

1. Relazioni.

Una coppia è un insieme contenente due elementi. Siccome una coppia è un insieme, l'ordine con cui vengono considerati i due elementi della coppia non ha importanza. Quindi, la coppia $\{x, y\}$ è uguale alla coppia $\{y, x\}$ ovvero $\{x, y\} = \{y, x\}$.

Una *coppia ordinata* è un insieme contenente due elementi in cui è importante l'ordine in cui vengono considerati i due elementi. Quindi, ci sarà un primo elemento ed un secondo elemento. Per indicare una coppia ordinata useremo le parentesi tonde e scriveremo (x, y) per indicare una coppia di elementi dove x è il primo elemento e y è il secondo elemento.

Diremo che due coppie ordinate (x, y) e (a, b) sono *uguali*, e scriveremo $(x, y) = (a, b)$, se il primo elemento di una delle due coppie è uguale al primo elemento dell'altra coppia e il secondo elemento di una delle due coppie è uguale al secondo elemento dell'altra coppia ovvero $x = a$ e $y = b$.

1.1 Definizione. Dati due insiemi A e B diremo *prodotto cartesiano di A per B* in questo ordine (A è il primo insieme e B è il secondo insieme) l'insieme che ha come elementi tutte e sole le coppie ordinate dove il primo elemento della coppia è un elemento del primo insieme A mentre il secondo elemento della coppia è un elemento del secondo insieme B , ovvero $A \times B = \{(a, b) \mid a \in A, b \in B\}$.

1.2 Definizione. Una *relazione tra un insieme A e un insieme B* è un sottoinsieme R del prodotto cartesiano $A \times B$, cioè $R \subseteq A \times B$. Per ogni coppia ordinata $(a, b) \in A \times B$ diremo che:

- l'elemento $a \in A$ è *in relazione* con l'elemento $b \in B$ (e scriveremo aRb) se $(a, b) \in R$;
- l'elemento $a \in A$ *non è in relazione* con l'elemento $b \in B$ (e scriveremo $a \nR b$) se $(a, b) \notin R$.

1.3 Osservazione. Data una relazione R tra un insieme A e un insieme B , un elemento $a \in A$ può essere in quella relazione con nessuno, esattamente uno o più elementi di B (anche tutti).

1.4 Esempio. $A = \{1, 7, -3\}$, $B = \{q, s, t\}$, $R = \{(7, s), (-3, q), (-3, s), (-3, t)\}$

R è una relazione tra A e B in quanto R è un sottoinsieme di $A \times B$.

L'elemento $1 \in A$ non è in relazione R con alcun elemento $b \in B$. L'elemento $7 \in A$ è in relazione R solo con l'elemento $s \in B$. L'elemento $(-3) \in A$ è in relazione con tutti gli elementi di B .

2. Funzioni.

2.1 Definizione. Diremo che una relazione f tra A e B è una *funzione* se ogni elemento di A è in relazione f con esattamente un elemento di B . Una funzione f tra A e B verrà indicata nel modo seguente $f : A \rightarrow B$. Inoltre, per ogni elemento $a \in A$, se $b \in B$ è l'unico elemento in relazione con a allora invece che afb scriveremo $f(a) = b$ e diremo che b è l'*immagine* di a tramite la funzione f .

2.2 Osservazione. Data una funzione $f : A \rightarrow B$, la definizione precedente non esclude che

(1) elementi distinti di A possano avere come immagine uno stesso elemento di B ;

(ATTENZIONE: il fatto che ogni elemento di A abbia una ed una sola immagine **NON** è in contraddizione col fatto che elementi distinti di A abbiano la stessa immagine)

(2) possano esistere in B elementi che non siano immagine di alcun elemento di A .

2.3 Esempio. $A = \{1, 7, -3\}$, $B = \{q, s, t\}$, $f = \{(1, q), (7, s), (-3, s)\}$

La relazione f tra A e B è una funzione in quanto ogni elemento di A è in relazione con esattamente un elemento di B : $f(1) = q$, $f(7) = s$ e $f(-3) = s$. Inoltre, si osservi che:

(1) gli elementi distinti 7 e (-3) di A hanno la stessa immagine s in B ;

(2) l'elemento t di B non è immagine di alcun elemento di A .

Col simbolo $f(A)$ indicheremo il sottoinsieme di B costituito dagli elementi di B che sono immagine di qualche elemento di A . Cioè, $f(A) := \{b \in B \mid \exists a \in A : f(a) = b\}$.

