CAPITOLO SECONDO

APPLICAZIONI TRA INSIEMI

E

RELAZIONI DI EQUIVALENZA

1 Applicazioni tra insiemi

Siano A, B insiemi. Una **corrispondenza** tra A e B è un qualsiasi sottoinsieme del prodotto cartesiano $A \times B$; Se D è una tale corrispondenza, gli elementi $a \in A$, $b \in B$ si *corrispondono* secondo D se $(a, b) \in D$.

Una **applicazione di** A **su** B è una *corrispondenza* φ tra A e B che soddisfa la seguente condizione:
per ogni elemento a del primo fattore di $A \times B$ esiste uno ed un solo elemento b del secondo fattore tale che $(a, b) \in \varphi$.

Data l'applicazione φ, si scrive $b = \varphi a$ invece di $(a, b) \in \varphi$; inoltre chiameremo
φa **immagine** di a (secondo φ),
se $C \subseteq A$, **immagine di** C secondo φ è l'insieme $\{\varphi a : \ a \in C\}$, si indica con φC,
se $C \subseteq B$ **l'immagine inversa** di C, secondo φ, indicata con $\varphi^{-1}C$, è $\{a \in A : \ \varphi a \in C\}$.

Un'applicazione φ di A su B si chiama anche una **funzione definita in** A, **valori in** B; in tal caso si scrive $\varphi(a)$ invece di φa; il $\varphi(a)$ si chiama il **valore di** φ in a.

L'applicazione φ di A su B si dice **surgettiva** oppure **su tutto** B se $\varphi A = B$, ovvero
$\forall b \in B \ \exists a \in A : \ b = \varphi a$
L'applicazione φ di A su B si dice **iniettiva** se $\forall a_1, \, a_2 \in A, \ a_1 \neq a_2 \Longrightarrow \varphi a_1 \neq \varphi a_2$.([1])
L'applicazione φ di A su B si dice **biunivoca** se è **iniettiva** e **surgettiva**.
Le applicazioni possono anche essere indicate con la notazione $A \xrightarrow{\varphi} B$

Siano date le applicazioni $A \xrightarrow{\varphi} B \xrightarrow{\psi} C$; è definita allora un'applicazione ω di A su C tale che, per ogni $a \in A$, $\omega a = \psi\varphi(a)$ la indicheremo con $\omega = \psi \circ \varphi$ e si chiama **prodotto di composizione** di φ e ψ. Otteniamo il seguente diagramma commutativo:

$$\begin{tikzcd} A \arrow[r, "\varphi"] \arrow[dr, "\psi\varphi"'] & B \arrow[d, "\psi"] \\ & C \end{tikzcd}$$

Quando parleremo di **diagramma** si intenderà un disegnino fatto di insiemi e frecce (queste rappresentano applicazioni); è **commutativo** se per ogni coppia di insiemi tutte le applicazioni dell'uno sull'altro, ottenute

[1]Non è iniettiva se: $\exists a_1, \, a_2 \in A : \ [a_1 \neq a_2] \wedge [\varphi a_1 = \varphi a_2]$.

come prodotto delle varie frecce in tutti i modi possibili per andare dall'uno all'altro, coincidono; ad esempio, il diagramma

$$\begin{tikzcd} A \arrow[r, "\alpha"] \arrow[d, "\gamma"] \arrow[dr, "\varepsilon"] & B \arrow[d, "\beta"] \arrow[dl, "\eta"'] \\ C \arrow[r, "\delta"] & D \end{tikzcd}$$

è commutativo se e solo se $\varepsilon = \delta\gamma = \beta\alpha$, $\delta\eta = \beta$, $\eta\alpha = \gamma$.

Dato un insieme A, esiste sempre l'applicazione **identica** di A su A, la incicheremo con i oppure i_A, ed è definita da $i_A a = a$, per ogni $a \in A$.

