Appunti di Geometria

Liam Ferretti

9 ottobre 2025

Sommario

Le informazioni sul corso si trovano sul sito del docente.

Di regola il lunedì verranno svolti esercizi o chiariti dubbi, e le lezioni saranno svolte da S. Molcho.

Ogni settimana (probabilmente il giovedì) verranno caricati degli esercizi su classroom da riconsegnare entro domenica sera.

Il ricevimento avrà luogo nello studio 137 nell'edificio CU006 il martedì dalle 11:15 alle 12:45.

Le dispense sono disponibili sul sito, il libro non è necessario.

Indice

1 Insiemi

Per insieme si intende una collezione di oggetti, detti elementi. Preso l'insieme X e a un elemento, allora:

$$a \in X : \text{ significa che "a è un elemento di X"}$$

$$a \notin X : \text{ significa che "a NON è un elemento di X"}$$

Per definire un insieme si usa questa notazione:

$$X := \{a | a \text{ ha la proprietà P}\}$$

Es:

$$X_a := \{a \in \mathbb{N} \mid 2|a\} = \{0, 2, 4, 6, 8, ...\}$$

Con $2 \mid a$ si intende che 2 è un divisore di a, quindi che a è pari.

Esiste un insieme chiamato insieme vuoto che non contiene nessun elemento ed è rappresentato con: $\varnothing$

È possibile dichiarare una famiglia di insiemi numerati da un altro insieme in questo modo:

$$\{X_i\}_{i \in I}$$

Es:

$$X_a := \{m \in \mathbb{Z} \mid a|m\}$$

Allora:

$$X_0 := \{0\}$$
$$X_1 := \mathbb{Z}$$
$$X_2 := \{0, \pm 2, \pm 4, ...\}$$

Insiemi che è necessario conoscere:

$$\mathbb{N} = \{\text{numeri naturali}\}$$
$$\mathbb{Z} = \{\text{numeri interi}\}$$
$$\mathbb{Q} = \{\text{numeri razionali}\} = \left\{ \frac{p}{q} \;\middle|\; p, q \in \mathbb{Z},\ q \neq 0 \right\}$$
$$\mathbb{R} = \{\text{numeri reali}\}$$
$$\mathbb{C} = \{\text{numeri complessi}\}$$

1.1 Sotto insieme

Presi due insiemi X, Y, X è sotto insieme di Y, se ogni elemento di X è elemento di Y, formalmente si esprime con:

$$X \subset Y \iff \forall x \in X, x \in Y$$

OSS: X è sotto insieme di se stessa in quanto contiene tutti i suoi elementi, quindi ha senso dire che:

$$X \subset X$$

1.2 Operazioni tra insiemi

Le operazioni che si possono effettuare tra insiemi sono diverse:

- Unione, rappresentata da $\cup$
- Intersezione, rappresentata da $\cap$
- Prodotto cartesiano, rappresentata da $\times$

1.2.1 Unione

Preso l'insieme:

$$X_i := \{m \in \mathbb{Z} \mid i|m\}$$

L'unione degli insiemi X_i è l'insieme $X \mid x \in X \iff \exists i \in I \mid x \in X_i$

$$X = \bigcup_{i \in I} X_i$$

Se $I = \{1, 2\} \to X_1 \cup X_2$
Se $I = \{1, 2, 3\} \to X_1 \cup X_2 \cup X_3$
Se $I = \mathbb{Z} \to \bigcup_{i \in I} X_i = \mathbb{Z}$

1.2.2 Intersezione

Preso l'insieme:

$$X_i := \{m \in \mathbb{Z} \mid i|m\}$$

L'intersezione degli insiemi X_i è l'insieme $X \mid x \in X \iff \forall i \in I \exists x \in X_i$

$$X = \bigcap_{i \in I} X_i$$

Se $I = \{1, 2\} \to X_1 \cap X_2$
Se $I = \{1, 2, 3\} \to X_1 \cap X_2 \cap X_3$
Se $I = \mathbb{Z} \to \bigcap_{i \in I} X_i = \{0\}$

1.2.3 Prodotto cartesiano

Il prodotto cartesiano di due insiemi X, Y, è definito come l'insieme i cui elementi sono le coppie ordinate (x, y), con $x \in X, y \in Y$.

$$X = Y = \mathbb{R} \to \mathbb{R} \times \mathbb{R} := \{(x, y) \mid x, y \in \mathbb{R}\}$$

$$\mathbb{R} \times \mathbb{R} \to \mathbb{R}^2$$

Se si hanno più insiemi:

$$X_1 \times X_2 \times X_3 \times ... \times X_n := \{(x_1, x_2, x_3, ..., x_n) \mid x_n \in X_n\}$$

2 Applicazione tra insiemi

Presi gli insiemi X, Y, si definisce un'applicazione f da X (insieme di input o **dominio**) a Y (insieme di output o **codominio**) come una legge che associa a ogni elemento $x \in X$ un elemento $f(x) \in Y$. La notazione è:

$$X \xrightarrow{f} Y$$

ovvero, l'applicazione manda l'insieme X nell'insieme Y. Se si considerano i singoli elementi degli insiemi, si scrive:

$$x \mapsto f(x)$$

Es:

$$\begin{aligned} \mathbb{Z} &\xrightarrow{f} \mathbb{Z} \\ m &\longmapsto 3m \end{aligned}$$

Affinché 2 applicazioni sono uguali devono coincidere: **dominio**, **codominio** e **funzione**.

