1. Relazioni.

Dati due insiemi possiamo stabilire in modo del tutto arbitrario una "*legge*" che associ elementi di un insieme ad elementi dell'altro insieme. Ovviamente, data la totale arbitrarietà di tale legge ad un elemento di un insieme è possibile associare nessun elemento dell'altro insieme o un solo elemento dell'altro insieme o più di un elemento dell'altro insieme (anche tutti).

1.1 Esempio. Siano A = {11, f, β, ♦, ♥, ♠} e B = {x, 11, ♠, ♣, ∇, α, γ} e le seguenti leggi:

Legge n.1
- agli elementi 11 e f di A non associo alcun elemento di B
- all'elemento β di A associo l'elemento x
- all'elemento ♦ associo gli elementi ∇, α, e γ
- all'elemento ♥ associo l'elemento x
- all'elemento ♠ associo tutti gli elementi di B

Legge n.2
- a ciascuno degli elementi x, ♣ e α di B non associo alcun elemento di A
- all'elemento 11 di B associo gli elementi 11 e ♠ di A
- all'elemento ♠ di B associo solo l'elemento 11 di A
- all'elemento ∇ di B associo gli elementi 11 e ♦ di A
- all'elemento γ di B associo gli elementi 11, f e β di A

Il problema che sorge spontaneo è come rappresentare in un modo più comodo tali leggi tra gli elementi degli insiemi A e B.

Osserviamo che per ricordare una legge è importante ricordare "*chi è associato a chi*" mentre si può dimenticare gli elementi che non sono associati tra loro. Per far ciò possiamo iniziare a scrivere solo degli insiemi che contengono gli elementi tra loro associati.

Per la Legge n.1 scriviamo perciò i seguenti insiemi
{β, x}, {♦, ∇}, {♦, α}, {♦, γ}, {♥, x}, {♠, x,}, {♠, 11}, {♠, ♠}, {♠, ♣}, {♠, γ}, {♠, ∇}, {♠, α}
Mentre per la Legge n.2 gli insiemi seguenti
{11, 11}, {11, ♠}, {♠, 11}, {∇, 11}, {∇,♦}, {γ, 11}, {γ, f}, {γ, β}

Questo risolve completamente il problema? Per poter rispondere affermativamente dobbiamo esser certi che non possano sorgere degli equivoci. Osserviamo che gli insiemi scritti sopra ci ricordano solamente "*chi è associato a chi*" ma non ci ricordano a quale insieme appartengono gli elementi. Per esempio, gli insiemi {11, ♠} e {♠, 11} della Legge n.2 sono UGUALI e, quindi, non ci sarebbe bisogno di scriverli due volte. Ma attenzione: come insiemi sono uguali invece per quanto riguarda la Legge n.2 ricordano due cosa diverse: l'insieme {11, ♠}, scritto proprio così, ci ricorda che l'elemento 11 di B è associato all'elemento ♠ di A, mentre lo STESSO insieme ma scritto così {♠, 11} ci ricorda che l'elemento ♠ di B è associato all'elemento 11 di A. E, comunque, in questo caso, ciò non sarebbe ancora un problema perché nella Legge n.2 si è scelto che accadano entrambe le cose. Ma ciò costituisce un problema nel caso della Legge n.1. Infatti, nella Legge n.1 abbiamo solamente che l'elemento ♠ di A è associato all'elemento 11 di B mentre NON è vero il viceversa. Quindi, per la Legge n.1 non è indifferente come viene scritto l'insieme che ci ricorda questo fatto: la scrittura {♠, 11} va bene mentre la scrittura {11, ♠} non va bene pur rappresentando entrambe lo STESSO insieme. Inoltre, si osservi che lo stesso insieme {11, ♠} scritto nello STESSO MODO ha un significato diverso per le due leggi: infatti {11, ♠} per la Legge n.1 ricorda che 11 di A è associato a ♠ di B mentre per la Legge n.2 ricorda che 11 di B è associato a ♠ di A.

Si vede che gli inconvenienti appena riscontrati sono dei problemi di "ordine". Infatti, il primo problema, quello della scrittura, è in realtà un problema di ordine in cui si susseguono gli elementi nell'insieme che ricorda i due elementi associati tra loro. Mentre il secondo problema è un problema legato all'ordine con cui consideriamo i due insiemi. Per ovviare ad entrambe questi inconvenienti è sufficiente stabilire un ordine tra i due insiemi e, quindi, parlare di una legge tra A e B in ***quest'ordine*** e distinguerla da una legge tra B e A ed utilizzare le coppie ordinate invece che gli insiemi per ricordare "chi è associato a chi". Per una legge tra A (primo insieme) e B (secondo insieme) scriveremo (a, b) per ricordare che l'elemento a di A è associato con l'elemento b di B.

