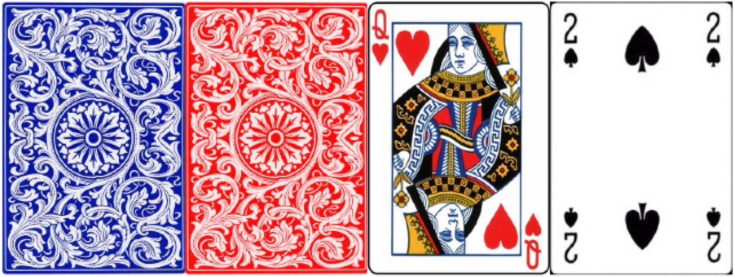
Indice

1. Cenni di logica
2. Elementi di teoria degli insiemi
3. Relazioni e funzioni
4. Strutture algebriche

1. Cenni di logica



Dispongo queste quattro carte da gioco davanti a voi, due coperte e due scoperte e faccio la seguente affermazione:

Ogni carta con il dorso blu è una figura.

Quali carte (almeno) bisogna voltare per dimostrare la verità o la falsità della mia affermazione?

Termini primitivi

$p, q, \ldots$	**proposizioni** (o affermazioni o enunciati)
	= frasi a cui ha senso associare un valore di verità
vero (V), falso (F)	**valori di verità**

Esempi:
p = '$7 > 3$' è una proposizione vera;
q = 'i matematici sono intelligenti' non è una proposizione.

Termini primitivi

$p, q, \dots$	**proposizioni** (o affermazioni o enunciati)
	$=$ frasi a cui ha senso associare un valore di verità
vero (V), falso (F)	**valori di verità**

Esempi:
$p \; = $ '$7 > 3$' è una proposizione vera;
$q \; = $ 'i matematici sono intelligenti' non è una proposizione.

Connettivi logici

Simboli

$\neg$	non
$\wedge$	e
$\vee$	o (nel senso di vel, inclusivo)
$\Rightarrow$	implica = è condizione sufficiente per = se ... allora
$\Leftarrow$	è condizione necessaria per
$\Leftrightarrow$	se e solo se = è condizione necessaria e sufficiente per = è equivalente a

Tavole di verità

p	$\neg p$
V	F
F	V

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

p	q	$p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

Esempi:

- 24 è divisibile per 4 e per 9
- 15 è maggiore di 20 o è divisibile per 3
- $\neg(p \wedge q) = \dots$

Compito. Dimostrare che

$$p \vee (q \vee r) = (p \vee q) \vee r \quad \text{e che}$$

$$p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$$

Tavole di verità

p	$\neg p$
V	F
F	V

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

p	q	$p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

Esempi:

- 24 è divisibile per 4 e per 9
- 15 è maggiore di 20 o è divisibile per 3
- $\neg(p \wedge q) = \dots$

Compito. Dimostrare che

$$p \vee (q \vee r) = (p \vee q) \vee r \quad \text{e che}$$

$$p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$$

Tavole di verità

p	$\neg p$
V	F
F	V

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

p	q	$p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

Esempi:

- 24 è divisibile per 4 e per 9
- 15 è maggiore di 20 o è divisibile per 3
- $\neg(p \wedge q) = \dots$

Compito. Dimostrare che

$$p \vee (q \vee r) = (p \vee q) \vee r \quad \text{e che}$$

$$p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$$

Tavole di verità

p	$\neg p$
V	F
F	V

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

p	q	$p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

Esempi:

- 24 è divisibile per 4 e per 9
- 15 è maggiore di 20 o è divisibile per 3
- $\neg(p \wedge q) = \dots$

Compito. Dimostrare che

$$p \vee (q \vee r) = (p \vee q) \vee r \quad \text{e che}$$

$$p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$$

Tavole di verità

p	q	$p \Rightarrow q$
V	V	V
V	F	F
F	V	V
F	F	V

Osservazione. $p \Rightarrow q$ è equivalente a $\neg q \Rightarrow \neg p$.

Simboli

Simboli

$:$ oppure $\mid$	tale che
$:=$	per definizione
$\forall$	per ogni
$\exists$	esiste
$\exists!$	esiste un unico

2. Elementi di teoria degli insiemi

Termini primitivi

$A, B, \ldots$	**insiemi** = collezioni di oggetti
$\in$ ($\notin$)	**relazione di appartenenza**

Definizione

Diciamo che a è un **elemento** dell'insieme A se $a \in A$.