Funzioni che escludano quanto osservato in (1) e/o in (2) saranno funzioni più "ricche".

2.4 Definizione. Data una funzione $f : A \rightarrow B$, diremo che essa è:

(1) *iniettiva* se elementi distinti di A hanno immagini distinte in B (ovvero, se due elementi di A hanno la stessa immagine allora essi sono necessariamente lo stesso elemento);

(2) *suriettiva* se ogni elemento di B è immagine di qualche elemento di A (ovvero $f(A) = B$).

(3) *biiettiva* se f è sia iniettiva che suriettiva.

2.5 Osservazione. Si noti che le condizioni (1) e (2) sono "*indipendenti*", cioè esistono funzioni che sono iniettive ma non suriettive e funzioni che sono suriettive ma non iniettive.

2.6 Esempio. Siano $A = \{1, 7\}$ e $B = \{q, s, t\}$. Si consideri la funzione $f : A \rightarrow B$ così definita $f = \{(1, q), (7, s)\}$. Si vede che gli elementi distinti 1 e 7 di A hanno in B immagini rispettivamente

$f(1) = q$ e $f(7) = s$ distinte. Quindi, la funzione f è iniettiva. Si vede anche che l'elemento t di B non è immagine di alcun elemento di A . Per cui la funzione f non è suriettiva.

2.7 Esempio. Siano $A = \{1, 7, -3\}$ e $B = \{q, s\}$. Si consideri la funzione $f : A \rightarrow B$ così definita $f = \{(1, q), (7, q), (-3, s)\}$. Si vede che gli elementi distinti 1 e 7 di A hanno la stessa immagine q in B . Quindi, la funzione f non è iniettiva. Invece, ogni elemento di B è immagine di qualche elemento di A . Per cui la funzione f è suriettiva.

2.9 Esempio. Siano $A = \{1, 7, -3\}$ e $B = \{q, s, t\}$. Si consideri la funzione $f : A \rightarrow B$ così definita $f = \{(1, q), (7, s), (-3, t)\}$. Si vede subito che f è una funzione biettiva tra A e B .

2.10 Osservazione. Data una relazione tra due insiemi A e B , il fatto che questa possa essere una funzione, una funzione iniettiva e/o suriettiva dipende anche dagli insiemi A e B .

Esempio. Siano A e B due sottoinsiemi dell'insieme \mathbb{R} dei numeri reali.

Consideriamo la seguente relazione $f = \{(x, y) \in A \times B \mid y = x^2\}$ tra gli insiemi A e B . Tale relazione rappresenta la legge seguente “all'elemento x di A associo l'elemento y di B se e solo se $y = x^2$ ”

1) se $A = \mathbb{R}$ e $B = \mathbb{R}^+ = \{y \in \mathbb{R} \mid y > 0\}$ allora

- f **non è una funzione** in quanto per l'elemento $0 \in A$ non esiste alcun elemento $y \in B$ tale che $y = x^2$.

2) se $A = \mathbb{R}$ e $B = \mathbb{R}$ allora

- f è una funzione in quanto per ogni $x \in \mathbb{R}$ esiste $y \in \mathbb{R}$ tale che $y = x^2$ cioè $y = f(x)$;

- f **non è iniettiva** in quanto sia $2 \in A$ che $(-2) \in A$ hanno la stessa immagine $4 \in B$;

- f **non è suriettiva** in quanto l'elemento $y = (-4) \in B$ non è immagine di alcun elemento $x \in A$.

3) se $A = \mathbb{R}_0^+ = \{x \in \mathbb{R} \mid x \geq 0\}$ e $B = \mathbb{R}$ allora

- f è una funzione in quanto per ogni $x \in \mathbb{R}_0^+$ esiste $y \in \mathbb{R}$ tale che $y = x^2$ cioè $y = f(x)$;

- f è iniettiva in quanto elementi distinti $x \in \mathbb{R}_0^+$ e $x' \in \mathbb{R}_0^+$ hanno immagini distinte x^2 e $(x')^2$ in \mathbb{R} ;

- f **non è suriettiva** in quanto l'elemento $y = (-4) \in B$ non è immagine di alcun elemento $x \in \mathbb{R}_0^+$.

