Quindi l'applicazione $f' = (A, B, \mathcal{R}')$ precedentemente introdotta si scriverà nel modo seguente:

$f' : A \to B$ tale che $f'(1) = a,\ f'(2) = a,\ f'(3) = b,\ f'(4) = c.$

Chiaramente due applicazioni $f : A \to B,\ g : C \to D$ sono uguali se e soltanto se $A = C,\ B = D$ e $\forall a \in A\ f(a) = g(a)$.

Si osservi che un'applicazione è una particolare relazione, mentre non è vero che una qualsiasi relazione è un'applicazione.

Esempi

1. Siano X e Y insiemi, $c \in Y$. Allora l'applicazione

   $$f_c : X \to Y \text{ tale che } \forall x \in X \ f_c(x) = c$$

   si dice applicazione costante di costante valore c

2. sia X un insieme. Allora l'applicazione

   $$\mathtt{id}_X : X \to X \text{ tale che } \forall x \in X \ \mathtt{id}_X(x) = x$$

   si dice applicazione identica di X

3. $f_1 : \mathbb{Z} \to \mathbb{Z}$ tale che $\forall n \in \mathbb{Z} \ f_1(n) = 2n$

4. $f_2 : \mathbb{Z} \to \mathbb{Z}$ tale che $\forall x \in \mathbb{Z}\ f_2(x) = \frac{x}{2}$ non è un'applicazione

5. $f_3 : \mathbf{P} \to \mathbb{Z}$ tale che $\forall x \in \mathbf{P}\ f_3(x) = \frac{x}{2}$

6. $f_4 : \mathbb{Q}^* \to \mathbb{Q}$ tale che $\forall x \in \mathbb{Q}\ f_4(x) = \frac{1}{x}$

7. $f_5 : \mathbb{Z} \to \mathbb{Z}$ tale che $\forall a \in \mathbb{Z}\ f_5(a) = a^2$.