Lemma 1. *Siano A, B insiemi e φ un'applicazione di A su tutto B; esiste un'applicazione ψ di B su A, che rende commutativo il diagramma*

$$\begin{tikzcd} A \arrow[r, "\varphi"] \arrow[dr, "i_A"'] & B \arrow[d, "\psi"] \\ & A \end{tikzcd}$$

se e solo se φ è biunivoca. In tal caso ψ è unica.

Dim.
Se φ è biunivoca la ψ si definisce così: dato $b \in B$, sia a l'unico elemento di A tale che $b = \varphi a$, e si pone $\psi b = a$; allora

$$(\psi\varphi)a = \psi(\varphi\, a) = \psi b = a = i_A a \qquad \text{ossia} \qquad \psi\varphi = i_A.$$

Per l'unicità: sia ψ' un'altra applicazione con la stessa proprietà; allora, dati b ed a tali che $b = \varphi a$, si deve avere

$$\psi' b = \psi'(\varphi a) = (\psi'\varphi)a = i_A a = a = \psi b, \qquad \text{da cui} \qquad \psi' = \psi.$$

Il reciproco è immediato.

La ψ della quale è dimostrata l'esistenza nel Lemma 1 si chiama **applicazione inversa** di φ, e si indica φ^{-1}.

Corollario 1. *Sia φ un'applicazione di A su tutto B tale che φ^{-1} esista; allora $\varphi\varphi^{-1} = i_B$, e $(\varphi^{-1})^{-1} = \varphi$.*

Dim. Infatti, per ogni $b \in B$ si ha $\varphi(\varphi^{-1}b) = \varphi a$ se $\varphi a = b$; quindi $(\varphi\varphi^{-1})b = b = i_B b$. L'eguaglianza $\varphi\varphi^{-1} = i_B$ dice che è commutativo il diagramma

$$\begin{tikzcd} B \arrow[r, "\varphi^{-1}"] \arrow[dr, "i_B"'] & A \arrow[d, "\varphi"] \\ & B \end{tikzcd}$$

che confrontato con quello del Lemma 1 ci dice appunto che $\varphi = (\varphi^{-1})^{-1}$.

Teorema 1. *Siano φ, ψ, ω applicazioni tali che $\varphi\psi$ e $\psi\omega$ esistano; allora esistono e coincidono tra loro, $(\varphi\psi)\omega$ e $\varphi(\psi\omega)$, onde si può scrivere $\varphi(\psi\omega)$= $(\varphi\psi)\omega = \varphi\psi\omega$. Se poi esistono φ^{-1} e ψ^{-1}, esite anche $(\varphi\psi)^{-1}$, e si ha $(\varphi\psi)^{-1} = \psi^{-1}\,\varphi^{-1}$.*

Dim.
Sia $A \xrightarrow{\omega} B \xrightarrow{\psi} C \xrightarrow{\varphi} D$; per ogni $a \in A$ si ha

$$[(\varphi\psi)\omega]a = (\varphi\psi)(\omega a) = \varphi[\psi(\omega a)] = \varphi[(\psi\omega)a] = [\varphi(\psi\omega)]a$$

da cui $(\varphi\psi)\omega = \varphi(\psi\omega)$. Per dimostrare infine l'ultima asserzione si osservi che per ogni $b \in B$

$$(\psi^{-1}\varphi^{-1})(\varphi\psi)b = \psi^{-1}(\varphi^{-1}\varphi)\psi b = \psi^{-1}i_C\psi b = \psi^{-1}\psi b = b = i_B b,$$

onde $\psi^{-1}\varphi^{-1} = (\varphi\psi)^{-1}$.

ESERCIZI

1.

Siano X, Y insiemi e $\psi : X \longrightarrow Y$. Dimostrare che $\psi(A \cap B) = \psi(A) \cap \psi(B)$ per ogni A, $B \subset X$ se e solo se ψ è iniettiva.

2.