4) se $A = \mathbb{R}$ e $B = \mathbb{R}_0^+ = \{y \in \mathbb{R} \mid y \geq 0\}$ allora

- f è una funzione in quanto per ogni $x \in \mathbb{R}$ esiste $y \in \mathbb{R}_0^+$ tale che $y = x^2$ cioè $y = f(x)$;

- f **non è iniettiva** in quanto sia $2 \in A$ che $(-2) \in A$ hanno la stessa immagine $4 \in \mathbb{R}_0^+$;

- f è suriettiva in quanto ogni elemento $y \in \mathbb{R}_0^+$ è immagine di $x = \sqrt{y} \in \mathbb{R}$.

5) se $A = \mathbb{R}_0^+ = \{x \in \mathbb{R} \mid x \geq 0\}$ e $B = \mathbb{R}_0^+ = \{y \in \mathbb{R} \mid y \geq 0\}$ allora f è una funzione biettiva.

3. Relazioni di equivalenza e partizioni.

3.1 Definizione. Una relazione $R \subseteq A \times A$, tra un insieme A e se stesso, viene detta *relazione in A* .

3.2 Definizione. Una relazione in A si dice

- *riflessiva* se vale la condizione (RIFL) $\forall a \in A \quad aRa$
- *simmetrica* se vale la condizione (SIMM) $\forall a, b \in A \quad (aRb \Rightarrow bRa)$
- *transitiva* se vale la condizione (TRAN) $\forall a, b, c \in A \quad (aRb \text{ et } bRc \Rightarrow aRc)$

3.3 Osservazione. Negli esempi che seguono vedremo che le condizioni (RIFL), (SIMM) e (TRAN) sono “*indipendenti*”, cioè esistono relazioni che ne soddisfano alcune e non altre.

3.4 Esempi. $A = \{2, b, \heartsuit\} \quad A \times A = \{(2,2), (2,b), (2,\heartsuit), (b,2), (b,b), (b,\heartsuit), (\heartsuit,2), (\heartsuit,b), (\heartsuit,\heartsuit)\}$

1) $R = \{(b,b), (\heartsuit,\heartsuit), (2,b), (b,\heartsuit)\}$ è una relazione in A non riflessiva (poiché $2 \not R 2$), non simmetrica (poiché $2Rb$ ma $b \not R 2$) e non transitiva (poiché $2Rb$ e $bR\heartsuit$ ma $2 \not R \heartsuit$).

2) $R = \{(b,b), (\heartsuit,\heartsuit), (2,b), (b,2), (b,\heartsuit), (\heartsuit,b)\}$ è una relazione in A simmetrica, non riflessiva (poiché $2 \not R 2$), simmetrica e non transitiva (poiché $2Rb$ e $bR\heartsuit$ ma $2 \not R \heartsuit$).

3) $R = \{(b,b), (\heartsuit,\heartsuit), (2,b), (b,\heartsuit), (2,\heartsuit)\}$ è una relazione in A transitiva, non riflessiva ($2 \not R 2$) e non simmetrica (poiché $2Rb$ ma $b \not R 2$).

4) $R = \{(2,2), (b,b), (2,b), (b,2)\}$ è una relazione in A simmetrica, transitiva e non riflessiva ($\heartsuit \not R \heartsuit$).

5) $R = \{(2,2), (b,b), (\heartsuit,\heartsuit), (2,b), (b,\heartsuit)\}$ è una relazione in A riflessiva, non simmetrica (poiché $2Rb$ ma $b \not R 2$) e non transitiva (poiché $2Rb$ e $bR\heartsuit$ ma $2 \not R \heartsuit$).

6) $R = \{(2,2), (b,b), (\heartsuit,\heartsuit), (2,b), (b,2), (b,\heartsuit), (\heartsuit,b)\}$ è una relazione in A riflessiva, simmetrica ma non transitiva (poiché $2Rb$ e $bR\heartsuit$ ma $2 \not R \heartsuit$).

7) $R = \{(2,2), (b,b), (\heartsuit,\heartsuit), (2,b), (b,\heartsuit), (2,\heartsuit)\}$ è una relazione in A riflessiva, transitiva ma non simmetrica (poiché $2Rb$ ma $b \not R 2$).

8) $R = \{(2,2), (b,b), (\heartsuit,\heartsuit), (2,b), (b,2)\}$ è una relazione riflessiva, simmetrica e transitiva.