Per cui per la Legge n.1 tra A e B scriviamo le seguenti coppie ordinate

(β, x), (♦, ∇), (♦, α), (♦, γ), (♥, x), (♠, x,), (♠, 11), (♠, ♠), (♠, ♣), (♠, γ), (♠, ∇), (♠, α)

Mentre per la Legge n.2 tra B e A scriviamo le seguenti coppie ordinate

(11, 11), (11, ♠), (♠, 11), (∇, 11), (∇, ♦), (γ, 11), (γ, f), (γ, β).

Tenendo conto dell'operazione di prodotto cartesiano tra due insiemi possiamo ora dare la seguente

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$\not R$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 $f : A \to B$. 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 $f : A \to B$, 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: 1fq, 7fs, (-3)fs. Quindi, scriveremo f(1) = q, f(7) = s e f(-3) = s. 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" e ad esse daremo dei nomi come segue.

2.4 Definizione. Data una funzione $f : A \to B$, diremo che essa è:
(1) *inettiva* 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).

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 $f : A \to B$ 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 $f : A \to B$ 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.

Per l'osservazione precedente ha senso anche la seguente:

2.8 Definizione. Diremo che una funzione $f : A \to B$ è *biettiva* se essa è sia iniettiva che suriettiva.

2.9 Esempio. Siano A={1, 7, -3} e B={q, s, t}. Si consideri la funzione $f : A \to B$ 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 relazione possa essere una funzione, una funzione iniettiva, una funzione suriettiva, una funzione biettiva dipende **anche** dagli insiemi A e B.

Esempio. Siano A e B due sottoinsiemi dell'insieme R dei numeri reali. Sia f la legge seguente:

"*all'elemento x di A associo l'elemento y di B se e solo se* $y = x^2$ "

Domanda 1) La relazione $f = \{(x, y) \in A \times B \mid y = x^2\}$ è una funzione tra A e B**?**

Domanda 2) In caso affermativo, la funzione f è iniettiva e/o suriettiva**?**

Pur avendo sempre la **stessa** legge f, le risposte a tali domande **dipenderanno** dalla scelta dagli insiemi A e B come vediamo negli esempi seguenti:

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

- 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) $A = R$ e $B = R$

- f è una funzione in quanto per ogni $x \in R$ esiste $y \in R$ tale che $y = x^2$ cioè $y=f(x)$;
- f **non** è iniettiva in quanto sia $2 \in A$ che $(-2) \in R$ hanno la stessa immagine $4 \in R$;
- f **non** è suriettiva in quanto l'elemento $y=(-4) \in R$ non è immagine di alcun elemento $x \in R$.

3) $A = R_0^+ = \{x \in R \mid x \geq 0\}$ e $B = R$

- f è una funzione in quanto per ogni $x \in R_0^+$ esiste $y \in R$ tale che $y = x^2$ cioè $y=f(x)$;
- f è iniettiva in quanto elementi distinti $x \in R_0^+$ e $x' \in R_0^+$ hanno immagini distinte x^2 e $(x')^2$ in R;
- f **non** è suriettiva in quanto l'elemento $y=(-4) \in R$ non è immagine di alcun elemento $x \in R_0^+$.

4) $A = R$ e $B = R_0^+ = \{y \in R \mid y \geq 0\}$

- f è una funzione in quanto per ogni $x \in R$ esiste $y \in R_0^+$ tale che $y = x^2$ cioè $y=f(x)$;
- f **non** è iniettiva in quanto sia $2 \in R$ che $(-2) \in R$ hanno la stessa immagine $4 \in R_0^+$;
- f è suriettiva in quanto ogni elemento $y \in R_0^+$ è immagine di $x=\sqrt{y} \in R$.