2. Elementi di teoria degli insiemi

Termini primitivi

$A, B, \ldots$	**insiemi** = collezioni di oggetti
$\in \; (\notin)$	**relazione di appartenenza**

Definizione

Diciamo che a è un **elemento** dell'insieme A se $a \in A$.

Notazioni

Un insieme si può assegnare:

- **per elencazione**: es. $A = \{0, 23, 44, 908\}$;
- se tutti e soli i suoi elementi possiedono un attributo comune, **per caratteristica**: es. $B = \{x \in \mathbb{N} \ : \ x = 3y, y \in \mathbb{N}\}$.

L'insieme vuoto (privo di elementi) si indica: $\emptyset$

Dato un insieme finito, si definisce **cardinalità** il numero dei suoi elementi. Si indica: $|...|$.

Esempi. $|\emptyset| = 0$; se $A = \{a, b, c, d\}$, abbiamo $|A| = 4$.

Inclusione

Definizione

Un insieme A è detto **sottoinsieme** di B (si scrive $A \subseteq B$) se ogni elemento di A appartiene a B. In simboli:

$$A \subseteq B \iff \forall a \in A \ : \ a \in B$$

Definizione

Dati due insiemi A e B, se A è sottoinsieme di B ed esiste un elemento di B che non appartiene ad A, allora si dice che A è un **sottoinsieme proprio** di B (si scrive $A \subsetneq B$). In simboli:

$$A \subsetneq B \iff A \subseteq B \ \wedge \ \exists b \in B \ : \ b \notin A$$

Inclusione

Definizione

Due insiemi A e B **coincidono** (sono uguali) se

$$A \subseteq B \wedge B \subseteq A$$

Proprietà

L'insieme vuoto è sottoinsieme di qualunque insieme. In simboli:

$$\forall A \ : \ \emptyset \subseteq A$$

Inclusione

Siano A, B, C insiemi. La relazione di inclusione gode delle seguenti proprietà:

- riflessiva: $A \subseteq A$;
- antisimmetrica: $A \subseteq B \wedge B \subseteq A \;\Rightarrow\; A = B$
- transitiva: $A \subseteq B \wedge B \subseteq C \;\Rightarrow\; A \subseteq C$

Inclusione

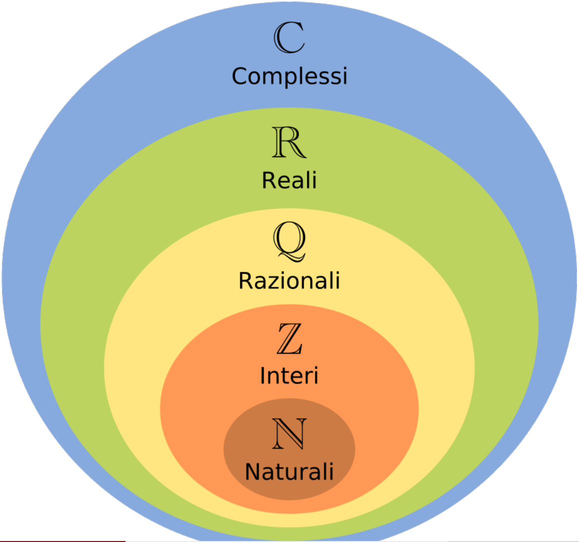
Definizione

Sia A un insieme. Si dice **insieme delle parti** di A l'insieme che contiene tutti e soli i suoi sottoinsiemi. In simboli:

$$\wp(A) = \{X \ : \ X \subseteq A\}$$

Come varia la cardinalità di $\wp(A)$ al variare della cardinalità di A?

Insiemi numerici



Operazioni tra insiemi

Definizione

Siano A e B due insiemi; si dice **intersezione** di A e B l'insieme

$$A \cap B := \{x : x \in A \wedge x \in B\}$$

Definizione

Siano A e B due insiemi; si dice **unione** di A e B l'insieme

$$A \cup B := \{x \; : \; x \in A \vee x \in B\}$$

Definizione

Siano A e B due insiemi; si dice **differenza** di A e B l'insieme

$$A \backslash B := \{x \; : \; x \in A \wedge x \notin B\}$$

Operazioni tra insiemi

Proprietà

Siano A, B e C insiemi. Allora:

1. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
2. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
3. $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$
4. $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$

Compito. Dimostrare le quattro proprietà.