2.1 Composizione di applicazioni

Presi gli insiemi X, Y, Z e le applicazioni f e g allora:

$$X \xrightarrow{\quad g \quad} Y \xrightarrow{\quad f \quad} Z$$

$$x \longmapsto g(x) \longmapsto f(g(x))$$

è possibile definire la composizione di g e f, ovvero una applicazione del tipo:

$$X \xrightarrow{f \circ g} Z$$

$f \circ g$, si legge f composto g, ed è definito come:

$$f \circ g := f(g(x)) \forall x \in X$$

Es: avendo tre insiemi $\mathbb{Z}$, e due applicazioni f e g, allora:

$$\begin{array}{ccccc} X & \xrightarrow{g} & Y & \xrightarrow{f} & Z \\ n & \longmapsto & 3n+1 & & \\ & & n & \longmapsto & n^2 \end{array}$$

Allora le composizioni di applicazioni sono:

$$(f \circ g)(n) := f(3n+1) = 9m^2 + 6m + 1$$

$$(g \circ f)(n) := g(n^2) = 3n^2 + 1$$

Bisogna notare che in questo caso ha senso sia $f \circ g$ sia $g \circ f$, ma $(f \circ g) \neq (g \circ f)$

OSS:

$$X \xrightarrow{g} Y \xrightarrow{f} X$$

In questo caso e solo nel caso in cui l'insieme iniziale è lo stesso di quello finale, hanno senso sia $f \circ g$ sia $g \circ f$:

$$\text{Per } f \circ g : X \xrightarrow{f \circ g} X \text{ e per } g \circ f : Y \xrightarrow{g \circ f} Y$$

Se $f \circ g = g \circ f$, allora $X = Y$, ma se $X = Y$ non è certo che $f \circ g = g \circ f$

2.2 Proprietà associativa della composizione

Avendo 4 insiemi X, Y, W, Z e applicazioni f, g, h

$$X \xrightarrow{f} Y \xrightarrow{g} W \xrightarrow{h} Z$$

allora vale

$$h \circ (g \circ f) = (h \circ g) \circ f$$

Dimostrazione:

$$(h \circ (g \circ f))(x) = h(g \circ f(x)) = h(g(f(x))) \tag{1}$$
$$((h \circ g) \circ f))(x) = (h \circ g)(f(x)) = h(g(f(x))) \tag{2}$$

Perciò $\forall x \in X : (h \circ (g \circ f))(x) = ((h \circ g) \circ f))(x)$, quindi la composizione di applicazioni è una proprietà associativa, in cui il modo in cui si raggruppano le parentesi non cambia il risultato finale

2.3 Insieme identità di una applicazione

L'insieme identità di X è l'applicazione:

$$\begin{array}{ccc} X & \xrightarrow{Id_x} & X \\ x & \longmapsto & x \end{array}$$

Può essere espressa sia come Id_x sia come 1_x

$$X \xrightarrow{1_X} X \xrightarrow{f} Y \tag{1}$$
$$X \xrightarrow{f} Y \xrightarrow{1_Y} Y \tag{2}$$

Nel caso (1) l'applicazione composta $(f \circ 1_x) = f$ e nel caso (2) l'applicazione $(1_y \circ f) = f$.

2.4 Iniettività

Presi due insiemi X, Y e una applicazione f:

$$X \xrightarrow{f} Y$$

$$f \text{ è iniettiva } \iff \forall x_1, x_2 \in X \to f(x_1) = f(x_2) \Rightarrow x_1 = x_2.$$

Se presi due elementi $x_1, x_2 \in X$ allora gli elementi del codominio sono diversi se e solo se $x_1 \neq x_2$

Es:

$$\begin{array}{ccc} \mathbb{R} & \xrightarrow{f} & \mathbb{R} \\ x & \longmapsto & 3x+1 \end{array}$$

è iniettiva in quanto:

$$f(x_1) = f(x_2) \iff 3x_1 + 1 = 3x_2 + 1 \iff 3(x_1 - x_2) = 0 \iff x_1 = x_2$$

2.5 Suriettività

Presi due insiemi X, Y e una applicazione f:

$$X \xrightarrow{f} Y$$

$$f \text{ è suriettiva} \iff \forall y \in Y \; \exists x \in X \mid f(x) = y.$$

L'immagine di f, ovvero, Im f è definito come:

$$\mathrm{Im}f := \{y \in Y \mid \exists x \in X \mid f(x) = y\}$$

OSS: f è suriettiva $\iff \mathrm{Im}f = Y$

2.6 Biettività

Presi due insiemi X, Y e una applicazione f:

$$X \xrightarrow{f} Y$$

$$f \text{ è biunivoca} \iff \forall y \in Y \; \exists! x \in X \text{ tale che } f(x) = y$$

(con $\exists!$ si intende esiste ed è unico)

2.7 Applicazione inversa

Presi due insiemi X, Y e una applicazione f biunivoca:

$$X \xrightarrow{f} Y$$

L'applicazione inversa di f è l'applicazione:

$$\begin{array}{ccc} Y & \xrightarrow{f^{-1}} & X \\ y & \longmapsto & x \in X \mid \exists! x \mid f^{-1}(x) = y \end{array}$$

Es: scelto

$$\begin{array}{ccc} \mathbb{R} & \xrightarrow{f} & \mathbb{R} \\ x & \longmapsto & 3x+1 \end{array}$$

è biunivoca in quanto è sia suriettiva sia iniettiva, perciò è possibile trovare f^{-1} risolvendo per x:

$$3x + 1 = y \Longrightarrow 3x = y - 1 \Longrightarrow x = \frac{y-1}{3}$$

Quindi l'applicazione inversa è:

$$\begin{array}{ccc} \mathbb{R} & \xrightarrow{f^{-1}} & \mathbb{R} \\ y & \longmapsto & \dfrac{y-1}{3} \end{array}$$

È quindi possibile vedere che l'applicazione composta tra f e f^{-1} in qualsiasi ordine rappresenta l'applicazione identità:

$$\begin{array}{lllll} X & \xrightarrow{f} & Y & \xrightarrow{f^{-1}} & X: \quad f^{-1} \circ f = Id_x \\ Y & \xrightarrow{f^{-1}} & X & \xrightarrow{f} & Y: \quad f \circ f^{-1} = Id_x \end{array}$$

