CAPITOLO 3

Strutture algebriche*

Questo capitolo non fa parte del programma del corso ed è inteso solo per lettori interessati. L'idea di questo capitolo è di dare informazioni di background che possano spiegare alcune scelte fatte nei capitoli seguenti.

1. Insiemi e funzioni

Cominciamo col dare una definizione formale di insieme.

DEFINIZIONE 3.1. Un *insieme* M è un raggruppamento di oggetti per cui esista un criterio oggettivo che permette di decidere univocamente se un qualunque oggetto ne faccia parte o meno.

ESEMPIO 3.2. I numeri reali $\mathbf{R}$ sono un insieme. I numeri primi

$$\{2, 3, 5, 7, 11, \dots\}$$

formano un insieme, 31 fa parte di questo insieme, 32 non ne fa parte. Anche $\{1, 2, 3\}$ è un insieme.

ESEMPIO 3.3. I nomi delle squadre della Serie A (Calcio) nella stagione 2017/18 sono un insieme. "AC Milan" fa parte di questo insieme, "Calcio Padova" non fa parte di questo insieme.

Abbiamo le seguenti notazioni per gli insiemi. Scriviamo $a \in A$, se a è un elemento di A e $a \notin A$ se non lo è. Scriviamo $A \subset B$ se per ogni $a \in A$ vale anche $a \in B$. (Facciamo presente che in questo caso qualche testo utilizza il simbolo $\subseteq$)

Per due insiemi scriviamo $A \cap B$ per *l'intersezione*, cioè

$$A \cap B = \{a \mid a \in A \text{ e } a \in B\}$$

Se abbiamo una collezione di insiemi A_i, dove $i \in I$. Allora

$$\cap_{i \in I} A_i = \{a \mid a \in A_i \text{ per ogni } i \in I\}$$

Per due insiemi scriviamo $A \cup B$ per *l'unione*, cioè

$$A \cup B = \{a \mid a \in A \text{ o } a \in B\}$$

Se abbiamo una collezione di insiemi A_i, dove $i \in I$. Allora

$$\cup_{i \in I} A_i = \{a \mid a \in A_i \text{ per un } i \in I\}$$

La *differenza* è definita come $A \setminus B = \{a \in A \mid a \notin B\}$.

Il *prodotto (cartesiano)* di A e B è l'insieme di coppie di elementi di A e B.

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

ESEMPIO 3.4.

$$\mathbf{R} \times \mathbf{R} = \{(x, y) \mid x, y \in \mathbf{R}\} = \mathbf{R}^2$$

DEFINIZIONE 3.5. Siano A e B due insiemi. Allora una *funzione* $f : A \to B$ è una procedura che ad ogni elemento di A associa un elemento di B.

ESEMPIO 3.6. La mappa $f : \mathbf{R} \to \mathbf{R}$ definita da $f(x) = x^2$ è una funzione, che manda ogni numero al suo quadrato.

Sia X l'insieme di tutto gli studenti iscritti al corso di Geometria. Allora $f : X \to \mathbf{N}$ che associa ad ogni studente il suo numero di matricola è una funzione.

DEFINIZIONE 3.7. Sia A un insieme. Allora $\mathrm{id}_A : A \to A$ è la *funzione identità*, che manda a ad a. Quindi $\mathrm{id}_A(a) = a$.

DEFINIZIONE 3.8. Sia $f : A \to B$ una funzione. *L'immagine* di f consiste di tutti gli elementi $b \in B$ tali che esiste un $a \in A$ con $b = f(a)$.

Sia $C \subset B$. Allora la *controimmagine* $f^{-1}(C)$ di C è

$$f^{-1}(C) = \{a \in A \mid f(a) \in C\}.$$

ESEMPIO 3.9. L'immagine di $f : \mathbf{R} \to \mathbf{R}$ con $f(x) = x^2$ è $\{x \in \mathbf{R} \mid x \geq 0\}$. Abbiamo che $f^{-1}([1, 4]) = [-2, -1] \cup [1, 2]$.