Per l'osservazione precedente ha senso dare la seguente:

3.5 Definizione. Una *relazione* in A si dice *di equivalenza* se è riflessiva, simmetrica e transitiva.

3.6 Definizione. Sia R una relazione di equivalenza in un insieme A . Per ogni elemento $a \in A$ definiamo *classe di equivalenza di a rispetto a R* , e la indichiamo con $[a]_R$, il sottoinsieme $\{b \in A \mid bRa\}$ di A contenente tutti e soli gli elementi di A che sono in relazione R con a .

3.7 Lemma. Per le classi di equivalenza valgono le seguenti proprietà:

$$(CE1) \quad \forall a \in A \quad a \in [a]_R$$

$$(CE2) \quad \forall a, b \in A \quad ([a]_R = [b]_R \Leftrightarrow aRb)$$

$$(CE3) \quad \forall a, b \in A \quad ([a]_R \cap [b]_R \neq \emptyset \Rightarrow [a]_R = [b]_R) \text{ ovvero } ([a]_R \neq [b]_R \Rightarrow [a]_R \cap [b]_R = \emptyset)$$

Dimostrazione.

$$(CE1) \quad aRa \Rightarrow a \in [a]_R$$

$$(CE2 \Rightarrow) \quad a \in [a]_R \text{ et } [a]_R = [b]_R \Rightarrow a \in [b]_R \Rightarrow aRb$$

$$(CE2 \Leftarrow)$$

$$(x \in [a]_R \text{ et } aRb \Rightarrow xRa \text{ et } aRb \Rightarrow xRb \Rightarrow x \in [b]_R) \Rightarrow [a]_R \subseteq [b]_R \quad |$$

$$| \Rightarrow [a]_R = [b]_R$$

$$(y \in [b]_R \text{ et } aRb \Rightarrow yRb \text{ et } bRa \Rightarrow yRa \Rightarrow y \in [a]_R) \Rightarrow [b]_R \subseteq [a]_R \quad |$$

$$(CE3) \quad [a]_R \cap [b]_R \neq \emptyset \Rightarrow \exists x \in A : x \in [a]_R \text{ et } x \in [b]_R \Rightarrow [x]_R = [a]_R \text{ et } [x]_R = [b]_R \Rightarrow [a]_R = [b]_R \quad \blacksquare$$

3.8 Definizione. Sia R una relazione di equivalenza in un insieme A . Definiamo *insieme quoziente dell'insieme A rispetto alla relazione di equivalenza R* , e lo indichiamo col simbolo A/R , l'insieme delle classi di equivalenza degli elementi di A rispetto a R .

3.9 Definizione. Dato un insieme A , diremo *partizione* di A un insieme \mathfrak{S} di sottoinsiemi di A che soddisfi le seguenti proprietà:

$$(P1) \quad \forall X \in \mathfrak{S} \quad X \neq \emptyset \quad \text{ogni elemento di } \mathfrak{S} \text{ è un sottoinsieme non vuoto di } A$$

$$(P2) \quad \forall X, Y \in \mathfrak{S} \quad (X \neq Y \Rightarrow X \cap Y = \emptyset) \quad \text{elementi distinti di } \mathfrak{S} \text{ sono sottoinsiemi di } A \text{ disgiunti}$$

$$(P3) \quad \forall a \in A \quad \exists X \in \mathfrak{S} : a \in X \quad \text{ogni elemento di } A \text{ è contenuto in un elemento di } \mathfrak{S}$$

3.10 Teorema. Dare una relazione di equivalenza in un insieme equivale a darne una partizione.

Dimostrazione. Se R è una relazione di equivalenza in A , allora l'insieme quoziente A/R (visto come famiglia di sottoinsiemi di A) è una partizione dell'insieme A . Infatti, (CE1) implica (P1) e (P3) mentre (CE3) implica (P2). Viceversa, se \mathfrak{S} è una partizione di A , allora è facile provare che la relazione $R := \{(a, b) \in A \times A \mid \exists X \in \mathfrak{S} : a, b \in X\}$ è una relazione di equivalenza in A . ■

4. Operazioni binarie e gruppi.

4.1 Definizione. Diremo

- operazione binaria ovunque definita in $A \times B$ a valori in C ogni funzione $f : A \times B \rightarrow C$
- operazione binaria ovunque definita in A a valori in C ogni funzione $f : A \times A \rightarrow C$
- operazione binaria ovunque definita ed interna ad A ogni funzione $f : A \times A \rightarrow A$

4.2 Definizione. Sia \oplus un'operazione binaria ovunque definita in $A \times B$ a valori in C . Dalla definizione 4.1, si ha che ogni coppia ordinata (x, y) di $A \times B$ ha un'unica immagine z in C .

