Istituzioni di A & G — ALGEBRA, lezione 1

3 Marzo 2021

Assumeremo come note alcune nozioni di base già a viste in anni precedenti come le seguenti.

- La nozione di insieme, di elemento di un insieme, di appartenenza e non appartenenza di un elemento a un insieme.
- Le relazioni di inclusione e inclusione stretta fra insiemi.
- Le operazioni di intersezione, unione, differenza fra insiemi.
- Le nozioni di insieme vuoto, prodotto cartesiano di insiemi e di insieme delle parti di un insieme. $\emptyset$ $X \times Y$ $\mathcal{P}(X)$

In realtà tutte queste nozioni, relazioni e operazioni si possono inquadrare in un contesto assiomatico, cioè in un contesto in cui partendo da un numero finito di assiomi si possono dedurre tutta una serie di definizioni e proposizioni.

Il sistema di assiomi accettato è il cosiddetto *sistema di assiomi di Zermelo–Fränkel*, che utilizzeremo implicitamente durante il corso.

Definizione 1. *Siano X e Y insiemi. Una* ***corrispondenza*** *F di dominio X e codominio Y è un sottoinsieme di $X \times Y$. Se $(x, y) \in F$ si dice che x è in corrispondenza con y tramite F e si scrive spesso $x \; F \; y$.*

F corrispondenza è un sottoinsieme di $X \times Y$

$$X \times Y = \{(x, y) \mid x \in X, y \in Y\}$$

es: $\emptyset$, $X \times Y$ corrispondenze banali

es: X = studenti del Poli
Y = docenti del Poli
$F = \{(x, y) \mid x$ segue un corso insegnato da $y\}$

Definizione 2. *Siano X e Y insiemi. Una corrispondenza F di dominio X e codominio Y è detta* ***funzione*** *da X a Y se*

$$\forall\, x \in X, \quad \exists\,!\, y \in Y : \quad x\ F\ y.$$

Se F è una funzione, si scrive $F\colon X \to Y$ e $y = F(x)$ invece di $F \subseteq X \times Y$ e $x\ F\ y$.
L'insieme di tutte le funzioni da X a Y si indica con Y^X.

(non) es: F definita sopra non è una funzione

es: $F \subseteq \mathbb{R} \times \mathbb{R}$

$= \{(x,y) \mid x+2y=5\}$ è una funzione

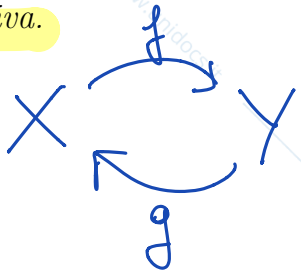
scelto $x \in \mathbb{R}$:

$x+2y=5 \Longrightarrow y = \frac{5-x}{2}$ è univoc. det.

Anche nel caso di funzioni diamo per scontate una serie di nozioni di base:

- immagine di una funzione e immagine inversa di un elemento del codominio
- nozione di funzione iniettiva, suriettiva, biiettiva
- composizione $\circ$ di funzioni.
- applicazione identità $id_X \colon X \to X$
- nozione di funzione inversa e la sua unicità
- l'equivalenza fra biiettività e invertibilità

Proposizione 3. *Siano X e Y insiemi e siano $f\colon X \to Y$, $g\colon Y \to X$. Se $g \circ f = id_X$ allora f è iniettiva e g è suriettiva.*



dim: • f è iniettiva: siano $x_1, x_2 \in X$ tali che

$$f(x_1) = f(x_2).$$

Allora $g(f(x_1)) = g(f(x_2))$, cioè $x_1 = x_2$ ✓

($g(f(x_1)) = x_1$, $g(f(x_2)) = x_2$)