Siano X, Y insiemi, $\psi : X \longrightarrow Y$, A, B, sottoinsiemi di X, e D sottoinsieme di Y. Dimostrare:

a. $A \subset B \Longrightarrow \psi(A) \subset \psi(B)$.

b. $\psi^{-1}(\mathcal{C}D) = \mathcal{C}\psi^{-1}(D)$.

3.

Siano X, Y insiemi, $\psi : X \longrightarrow Y$ e A sottoinsieme di X.

a. ψ è inietiva se e solo se $\forall y \in Y$ $f^{-1}y = \varnothing$ oppure un singolo punto se e solo se per ogni $A \subset X : \psi(\mathcal{C}A) \subset \mathcal{C}\psi(A)$.
b. ψ è surgettiva se e solo se per ogni $y \in Y$ $\psi^{-1}y \neq \varnothing$ se e solo se per ogni $A \subset X : \psi(\mathcal{C}A) \supset \mathcal{C}\psi(A)$.

4.

Siano X, Y insiemi, $\psi : X \longrightarrow Y$, B_1, B_2 sottoinsiemi di Y. Dimostrare

a. $\psi^{-1}(B_1 \cup B_2) = \psi^{-1}(B_1) \cup \psi^{-1}(B_2)$
b. $\psi^{-1}(B_1 \cap B_2) = \psi^{-1}(B_1) \cap \psi^{-1}(B_2)$
c. $\psi^{-1}(B_1 \setminus B_2) = \psi^{-1}(B_1) \setminus \psi^{-1}(B_2)$

5.

Siano X, Y insiemi, $\psi : X \longrightarrow Y$, A_1, A_2 sottoinsiemi di X. Dimostrare

a. $\psi(A_1 \cup A_2) = \psi(A_1) \cup \psi(A_2)$
b. $\psi(A_1 \cap A_2) \subset \psi(A_1) \cap \psi(A_2)$
(trovare un controesempio al fatto che nella relazione sopra non può valere =).

6.

Siano X, Y insiemi, $\psi : X \longrightarrow Y$, dimostrare

a. Per ogni $A \subset X$, $\psi^{-1}[\psi(A)] \supset A$.
b. Per ogni $A \subset X$, e $B \subset Y$, $\psi[\psi^{-1}(B) \cap A] = B \cap \psi(A)$; in particolare $\psi[\psi^{-1}(B)] = B \cap \psi(X)$.

2 Relazioni, equivalenze, ordinamenti e partizioni

Una relazione binaria R in un insieme A è, intuitivamente una proposizione tale che per ogni coppia ordinata (a, b) di elementi di A, si può determinare se aRb ("a è in relazione R con b") è vera o no. Si tratta quindi di una corrispondenza fra l'insieme e se stesso. Definiamo questo formalmente.

Definizione 1. *Una relazione binaria R in un insieme A è un sottoinsieme $R \subset A \times A$. Scriveremo aRb in luogo di $(a, b) \in R$.*

Esempio 1. La relazione $\leq$ tra numeri reali è l'insieme $\{(x, y) : \ x \leq y\} \subset \mathbb{R} \times \mathbb{R}$

Esempio 2. La relazione di inclusione in $\mathcal{P}(X)$ è $\{(A, B) : A \subset B\} \subset \mathcal{P}(X) \times \mathcal{P}(X)$

Definizione 2. *Sia R una relazione binaria in A. diremo che*

1. *R è* **riflessiva** *se, per ogni $x \in A$, risulta xRx;*
2. *R è* **simmetrica** *se xRy implica yRx, dove $x, y \in A$;*
3. *R è* **transitiva** *se $xRy \wedge yRz$ implica xRz, dove $x, y, z \in A$.*

Definizione 3. *Una relazione binaria in A è detta* **relazione di equivalenza** *se è* **riflessiva**, **simmetrica** *e* **transitiva**. *Se aRb diremo che a e b sono equivalenti.*

Esempio 3. Nell'insieme dei vettori di $\mathbb{R}^3$, non nulli, uRv indica che u e v hanno la stessa direzione. Allora R è una relazione di equivalenza.