Presi due insiemi X, Y e l'applicazione f:

$$X \xrightarrow{f} Y$$

se $y \in Y \rightarrow f^{-1}(y) := \{x \in X | f(x) = y\}$, in questo caso ha senso anche se non si tratta di applicazioni biunivoche in quanto restituisce un insieme e non un singolo elemento, quindi nel caso esistano più $x|f(x) = y$ si otterrà come risultato l'insieme numerico che contiene tutte le x

3 Relazioni

Preso X un insieme, una relazione su X è un sottoinsieme $R \subset X^2 = X \times X$

Per xRy si intende che $(x, y) \in R$

Es 1:

$$X = \{\text{cittadini italiani}\}$$

$$R = \{(x, y) \mid \text{x e y sono coetanei}\}$$

$$xRy \rightarrow \text{x e y sono coetanei}$$

Es 2:

$X = \mathbb{Z}$, scelto $n \in \mathbb{Z}$

$R_n = \{(x, y) \mid n|(x-y), x, y \in X\} = x \equiv y \pmod{n}$, questa è la relazione di congruenza modulo n

3.1 Relazioni di equivalenza

Per relazione di equivalenza si intende una relazione R su X, con X un insieme qualsiasi, in cui valgono 3 proprietà:

- Riflessiva: $xRx,$ con $x \in X$
- Simmetrica: $xRy \rightarrow yRx,$ con $x, y \in X$
- Transitiva: $xRy \wedge yRz \rightarrow xRz,$ con $x, y, z \in X$

Controllo se l´esempio 2 è una relazione di equivalenza:

$$X = \mathbb{Z}, n \in \mathbb{Z}$$

$$xRy \text{ se } x \equiv y \pmod{n}$$

- Riflessiva: $x \equiv x \pmod{n}$ se $n|(x-x) \rightarrow n|0$, vera
- Simmetrica: $x \equiv y \pmod{n}$ se $n|(x-y) \rightarrow x-y = n*q \rightarrow -x+y = n*(-q)$, vera
- Transitiva: $x \equiv y \pmod{n} \land y \equiv z \pmod{n} \rightarrow x \equiv z \pmod{n}$, dimostrazione:

  $$n|(x-y) \land n|(y-x) = (x-y = q*n) \land (y-z = r*n)$$

  sommando due numeri multipli di n ottengo un multiplo di n

  $$(x-y)+(y-z) = q*n+r*n = n(q+r)$$

  quindi è verificata la proprietà transitiva

3.1.1 Classe di equivalenza

Sia $x \in X$, allora la classe di equivalenza di x è:

$$[x] := \{y \in X \mid xRy\}$$

fissato x, $[x]$ è l'insieme composta dagli elementi y *t.c.* xRy

3.1.2 Quoziente di X modulo R o insieme quoziente

Definiti X un insieme e R una relazione, il quoziente di X modulo R è l'insieme i cui elementi sono le classi R-equivalenza, ovvero le classi di equivalenza rispetto alla relazione R su X, quindi l'insieme quoziente è l'insieme composto dalle classi di equivalenza in X generate da R ed è rappresentato da: X/R

$$X/R := \{[x] \text{ t.c. } x \in X\}$$

In riferimento all'esempio 1:

$$C/R := \{[0], [1], [2], ..., \text{ [età massima] }\}$$

, e ogni elemento ad esempio [19], ha la proprio classe di equivalenza:

$$[19] = \{x \in C \mid eta(x) = 19\}$$

3.2 Insieme delle parti

Una partizione P di S è un insieme di sottoinsiemi $S_p \subset S$ t.c.

- $S_p \neq \emptyset, p \in P$
- $S_p \neq S_q \Rightarrow S_p \cap S_q = \emptyset$, quindi sono disgiunti.
- $\bigcup_{p \in P} S_p = S$, quindi l'unione di tutti i sotto insiemi coprono S.

Esempio:

$$S = \{1, 2, 3\}$$

allora, l'insieme delle parti di S è:

$$\{1, 2, 3\}$$
$$\{\{1, 2\}, \{3\}\}$$
$$\{1, \{2, 3\}\}$$
$$\{\{1, 3\}, \{2\}\}$$
$$\{\{1\}, \{2\}, \{3\}\}$$

Partendo da una relazione di equivalenza su S, con $x \in S$:

$$[x] := \{y \in S \text{ t.c. } xRy\}$$

allora, una partizione di S è definita come:

$$\{[x] \text{ t.c. } x \in S\}$$

Dimostrazione:

1. $[x] \neq \emptyset, \forall x \in \mathbb{R}, xRx \Rightarrow [x]$
2. presi $[x], [y]$, si suppone che $z \in [x] \cap [y]$, se:
   $z \in [x] \rightarrow xRz$
   $z \in [y] \rightarrow yRz$
   allora $xRz \wedge yRz \iff xRy \Rightarrow [x] = [y]$
3. $\bigcup_{x \in S} [x] = S \rightarrow \forall x \in S \Rightarrow x \in [x] \Rightarrow x \in \bigcup_{y \in S} [y]$

Per ogni R si può ottenere una partizione, e per ogni partizione si può ottenere la relazione inziale.

$$P, Sp \subset S, xRy \iff x, y \in S \text{ per lo stesso p}$$

3.2.1 Lemma corrispondenza biunivoca tra relazione e partizione

Esiste una corrispondenza biunivoca tra:

$$\{R \text{ su } S\} \iff \{ \text{ Partizione di } S\}$$

$$R \rightarrow P_R = \{[x] \text{ t.c. } x \in S\}$$
$$(xR_Py \iff x, y \in S_p, p \in S) \leftarrow R_P \leftarrow P$$

4 Anello e campo

A è un insieme i cui elementi sono coppie ordinate (x, y), ed ha 2 operazioni:

- somma:
$$\begin{array}{ccc} A \times A & \xrightarrow{somma} & A \\ (x, y) & \longmapsto & x + y \end{array}$$
- prodotto:
$$\begin{array}{ccc} A \times A & \xrightarrow{prodotto} & A \\ (x, y) & \longmapsto & x * y \end{array}$$

Le proprietà che rendono un insieme un anello o un campo sono:

1. Esistenza ed unicità dell'elemento neutro della somma, quindi:
$$\exists! 0 \in A \text{ t.c. } 0 + z = z + 0 = z \forall z \in A$$
dimostrazione: presi $a \in A, b, c \in A$ t.c. $a + b = 0 \wedge a + c = 0, b \neq c$
ipotesi: $b \stackrel{?}{=} c$
$$0 = 0 \rightarrow a + b = a + c \rightarrow b = c$$
$$Q.E.D$$
2. Proprietà commutativa della somma, quindi:
$$z_1 + z_2 = z_2 + z_1, \forall z_1, z_2 \in A$$
3. Proprietà associativa della somma, quindi:
$$z_1 + (z_2 + z_3) = (z_1 + z_2) + z_3, \forall z_1, z_2, z_3 \in A$$
4. Esistenza ed unicità dell'opposto di $z \in A$, quindi:
$$\forall z \in A \exists! w \in A \text{ t.c. } z + w = 0$$
5. Proprietà associativa del prodotto, quindi:
$$(z_1 * z_2) * z_3 = z_1 * (z_2 * z_3), \forall z_1, z_2, z_3 \in A$$
6. Proprietà distributiva del prodotto rispetto alla somma, quindi:
$$z_1 * (z_2 + z_3) = z_1 * z_2 + z_1 * z_3 \wedge (z_1 + z_2) * z_3 = z_1 * z + 3 + z_2 * z_3, \forall z_1, z_2, z_3 \in A$$
7. Proprietà commutativa rispetto al prodotto, quindi:
$$w * z = z * w, \forall w, z \in A$$
8. L'esistenza ed unicità dell'unità neutra del prodotto ($u \in A$) (unità moltiplicativa), diversa dall'unità neutra della somma, quindi $\neq 0$:
$$u * x = x * u = x, \forall x \in A$$
9. L'esistenza ed unicità dell'inverso moltiplicativo, quindi:
$$\forall x \neq 0 \in A, \exists! w \in A \text{ t.c. } x * w = 1 \rightarrow w = x^{-1}$$

4.1 Anello

A (con le operazioni definite) è un anello se valgono le prime 6 proprietà (o assiomi).

D'ora in avanti per completezza e facilità in diverse situazioni, per anello si intende un anello commutativo rispetto al prodotto e che presenta l'unità moltiplicativa, quindi in cui valgono anche le proprietà 7 e 8.

4.2 Campo

A (con le operazioni definite) è un campo se valgono le prime 9 proprietà (o assiomi).

4.3 Definizione di R_n su $\mathbb{Z}$

$$xR_ny \iff n|(y-x) \iff y = x + kn, k \in \mathbb{Z}$$

4.3.1 Lemma

$\mathbb{Z}/n\mathbb{Z}$ è un anello dato che:

$$\left.\begin{matrix}[x]+[y]=[x+y]\\ [x]\cdot[y]=[x\cdot y]\end{matrix}\right\} \text{ sono ben definite}$$

Dimostrazione:

$$[x] = [x'] \leftarrow x' = x + nk$$
$$[y] = [y'] \leftarrow y' = y + nk$$

Verifichiamo:

$$[x+y] = [x'+y']$$
$$x'+y' = x+nk+y+nl = x+y+n(k+l) \Rightarrow [x'+y'] = [x+y]$$
$$[xy] = [x'y']$$
$$[x'y'] = (x+nk)(y+nl) = xy + n(xl+yk+nkl) \Rightarrow [x'y'] = [xy]$$

Esempio di $\mathbb{Z}/n\mathbb{Z}$:

Tabella 1: *
Somma modulo 5

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Tabella 2: *
Prodotto modulo 5

$\cdot_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Mettendo a confronto le tabelle 2 e 4, si può notare che per la tabella 4 non esiste l'inverso moltiplicativo.

Tabella 3: *
Somma modulo 6

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Tabella 4: *
Prodotto modulo 6

$\cdot_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

4.3.2 Teorema del campo, con n primo

$\mathbb{Z}/n\mathbb{Z}$ è un campo $\iff$ n è primo. Dimostrazione per assurdo:

$$n = m * l, 0 < m < n \land 0 < l < n$$

$$m * l = 0 \mod n$$

se $\exists 1/m \to 1/m * m * l = 0 \Rightarrow l = 0$, però si ha una contraddizione in quanto l è maggiore di 0, quindi n deve essere primo.

4.3.3 Lemma di Bezout

se si hanno due numeri a, b con $MCD(a, b) = d$, allora $\exists x, y \in \mathbb{Z}$ t.c. $ax + by = d$, quindi applicando il teorema di Bezout ad a e p, in modo che $MCD(a, p) = 1$, allora:

$$\exists x, y \text{ t.c. } ax + py = 1 \to \mathbb{Z}/p\mathbb{Z}, ax = 1 \mod p \to x = \frac{1}{a}$$

5 Numeri complessi

Definite due operazioni in $\mathbb{R}^2$:

- Somma:
$$(x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$$
$$(x_1, y_1) + (x_2, y_2) := (x_1 + x_2, y_1 + y_2)$$
- Prodotto:
$$(x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$$
$$(x_1, y_1) * (x_2, y_2) := ((x_1 * x_2 - y_1 * y_2), (x_1 * y_2 + x_2 * y_1))$$

il prodotto è così perchè se fosse definito come$(x_1 * x_2, y_1 * y_2)$ allora $\mathbb{R}^2$ non sarebbe un anello (commutativo ed unitario)

5.1 Verifica $\mathbb{R}^2$

Verifichiamo che $\mathbb{R}^2$ con le proprietà definite è un campo:

1. Unicità dell'elemento neutro della somma:

$$(0,0) \neq (0',0')$$

$$(0,0)+(x,y)=(x,y) \wedge (0',0')+(x,y)=(x,y)$$
$$(x,y)=(x,y) \rightarrow (0,0)=(0',0')$$

2. Proprietà commutativa della somma:

$$(a,b)+(c,d)=(a+c,b+d)=(c+d)+(a+b)$$

   la proprietà commutativa degli elementi a,b,c,d non va dimostrata in questo momento essendo essi elementi di $\mathbb{R}$ commutativi.