Compito. Da un sondaggio risulta che il 10% dei telespettatori vede abitualmente RAI1, RAI2 e RAI3; il 20% vede RAI1 e RAI3; il 20% RAI2 e RAI3; il 40% RAI1 e RAI2; il 70% RAI1, il 55% RAI2 e il 30% RAI3. Quanti telespettatori non guardano nessuno di questi tre canali?

Compito. In un'aula universitaria sono presenti 65 studenti. 27 amano leggere fumetti, 43 studenti amano gli sport all'aria aperta e a 14 piacciono entrambe le attività. Quanti sono gli studenti che non amano nessuno dei due passatempi?

3. Relazioni e funzioni

Prodotto cartesiano

Definizione

Siano A e B due insiemi; si dice **prodotto cartesiano** di A e B l'insieme delle coppie ordinate aventi il primo elemento in A e il secondo in B:

$$A \times B := \{(a, b) : a \in A \wedge b \in B\}.$$

Definizione

Siano $A_1, A_2, \dots, A_n$ insiemi; il loro prodotto cartesiano è l'insieme delle n-uple ordinate:

$$A_1 \times A_2 \times \cdots \times A_n := \{(a_1, a_2, \dots, a_n) : a_i \in A_i,\ \ i = 1, 2, \dots, n\}.$$

Relazioni

Definizione

Dati due insiemi A e B, una **relazione** R da A in B è un sottoinsieme del prodotto cartesiano $A \times B$.
L'insieme A è detto **dominio** della relazione, l'insieme B **codominio**.
Se la coppia $(a, b) \in R$, allora si scrive aRb.

Due relazioni coincidono se sono definite sugli stessi insiemi (se hanno cioè stesso dominio e stesso codominio) e contengono le stesse coppie ordinate.

Relazioni

Definizione

Sia R una relazione definita su un insieme A (cioè $R \subseteq A \times A$).

- R si dice **riflessiva** se $\forall a \in A \ : \ aRa$;
- R si dice **simmetrica** se $\forall a, b \in A \ : \ aRb \ \Rightarrow \ bRa$;
- R si dice **antisimmetrica** se $\forall a, b \in A \ : \ aRb \wedge bRa \ \Rightarrow \ a = b$;
- R si dice **transitiva** se $\forall a, b, c \in A \ : \ aRb \wedge bRc \ \Rightarrow \ aRc$.

Definizione

Sia R una relazione definita su un insieme A. Allora:

- R si dice **relazione di equivalenza** se è riflessiva, simmetrica e transitiva;
- R si dice **relazione d'ordine** se è riflessiva, antisimmetrica, transitiva.

Esempi di relazioni

- Sia A un insieme e sia $\wp(A)$ l'insieme delle parti di A. Definiamo:
$$\forall X, Y \in \wp(A) \, : \, XRY \iff X \subseteq Y.$$

- Sia A un insieme, definiamo:
$$\forall x, y \in A \, : \, xRy \iff x = y.$$

- Sia $\mathscr{R}$ l'insieme delle rette del piano euclideo. Su $\mathscr{R}$ definiamo:
$$\forall r, s \in \mathscr{R} \, : \, rRs \iff r || s.$$

- Consideriamo l'insieme $\mathbb{Z}$ dei numeri interi:
$$\forall x, y \in \mathbb{Z} \, : \, xRy \iff x \leq y.$$

- Sull'insieme $\mathbb{C}$ dei numeri complessi:
$$\forall z = a + ib, w = c + id \in \mathbb{C} \, : \, zRw \iff a \leq c \wedge b \leq d.$$

Esempi di relazioni

- Sia A un insieme e sia $\wp(A)$ l'insieme delle parti di A. Definiamo:
$$\forall X, Y \in \wp(A) \,:\, XRY \iff X \subseteq Y.$$

- Sia A un insieme, definiamo:
$$\forall x, y \in A \,:\, xRy \iff x = y.$$

- Sia $\mathscr{R}$ l'insieme delle rette del piano euclideo. Su $\mathscr{R}$ definiamo:
$$\forall r, s \in \mathscr{R} \,:\, rRs \iff r || s.$$