Invece di $\oplus(x, y) = z$ scriveremo $x \oplus y = z$ e diremo che z è il risultato (unico) dell'operazione \oplus tra x e y (in quest'ordine).

Tenendo conto dell'unicità del risultato si ha che:

$$(U1) \forall x, y \in A, \forall z \in B \quad x = y \Rightarrow x \oplus z = y \oplus z$$

$$(U2) \forall x \in A, \forall w, z \in B \quad w = z \Rightarrow x \oplus w = x \oplus z$$

4.3 Definizione. Se \oplus è un'operazione binaria ovunque definita in $G \times G$ a valori in G , allora diremo che \oplus è un'operazione binaria ovunque definita ed interna a G .

4.4 Definizione. Diremo *gruppo* una coppia (G, \oplus) dove G è un insieme non vuoto e \oplus è un'operazione binaria ovunque definita ed interna a G tale che valgano le proprietà seguenti:

$$(G1) \forall a, b, c \in G \quad (a \oplus b) \oplus c = a \oplus (b \oplus c) \quad (\text{si dice che } \oplus \text{ è } \textit{associativa})$$

$$(G2) \exists 0 \in G : \forall a \in G \quad a \oplus 0 = a = 0 \oplus a \quad (\text{si dice che } 0 \text{ è l'elemento neutro rispetto a } \oplus)$$

$$(G3) \forall a \in G \exists -a \in G : a \oplus (-a) = 0 = (-a) \oplus a \quad (\text{si dice che } -a \text{ è il } \textit{simmetrico} \text{ di } a \text{ rispetto a } \oplus)$$

4.5 Definizione. Un gruppo (G, \oplus) si dice *abeliano* o *commutativo* se vale la proprietà seguente:

$$(G4) \forall a, b \in G \quad a \oplus b = b \oplus a \quad (\text{si dice che } \oplus \text{ è } \textit{commutativa})$$

4.6 Osservazione. Se, come nelle Definizioni 4.4 e 4.5. utilizziamo la notazione additiva \oplus per indicare l'operazione del gruppo G , allora l'elemento neutro rispetto a \oplus viene indicato con 0 (zero) e il simmetrico di un elemento a viene indicato con $(-a)$ e viene detto l'*opposto* di a .

Se, invece, utilizziamo la notazione moltiplicativa \otimes per indicare l'operazione del gruppo G , allora l'elemento neutro rispetto a \otimes viene indicato con 1 (uno) e il simmetrico di un elemento a viene indicato con a^{-1} e viene detto l'*inverso* di a .

4.7 Esempio. Sia \mathbb{R} l'insieme dei numeri reali.

Le classiche operazioni $+$ e \bullet di somma e prodotto tra due numeri reali sono due operazioni binarie ovunque definite ed interne a \mathbb{R} . Inoltre, tali operazioni sono sia associative che commutative.

Rispetto a $+$ esiste il numero reale *zero* 0 che si comporta da elemento neutro e per ogni numero reale x esiste il suo simmetrico (opposto) $-x$. Quindi, la coppia $(\mathbb{R}, +)$ è un gruppo abeliano.

Rispetto a \bullet esiste il numero reale *uno* 1 che si comporta da elemento neutro e per ogni numero reale $x \neq 0$ esiste il suo simmetrico (inverso) x^{-1} . Quindi, la coppia $(\mathbb{R}-\{0\}, \bullet)$ è un gruppo abeliano.

4.8 Definizione. Diremo che una terna (K, \oplus, \otimes) è un *campo* se valgono le seguenti proprietà:

(C1) \oplus e \otimes sono due operazioni binarie ovunque definite ed interne a K ;

(C2) (K, \oplus) è un gruppo abeliano

(C3) $(K-\{0\}, \otimes)$ è un gruppo abeliano (dove 0 l'elemento neutro rispetto a \oplus)

(C4) $\forall a, b, c \in K \quad a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$ (si dice che \otimes è *distributiva rispetto a \oplus*)

4.9 Esempio. La terna $(\mathbb{R}, +, \bullet)$ è un campo. Infatti, abbiamo già visto che sono soddisfatte le proprietà (C1), (C2) e (C3). Inoltre, per i numeri reali vale la proprietà distributiva del prodotto rispetto alla somma, cioè: $\forall a, b, c \in \mathbb{R} \quad a(b + c) = (ab) + (ac)$.