Sia $g : \mathbf{R} \to \mathbf{R}$ tale che $g(x) = \sin(x)$ allora l'immagine di g è l'intervallo $[-1, 1]$.

DEFINIZIONE 3.10. Sia $f : A \to B$ una funzione e $A' \subset B$ un sottoinsieme. Allora la restrizione di f ad A' è $f|_{A'} : A' \to B$, cioè la mappa f considerata come una funzione da A' a B.

Sia $g : B \to C$ un'altra funzione. Allora la composizione $g \circ f : A \to C$ è la mappa definita da

$$(g \circ f)(a) = g(f(a))$$

DEFINIZIONE 3.11. Un funzione $f : A \to B$ è *iniettiva* se per ogni $a, a' \in A$ con $a \neq a'$ abbiamo $f(a) \neq f(a')$.

Una funzione $f : A \to B$ è *suriettiva* se per ogni $b \in B$ esiste un elemento $a \in A$ tale che $f(a) = b$.

Una funzione $f : A \to B$ è *biettiva* se è sia iniettiva che suriettiva.

OSSERVAZIONE 3.12. Una funzione è iniettiva se e solo se per ogni $b \in B$ l'insieme $f^{-1}(b)$ è vuoto o ha un unico elemento.

Una funzione è suriettiva se e solo se per ogni $b \in B$ l'insieme $f^{-1}(b)$ ha almeno un elemento.

Una funzione è biiettiva se e solo se per ogni $b \in B$ l'insieme $f^{-1}(b)$ ha precisamente un elemento.

Se f è biettiva alllora possiamo definire $f^{-1} : B \to A$ con $f^{-1}(b) = a$ dove a è l'unico elemento della controimmagine $f^{-1}(\{b\})$.

In questo caso abbiamo che $f \circ f^{-1} = \mathrm{id}_B$ e $f^{-1} \circ f = \mathrm{id}_A$.

2. Leggi di composizione

In questa sezione ci occuperemo di funzioni $M \times M \to M$.

Sia $\mathbf{Z}$ l'insieme degli interi. Un esempio di una funzione di questo tipo è la somma di due interi, che definisce una mappa $\mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}$

DEFINIZIONE 3.13. Un *semigruppo* è un insieme H dotato di un'operazione $\cdot : H \times H \to H$, scritto $a \cdot b$, tale che per ogni $a, b, c \in H$ abbiamo $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (associatività).

Un semigruppo è un *monoide* se esiste un elemento $e \in H$, chiamato elemento neutro, tale che per ogni $h \in H$ si abbia $e \cdot h = h \cdot e = h$.

Un monoide è un *gruppo* se per ogni $g \in H$ esiste un elemento $h \in H$ tale che $g \cdot h = h \cdot g = e$. Chiamiamo l'elemento h l'inverso di g.

ESEMPIO 3.14. L'insieme delle matrici $M_{n\times n}(\mathbf{R})$ con la moltiplicazione di matrici è un monoide: dalle regole di calcolo per le matrici segue che

$$(AB)C = A(BC).$$

Inoltre abbiamo che I_n è l'elemento neutro:

$$AI_n = I_n A = A$$

Se prendiamo $GL_n(\mathbf{R})$, l'insieme di tutte le matrici invertibili, allora $GL_n(\mathbf{R})$ è un esempio di gruppo.

Anche gli interi (con l'operazione di addizione) sono un gruppo. Invece gli interi con la moltiplicazione sono soltanto un monoide. Anche i numeri naturali con l'addizione sono un monoide.