- Consideriamo l'insieme $\mathbb{Z}$ dei numeri interi:
$$\forall x, y \in \mathbb{Z} \,:\, xRy \iff x \leq y.$$

- Sull'insieme $\mathbb{C}$ dei numeri complessi:
$$\forall z = a + ib, w = c + id \in \mathbb{C} \,:\, zRw \iff a \leq c \wedge b \leq d.$$

Esempi di relazioni

- Sia A un insieme e sia $\wp(A)$ l'insieme delle parti di A. Definiamo:
$$\forall X, Y \in \wp(A) \, : \, XRY \Longleftrightarrow X \subseteq Y.$$
- Sia A un insieme, definiamo:
$$\forall x, y \in A \, : \, xRy \Longleftrightarrow x = y.$$
- Sia $\mathscr{R}$ l'insieme delle rette del piano euclideo. Su $\mathscr{R}$ definiamo:
$$\forall r, s \in \mathscr{R} \, : \, rRs \Longleftrightarrow r||s.$$
- Consideriamo l'insieme $\mathbb{Z}$ dei numeri interi:
$$\forall x, y \in \mathbb{Z} \, : \, xRy \Longleftrightarrow x \leq y.$$
- Sull'insieme $\mathbb{C}$ dei numeri complessi:
$$\forall z = a + ib, w = c + id \in \mathbb{C} \, : \, zRw \Longleftrightarrow a \leq c \wedge b \leq d.$$

Esempi di relazioni

- Sia A un insieme e sia $\wp(A)$ l'insieme delle parti di A. Definiamo:
$$\forall X, Y \in \wp(A) \, : \, XRY \iff X \subseteq Y.$$

- Sia A un insieme, definiamo:
$$\forall x, y \in A \, : \, xRy \iff x = y.$$

- Sia $\mathscr{R}$ l'insieme delle rette del piano euclideo. Su $\mathscr{R}$ definiamo:
$$\forall r, s \in \mathscr{R} \, : \, rRs \iff r || s.$$

- Consideriamo l'insieme $\mathbb{Z}$ dei numeri interi:
$$\forall x, y \in \mathbb{Z} \, : \, xRy \iff x \leq y.$$

- Sull'insieme $\mathbb{C}$ dei numeri complessi:
$$\forall z = a + ib, w = c + id \in \mathbb{C} \, : \, zRw \iff a \leq c \wedge b \leq d.$$

Esempi di relazioni

- Sia A un insieme e sia $\wp(A)$ l'insieme delle parti di A. Definiamo:
$$\forall X, Y \in \wp(A) \,:\, XRY \iff X \subseteq Y.$$
- Sia A un insieme, definiamo:
$$\forall x, y \in A \,:\, xRy \iff x = y.$$
- Sia $\mathscr{R}$ l'insieme delle rette del piano euclideo. Su $\mathscr{R}$ definiamo:
$$\forall r, s \in \mathscr{R} \,:\, rRs \iff r || s.$$
- Consideriamo l'insieme $\mathbb{Z}$ dei numeri interi:
$$\forall x, y \in \mathbb{Z} \,:\, xRy \iff x \leq y.$$
- Sull'insieme $\mathbb{C}$ dei numeri complessi:
$$\forall z = a + ib, w = c + id \in \mathbb{C} \,:\, zRw \iff a \leq c \wedge b \leq d.$$

Relazioni

Definizione

Sia R una relazione d'ordine definita su un insieme A. R si dice relazione **d'ordine totale** se per ogni $a, b \in A$ si ha $aRb \vee bRa$.

Osservazione. Le relazioni del primo e dell'ultimo esempio della slide precedente sono *d'ordine*, ma *non totale*, mentre la relazione del quarto esempio è di *ordine totale*.
Le relazioni degli altri due esempi sono di *equivalenza*.

Insieme quoziente

Definizione

Sia R una relazione di equivalenza definita su un insieme A. Per ogni $x \in A$, definiamo **classe di equivalenza** l'insieme

$$[x] := \{y \in A \ : \ xRy\}.$$

Proprietà

Sia R una relazione di equivalenza definita su un insieme A. Per ogni $x, y \in A$ si ha:

- $[x] \neq \emptyset$;
- $[x] \cap [y] \neq \emptyset \iff xRy \iff [x] = [y]$.