Nel seguito indicheremo brevemente con \mathbb{R} il campo dei numeri reali $(\mathbb{R}, +, \bullet)$.

4.10 Teorema. Se (G, \oplus) è un gruppo allora valgono anche le proprietà seguenti:

(G5) l'elemento neutro 0 è unico

(G6) $\forall a \in G$ il simmetrico $(-a)$ di a è unico

(G7) Se $(-a)$ è il simmetrico di a allora il simmetrico di $(-a)$ è a , cioè, $(-(-a)) = a$.

(G8) $\forall a, b, c \in G \quad a \oplus b = c \Rightarrow b = (-a) \oplus c$ (spostabilità attraverso = dalla sinistra di \oplus)

(G9) $\forall a, b, c \in G \quad a \oplus b = c \Rightarrow a = c \oplus (-b)$ (spostabilità attraverso = dalla destra di \oplus)

(G10) $\forall a, b, c \in G \quad c \oplus a = c \oplus b \Rightarrow a = b$ (cancellabilità a sinistra rispetto a \oplus)

(G11) $\forall a, b, c \in G \quad a \oplus c = b \oplus c \Rightarrow a = b$ (cancellabilità a destra rispetto a \oplus)

(G12) $\forall a \in G \quad a \oplus a = a \Leftrightarrow a = 0$

Dimostrazione.

(G5) Se $k \in G$ è un altro elemento neutro, allora $0 \oplus k = 0$.

Ma, per (G2) è anche $0 \oplus k = k$.

Essendo unico il risultato dell'operazione $0 \oplus k$ si ha che $0 = k$.

(G6) Supponiamo che, oltre ad $(-a)$, esista un altro simmetrico a' di a ; quindi $a' \oplus a = 0 = a \oplus a'$
 $0 = a \oplus a' \Rightarrow (-a) \oplus 0 = (-a) \oplus (a \oplus a') \Rightarrow (-a) \oplus 0 = [(-a) \oplus a] \oplus a' \Rightarrow (-a) = 0 \oplus a' \Rightarrow (-a) = a'$

(G7) da (G3) si ha che a è il simmetrico di $(-a)$; per (G6) il simmetrico è unico, quindi $(-(-a)) = a$

(G8) $a \oplus b = c \Rightarrow_{(G3 \text{ e } U2)} (-a) \oplus (a \oplus b) = (-a) \oplus c \Rightarrow_{(G1)} [(-a) \oplus a] \oplus b = (-a) \oplus c \Rightarrow_{(G3)} 0 \oplus b = (-a) \oplus c$
 $\Rightarrow_{(G2)} b = (-a) \oplus c$

(G9) $a \oplus b = c \Rightarrow_{(G3 \text{ e } U1)} (a \oplus b) \oplus (-b) = c \oplus (-b) \Rightarrow_{(G1)} a \oplus [b \oplus (-b)] = c \oplus (-b) \Rightarrow_{(G3)} a \oplus 0 = c \oplus (-b)$
 $\Rightarrow_{(G2)} a = c \oplus (-b)$

(G10) $c \oplus a = c \oplus b \Rightarrow_{(G8)} a = (-c) \oplus (c \oplus b) \Rightarrow_{(G1)} a = [(-c) \oplus c] \oplus b \Rightarrow_{(G3)} \Rightarrow a = 0 \oplus b \Rightarrow_{(G2)} a = b$

(G11) $a \oplus c = b \oplus c \Rightarrow_{(G9)} a = (b \oplus c) \oplus (-c) \Rightarrow_{(G1)} a = b \oplus [c \oplus (-c)] \Rightarrow_{(G3)} \Rightarrow a = b \oplus 0 \Rightarrow_{(G2)} a = b$

(G12) ovviamente $0 \oplus 0 = 0$; viceversa $a \oplus a = a \Rightarrow_{(G2)} a \oplus a = a \oplus 0 \Rightarrow_{(G10)} a = 0$ ■

5. Spazi vettoriali reali.

5.1 Definizione. Indicato con \mathbb{R} il campo dei numeri reali, diremo *spazio vettoriale reale* una terna $(V, \oplus, *)$ dove (V, \oplus) è un gruppo abeliano ovvero