ESEMPIO 3.15. Studiamo adesso $\mathrm{Hom}(\mathbf{R}, \mathbf{R})$, l'insieme di tutte le funzione $f : \mathbf{R} \to \mathbf{R}$. Allora la composizione di due funzioni (Per $f, g : V \to V$ definiamo $g \circ f : V \to V$ come $(g \circ f)(x) = g(f(x))$) è una legge di composizione associativa: $(h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x))) = (h \circ (g \circ f))(x)$. La funzione $\mathrm{id}_{\mathbf{R}}$ è l'elemento neutro $(\mathrm{id} \circ f)(x) = \mathrm{id}(f(x)) = f(x) = f(\mathrm{id}(x)) = (f \circ \mathrm{id})(x)$.

Quindi $\mathrm{Hom}(\mathbf{R}, \mathbf{R})$ è un monoide. Se $f \in \mathrm{Hom}(\mathbf{R}, \mathbf{R})$ ed esiste una funzione $g : \mathbf{R} \to \mathbf{R}$ tale che $g \circ f = f \circ g = \mathrm{id}$, allora per ogni $x \in R$ troviamo che $x = f(g(x))$, quindi $\mathrm{im}(f) = \mathbf{R}$, ed f è suriettiva. Se $x \neq y$ allora $g(f(x)) = x \neq y = g(f(y))$, quindi $f(x) \neq f(y)$ e f è iniettiva.

Quindi solo le funzioni biiettive possono ammettere una funzione inversa. Le funzione biiettive $\mathrm{Iso}(\mathbf{R}, \mathbf{R})$ sono un sottoinsieme di $\mathrm{Hom}(\mathbf{R}, \mathbf{R})$. La composizione di due funzioni biiettive è di nuovo biiettiva, e la funzione id_R è anche biiettiva. Anche la funzione inversa di una funzione biiettive è biettiva, quindi $\mathrm{Iso}(\mathbf{R}, \mathbf{R})$ è un gruppo.

LEMMA 3.16. *Se H è un monoide allora esiste un unico elemento neutro. Se G è un gruppo allora per ogni $g \in G$ esiste un unico elemento inverso.*

DIMOSTRAZIONE. Le dimostrazioni sono uguali al risultato equivalente descritto per le matrici.

Se $e, e' \in H$ sono elementi neutri, allora abbiamo $e \cdot e' = e'$, perché e è un elemento neutro, e abbiamo $e \cdot e' = e$ perché e' è un elemento neutro. Quindi $e = e'$.

Se h_1 e h_2 sono inversi di g allora troviamo

$$h_1 = h_1 \cdot e = h_1 \cdot g \cdot h_2 = e \cdot h_2 = h_2.$$

□

3. Gruppi abeliani

DEFINIZIONE 3.17. Un gruppo G è *abeliano* se per ogni $g, h \in G$ abbiamo che $g \circ h = h \circ g$.

Similmente si possono definire semigruppi abeliani e monoidi abeliani.

ESEMPIO 3.18. $(\mathbf{Z}, +)$ e $(M_{n \times m}(\mathbf{R}), +)$ sono gruppi abeliani: per ogni $n, m \in \mathbf{Z}$ abbiamo $n + m = m + n$ e per due matrici $m \times n$ abbiamo $A + B = B + A$.

ESEMPIO 3.19. $(\mathrm{GL}_n(\mathbf{R}), \cdot)$ non è abelino, possiamo costruire facilmente due matrici tali che $AB \neq BA$. Anche $\mathrm{Iso}(V, V)$ non è abeliano: Se f è definita da $f(x) = x + 1$ e g è definita da $g(y) = y^3$. Allora $g(f(x)) = g(x + 1) = (x + 1)^3 = x^3 + 3x^2 + 3x + 1$ e $f(g(x)) = f(x^3) = x^3 + 1$. Quindi per ogni x tale che $3x(x+1) \neq 0$ abbiamo che $g(f(x)) \neq f(g(x))$.