5) $A = R_0^+ = \{x \in R \mid x \geq 0\}$ e $B = R_0^+ = \{y \in R \mid y \geq 0\}$

- f è una funzione in quanto per ogni $x \in R_0^+$ esiste $y \in R_0^+$ tale che $y = x^2$ cioè $y=f(x)$;
- f è iniettiva in quanto elementi distinti $x \in R_0^+$ e $x' \in R_0^+$ hanno immagini distinte x^2 e $(x')^2$ in R_0^+;
- f è suriettiva in quanto ogni elemento $y \in R_0^+$ è immagine di $x=\sqrt{y} \in R_0^+$.

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

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, ♥} A×A={(2,2), (2,b), (2,♥), (b,2), (b,b), (b,♥), (♥,2),(♥,b), (♥,♥)}

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

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

3) R={(b,b), (♥,♥), (2,b), (b,♥), (2,♥)} 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 (♥$\not R$♥).

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

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

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

8) R={(2,2), (b,b), (♥,♥), (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) $\forall a \in A \quad a \in [a]_R$

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

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

Dimostrazione.

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

(CE2$\Rightarrow$) $a \in [a]_R$ et $[a]_R = [b]_R \Rightarrow a \in [b]_R \Rightarrow aRb$

(CE2$\Leftarrow$)

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

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

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

(CE3) $[a]_R \cap [b]_R \neq \varnothing \Rightarrow \exists x \in A : x \in [a]_R$ et $x \in [b]_R \Rightarrow [x]_R = [a]_R$ et $[x]_R = [b]_R \Rightarrow [a]_R = [b]_R$ ■

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 $\Im$ di sottoinsiemi di A che soddisfi le seguenti proprietà:

(P1) $\forall X \in \Im \quad X \neq \varnothing$ ogni elemento di $\Im$ è un sottoinsieme non vuoto di A

(P2) $\forall X,Y \in \Im \quad (X \neq Y \Rightarrow X \cap Y = \varnothing)$ elementi distinti di $\Im$ sono sottoinsiemi di A disgiunti

(P3) $\forall a \in A \quad \exists X \in \Im : a \in X$ ogni elemento di A è contenuto in un elemento di $\Im$

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 $\Im$ è una partizione di A, allora è facile provare che la relazione $R := \{(a, b) \in A \times A \mid \exists X \in \Im : a,b \in X\}$ è una relazione di equivalenza in A. ■

4. Operazioni binarie, gruppi e campi.

4.1 Definizione. Diremo

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

4.2 Definizione. Sia $\perp$ un'operazione binaria ovunque definita in A×B a valori in C. Dalla definizione 4.1, si ha che ogni coppia ordinata (x, y) di A×B ha un'unica immagine z in C. Invece di $\perp(x, y) = z$ scriveremo $x \perp y = z$ e diremo che z è il *risultato dell'operazione* $\perp$ tra x e y (in quest'ordine).

Tenendo conto dell'unicità del risultato si ha che:

(U1) $\forall x,y\in A\ ,\ \forall z\in B \qquad x = y \ \Rightarrow\ x \perp z = y \perp z$

(U2) $\forall z\in A\ ,\ \forall x,y\in B \qquad x = y \ \Rightarrow\ z \perp x = z \perp y$

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

(G1) $\forall a,b,c\in G$ $\quad (a \perp b) \perp c = a \perp (b \perp c)$ (si dice che $\perp$ è *associativa*)

(G2) $\exists h\in G : \forall a\in G$ $\quad a \perp h = a = h \perp a$ (si dice che h è l'*elemento neutro* rispetto a $\perp$)

(G3) $\forall a\in G\ \exists \underline{a}\in G :$ $\quad a \perp \underline{a} = h = \underline{a} \perp a$ (si dice che $\underline{a}$ è il *simmetrico* di a rispetto a $\perp$)

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

(G4) $\forall a,b\in G$ $\quad a \perp b = b \perp a$ (si dice che $\perp$ è *commutativa*)

4.5 Esempio. Sia R l'insieme dei numeri reali.

Le classiche operazioni + e • di somma e prodotto tra due numeri reali sono due operazioni binarie ovunque definite ed interne a 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 (R, +) è un gruppo abeliano.