• g è suriettiva: sia $x \in X$ qualsiasi, e sia $y = f(x)$ poiché

$$x = id_X(x) = g(f(x)) = g(y)$$

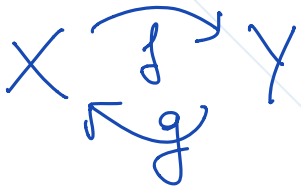
cioè $x = g(y) \in \mathrm{Im}(g)$. ✓

‡

Definizione 4. *Siano X e Y insiemi. Se $f\colon X \to Y$ una funzione $g\colon Y \to X$ si dice:*

- *inversa destra di f se $f \circ g = id_Y$;*
- *inversa sinistra di f se $g \circ f = id_X$.*

Quindi la proposizione sopra dice che se f ha inversa destra allora f è suriettiva, mentre se ha inversa sinistra è iniettiva.



Proposizione 5. *Siano X e Y insiemi e $f: X \to Y$ una funzione. f ha inversa sinistra se e solo se è iniettiva.*

$\iff$ $\quad \exists\, g: Y \to X$ t.c. $g \circ f = id_X$

dim: • ($\Rightarrow$) ✓

• ($\Leftarrow$) supponiamo f iniettiva e costruiamo una sua inversa sinistra:

Sia $y \in Y$, allora se $y \in Im(f)$,

$f^{-1}(y) = \{1 \text{ punto}\} = \{x_y\}$.

Definiamo: $g(y) = \begin{cases} \text{se } y \in Im(f): g(y) = x_y \\ \text{se } y \notin Im(f): g(y) = x_0, \ x_0 \text{ punto fissato di } X. \end{cases}$

Allora: ① g è una funzione $Y \to X$

② $\forall x \in X \quad g \circ f(x) = g(f(x)) = g(y) = x$ $\quad \#$

Dimostrare l'esistenza di inverse destre per una funzione suriettiva è più delicato. È facile vedere che per costruire un'inversa destra di $f : X \to Y$, dobbiamo, per ogni $y \in Y$ scegliere uno e un solo elemento $x_y \in f^{-1}(y)$ e definire g come $y \mapsto x_y$.

Se Y è un insieme finito è intuitivamente chiaro che un tale insieme di scelte si può fare, ma purtroppo se Y è infinito abbiamo bisogno di una precisa regola di scelta.

Definizione 6. *Sia $\mathfrak{X} = \{ X_i \}_{i \in I}$ una famiglia di insiemi non vuoti. Una* ***funzione di scelta*** *per $\mathfrak{X}$ è una funzione*

$$s \colon I \longrightarrow \bigcup_{i \in I} X_i$$

tale che $s(i) \in X_i$ per ogni $i \in I$.

Assioma della scelta *Sia $\mathfrak{X} = \{ X_i \}_{i \in I}$ una famiglia di insiemi non vuoti. Allora esiste una funzione di scelta per $\mathfrak{X}$.*

Se I è un insieme di indici finito, l'assioma della scelta è in realtà una proposizione dimostrabile all'interno del sistema di assiomi di Zermelo–Fränkel.

Esempi di funzione di scelta:

- $I = \{\text{rosso, giallo, blu}\}$
  X_i = insieme di biglie del colore i
  $\bigcup X_i$ = tutte le biglie
  $f: I \to \bigcup X_i$ funzione
  è di scelta se $f(\text{rosso})$ è una biglia rossa ... etc.

- $I = \mathbb{N}$
  $X_i = \{2^i, 3^i\}$

$\mathbb{N} = \{1, 2, \dots\}$
$\mathbb{N}_0 = \mathbb{N} \cup \{0\}$

$f: I \longrightarrow \bigcup X_i = \{2, 3, 4, 9, 8, 27 \dots\}$
$i \longmapsto f(i) \in \bigcup X_i$

f è di scelta se $f(i) \in X_i$, cioè:

$1 \longmapsto \begin{cases} 2 \\ 3 \end{cases}$

$2 \longmapsto \begin{cases} 4 \\ \end{cases}$

Proposizione 7. *Siano X e Y insiemi e $f\colon X \to Y$ una funzione. f ha inversa destra se e solo se è suriettiva.*