3. Associatività della somma:

$$(a,b)+((c,d)+(e,f))=(a,b)+(c+e,d+f)=(c+e+a,d+f+b)$$

$$((a,b)+(c,d))+(e,f)=(a+c,b+d)+(e,f)=(a+c+e,b+d+f)$$
$$(c+e+a,d+f+b)=(a+c+e,b+d+f)$$

   per la proprietà commutativa in $\mathbb{R}$

4. Esistenza ed unicità dell'opposto:

$$(z,w) \neq (z',w')$$

$$(x,y)+(z,w)=(0,0) \wedge (x,y)+(z',w')=(0,0)$$
$$(0,0)=(0,0) \rightarrow (x,y)+(z,w)=(x,y)+(z',w')$$
$$(z,w)=(z',w')$$

   quindi esiste ed è unico l'opposto della somma

Oss:

$$(1,0)*(x,y)=(1*x-0*y,1*y+0*x)=(x,y)$$

quindi la coppia $(1,0)$ è l'elemento neutro del prodotto

5.2 Notazione

$$\begin{cases} 1:=(1,0) & i:=(0,1) \\ \forall a \in \mathbb{R} & a(x,y):=(ax,ay) \\ i^2=-1 & \end{cases}$$

Un numero complesso $z=a1+bi=a+bi:=(a,0)+(0,b)=(a,b)$

Allora abbiamo che un prodotto tra numeri complessi è in questa forma:

$$(a+bi)*(c+di)=a*c-bi*c+a*di+b*d*i^2=(a*c-b*d+(a*d+b*c)i)$$

Il prodotto in C, tra coppie, deriva:

$$z = a + bi = (a, b) \wedge w = c + di = (c, d)$$

$$z * w = (a, b) * (c, d) = (a + bi) * (c + di)$$

A questo punto svolgo le normali moltiplicazioni tra parentesi in R, perché non sono più coppie, ma sono numeri, da questo ottengo una somma tra una parte reale e una parte immaginaria, da cui deriva il prodotto in $\mathbb{C}$.

$$(a * c - b * d + (a * d + b * c)i) = ((a * c - b * d), (a * d + b * c))$$

5.3 Continuo verifica $\mathbb{R}$

continuo con la verifica delle proprietà dalla 5 alla 9

5. Associatività del prodotto:

$$((a, b) * (c, d)) * (x, y) = (a * c - b * d, a * d + b * c) * (x, y)$$

$$(A, B) := (a * c - b * d, a * d + b * c) \rightarrow (A, B) * (x, y)$$

$$(A*x-B*y, A*y+B*x) = ((a*c-b*d)*x-(a*d+b*c)*y, (a*c-b*d)*y+(a*d+b*c)*x)$$

$$((a * c * x - b * d * x - a * d * y - b * c * y), (a * c * y - b * d * y + a * d * x + b * c * x))$$

ora vediamo se la proprietà associativa vale:

$$(a, b) * ((c, d) * (x, y)) = (a, b) * (c * x - d * y, c * y + d * x)$$

$$(C, D) := (c * x - d * y, c * y + d * x) \rightarrow (a, b) * (C, D)$$

$$(a*C-b*D, a*D+b*C) = (a*(c*x-d*y)-b*(c*y+d*x), a*(c*y+d*x)+b*(c*x-d*y))$$

$$((a * c * x - a * d * y - b * c * y - b * d * x), (a * c * y + a * d * x + b * c * x - b * d * y))$$

secondo la proprietà commutativa della somma, i due prodotti sono equivalenti, quindi la proprietà associativa è verificata

6. Proprietà associativa del prodotto rispetto alla somma:

$$z_1 * (z_2 + z_3) = (a, b) * ((c, d) + (x, y))$$

$$(c, d) + (x, y) = (c + x, d + y) \rightarrow (a, b) * (c + x, d + y)$$

$$(a, b) * (c + x, d + y) = (a * (c + x) - b * (d + y), a * (d + y) + b * (c + x))$$

$$(a * c + a * x - b * d - b * y, a * d + a * y + b * c + b * x)$$

$$(a * c - b * d, a * d + b * c) + (a * x - b * y, a * y + b * x)$$

$$(a, b) * (c, d) + (a, b) * (x, y)$$

$$\Rightarrow z_1 * (z_2 + z_3) = z_1 * z_2 + z_1 * z_3$$

7. unità neutra del prodotto

8. Esistenza ed unicità dell'inverso moltiplicativo:

$$(a,b) * (x,y) = (1,0) = 1 + 0i$$

$$(ax - by, ay + bx)$$

Dato che vogliamo che la parte reale del prodotto sia uguale a uno e quella immaginaria sia zero, possiamo scrivere questa equazione come un sistema.

$$\begin{cases} ax - by = 1 \\ ay + bx = 0 \end{cases}$$

Dal secondo:

$$ay + bx = 0 \implies y = -\frac{b}{a}x, a \neq 0$$

Sostituendo nella prima equazione:

$$ax - b(-\frac{b}{a}x) = 1 \implies ax + \frac{b^2}{a}x = 1 \implies a^2x + b^2x = a \implies x = \frac{a}{a^2 + b^2}$$