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

4.6 Teorema. Se (G, $\perp$) è un gruppo allora valgono anche le proprietà seguenti:

(G5) l'elemento neutro h è unico

(G6) $\forall a \in G$ il simmetrico $\underline{a}$ di a è unico

(G7) Se $\underline{a}$ è il simmetrico di a allora il simmetrico di $\underline{a}$ è a, cioè, $\underline{\underline{a}} = a$

(G8) $\forall a,b,c \in G$ $\quad a \perp b = c \Rightarrow b = \underline{a} \perp c$ (spostabilità attraverso = dalla sinistra di $\perp$)

(G9) $\forall a,b,c \in G$ $\quad a \perp b = c \Rightarrow a = c \perp \underline{b}$ (spostabilità attraverso = dalla destra di $\perp$)

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

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

(G12) $\forall a \in G$ $\quad a \perp a = a \Leftrightarrow a = h$

Dimostrazione.

(G5) Se $k \in G$ è un altro elemento neutro, allora $h \perp k = h$. Ma, per (G2) è anche $h \perp k = k$. Essendo unico il risultato dell'operazione $h \perp k$ si ha che $h = k$.

(G6) Supponiamo che, oltre ad $\underline{a}$, esista un altro simmetrico a' di a; quindi $a' \perp a = h = a \perp a'$

$h = a \perp a' \Rightarrow \underline{a} \perp h = \underline{a} \perp (a \perp a') \Rightarrow \underline{a} \perp h = (\underline{a} \perp a) \perp a' \Rightarrow \underline{a} = h \perp a' \Rightarrow \underline{a} = a'$

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

(G8) $a \perp b = c \Rightarrow_{(G3 \text{ e } U2)} \underline{a} \perp (a \perp b) = \underline{a} \perp c \Rightarrow_{(G1)} (\underline{a} \perp a) \perp b = \underline{a} \perp c \Rightarrow_{(G3)} h \perp b = \underline{a} \perp c \Rightarrow_{(G2)} b = \underline{a} \perp c$

(G9) $a \perp b = c \Rightarrow_{(G3 \text{ e } U1)} (a \perp b) \perp \underline{b} = c \perp \underline{b} \Rightarrow_{(G1)} a \perp (b \perp \underline{b}) = c \perp \underline{b} \Rightarrow_{(G3)} a \perp h = c \perp \underline{b} \Rightarrow_{(G2)} a = c \perp \underline{b}$

(G10) $c \perp a = c \perp b \Rightarrow_{(G8)} a = \underline{c} \perp (c \perp b) \Rightarrow_{(G1)} a = (\underline{c} \perp c) \perp b \Rightarrow_{(G3)} \Rightarrow a = h \perp b \Rightarrow_{(G2)} a = b$

(G11) $a \perp c = b \perp c \Rightarrow_{(G9)} a = (b \perp c) \perp \underline{c} \Rightarrow_{(G1)} a = b \perp (c \perp \underline{c}) \Rightarrow_{(G3)} \Rightarrow a = b \perp h \Rightarrow_{(G2)} a = b$

(G12) ovviamente $h \perp h = h$; $\quad a \perp a = a \Rightarrow_{(G2)} a \perp a = a \perp h \Rightarrow_{(G10)} a = h$ ■

4.7 Definizione. Diremo che una terna (K, $\perp$, ∇) è un *campo* se valgono le seguenti proprietà:

(C1) $\perp$ e ∇ sono due operazioni binarie ovunque definite ed interne a K;

(C2) (K, $\perp$) è un gruppo abeliano

(C3) (K-{h}, ∇) è un gruppo abeliano (dove h l'elemento neutro rispetto a $\perp$)

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

4.8 Esempio. La terna (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: $\forall a,b,c \in R$ $\quad a(b + c) = (ab) + (ac)$.

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

5. Spazi vettoriali <u>reali</u>.

5.1 Definizione. Indicato con R il campo dei numeri reali, diremo *spazio vettoriale reale* una terna $(V, \perp, *)$ dove $(V, \perp)$ è un gruppo abeliano e $* : R\times V \to V$ è un'operazione tale che:

(PS1) $\forall \alpha\in R , \forall \mathbf{u}, \mathbf{v}\in V$ $\quad \alpha*(\mathbf{u}\perp\mathbf{v}) = (\alpha*\mathbf{u}) \perp (\alpha*\mathbf{v})$ $\quad$ (*distributività* di * rispetto a $\perp$)

(PS2) $\forall \alpha, \beta\in R , \forall \mathbf{u}\in V$ $\quad (\alpha+\beta)*\mathbf{u} = (\alpha*\mathbf{u}) \perp (\beta*\mathbf{u})$ $\quad$ (*distributività* di * rispetto a +)

(PS3) $\forall \alpha, \beta\in R , \forall \mathbf{u}\in V$ $\quad (\alpha\beta)*\mathbf{u} = \alpha*(\beta*\mathbf{u})$ $\quad$ (*associatività* "mista")

(PS4) $\forall \mathbf{u}\in V$ $\quad 1*\mathbf{u} = \mathbf{u}$ $\quad$ (1 è *elemento neutro* rispetto a *)

Gli elementi di V si diranno *vettori*, mentre quelli di R *scalari*. Quindi, l'operazione $* : R\times V \to V$ è un'operazione tra uno scalare e un vettore il cui (<u>unico</u>) risultato è un vettore.

