3. Relazioni su un insieme

Per introdurre il concetto di *relazione su un insieme*, conviene partire dal concetto di *grafico* associato alla relazione.

Definizione 1. *Sia A un insieme non vuoto. Ogni sottoinsieme $\mathfrak{R}$ di $A\times A$ è detto grafico di una relazione ρ su A [associata a $\mathfrak{R}$]. Tale relazione ρ è così definita: presa comunque una coppia $(a_1, a_2) \in A\times A$, si dice che a_1 e a_2 sono in relazione ρ [e si scrive $a_1\,\rho\, a_2$] se $(a_1, a_2) \in \mathfrak{R}$. Si dice invece che a_1 e a_2 non sono in relazione ρ [e si scrive $a_1 \not\rho\, a_2$] se $(a_1, a_2) \notin \mathfrak{R}$.*

Le relazioni su un insieme A sono quindi quante i sottoinsiemi di $A\times A$. Ogni insieme non vuoto A possiede in particolare le seguenti tre relazioni:

- la *relazione di uguaglianza* (o *relazione identica*) *su* A: $a\,\rho\, b \iff a = b,\ \forall\, a,\, b \in A$ [il grafico è l'insieme $\{(a, a),\ \forall\, a \in A\}$, detto *diagonale di* A].
- la *relazione caotica*: $a\,\rho\, b \iff a,\, b \in A$ [il grafico è l'insieme $A\times A$].
- la *relazione vuota*: $a \not\rho\, b,\ \forall\, a,\, b \in A$ [il grafico è l'insieme vuoto].

Se $A = \{a_1,\, a_2,\, \dots ,\, a_n\}$ è un insieme finito, ogni relazione ρ su A può essere rappresentata in "forma cartesiana" (o "matriciale"), ponendo

$$a_i \times a_j = \begin{cases} 0, & \text{se } a_i \not\rho\, a_j \\ 1, & \text{se } a_i\,\rho\, a_j\,. \end{cases}$$

Ad esempio, se $A = \{a, b, c, d\}$ ed il grafico di ρ è $\{(a, a), (b, b), (c, c), (a, d), (c, d)\}$, allora ρ è rappresentata con la seguente tavola di valori 0, 1:

ρ	a	b	c	d
a	1	0	0	1
b	0	1	0	0
c	0	0	1	1
d	0	0	0	0

Definizione 2. *Una relazione ρ su A è detta:*

- *riflessiva, se $a\,\rho\, a,\ \forall\, a \in A$;*
- *simmetrica, se $a\,\rho\, b \implies b\,\rho\, a,\ \forall\, a,\, b \in A$;*
- *transitiva, se $a\,\rho\, b$ e $b\,\rho\, c \implies a\,\rho\, c,\ \forall\, a,\, b,\, c \in A$;*
- *antisimmetrica, se $a\,\rho\, b$ e $b\,\rho\, a \implies a = b,\ \forall\, a,\, b \in A$*
- *totale,* se risulta *$a\,\rho\, b$ oppure $b\,\rho\, a,\ \forall\, a,\, b \in A$.*

Una relazione riflessiva, simmetrica e transitiva è detta relazione di equivalenza. Una relazione riflessiva e transitiva è detta relazione di pre-ordine. Una relazione riflessiva, antisimmetrica e transitiva è detta relazione di ordine. Infine una relazione di ordine che è anche totale è detta relazione di ordine totale.

Esempi 1. (*i*) La relazione di uguaglianza è riflessiva, simmetrica, transitiva, antisimmetrica, ma non totale (se $|A| \geq 2$). Dunque è una relazione di equivalenza e di ordine (non totale).

(*ii*) La relazione caotica è riflessiva, simmetrica, transitiva, totale, ma non antisimmetrica. La relazione vuota è simmetrica, antisimmetrica, transitiva [in modo banale], ma non è riflessiva né totale.

(*iii*) La relazione ρ definita sopra non ha alcuna di queste proprietà.