Sapendo che $y = -\frac{b}{a}x$, allora:

$$y = -\frac{b}{a}\frac{a}{a^2 + b^2} = \frac{b}{a^2 + b^2}$$

Quindi abbiamo dimostrato che la coppia $\left(\frac{a}{a^2 + b^2}, \frac{b}{a^2 + b^2}\right) = (a,b)^{-1}$ quindi:

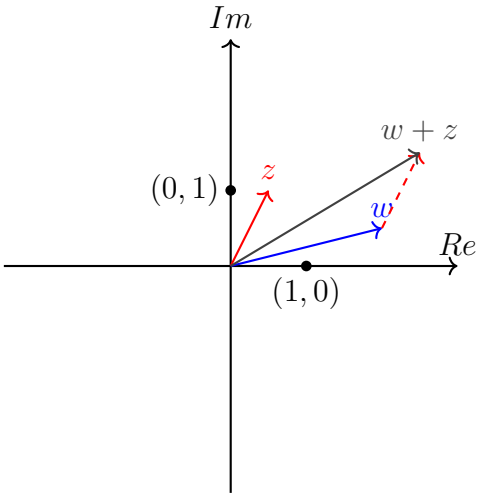
$$(a,b) * \left(\frac{a}{a^2 + b^2}, \frac{b}{a^2 + b^2}\right) = (1,0)$$

5.4 Caratteristiche

Un numero $z \in \mathbb{C} = a + bi, a, b \in \mathbb{R}$, e con $\mathbb{R}$ in intende $\mathbb{R}^2$ con le operazioni di somma e prodotto definite. La parte reale dei numeri complessi è definita da $Re(z) := a$ e la parte immaginaria $Im(z) := b$

5.5 Rappresentazione grafica

Scelto un sistema di coordinate cartesiano del piano, allora ad $a + bi \in C$, corrisponde un punto/vettore $P(a,b)$. Presi $z = a + bi, w = c + di$



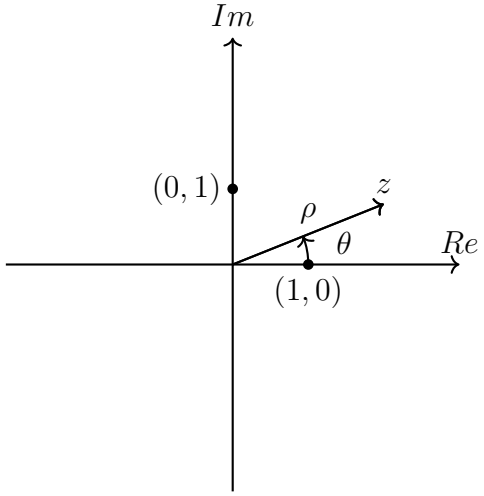
la somma tra due numeri $w, z \in \mathbb{C}$ equivale alla somma tra vettori.

Per il prodotto tra $z_1, z_2 \in \mathbb{C}$ bisogna definire il modulo di numero complesso:

$$|z| = \rho := \sqrt{a^2 + b^2}$$

e l'argomento di z:

$$Arg(z) = \theta, \text{ determinato a meno di sommare un multiplo intero di } 2\pi, z \neq 0$$



sapendo che le coordinate di z son (a, b), allora posso definirle in funzione di ρ, θ:

$$\begin{cases} a = \rho * \cos\theta \\ b = \rho * \sin\theta \end{cases} \Rightarrow z = \rho * \cos\theta + i\rho * \sin\theta = \rho(\cos\theta + i\sin\theta)$$

Allora presi: $z_1 = \rho_1(\cos\theta_1 + i\sin\theta_1), z_2 = \rho_2(\cos\theta_2 + i\sin\theta_2)$

$$z * w = \rho_1 * \rho_2(\cos\theta_1 + i\sin\theta_1) * (\cos\theta_2 + i\sin\theta_2) =$$

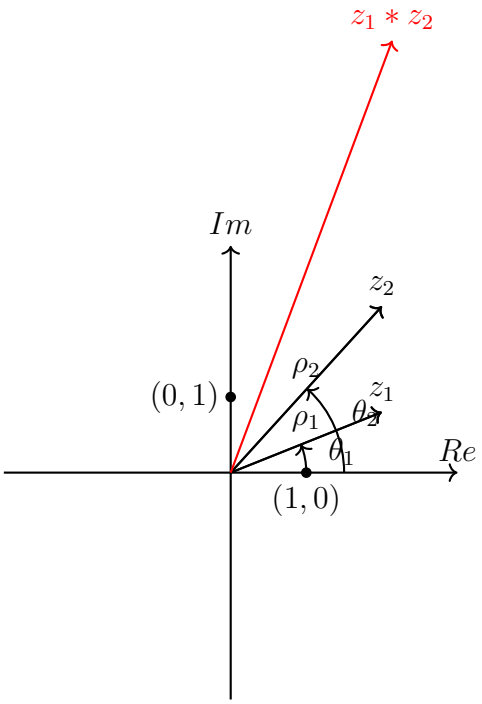
$$= \rho_1 * \rho_2(\cos\theta_1 * \cos\theta_2 - \sin\theta_1 * \sin\theta_2) + i(\cos\theta_1 * \sin\theta_2 + \sin\theta_1 * \cos\theta_2) =$$

$$= \rho_1 * \rho_2(\cos(\theta_1 + \theta_2) + i\sin(\theta_1 + \theta_2))$$

quindi:

$$\begin{cases} |z_1 * z_2| = |z_1| * |z_1| = \rho_1 * \rho_2 \\ Arg(z_1 * z_2) = Arg(z_1) + Arg(z_2) \end{cases}$$