Ne segue che le classi di equivalenza definiscono una partizione di A (una collezione di sottoinsiemi di A non vuoti, a due a due disgiunti, la cui unione è A).

Insieme quoziente

Definizione

Sia R una relazione di equivalenza definita su un insieme A. L'insieme

$$A/R := \{[x] \ : \ x \in A\}.$$

si chiama **insieme quoziente** di A rispetto a R.

Funzioni

Definizione

Siano $A \neq \emptyset$ e B due insiemi. Una relazione $f \subseteq A \times B$ è una **funzione** se

$$\forall a \in A, \exists! \ b \in B \ : \ (a, b) \in f$$

Notazioni. Poiché b è univocamente determinato da a, si scrive $b = f(a)$ e

$$f \ : \begin{cases} A \longrightarrow B \\ a \longmapsto f(a) \end{cases} .$$

Funzioni

Definizione

Sia $f : A \longrightarrow B$ una funzione. f si dice:

- **iniettiva** se $\forall x, y \in A \ : \ x \neq y \Rightarrow f(x) \neq f(y)$ (equivalentemente $\forall x, y \in A \ : \ f(x) = f(y) \Rightarrow x = y$);
- **suriettiva** se $\forall y \in B$, $\exists x \in A \ : \ y = f(x)$;
- **bijettiva** se è sia iniettiva sia suriettiva (cioè se $\forall y \in B$, $\exists !\, x \in A \ : \ y = f(x)$).

Si chiama **immagine** f il sottoinsieme del codominio:

$$\mathrm{Im} f := \{y \in B \ : \ \exists x \in A \ : \ y = f(x)\} = f(A).$$

Due funzioni f, g coincidono, se coincidono come relazioni: se hanno lo stesso dominio, lo stesso codominio e la stessa azione sugli elementi del dominio, cioè lo stesso grafico ($\forall x \in A \ : \ f(x) = g(x)$).

Funzioni

Definizione

Siano $f : A \longrightarrow B$, $g : B \longrightarrow C$ due funzioni. La **funzione composta** è

$$g \circ f \ : \ \begin{cases} A \longrightarrow C \\ a \longmapsto g(f(a)) \end{cases} .$$

Osservazione. La composizione di funzioni è associativa.

Funzioni

Definizione

Sia A un insieme non vuoto. La funzione

$$\mathrm{id}_A \;:\; \begin{cases} A \longrightarrow A \\ a \longmapsto a \end{cases} .$$

è detta **funzione identica** (o funzione identità) su A.

Definizione

Sia $f : A \longrightarrow B$ una funzione. Se esiste una funzione $g : B \longrightarrow A$ tale che $g \circ f = \mathrm{id}_A$ e $f \circ g = \mathrm{id}_B$, diremo che g è la **funzione inversa** di f e che f è **invertibile**.

Funzioni

Proposizione

- Sia $f : A \longrightarrow B$ una funzione invertibile. Allora f ammette un'unica inversa (che si indica con f^{-1});
- Una funzione $f : A \longrightarrow B$ è invertibile se e solo se è bijettiva.

Esempi di funzioni.

1. $f : \begin{cases} \mathbb{R}\backslash\{0\} \longrightarrow \mathbb{R}\backslash\{0\} \\ r \longmapsto \frac{1}{r} \end{cases}.$
2. $f : \begin{cases} \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} \\ (a,b) \longmapsto (a+b) \end{cases}.$
3. $f : \begin{cases} \mathbb{N}\backslash\{0\} \times \mathbb{N}\backslash\{0\} \longrightarrow \mathbb{N}\backslash\{0\} \\ (a,b) \longmapsto a^b \end{cases}.$

Operazioni

Definizione

Sia $A \neq \emptyset$ un insieme. Un'**operazione binaria** $\star$ su A è una funzione $f\ :\ A \times A \longrightarrow A$.

Se indichiamo con $\star$ tale operazione, scriveremo

$$\forall a, b \in A : \quad a \star b = f(a, b).$$

Quali delle funzioni degli esempi della slide precedente sono operazioni binarie?