- (G1) $\forall \mathbf{u}, \mathbf{v}, \mathbf{w} \in V \quad (\mathbf{u} \oplus \mathbf{v}) \oplus \mathbf{w} = \mathbf{u} \oplus (\mathbf{v} \oplus \mathbf{w})$ \oplus è associativa
- (G2) $\exists \mathbf{0} \in V : \forall \mathbf{u} \in V \quad \mathbf{u} \oplus \mathbf{0} = \mathbf{u} = \mathbf{0} \oplus \mathbf{u}$ $\mathbf{0}$ è l'elemento neutro rispetto a \oplus
- (G3) $\forall \mathbf{u} \in V \quad \exists (-\mathbf{u}) \in V : \mathbf{u} \oplus (-\mathbf{u}) = \mathbf{0} = (-\mathbf{u}) \oplus \mathbf{u}$ $(-\mathbf{u})$ è il simmetrico di \mathbf{u} rispetto a \oplus
- (G4) $\forall \mathbf{u}, \mathbf{v} \in V \quad \mathbf{u} \oplus \mathbf{v} = \mathbf{v} \oplus \mathbf{u}$ \oplus è commutativa

e $*$: $\mathbb{R} \times V \rightarrow V$ è un'operazione tale che:

- (PS1) $\forall \alpha \in \mathbb{R}, \forall \mathbf{u}, \mathbf{v} \in V \quad \alpha * (\mathbf{u} \oplus \mathbf{v}) = (\alpha * \mathbf{u}) \oplus (\alpha * \mathbf{v})$ distributività di $*$ rispetto a \oplus
- (PS2) $\forall \alpha, \beta \in \mathbb{R}, \forall \mathbf{u} \in V \quad (\alpha + \beta) * \mathbf{u} = (\alpha * \mathbf{u}) \oplus (\beta * \mathbf{u})$ distributività di $*$ rispetto a $+$
- (PS3) $\forall \alpha, \beta \in \mathbb{R}, \forall \mathbf{u} \in V \quad (\alpha \bullet \beta) * \mathbf{u} = \alpha * (\beta * \mathbf{u})$ associatività "mista"
- (PS4) $\forall \mathbf{u} \in V \quad 1 * \mathbf{u} = \mathbf{u}$ 1 è elemento neutro rispetto a $*$

Gli elementi di V si diranno *vettori*, mentre quelli di \mathbb{R} *scalari*.

L'operazione $\oplus : V \times V \rightarrow V$ (tra due vettori) viene detta *somma di due vettori*.

L'operazione $*$: $\mathbb{R} \times V \rightarrow V$ (tra uno scalare e un vettore il cui unico risultato è un vettore) viene detta *prodotto di uno scalare per un vettore*.

5.2 Teorema. Se $(V, \oplus, *)$ è uno spazio vettoriale reale, allora valgono anche le proprietà seguenti:

- (PS5) $\forall \mathbf{u} \in V \quad 0 * \mathbf{u} = \mathbf{0}$ (dove 0 è lo zero di \mathbb{R} e $\mathbf{0}$ è l'elemento neutro di V rispetto a \oplus)
- (PS6) $\forall \alpha \in \mathbb{R} \quad \alpha * \mathbf{0} = \mathbf{0}$
- (PS7) $\forall \alpha \in \mathbb{R}, \forall \mathbf{u} \in V \quad \alpha * \mathbf{u} = \mathbf{0} \text{ et } \alpha \neq 0 \Rightarrow \mathbf{u} = \mathbf{0}$
- (PS8) $\forall \alpha \in \mathbb{R}, \forall \mathbf{u} \in V \quad \alpha * \mathbf{u} = \mathbf{0} \Leftrightarrow \alpha = 0 \text{ vel } \mathbf{u} = \mathbf{0}$ (legge di annullamento del prodotto)
- (PS9) $\forall \mathbf{u} \in V \quad (-1) * \mathbf{u} = -\mathbf{u}$ (dove $-\mathbf{u}$ è il simmetrico di \mathbf{u})
- (PS10) $\forall \mathbf{u} \in V \quad (-\alpha) * \mathbf{u} = -(\alpha * \mathbf{u})$ (dove $-(\alpha * \mathbf{u})$ è il simmetrico di $\alpha * \mathbf{u}$)
- (PS11) $\forall \alpha \in \mathbb{R}, \forall \mathbf{u}, \mathbf{v} \in V \quad \alpha * \mathbf{u} = \alpha * \mathbf{v} \text{ et } \alpha \neq 0 \Rightarrow \mathbf{u} = \mathbf{v}$ (cancellabilità di $\alpha \neq 0$)
- (PS12) $\forall \alpha, \beta \in \mathbb{R}, \forall \mathbf{u} \in V \quad \alpha * \mathbf{u} = \beta * \mathbf{u} \text{ et } \mathbf{u} \neq \mathbf{0} \Rightarrow \alpha = \beta$ (cancellabilità di $\mathbf{u} \neq \mathbf{0}$)