(*iv*) Negli insiemi numerici $\boldsymbol{N}, \boldsymbol{Z}, \boldsymbol{Q}, \boldsymbol{R}$ è definita la *relazione di disuguaglianza* $\leq$, in questo modo:

in $\boldsymbol{N}$ e $\boldsymbol{Z}$: $a \leq b \overset{def}{\iff} b = a + t, \exists\, t \in \boldsymbol{N}$; in $\boldsymbol{Q}$ ed $\boldsymbol{R}$: $a \leq b \overset{def}{\iff} b = a + t, \exists\, t \geq 0$.

Si tratta di una relazione di ordine totale.

Esaminiamo ora tre relazioni che ci interesseranno particolarmente nel seguito: la *relazione di divisibilità in* $\boldsymbol{N}$ (o in $\boldsymbol{Z}$), la *relazione di congruenza modulo un intero* e la *relazione di equipotenza tra insiemi.*

Definizione 3. *In* $\boldsymbol{N}$ *introduciamo la seguente relazione di divisibilità. Presi comunque* $a, b \in \boldsymbol{N}$*:*

$$a \mid b \overset{def}{\iff} b = at,\ \exists\, t \in \boldsymbol{N},$$

[$a \mid b$ *si legge:* a *divide* b*, oppure* a *è un divisore di* b*, oppure anche* b *è un multiplo di* a*. Se* a *non divide* b *si scrive* $a \nmid b$*].*

Proposizione 1. *La relazione di divisibilità in* $\boldsymbol{N}$ *è una relazione di ordine (non totale).*

Dim. Presi comunque $a, b, c \in \boldsymbol{N}$ sono verificate le proprietà:

riflessiva: $a \mid a$ [infatti $a = a \cdot 1$];

transitiva: $a \mid b,\ b \mid c \implies a \mid c$ [infatti $b = at,\ c = bs \implies c = ats$];

antisimmetrica: $a \mid b,\ b \mid a \implies a = b$ [infatti $b = at,\ a = bs \implies b = bst \implies st = 1 \implies s = 1 \implies b = a$].

La relazione di divisibilità su $\boldsymbol{N}$ è quindi una relazione d'ordine. Ma non è totale: ad esempio $2 \nmid 3$ e $3 \nmid 2$. Non è neppure simmetrica: infatti $a \mid b \not\Longrightarrow b \mid a$ [ad esempio $2 \mid 4$ ma $4 \nmid 2$].

N.B. La relazione di divisibilità può essere introdotta anche in $\boldsymbol{Z}$ [con definizione analoga: $a \mid b \iff b = at,\ \exists\, t \in \boldsymbol{Z}$]. In tal caso è solo una relazione di pre-ordine, in quanto non è verificata l'antisimmetria [ad esempio $2 \mid -2,\ -2 \mid 2$ ma $2 \neq -2$].

Definizione 4. *Sia* n *un intero* ≥ 2*. Si chiama relazione di congruenza modulo* n *la seguente relazione su* $\boldsymbol{Z}$*. Presi comunque* $a, b \in \boldsymbol{Z}$*:*

$$a \equiv b\ (mod\, n) \overset{def}{\iff} n \mid b - a$$

[cioè $b - a = nt,\ \exists\, t \in \boldsymbol{Z}$*]. Si dice in tal caso che* a *è conguente (o congruo)* a b *modulo* n*. In luogo di* $a \equiv b\ (mod\, n)$ *si può anche scrivere* $a \equiv b\ (n)$ *oppure* $a \equiv_n b$*.*

Proposizione 2. *La relazione* $\equiv_n$ *è una relazione di equivalenza su* $\boldsymbol{Z}$*.*

Dim. Presi comunque $a, b, c \in \boldsymbol{Z}$, sono verificate le proprietà

riflessiva: $a \equiv a\ (mod\, n)$ [infatti $a - a = n \cdot 0$];

simmetrica: $a \equiv b\ (mod\, n) \implies b \equiv a\ (mod\, n)$ [infatti $b - a = nt \implies a - b = n(-t)$];

transitiva: $a \equiv b\ (mod\, n),\ b \equiv c\ (mod\, n) \implies a \equiv c\ (mod\, n)$ [infatti, se $b - a = nr,\ c - b = ns$ (con $r, s \in \boldsymbol{Z}$), allora $c - a = (c - b) + (b - a) = n(s + r)$ e quindi $n \mid c - a$].

