Lezione 2.
Relazioni d'Equivalenza e d'Ordine

Definizione 2.5. 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 2.6. Sia X un insieme. Una relazione $\sim$ in X si dice d'equivalenza se è riflessiva, transitiva e simmetrica. Se $x \in X$ l'insieme

$$\overline{x} = \{ \ y \in X \mid y \sim x \ \}$$

è detta classe d'equivalenza di x.

Definizione 2.7. Sia X un insieme. Una relazione $\prec$ si dice 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 $\leq$ invece di $\prec$.

Esempio 2.7. L'uguaglianza in un insieme X è sia una relazione d'equivalenza, che d'ordine totale. La relazione $\leq$ in $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ è una relazione d'ordine totale: invece la relazione $<$ non è una relazione d'ordine.

Si noti che anche in $\mathbb{C}$ si possono introdurre relazioni d'ordine totale: per esempio possiamo definire $x \leq y$ se o $|x| < |y|$, oppure $|x| = |y|$ ma $\arg(x) < \arg(y)$, ove $\arg(z)$ indica l'argomento principale di z in $[0, 2\pi[$.

Quando si dice che $\mathbb{C}$ non è ordinabile si intende che non è possibile dare un ordinamento su x che sia compatibile con la struttura algebrica cioè in modo tale che:

- se $x \leq y$ allora $x + z \leq y + z$ per ogni $x, y, z \in \mathbb{C}$;

- se $x \leq y$ allora $xz \leq yz$ per ogni $x, y, z \in \mathbb{C}$, $z \geq 0$.

Una dei vari enunciati equivalenti all'Assioma della scelta afferma che ogni insieme X è *bene ordinabile*, ovvero che è possibile definire su X un ordinamento totale in modo che ogni suo sottoinsieme non vuoto abbia un primo elemento.

Esempio 2.8. Se X è un insieme, la relazione $\subseteq$ in $\mathscr{P}(X)$ è una relazione d'ordine. Se X ha almeno due elementi la relazione non è d'ordine totale.

Esempio 2.9. Sia X o $\mathbb{N}_0 = \mathbb{N} \cup \{ 0 \}$ o $\mathbb{Z}$. In X diciamo che a è multiplo di b se esiste $c \in X$ tale che $a = bc$. Fissiamo $n \in \mathbb{N} \subseteq X$ e definiamo la relazione $\equiv_n$ come segue: $a \equiv_n b$ se e solo se $a - b$ è multiplo di n.

Si osservi che tale relazione è riflessiva e transitiva sia su $\mathbb{N}_0$ che su $\mathbb{Z}$. Invece è simmetrica solo in $\mathbb{Z}$. Quindi abbiamo una relazione di equivalenza in $\mathbb{Z}$ ma non in $\mathbb{N}_0$.

Esempio 2.10. Sia $\mathfrak{X} = \{ X_i \}_{i \in I}$ una famiglia di insiemi. Diciamo che X_i è equipotente (o equicardinale) a X_j se esiste $f \colon X_i \to X_j$ biiettiva: in tal caso si scrive $X_i \approx X_j$. La relazione di equipotenza è una relazione di equivalenza.

Fissiamo, per il momento, la nostra attenzione alle relazioni d'equivalenza.

Definizione 2.8. Sia X un insieme. Una partizione di X è una famiglia $\{ X_i \}_{i \in I} \subseteq \mathscr{P}(X)$ di insiemi non vuoti tali che:

- se $X_I \cap X_j \neq \emptyset$ allora $X_i = X_j$;
- $\bigcup_{i \in I} X_i = X$.

Proposizione 2.4. *Sia X un insieme. Se $\sim$ è una relazione d'equivalenza in X allora*

$$\{ \overline{x} \}_{x \in X}$$

è una partizione di X.

Dimostrazione. Chiaramente $x \in \overline{x}$, dunque

$$\bigcup_{x \in X} \overline{x} = X.$$

Se poi $z \in \overline{x} \cap \overline{y}$, allora $x \sim z$ e $z \sim y$, quindi per transitività $x \sim y$. In particolare $x \in \overline{x}$ sicché $\overline{x} \subseteq \overline{y}$. Analogamente si verifica che $\overline{y} \subseteq \overline{x}$, dunque deve valere l'uguaglianza. □

Se X è un insieme e $\sim$ è una relazione d'equivalenza in X allora si definisce il *quoziente di X rispetto a $\sim$* come

$$X/\sim = \{ \overline{x} \}_{x \in X}.$$

Esempio 2.11. Consideriamo la relazione definita in $\mathbb{Z}$ nell'esempio 2.9. Si scrive $\mathbb{Z}_n = \mathbb{Z}/\equiv_n$.