Relazioni e funzioni

Compito. Siano n un numero naturale, X un insieme di cardinalità n e A l'insieme delle parti di X. Posto

$$R = \{(B, C) \in A \times A \ : \ \text{esiste una funzione bijettiva } f \ : \ B \longrightarrow C\},$$

mostrare che R è una relazione di equivalenza su A. Quali sono le classi di equivalenza?

4. Strutture algebriche

Gruppi

Definizione

Sia G un insieme non vuoto e sia $\star$ un'operazione binaria su G. Diremo che $(G,\star)$ è un **gruppo** se:

- $\forall x, y, z \in G \ : \ x \star (y \star z) = (x \star y) \star z$;
- $\exists x \in G \ : \ \forall g \in G$ si ha $g \star x = g = x \star g$ (x viene detto **unità** o **elemento neutro** di G e si indica con 1_G);
- $\forall g \in G, \exists \overline{g} \in G \ : \ g \star \overline{g} = 1_G = \overline{g} \star g$.

Definizione

Un gruppo $(G,\star)$ si dice **abeliano** se $\forall x, y \in G \ : \ x \star y = y \star x$.

Gruppi

Proposizione

Sia $(G, \star)$ un gruppo. Allora:

- l'elemento neutro 1_G è unico;
- per ogni $g \in G$, l'inverso $\overline{g}$ di g è unico e si indica con g^{-1};
- $\forall x, y, z \in G$:

$$x \star y = x \star z \iff y = z,$$

$$y \star x = z \star x \iff y = z$$

  (leggi di cancellazione);
- $\forall a, b \in G$ le equazioni in x e y

$$a \star x = b \quad \text{e} \quad y \star a = b$$

  ammettono una e una sola soluzione.

Gruppi

Esempi e controesempi.

1. $(\mathbb{N}, +)$
2. $(\mathbb{N}, \cdot)$
3. $(\mathbb{Z}, +)$
4. $(\mathbb{Q}, +)$
5. $(\mathbb{Q}^*, \cdot)$
6. $(\mathbb{R}, +)$
7. $(\mathbb{R}^*, \cdot)$
8. $(\mathbb{C}, +)$
9. $(\mathbb{C}^*, \cdot)$
10. In $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ consideriamo la seguente operazione:

$$\forall (x_1, x_2), (y_1, y_2) \in \mathbb{R}^2 : (x_1, x_2) \oplus (y_1, y_2) := (x_1 + y_1, x_2 + y_2).$$

Allora $(\mathbb{R}^2, \oplus)$ è un gruppo abeliano.
In generale, $(\mathbb{R}^n, \oplus)$ è un gruppo abeliano.

Campi

Definizione

Sia $\mathbb{K}$ un insieme non vuoto, dotato di due operazioni binarie $\oplus$ e $\odot$. La struttura $(\mathbb{K}, \oplus, \odot)$ è un **campo** se:

- $(\mathbb{K}, \oplus)$ è un gruppo abeliano (elemento neutro 0, $-a$ inverso di a);
- $(\mathbb{K}^* = \mathbb{K} \setminus \{0\}, \odot)$ è un gruppo abeliano (elemento neutro 1, a^{-1} inverso di a);
- $\forall a, b, c \in \mathbb{K}$:
$$(a \oplus b) \odot c = (a \odot c) \oplus (b \odot c).$$

Campi

Esempi e controesempi.

1. $(\mathbb{N}, +, \cdot)$
2. $(\mathbb{Z}, +, \cdot)$
3. $(\mathbb{Q}, +, \cdot)$
4. $(\mathbb{R}, +, \cdot)$
5. $(\mathbb{C}, +, \cdot)$
6. $(\mathbb{Z}_2, +, \cdot)$

Campi

Proposizione

Sia $(\mathbb{K}, +, \cdot)$ un campo, allora:

- $\forall a \in \mathbb{K} \quad a \cdot 0 = 0 \cdot a = 0$;
- se $a, b \in \mathbb{K}$ e $a \cdot b = 0$, si ha $a = 0$ oppure $b = 0$;
- $\forall a, b, c \in \mathbb{K}$, con $a \neq 0$, l'equazione

$$a \cdot (x + b) = c$$

  ha una e una sola soluzione ($x = a^{-1} \cdot c - b$).