Definizione 5. *Due insiemi* X, Y *sono detti equipotenti (e si scrive* $X \sim Y$*) se esiste un'applicazione biiettiva* $f : X \to Y$*. La relazione* $\sim$ *è detta relazione di equipotenza (nella famiglia di tutti gli insiemi).*

Proposizione 3. *La relazione di equipotenza tra insiemi è una relazione di equivalenza.*

Dim. Presi comunque tre insiemi X, Y, Z, sono verificate le proprietà

riflessiva: $X \sim X$ [tramite la biiezione identica $\mathbf{1}_X$];

simmetrica: $X \sim Y \implies Y \sim X$ [se $f : X \to Y$ è biiettiva, anche $f^{-1} : Y \to X$ lo è];

transitiva: $X \sim Y,\ Y \sim Z \implies X \sim Z$ [se $f : X \to Y,\ g : Y \to Z$ sono biiettive, anche $g \circ f : X \to Z$ lo è].

Ci occuperemo ora esclusivamente delle *relazioni di equivalenza*, cioè delle relazioni riflessive, simmetriche e transitive.

Definizione 6. *Sia ρ una relazione di equivalenza su A. Per ogni $a \in A$, il sottoinsieme di A*

$$[a] = [a]_\rho := \{x \in A \ : \ a \,\rho\, x\}$$

è detto classe di equivalenza di a modulo ρ. Poiché ρ è simmetrica, $[a] = \{x \in A \ : \ x \,\rho\, a\}$.

Proposizione 4. *Sia ρ una relazione di equivalenza su A. Si ha:*

(i) $a \in [a],\ \ \forall\, a \in A$.

(ii) $[a] = [b] \iff a \,\rho\, b$.

(iii) $[a] \cap [b] = \emptyset \iff a \not\rho\, b$.

(iv) Le classi di equivalenza modulo ρ (a due a due distinte) formano una partizione di A.

Dim. (i) Da $a \,\rho\, a$ segue che $a \in [a]$.

(ii) $(\implies)$. Poiché $b \in [b] = [a]$, allora $a \,\rho\, b$.

$(\Longleftarrow)$. Sia $x \in [a]$. Si ha: $x \,\rho\, a,\ a \,\rho\, b$ e quindi, per transitività, $x \,\rho\, b$, cioè $x \in [b]$. Dunque $[a] \subseteq [b]$. In modo analogo si verifica che $[b] \subseteq [a]$.

(iii) Dimostreremo, equivalentemente, che $[a] \cap [b] \neq \emptyset \iff a \,\rho\, b$.

$(\implies)$. Se $x \in [a] \cap [b]$, allora $a \,\rho\, x,\ x \,\rho\, b$ e quindi (per transitività) $a \,\rho\, b$.

$(\Longleftarrow)$. Segue da (ii) e (i).

(iv) La famiglia

$$\mathfrak{U} = \mathfrak{U}_\rho = \big\{[a],\ \ \forall\, a \in A\big\},$$

formata da tutte le classi di equivalenza [a due a due distinte] di A (modulo ρ), è un ricoprimento di A [in base a (i)]; inoltre due classi distinte sono disgiunte [in base a (ii) e (iii)]. Ne segue che $\mathfrak{U}$ è una partizione di A.

Osservazione 1. Dalla proposizione precedente segue che ogni relazione di equivalenza ρ induce una partizione $\mathfrak{U}_\rho$.