$\iff$

$\exists\, g: Y \to X$ t.c. $f \circ g = id_Y$

dim: • ($\Longrightarrow$) ✓

• ($\Longleftarrow$) Sia f suriettiva _ Sia $\mathcal{X} = \{f^{-1}(y)\}_{y \in Y}$

Poiché f è suriettiva $\Longrightarrow f^{-1}(y) \neq \emptyset \quad \forall y \in Y$

$\Longrightarrow \exists$ una funzione di scelta per $\mathcal{X}$, diciamo g -

$$g: Y \longrightarrow \bigcup_{y \in Y} f^{-1}(y) \subseteq X \rightsquigarrow g: Y \longrightarrow X$$

$\forall y \in Y$: $g(y) \in f^{-1}(y) \Longrightarrow f \circ g(y) = y$ ⁂

[Si può dimostrare che l'Assioma della scelta è equivalente ad affermare che ogni applicazione suriettiva ha inversa destra.]

oss: $\emptyset$ e la relazione identità: $\{(x,x) \mid x \in X\} \subseteq X \times X$ sono le uniche relazioni simm. e antisimm.

Definizione 8. *Sia X un insieme. Una* ***relazione*** *R in X è una corrispondenza da X in X. La relazione R si dice:*

- ***riflessiva*** *se $x \; R \; x$ per ogni $x \in X$;*
- ***transitiva*** *se $x \; R \; y$ e $y \; R \; z$ implica $x \; R \; z$ per ogni $x, y, z \in X$;*
- ***simmetrica*** *se $x \; R \; y$ implica $y \; R \; x$ per ogni $x, y \in X$;*
- ***antisimmetrica*** *se $x \; R \; y$ e $y \; R \; x$ implica $x = y$ per ogni $x, y \in X$.*

Definizione 9. *Sia X un insieme. Una relazione $\sim$ in X si dice* ***relazione d'equivalenza*** *se è riflessiva, transitiva e simmetrica. Se $x \in X$ l'insieme*

$$\overline{x} = \{ \, y \in X \mid y \sim x \, \} = [x] \text{ (altra notazione)}$$

è detto classe d'equivalenza di x.

Definizione 10. *Sia X un insieme. Una relazione $\prec$ si dice* ***relazione d'ordine*** *se è riflessiva, transitiva e antisimmetrica. Si dice* ***d'ordine totale*** *se è d'ordine e per ogni $x, y \in X$ o $x \prec y$ o $y \prec x$.*

Di solito, quando una relazione è d'ordine totale, si usa il simbolo $\leqslant$ invece di $\prec$.

Esempi

(1) $X = \mathbb{N}_0 = \mathbb{N} \cup \{0\}$ - fissato $n \in \mathbb{N} \subseteq X$ definiamo

$a \equiv_n b \iff a-b$ è multiplo di n,
cioè se $\exists\, c \in X$ t.c. $b-a = cn$

- riflessiva? $a \equiv_n a$ ✓
- transitiva?

$$\left.\begin{array}{l} a \equiv_n b \\ b \equiv_n c \end{array}\right\} \overset{?}{\Longrightarrow} a \equiv_n c$$

$c-a = (c-b)+(b-a)$ è multiplo di n ✓

- simmetrica? non se $X = \mathbb{N}_0$
se $X = \mathbb{Z}$ sì ✓

$\equiv_n$ è una relazione di equivalenza su $\mathbb{Z}$, detta congruenza.

(2) X insieme

$\subseteq$ è una relazione d'ordine su $\mathcal{P}(X)$

$Y_1 \subseteq Y_2$ se tutti gli elt. di Y_1 appartengono a Y_2

totale?

se $|X| \geq 2$ non è tot.

(3) $|$ la relazione di divisibilità

su $\mathbb{N}_0$ è di ordine:

$a, b \in \mathbb{N}_0$ $a|b$ se $\exists\, c \in \mathbb{N}$ t.c. $ac = b$