5.2 Teorema. Se $(V, \perp, *)$ è uno spazio vettoriale reale, allora valgono <u>anche</u> le proprietà seguenti:

(PS5) $\forall \mathbf{u}\in V$ $\quad 0*\mathbf{u} = \mathbf{h}$ $\quad$ (dove **h** indica l'elemento neutro rispetto a $\perp$)

(PS6) $\forall \alpha\in R$ $\quad \alpha*\mathbf{h} = \mathbf{h}$

(PS7) $\forall \alpha\in R , \forall \mathbf{u}\in V$ $\quad \alpha*\mathbf{u} = \mathbf{h}$ et $\alpha \neq 0 \Rightarrow \mathbf{u} = \mathbf{h}$

(PS8) $\forall \alpha\in R , \forall \mathbf{u}\in V$ $\quad \alpha*\mathbf{u} = \mathbf{h} \Leftrightarrow \alpha = 0$ vel $\mathbf{u} = \mathbf{h}$

(PS9) $\forall \mathbf{u}\in V$ $\quad (-1)*\mathbf{u} = \underline{\mathbf{u}}$ $\quad$ (dove $\underline{\mathbf{u}}$ è il simmetrico dell'elemento **u**)

(PS10) $\forall \mathbf{u}\in V$ $\quad (-\alpha)*\mathbf{u} = \underline{\alpha*\mathbf{u}}$ $\quad$ (dove $\underline{\alpha*\mathbf{u}}$ è il simmetrico dell'elemento $\alpha*\mathbf{u}$)

(PS11) $\forall \alpha\in R , \forall \mathbf{u}, \mathbf{v}\in V$ $\quad \alpha*\mathbf{u} = \alpha*\mathbf{v}$ et $\alpha \neq 0 \Rightarrow \mathbf{u} = \mathbf{v}$ $\quad$ (cancellabilità di $\alpha \neq 0$)

(PS12) $\forall \alpha, \beta\in R , \forall \mathbf{u}\in V$ $\quad \alpha*\mathbf{u} = \beta*\mathbf{u}$ et $\mathbf{u} \neq \mathbf{h} \Rightarrow \alpha = \beta$ $\quad$ (cancellabilità di $\mathbf{u} \neq \mathbf{h}$)

Dimostrazione.

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

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

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

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

(PS9) $[1+(-1)] = 0 \Rightarrow_{(U1)} [1+(-1)]*\mathbf{u} = 0*\mathbf{u} \Rightarrow_{(PS2 \text{ e } PS5)} (1*\mathbf{u})\perp[(-1)*\mathbf{u}] = \mathbf{h} \Rightarrow_{(PS4)}$

$\Rightarrow \mathbf{u} \perp[(-1)*\mathbf{u}] = \mathbf{h} \Rightarrow$ $[(-1)*\mathbf{u}]$ è simmetrico di **u** $\Rightarrow_{(G6)} (-1)*\mathbf{u} = \underline{\mathbf{u}}$

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

(PS11) $\alpha*\mathbf{u} = \alpha*\mathbf{v}$ 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) $\alpha*\mathbf{u} = \beta*\mathbf{u} \Rightarrow_{(G3)} (\alpha*\mathbf{u})\perp(\underline{\beta*\mathbf{u}}) = \mathbf{h} \Rightarrow_{(PS10)} (\alpha*\mathbf{u})\perp[(-\beta)*\mathbf{u}] = \mathbf{h} \Rightarrow_{(PS2)} [\alpha+(-\beta)]*\mathbf{u} = \mathbf{h}$

$[\alpha+(-\beta)]*\mathbf{u} = \mathbf{h}$ et $\mathbf{u} \neq \mathbf{h} \Rightarrow_{(PS8)} [\alpha+(-\beta)] = 0 \Rightarrow \alpha = \beta$ ■