Vale anche il viceversa. Sia infatti $\mathfrak{U} = \{A_i\,,\ i \in I\}$ una partizione di A (formata quindi da sottoinsiemi non vuoti); possiamo definire su A la seguente relazione $\rho = \rho_{\mathfrak{U}}$:

$$a \,\rho\, b \iff a, b \in A_i\,,\ \exists\, i \in I.$$

Si verifica subito che ρ è una relazione di equivalenza su A. Le classi di equivalenza *modulo* ρ sono gli insiemi $A_i \in \mathfrak{U}$. Si verifichi poi che $\mathfrak{U}_{\rho_{\mathfrak{U}}} = \mathfrak{U}$ e che $\rho_{\mathfrak{U}_\rho} = \rho$.

Definizione 7. *Sia ρ una relazione di equivalenza su A. Si chiama insieme quoziente di A modulo ρ l'insieme - denotato $A/_\rho$ - formato dalle classi di equivalenza (a due a due distinte) di A modulo ρ, cioè*

$$A/_\rho = \big\{[a],\ \ \forall\, a \in A\big\}.$$

L'applicazione

$$\pi : A \to A/_\rho,\ \ \text{tale che}\ \ \pi(a) = [a],\ \ \forall\, a \in A,$$

è ovviamente suriettiva ed è chiamata proiezione canonica di A su $A/_\rho$.

Delle classi di equivalenza e dell'insieme quoziente modulo la relazione di congruenza introdotta nella **Def. 4** parleremo diffusamente nel prossimo capitolo.

Consideriamo invece la relazione di equipotenza $\sim$ introdotta nella **Def. 5**. Dato un insieme X, la sua classe di equivalenza $[X]_\sim$, denotata usualmente $|X|$, è detta *cardinalità di* X. $|X|$ è formata da tutti gli insiemi Y tali che esista una biiezione $f : X \to Y$.

In particolare, ogni insieme finito formato da n elementi (a due a due distinti) è equipotente a $\{1, 2, \dots, n\}$ ovvero a $\{0, 1, \dots, n-1\}$. Se infatti $A = \{a_1, a_2, , \dots, a_n\}$, l'applicazione

$$f : \{0, 1, \dots, n-1\} \to A \text{ tale che } f(i) = a_{i+1}, \ \forall\, i = 0, \dots, n-1,$$

è certamente biiettiva.

Per indicare le cardinalità finite si utilizzano usualmente i numeri naturali - come del resto abbiamo già fatto nel primo paragrafo - in questo modo:

$$0 := |\emptyset|, \ 1 := |\{0\}|, \ 2 := |\{0, 1\}|, \ \dots, \ k := |\{0, 1, \dots, k-1\}|, \ \dots.$$

Le cardinalità degli insiemi $\boldsymbol{N}$ ed $\boldsymbol{R}$ sono dette rispettivamente *cardinalità del numerabile* e *cardinalità del continuo*.

Utilizzando la definizione di cardinalità data sopra siamo ora in grado di dimostrare il *Principio della somma*, presentato nel primo paragrafo (cfr. **Prop. 1.1**).

Dim. (*Principio della somma*). Siano A, B due insiemi finiti disgiunti, di cardinalità rispettivamente m, n. Sia $A = \{a_1, \dots, a_m\}$ e $B = \{b_1, \dots, b_n\}$. Si consideri l'applicazione $f : \{1, \dots, m+n\} \to A \cup B$ così definita:

$$f(1) = a_1, \dots, f(m) = a_m, \ f(m+1) = b_1, \dots, f(m+n) = b_n.$$

Tale applicazione è ovviamente biiettiva e quindi $|A \cup B| = |\{1, \dots, m+n\}| = m+n = |A| + |B|$.

Torniamo allo studio delle relazioni di equivalenza, verificando per prima cosa che ogni applicazione definisce una relazione di equivalenza sul suo insieme di partenza.