4. Anelli e campi

Un *anello* è un insieme R con due operazione $+ : R \times R \to R$ e $\cdot : R \times R \to R$ tali che

(1) $(R, +)$ è un gruppo abeliano

(2) $(R, \cdot)$ è un monoide.
(3) per ogni $a, b, c \in R$ abbiamo $(a+b)c = ac + bc$, $a(b+c) = ac + bc$.

Un tipico esempio di un annello sono gli interi $\mathbf{Z}$ con la solita somma e solita moltiplicazione. Anche $M_{n\times n}(\mathbf{R})$ è un anello con la somma di matrici e il prodotto di matrici.

I numeri naturali con solite somme e moltiplicazione non sono un anello, perchè $(\mathbf{N}, +)$ è un monoide abeliano, ma non è un gruppo.

Quindi gli anelli sono oggetti che conosciamo già (interi, matrici) ecc. Non vogliamo approfondire il loro studio, ma c'è una classe di anelli un po' speciale, che useremo più avanti.

DEFINIZIONE 3.20. Un *campo* $(K, +, \cdot)$ è un anello tale che

(1) $(K, \cdot)$ è un gruppo abeliano.
(2) Sia $0 \in K$ l'elemento neutro per $+$ e sia $1 \in K$ l'elemento neutro per $\cdot$, allora $0 \neq 1$ e per ogni $a \in K \setminus \{0\}$ esiste un elemento a^{-1} tale che $a^{-1} = a^{-1}a = 1$.

Nel prossimo capitolo daremo un'altra definizione di campo, che è più lunga. In quella definizione renderemo esplicito che cosa significa essere un anello con moltiplicazione abeliana.

ESEMPIO 3.21. Le frazione $\mathbf{Q}$ con le solite addizione e moltiplicazione sono un campo. È chiaro che $+$ e $\cdot$ sono associative e commutative. Inoltre 0 è l'elemento neutro per la somma, 1 è l'elemento neutro per la moltiplicazione. Se $\frac{a}{b} \in \mathbf{Q}$ (quindi $b \neq 0$), allora $\frac{a}{b} + \frac{-a}{b} = \frac{-a}{b} + \frac{a}{b} = 0$ e se $a \neq 0$ allora

$$\frac{a}{b} \cdot \frac{b}{a} = 1 = \frac{b}{a} \cdot \frac{a}{b}$$

e $(\frac{a}{b})^{-1} = \frac{b}{a}$.

Anche i numeri reali $\mathbf{R}$ e i numeri complessi $\mathbf{C} = \{a + bi \mid a, b \in \mathbf{R}\}$ (con $i \circ i = -1$) sono campi.

5. Spazi vettoriali

A questo punto vogliamo indicare un paio di riformulazioni di definizione e risultati che si trovano nei seguenti capitoli.

Nel prossimo capitolo introdurremo gli spazi vettoriali. Questi spazi consistono di una scelta di un campo K, un insieme V e due operazioni $+ : V \times V \to V$ e $\cdot : K \times V \to V$. La definizione consiste di 8 condizioni, le prime quattro significano soltanto che $(V, +)$ è un gruppo abeliano. La mappa $\cdot$ non si puo studiare con la teoria di questo capitolo, perchè $\cdot$ non è una legge di composizione.

Anche l'insieme delle funzioni lineari non entra bene nella teoria finora discussa. Invece se V è un spazio vettoriale, allora l'insieme $\mathrm{Hom}(V, V) = \mathrm{End}(V)$ di tutte le mappe lineare $f : V \to V$ (endomorfismi) è un anello. La somma è la somma di due funzioni $((f + g)(v) := f(v) + g(v))$ e il prodotto è definito come la composizione di due endomorfismi.

Quando si scelglie una base B di V allora si può identificare $\mathrm{End}(V)$ con lo spazio delle matrici $M_{n\times n}(K)$, e si controlla facilmente che questa identificazione induce anche la somma e il prodotto di $\mathrm{End}(V)$ tramite quelli di $M_{n\times n}(K)$.