Esempio 4. Sia $\psi : X \longrightarrow Y$ un'applicazione.
La relazione $\{(x, x') : \ \psi(x) = \psi(x')\}$ è una relazione di equivalenza in X.

Esempio 5. In $\mathbb{R}$ la relazione $[0, 1] \times [0, 1]$ è simmetrica e transitiva ma non riflessiva.

Esempio 6. In $\mathbb{R}$ la relazione $\leq$ non è simmetrica.

Esempio 7. In $\mathbb{R}$ la relazione $\{(x, y) : \ |x - y| \leq 1\}$ non è transitiva.

Sia R una relazione di equivalenza in A. Per ogni $a \in A$ $[a] = \{b \in A : \ bRa\}$ è chiamata **classe di equivalenza di** a.

Lemma 2. *Sia R una relazione di equivalenza in A. Allora:*

1. $\bigcup\{[a] : \ a \in A\} = A$.
2. *Se aRb allora $[a] = [b]$.*
3. *Se $\neg(aRb)$ allora $[a] \cap [b] = \varnothing$.*

Dim.

1. Poiché R è riflessivo, abbiamo che $a \in [a]$ quindi $\bigcup\{[a] : a \in A\} = A$.
2. Sia $x \in [a]$, usando la transitività di R abbiamo

$$x \in [a] \iff xRa \iff xRb \iff x \in [b] \Longrightarrow [a] \subset [b].$$

Viceversa, dalla simetria di R, e dalla trasitività, segue

$$aRb \iff bRa \Longrightarrow x \in [b] \iff xRb \iff xRa \iff x \in [a] \Longrightarrow [b] \subset [a].$$

3. Per assurdo: supponiamo $[a] \cap [b] \neq \varnothing$. Scegliamo $x \in [a] \cap [b]$, onde $xRa \wedge xRb$, di conseguenza dalle proprietà simmetrica e transitiva segue aRb.

Definizione 4. *Un* **partizione** *in A è una famiglia $\mathcal{F}$ di sottoinsiemi di A a due a due disgiunti tali che* $\bigcup_{c\in\mathcal{F}} C = A$ *ed inoltre nessun elemento di $\mathcal{F}$ sia vuoto se $A \neq \varnothing$.*

Teorema 2. *Sia A un insieme, $\mathcal{F}$ una partizone in A; si definisce una relazione binaria R in A nel modo seguente:*

$$xRy \iff \exists C \in \mathcal{F} \qquad \text{tale che} \qquad x \in C \wedge y \in C;$$

allora R è una relazione di equivalenza.
Viceversa sia R una relazione di equivalenza in A, si definisce una famiglia di $\mathcal{F}$ di sottoinsiemi di A nel modo seguente:

$$C \in \mathcal{F} \iff \exists c \in A \qquad \text{tale che} \qquad C = \{x : \; xRc;\}$$

allora $\mathcal{F}$ è una partizione in A. Questa corrispondenza tra l'insieme delle equivalenze e l'insieme delle partizioni di A è biunivoca.

Dim.

Data la partizione $\mathcal{F}$ e costruita R ne dimostriamo le tre proprietà;
riflessiva: xRx perché $x \in C$ per qualche $C \in \mathcal{F}$, dato che $\bigcup_{c\in\mathcal{F}} C = A$;
simmetrica: per definizione;
transitiva: se xRy esiste un $C \in \mathcal{F}$ che contiene x e y; è unico perché gli elementi di $\mathcal{F}$ sono a due a due disgiunti; se allora yRz ciò comporta che $z \in C$, onde xRz.

Viceversa, data R costruiamo $\mathcal{F}$ e osserviamo che le proprietà sono una conseguenza del Lemma 2.