Definizione 8. *Ad ogni applicazione $f : A \to B$ resta "canonicamente" associata una relazione ρ_f su A, così definita:*

$$a_1 \,\rho_f\, a_2 \iff f(a_1) = f(a_2), \ \ \forall\, a_1, a_2 \in A.$$

Si verifica subito che ρ_f è una relazione di equivalenza su A, detta relazione di equivalenza associata ad f.

Si noti che, se f è iniettiva, la relazione ρ_f è la relazione identica su A (e viceversa). Inoltre

$$[a]_{\rho_f} = \{x \in A \ : \ f(x) = f(a)\} = f^{-1}(f(a)), \ \ \forall\, a \in A.$$

Ne segue che l'insieme quoziente di A modulo ρ_f è dato da

$$A/_{\rho_f} = \{f^{-1}(b), \ \forall\, b \in Im(f)\}.$$

Vedremo ora come attraverso questo insieme quoziente sia possibile "iniettivizzare" una qualsiasi applicazione f.

Proposizione 5. *Sia $f : A \to B$ un'applicazione e sia ρ_f la relazione di equivalenza associata ad f. È ben definita l'applicazione*

$$F : A/_{\rho_f} \to B \ \text{ tale che } \ F([a]) = f(a), \ \ \forall\, [a] \in A/_{\rho_f}.$$

Inoltre F è iniettiva.

Dim. Dimostrare che F è "ben definita", significa dimostrare che la definizione di F non dipende dal rappresentante scelto in ogni classe, cioè che

$$[a] = [a_1] \implies F([a]) = F([a_1]).$$

Infatti: $[a] = [a_1] \iff a \,\rho_f\, a_1 \iff f(a) = f(a_1) \iff F([a]) = F([a_1])$.

Dalle precedenti implicazioni (lette da destra a sinistra) segue che $F([a]) = F([a_1]) \implies [a] = [a_1]$, cioè che F è iniettiva.

L'applicazione F agisce dunque come f, ma è definita su $A/_{\rho_f}$ (e non su A). La sua prerogtiva è quella di trattare tutti gli elementi di A aventi la stessa immagine come se si trattasse di un unico elemento: dunque "iniettivizza" f.

N.B. Perché per iniettivizzare f non abbiamo semplicemente "rimpicciolito" A, eliminando da A tutti gli elementi che hanno la stessa immagine tranne uno? In qualche caso si potrebbe anche fare, ma quale elemento conservare? Si porrebbe dunque un problema di scelta e la costruzione non sarebbe "standard".

Osservazione 2. (i) Si noti che F è l'unica applicazione tale che $F \circ \pi = f$, cioè tale che il seguente diagramma (di insiemi e applicazioni)

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\pi"'] & B \\ A/_{\rho_f} \arrow[ur, "F"'] & \end{tikzcd}$$

è commutativo [nel senso che "il passaggio da un insieme ad un altro è indipendente da ogni possibile percorso (che usi le applicazioni assegnate)"]. Infatti, se $\tilde{F} : A/_{\rho_f} \to B$ verifica $\tilde{F} \circ \pi = f$, allora $\tilde{F}([a]) = (\tilde{F} \circ \pi)(a) = f(a) = F([a])$, $\forall [a] \in A/_{\rho_f}$. Dunque $\tilde{F} = F$.

(ii) Risulta: F è suriettiva $\iff$ f è suriettiva. Infatti:

F è suriettiva $\iff \forall b \in B, \exists [a] \in A/_{\rho_f}$ tale che $F([a]) = b \iff$

$\iff \forall b \in B, \exists a \in A$ tale che $f(a) = b \iff f$ è suriettiva.