$Arg(z_1 * z_2)$ è determinato a meno di un multiplo intero di 2π



moltiplicare un numero complesso per i, vuol dire ruotarlo di 90 gradi verso sinistra

5.6 Teorema fondamentale dell'algebra

Sia $P(z) = a_0 z^n + a_1 z^{n-1} + a_2 z^{n-2} + ... + a_n$, polinomio in z a coefficienti in $\mathbb{C}$ di grado $n > 0$ con $a_0 \neq 0$, allora:

$$\exists \xi \in \mathbb{C} \text{ t.c. } P(\xi) = 0$$

(ξ è una "radice di $P(z) = 0$")

T.F.A $\implies \exists \lambda_1, \lambda_2, ..., \lambda_n \in \mathbb{C}$ t.c. $P(z) = a_0(z - \lambda_1)(z - \lambda_2) * ... * (z - \lambda_n)$

Per via del teorema di Ruffini in quanto:

essendo λ_1 radice di $P(z) = 0 \to P(z) = (z - \lambda_1) * q(z)$, in cui il grado di $q(z)$ = grado di $P(z)$ - 1

Es:

$$p(z) = z^n - a$$

si cercano le radici di $z^n - a = 0$:

- $a = 0 \to z^n = 0$, la radice è unica con molteplicità n
- $a \neq 0$, se $n = 3$:

$$\begin{aligned} z &= \rho(\cos\theta + i\sin\theta) \\ z^n &= \rho(\cos n\theta + i\sin n\theta) \\ a &= \rho_0(\cos\theta_0 + i\sin\theta_0) \end{aligned}$$

$$z^n = a \iff \begin{cases} \rho^n = \rho_0 \to \rho = \sqrt[n]{\rho_0} \\ n\theta = \theta_0 \text{ a meno di multipli interi di } 2\pi \end{cases}$$

$$Arg(z = \sqrt[n]{a}) = \theta = \left\{ \frac{\theta_0}{n} + \frac{k2\pi}{n}, k \in \{0, 1, ..., n-1\} \right\}$$

6 Spazi vettoriali

$\mathbb{K}$ è un campo, $\mathbb{K}^n = \mathbb{K} \times \cdots \times \mathbb{K} = \{(x_1, \ldots, x_n) \text{ t.c. } x_i \in \mathbb{K}\}$, usato una notazione impropria possiamo definire la n-tupla $(x_1, \ldots, x_n)$, come X

Definiamo l'operazione di somma tra n-uple:

$$\begin{array}{ccc} \mathbb{K}^n \times \mathbb{K}^n & \xrightarrow{somma} & \mathbb{K}^n \\ (X, Y) & \longmapsto & (x_1 + y_1, \ldots, x_n + y_n) \end{array}$$

ed il prodotto per uno scalare:

$$\begin{array}{ccc} \mathbb{K} \times \mathbb{K}^n & \xrightarrow{prodotto} & \mathbb{K}^n \\ (\lambda, X) & \longmapsto & (\lambda x_1, \ldots, \lambda x_n) \end{array}$$

$\mathbb{K}^n$ con le proprietà definite è il prototipo di uno spazio vettoriale su $\mathbb{K}$.

Uno spazio vettoriale su $\mathbb{K}$ è definito come un insieme $\mathbb{V}$, provvisto di una operazione somma:

$$\begin{array}{ccc} \mathbb{V} \times \mathbb{V} & \xrightarrow{somma} & \mathbb{V} \\ (v, w) & \longmapsto & v + w \end{array}$$

e il prodotto per uno scalare:

$$\begin{array}{ccc} \mathbb{K} \times \mathbb{V} & \xrightarrow{prodotto} & \mathbb{V} \\ (\lambda, v) & \longmapsto & \lambda v \end{array}$$

tali che:

1. $\exists \underline{0} \in \mathbb{V}$ t.c. $\underline{0} + v = v, \forall v \in \mathbb{V}$
2. Dato $v \in \mathbb{V}, \exists w \in \mathbb{V}$ t.c. $v + w = \underline{0}$
3. $(v + w) + u = v + (w + u) \forall v, w, u \in \mathbb{V}$
4. $u + v = v + u, \forall u, v \in \mathbb{V}$
5. $1v = v$
6. $v(\lambda + \mu) = \lambda v + \mu v, \forall \lambda, \mu \in \mathbb{K}, \forall v \in \mathbb{V}$
7. $\lambda(v + w) = \lambda v + \lambda w, \forall \lambda \in \mathbb{K}, \forall v, w \in \mathbb{V}$
8. $(\lambda\mu)v = \lambda(\mu v), \forall \lambda, \mu \in \mathbb{K}, \forall u \in \mathbb{V}$

Osservazione, l'elemento neutro di $\mathbb{K}$ è diverso dall'elemento neutro di $\mathbb{V}$:

$$0 \in \mathbb{K} \neq \underline{0} \in \mathbb{V}$$

$$0 \neq (0, \ldots, 0)$$

Proposizione: $\mathbb{V}$ spazio vettoriale:

1. Esiste un unico elemento neutro di $\mathbb{V}$, dimostrazione:

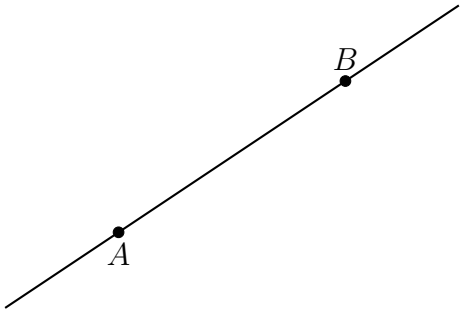
$$\underline{0}_1 + v = v \quad \wedge \quad \underline{0}_2 + v = v, \forall v \in \mathbb{V}$$

$$\underline{0}_2 = \underline{0}_1 + \underline{0}_2 = \underline{0}_1 \Rightarrow \underline{0}_1 = \underline{0}_2 = \underline{0}$$

2. Dato $v \in \mathbb{V}$ esiste un unico $w \in \mathbb{V}$ t.c. $v + w = \underline{0}$
3. $0 \cdot v = \underline{0}$

6.1 Vettori nel piano euclideo

Sia $\mathbb{E}^2$, un piano euclideo, allora un vettore nel piano è una classe di equivalenza di segmenti ordinato nel piano. Se $A \neq B \in \mathbb{E}^2$, $\overline{AB}$ è l'unica retta passante in $\mathbb{E}^2$ contenente A e B.