La biunivocità della corrispondenza deriva dal fatto che se $\mathcal{F}$ determina R e R determina $\mathcal{F}'$ allora $\mathcal{F} = \mathcal{F}'$, come conseguenza del Lemma 1.

Definizione 5. *Data l'equivalenza R in A, si dice* **insieme quoziente di A rispetto ad R**, *o anche* **modulo** *R, la partizione $\mathcal{F}$ da essa determinata in A. Scriveremo $\mathcal{F} = A/R$. L'applicazione $p_A : \; A \longrightarrow A/R$, che ad ogni $a \in A$ associa la sua classe di equivalenza $[a]$, è chiamata* **proiezione** *oppure* **applicazione naturale** *o* **canonica** *di A su tutto A/R.*

Esempio 8. Se poniamo in R^3 la relazione di equivalenza dell'esempio 3 il vettore unitario di ogni classe può essere preso come rappresentante.

Esempio 9. Nell'esempio 4 le classi di equivalenza sono $\{\psi^{-1}y : \; y \in Y\}$

Esempio 10. In $\mathbb{N}$ mettiamo come relazione di equivalenza: nRm, se n e m sono entrambi pari o entrambi dispari. Allora A/R è costituito da due insiemi: quello dei pari e quello dei dispari. 0 e 1 sono i rappresentanti di ciascuna classe.

Esempio 11. Siano R ed S relazioni binarie rispettivamente in A e in B.
Definiamo la relazione binaria $R \times S$ in $A \times B$ nel modo seguente
$(a,b)R \times S(x,y) \iff aRx \wedge bSy$.
Dimostrare che se R ed S sono relazioni di equivalenza allora anche $R \times S$ è una relazione di equivalenza.

Teorema 3. *(Primo teorema di omomorfismo per gli insiemi)*
Sia f un'applicazione di un insieme A in un insieme B; esitono un'unica relazione di equivalenza R su A ed un'unica applicazione biunivoca f^*, su B, del quoziente A/R, che rendono commutativo il diagramma.

$$\begin{tikzcd} A \arrow[r, "p_A"] \arrow[dr, "f"'] & A/R \arrow[d, "f^*"] \\ & B \end{tikzcd}$$

Dim.

Definiamo R nel modo seguente
$$xRy \iff f(x) = f(y)$$
Si vede facilmente che R è una relazione di equivalenza. Consideriamo l'insieme quoziente A/R determinato da R su A. Per ogni $C \in A/R$ consideriamo $c \in C$ e definiamo $f^*(C) = f(c)$ (ovvero $f^*([c]) = f(c)$). Questa è una "buona definizione" perché $f^*(C)$ dipende solo da C e non da c : infatti se anche $c' \in C$ si ha $c'Rc$ onde $f(c') = f(c)$. È ora chiaro che per ogni $c \in A$ si ha $f^*(p_A(c))) = f^*(C) = f(c)$, ossia il diagramma è commutativo.

La funzione f^* definita sopra è biunivoca: se $f^*(p_A(c)) = f^*(p_A(c'))$ allora $f(c) = f(c')$, ovvero cRc', da cui $p_A(c) = p_A(c')$.
La R e la f^* sono le sole che soddisfano le condizioni richieste; se infatti anche R' e f^{**} vi soddisfano e se p'_A è l'applicazione canonica di A in A/R', si ha:
$$aR'a' \iff p'_A(a) = p'_A(a') \iff f^{**}(p'_A(a)) = f^{**}(p'_A(a')) \iff f(a) = f(a') \iff aRa';$$
questo dimostra che R coincide con R'. Ma allora $A/R = A/R'$ e $p_A = p'_A$. Se poi $C = p_A(a) \in A/R$ si ha $f^{**}(C) = f(a) = f^*(a)$ onde $f^* = f^{**}$.