Concludiamo con il seguente risultato, che ci consentirà di esprimere in maniera "standard" ogni applicazione come prodotto operatorio di tre applicazioni: una suriettiva, una biiettiva ed una iniettiva

Proposizione 6. (*Teorema di decomposizione delle applicazioni*). *Sia $f : A \to B$ un'applicazione tra insiemi. Esiste un'unica biiezione $\varphi : A/_{\rho_f} \to Im(f)$ tale che $f = i \circ \varphi \circ \pi$, cioè tale che rende commutativo il diagramma:*

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\pi"'] & B \\ A/_{\rho_f} \arrow[r, "\varphi"] & Im(f) \arrow[u, hook, "i"'] \end{tikzcd}$$

Dim. In base alla **Prop. 5**, l'applicazione

$$F : A/_{\rho_f} \to B \text{ tale che } F \circ \pi = f$$

è iniettiva . La sua suriettificazione F_{su} è quindi biiettiva. Si osserva poi subito che $Im\, f = Im\, F$. Posto $\varphi := F_{su}$ e considerata l'inclusione canonica $i : Im\, f \hookrightarrow B$, si ha, $\forall a \in A$:

$$(i \circ \varphi \circ \pi)(a) = (i \circ \varphi)([a]) = i(\varphi([a])) = i(F([a])) = i(f(a)) = f(a).$$

Quindi $f = i \circ \varphi \circ \pi$.

L'unicità di φ è evidente [si verifichi che se $i \circ \psi \circ \pi = i \circ \varphi \circ \pi$, allora $\psi = \varphi$].

Ad esempio, assegnata l'applicazione

$$f : \boldsymbol{R} \to \boldsymbol{R} \text{ tale che } f(x) = x^2 - 1, \ \forall x \in \boldsymbol{R},$$

vogliamo decomporla nel senso descritto nella proposizione precedente. Si ha:

$$Im\, f = \{r \in \boldsymbol{R} : r \geq -1\} =: [-1, \infty) \text{ [intervallo di } \boldsymbol{R}].$$

Infatti: $r \in Im\, f \iff \exists\, x \in \boldsymbol{R} : x^2 - 1 = r \iff \exists\, x \in \boldsymbol{R} : x^2 = r + 1 \iff r + 1 \geq 0.$

Inoltre, $\forall\, x,\, y \in \boldsymbol{R} :\ x\, \rho_f\, y \iff x^2 - 1 = y^2 - 1 \iff y = \pm x$. Dunque

$$[x] = \{\pm x\}, \quad \forall\, x \in \boldsymbol{R}.$$

L'insieme $\boldsymbol{R}/_{\rho_f}$ si identifica con l'insieme $\boldsymbol{R}^{\geq 0}$ dei reali ≥ 0 e risulta: $f = i \circ \varphi \circ \pi$, con

$\pi : \boldsymbol{R} \to \boldsymbol{R}/_{\rho_f}$ tale che $\pi(x) = [x], \quad \forall\, x \in \boldsymbol{R}$;

$\varphi : \boldsymbol{R}/_{\rho_f} \to [-1, \infty)$ tale che $\varphi([x]) = x^2 - 1, \quad \forall\, [x] \in \boldsymbol{R}/_{\rho_f}$;

$i : [-1, \infty) \hookrightarrow \boldsymbol{R}$ tale che $i(x) = x, \quad \forall\, x \in [-1, \infty)$.

ESERCIZI PROPOSTI

1.3.1. Sia $A = \{a,\, b,\, c\}$ un insieme (di cardinalità 3). Sia ρ la relazione su A avente grafico

$$\mathfrak{R} = \{(a, a),\, (a, b),\, (a, c),\, (b, b),\, (b, c),\, (c, c)\}.$$

Verificare se ρ è una relazione d'ordine totale su A.

1.3.2. Dimostrare il principio generalizzato del prodotto: *se* $k \geq 2$ *e* $A_1,\, A_2,\, \ldots,\, A_k$ *sono insiemi finiti, si ha:*

$$|A_1 \times A_2 \times\ \ldots\ \times A_k| = |A_1| \cdot |A_2| \cdot\ \ldots\ \cdot |A_k|.$$

1.3.3. Determinare una biiezione tra $\boldsymbol{N}$ e $\boldsymbol{Z}$ [ciò dimostra che $|\boldsymbol{Z}| = |\boldsymbol{N}|$, cioè che $\boldsymbol{Z}$ è numerabile].