Dimostrazione.

$$(PS5) (0+0) = 0 \Rightarrow_{(U1)} (0+0)*\mathbf{u} = 0*\mathbf{u} \Rightarrow_{(PS2)} (0*\mathbf{u})\oplus(0*\mathbf{u}) = 0*\mathbf{u} \Rightarrow_{(G12)} 0*\mathbf{u} = \mathbf{0}$$

$$(PS6) (G12) \Rightarrow (\mathbf{0}\oplus\mathbf{0}) = \mathbf{0} \Rightarrow_{(U2)} \alpha*(\mathbf{0}\oplus\mathbf{0}) = \alpha*\mathbf{0} \Rightarrow_{(PS1)} (\alpha*\mathbf{0})\oplus(\alpha*\mathbf{0}) = \alpha*\mathbf{0} \Rightarrow_{(G12)} \alpha*\mathbf{0} = \mathbf{0}$$

$$(PS7) \alpha*\mathbf{u} = \mathbf{0} \text{ et } \alpha \neq 0 \Rightarrow_{(U2)} \alpha^{-1}*(\alpha*\mathbf{u}) = \alpha^{-1}*\mathbf{0} \Rightarrow_{(PS3 \text{ e } PS6)} (\alpha^{-1}\alpha)*\mathbf{u} = \mathbf{0} \Rightarrow 1*\mathbf{u} = \mathbf{0} \Rightarrow_{(PS4)} \mathbf{u} = \mathbf{0}$$

(PS8) immediata conseguenza di (PS5), (PS6) e (PS7)

$$(PS9) [1+(-1)] = 0 \Rightarrow_{(U1)} [1+(-1)]*\mathbf{u} = 0*\mathbf{u} \Rightarrow_{(PS2 \text{ e } PS5)} (1*\mathbf{u})\oplus[(-1)*\mathbf{u}] = \mathbf{0} \Rightarrow_{(PS4)} \\ \Rightarrow \mathbf{u}\oplus[(-1)*\mathbf{u}] = \mathbf{0} \Rightarrow [(-1)*\mathbf{u}] \text{ è un simmetrico di } \mathbf{u} \Rightarrow_{(G6)} (-1)*\mathbf{u} = -\mathbf{u}$$

$$(PS10) (-\alpha)*\mathbf{u} = [(-1)\alpha]*\mathbf{u} \stackrel{(PS3)}{=} (-1)*(\alpha*\mathbf{u}) \stackrel{(PS9)}{=} -(\alpha*\mathbf{u})$$

$$(PS11) \alpha*\mathbf{u} = \alpha*\mathbf{v} \text{ et } \alpha \neq 0 \Rightarrow_{(U2)} \alpha^{-1}*(\alpha*\mathbf{u}) = \alpha^{-1}*(\alpha*\mathbf{v}) \Rightarrow_{(PS3)} (\alpha^{-1}\alpha)*\mathbf{u} = (\alpha^{-1}\alpha)*\mathbf{v} \Rightarrow \\ \Rightarrow 1*\mathbf{u} = 1*\mathbf{v} \Rightarrow_{(PS4)} \mathbf{u} = \mathbf{v}$$

$$(PS12) \alpha*\mathbf{u} = \beta*\mathbf{u} \text{ et } \mathbf{u} \neq \mathbf{0} \Rightarrow_{(G3)} (\alpha*\mathbf{u})\oplus[-(\beta*\mathbf{u})] = \mathbf{0} \text{ et } \mathbf{u} \neq \mathbf{0} \Rightarrow_{(PS10)}$$

$$(\alpha*\mathbf{u})\oplus[(-\beta)*\mathbf{u}] = \mathbf{0} \text{ et } \mathbf{u} \neq \mathbf{0} \Rightarrow_{(PS2)} [\alpha+(-\beta)]*\mathbf{u} = \mathbf{0} \text{ et } \mathbf{u} \neq \mathbf{0} \Rightarrow_{(PS8)} [\alpha+(-\beta)] = 0 \Rightarrow \alpha = \beta \quad \blacksquare$$