Preso $n = 4$ determiniamo le classi d'equivalenza rispetto a $\equiv_4$. Chiaramente

$$\overline{0} = \{\ 0, \pm 4, \pm 8, \dots\ \} = 4\mathbb{Z}.$$

Si noti che $1, 2, 3 \notin \overline{0}$. Risulta

$$\begin{aligned}\overline{1} &= \{\ 1, 1 \pm 4, 1 \pm 8, \dots\ \} = \{\ 1, -3, 5, -7, 9, \dots\ \},\\ \overline{2} &= \{\ 2, 2 \pm 4, 2 \pm 8, \dots\ \} = \{\ 2, -2, 6, -6, 10, \dots\ \},\\ \overline{3} &= \{\ 3, 3 \pm 4, 3 \pm 8, \dots\ \} = \{\ 3, -1, 7, -5, 11, \dots\ \}.\end{aligned}$$

È facile verificare che $\mathbb{Z}_4 = \{\ \overline{0}, \overline{1}, \overline{2}, \overline{3}\ \}$. Infatti se $x \in \mathbb{Z}$, l'algoritmo della divisione euclidea implica che esistono unici $q \in \mathbb{Z}$ e $r \in \mathbb{Z}$ con $0 \le r \le 3$ tali che $x = 4q + r$, sicché

$$x \equiv_4 r \in \{\ 0, 1, 2, 3\ \}.$$

Passiamo ora a fare qualche osservazione sulle relazioni d'ordine.

Definizione 2.9. Sia X un insieme e sia $\prec$ un ordinamento su X.

- Se $Y \subseteq X$, diciamo che $x \in X$ è un maggiorante si Y se $y \prec x$ per ogni $y \in Y$.
- Diciamo che $m \in X$ è massimale se per ogni $x \in X$ tale che $m \prec x$ risulta $x = m$.
- X is dice induttivo se ogni $Y \subseteq X$ totalmente ordinato ha almeno un maggiorante in X.

Esempio 2.12. Chiaramente ogni insieme con un numero finito di elementi ha elementi massimali ed è parzialmente ordinato e induttivo, qualsiasi ordinamento sia definito in esso.

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ con l'ordinamento usuale non sono induttivi.

Sia X un insieme e si consideri $\mathscr{P}(X)$ ordinato per inclusione. Allora X è maggiorante di ogni sottoinsieme di $\mathscr{P}(X)$. Inoltre X è l'unico elemento massimale in $\mathscr{P}(X)$. Si noti infine che $\mathscr{P}(X)$ è banalmente induttivo.

Osservazione 2.2. *Si noti che un elemento massimale può non essere maggiorante.*

Per esempio si consideri l'insieme $I = \{\ 1, 2, 3, 4\ \}$ *e sia* $X = \mathscr{P}(I) \setminus \{\ I\ \}$ *ordinato per inclusione. Allora* $\{\ 1, 2, 3\ \}$ *è massimale, ma non è maggiorante di* X*: infatti* $\{\ 4\ \}$ *e* $\{\ 1, 2, 3\ \}$ *non sono confrontabili.*

Inoltre di elementi massimali ne possono esistere più di uno: nel caso sopra, oltre a $\{\ 1, 2, 3\ \}$*, anche* $\{\ 1, 2, 4\ \}$, $\{\ 1, 3, 4\ \}$, $\{\ 2, 3, 4\ \}$ *sono elementi massimali.*

Si può dimostrare che l'Assioma della scelta è equivalente al seguente enunciato, noto come *Lemma di Zorn*.

Lemma 2.1 (Lemma di Zorn)**.** *Sia* X *un insieme parzialmente ordinato induttivo. Allora* X *ha elementi massimali.*

Utilizzeremo il Lemma di Zorn più volte durante il corso. Come prima applicazione diamo una dimostrazione generale dell'esistenza di insiemi liberi di generatori per ogni spazio vettoriale non nullo. Prima di enunciare il risultato richiamiamo alcune nozioni viste nel corso di Algebra Lineare del primo anno.