Teorema 4. *Siano A e B due insiemi ed $f : A \longrightarrow B$. Supponiamo che f sia un'applicazione che* conserva le relazioni *cioè tale che se aRa' allora $f(a)Sf(a')$. Dimostrare che esiste una ed una sola applicazione $f^* : A/R \longrightarrow B/S$ che rende commutativo il diagramma:*

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "p_A"] & B \arrow[d, "p_B"] \\ A/R \arrow[r, "f^*"] & B/S \end{tikzcd}$$

f^* si chiama applicazione indotta da f *nel passaggio al quoziente. Viceversa se f e f^* sono due applicazioni che rendono commutativo il diagramma sopra, allora f necessariamente è un'applicazione che conserva le relazioni e f^* è un'applicazione indotta da f.*

Dim.

Per ogni classe di equivalenza $[a]$ in A/R definiamo l'applicazione $f^* : \ A/R \longrightarrow B/S$ nel modo seguente $f^*([a]) = [f(a)]$. La classe di equivalenza in B, rispetto a S, di $[f(a)]$ è indipendente dalla scelta del rappresentante di $[a]$. Se infatti $a' \in [a]$ allora aRa' e $[a] = [a']$ (vedi Lemma 2). Poiché f conserva le relazioni: $f(a)Sf(a')$ e quindi $[f(a)] = [f(a')]$. Onde f^* è univocamente definito. La commutatività segue osservando che
$$p_B \circ f(a) = [f(a)] = f^*([a]) = f^* \circ p_A(a).$$
Infine f^* è unica, infatti: se g^* è un'altra appplicazione per la quale il diagramma commuta, allora sia $g^*([a]) \neq f^*([a])$ per almeno una classe di equivalenza $[a]$; poiché p_A è surgettiva $g^*(p_A(a)) \neq f^*(p_A(a))$ per qualche $a \in A$. Questo è impossibile perché per la commutatività del diagramma:
$$[f(a)] = p_B(f(a)) = g^*(p_A(a)) \neq f^*(p_A(a)) = p_B(f(a)) = [f(a)].$$

Viceversa, supponiamo che f e f^* rendano commutativo il diagramma. Sia aRa'; allora $p_A(a) = p_A(a')$ per la commutatività del diagramma abbiamo:

$$f^*(p_A(a)) = f^*(p_A(a')) \iff p_B(f(a)) = p_B(f(a')) \iff [f(a)] = [f(b)] \iff f(a)Sf(a').$$

Questo prova che f conserva le relazioni.

Esempi

Esempio 1. Si consideri l'insieme $\mathbb{Z}$ dei numeri interi, su di esso la seguente relazione di equivalenza:

fissato $p \in \mathbb{Z}$, diremo che m è equivalente n modulo p se $m - n$ è divisibile per p e scriveremo

$$\forall m, n \in \mathbb{Z}, \quad m \equiv n \pmod{p} \iff \exists h \in \mathbb{Z} \text{ tale che } m - n = hp. \tag{1}$$

Si verifica facilmente che questa è una relazione di equivalenza su $\mathbb{Z}$. Indicheremo l'insieme quoziente da essa determinata con $\mathbb{Z}_p$. Possono essere presi come rappresentanti delle classi di equivalenza: $0, 1, , 2, \cdots, p - 1$.

Esempio 2. Come esempio di applicazione del Teorema 4 possiamo considerare $A = B = \mathbb{Z}$ e $R = \{(m, n) : m \equiv n \,(\mathrm{mod}\, 4)\}$, $S = \{(h, k) : \; h \equiv k \,(\mathrm{mod}\, 2)\}$. Sia $f : A \longrightarrow B$ così definita $\forall n \in \mathbb{Z} : f(n) = n$. Questa è una applicazione che conserva le relazioni. Osserviamo che l'applicazione $f^* : \mathbb{Z}_4 \longrightarrow Z_2$ verifica: $f^*(0) = f^*(2) = 0$, $f^*(1) = f^*(2) = 1$.