Sia V uno spazio vettoriale su un campo k. Sia $X = \{ v_i \}_{i \in I}$ un insieme, non necessariamente finito, di vettori di V. Ricordiamo che l'insieme X si dice:

- un *insieme di generatori di* V se per ogni $v \in V$ esistono indici $i_1, \ldots, i_n \in I$ e scalari $\alpha_1, \ldots, \alpha_n \in k$ tali che
$$v = \sum_{j=1}^{n} \alpha_j v_{i_j};$$
- un *insieme libero di vettori di* V se per ogni scelta di indici $i_1, \ldots, i_n \in I$ i vettori $v_{1 i_1}, \ldots, v_{i_n}$ sono linearmente indipendenti, cioè l'uguaglianza
$$\sum_{j=1}^{n} \alpha_j v_{i_j} = 0,$$
con $\alpha_1, \ldots, \alpha_n \in k$, implica $\alpha_1 = \cdots = \alpha_n = 0$.

È noto che ogni spazio vettoriale non nullo e finitamente generato V ammette insiemi liberi di generatori: fissato un ordine degli elementi possiamo allora dire che ogni spazio vettoriale non nullo e finitamente generato V ammette basi. La dimostrazione di questo fatto vista durante il corso di Algebra Lineare del primo anno dipende pesantemente dall'ipotesi che lo spazio vettoriale sa finitamente generato. Ammettendo la validità dell'Assioma della scelta (e, quindi, del Lemma di Zorn) tale risultato si può estendere anche a spazi vettoriali non finitamente generati.

Proposizione 2.5. *Sia V uno spazio vettoriale non nullo sul campo k. Allora esistono in V insiemi liberi di generatori.*

Dimostrazione. Sia $S \subseteq \mathscr{P}(V)$ la famiglia di tutti i sottoinsiemi liberi di V. Poiché V non è nullo, allora $S \neq \emptyset$. Consideriamo in S l'ordinamento per inclusione (che non è totale) e consideriamo un sottoinsieme $\mathfrak{L} = \{ L_i \}_{i \in I}$ totalmente ordinato: sia
$$L = \bigcup_{i \in I} L_i \in \mathscr{P}(V).$$

Fissiamo dei vettori $v_1, \ldots, v_n \in L$: allora la definizione di L ci permette d'affermare che esistono indici $i_1, \ldots, i_n \in I$ tali che $v_{i_j} \in L_{i_j}$. Poiché abbiamo un numero finito di elementi di $\mathfrak{L}$ che, per ipotesi, è totalmente ordinato per inclusione, sappiamo che esiste un indice $\widehat{\imath} \in \{ i_1, \ldots, i_n \}$ tale che $L_{i_j} \subseteq L_{\widehat{\imath}}$ per ogni $j = 1, \ldots, n$: in particolare $v_1, \ldots, v_n \in L_{\widehat{\imath}} \in \mathfrak{L}$.

Poiché gli elementi di $\mathfrak{L}$ sono insiemi liberi, allora $v_1, \ldots, v_n$ sono linearmente indipendenti, cioè ogni sottoinsieme finito di L è costituito da vettori linearmente indipendenti, cioè L è libero, da cui segue che $L \in S$ è un maggiorante di $\mathfrak{L}$.

Per il Lemma di Zorn allora S contiene un elemento massimale M: M è un insieme libero. Se $v \in V$ allora o $v \in M$ oppure $v \notin M$, dunque $M \cup \{ v \}$ non è più libero. In particolare esistono $v_1, \dots, v_n \in M$ e scalari $\alpha_1, \dots, \alpha_n, \alpha \in k$ non tutti nulli tali che

$$\alpha v + \sum_{i=1}^{n} \alpha_i v_i = 0.$$

Se fosse $\alpha = 0$ si dovrebbe avere anche $\alpha_1 = \cdots = \alpha_n = 0$ poiché M è libero e, dunque, $v_1, \dots, v_n$ sono linearmente indipendenti. Allora $\alpha \neq 0$, dunque con semplici passaggi algebrici otteniamo

$$v = \sum_{i=1}^{n} \left(-\frac{\alpha_i}{\alpha} \right) v_i.$$

In particolare M è anche un insieme di generatori di V. $\square$