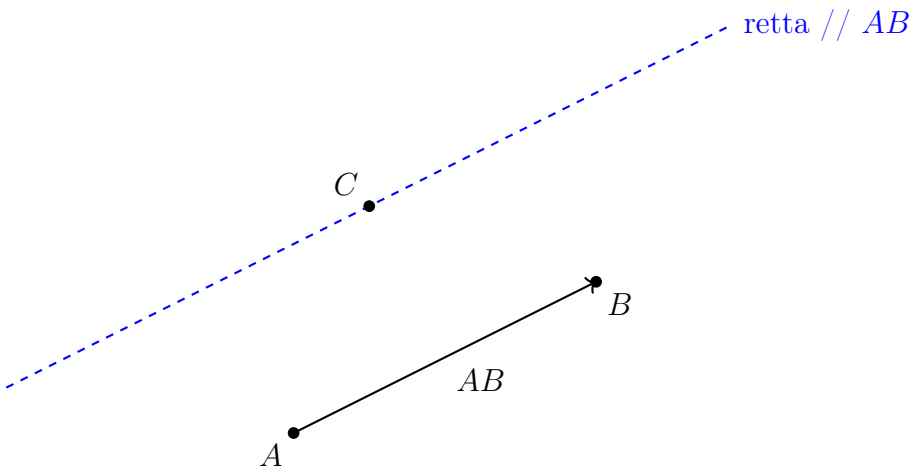
- Due rette R_1, R_2 in $\mathbb{E}^2$ sono parallele se: $\begin{cases} R_1 \cap R_2 = \emptyset \\ R_1 = R_2 \end{cases}$
- A, B, C, D in $\mathbb{E}^2$ $\overline{AB} \parallel \overline{CD}$, significa che:

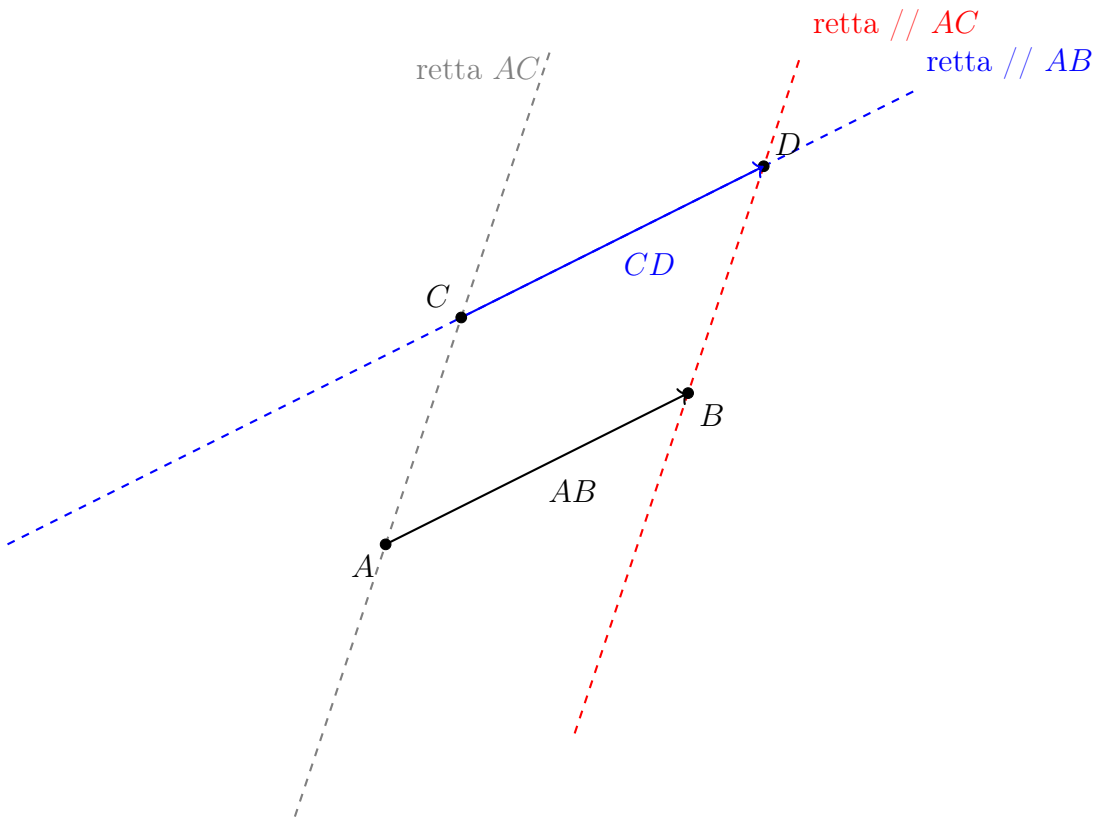
$$\begin{cases} A \neq B, C \neq D, \text{ quindi le retta } \overline{AB} \text{ e } \overline{CD} \text{ sono parallele} \\ A = B \vee C = D \end{cases}$$

Un segmento orientato in $\mathbb{E}^2$ è una coppia ordinata $(A, B) = \mathbb{E}^2 \times \mathbb{E}^2$, con $A, B \in \mathbb{E}^2$, si definisce $AB = (A, B)$

Due segmenti orientati AB, CD si dicono equipollenti se:

$$AB \parallel CB, \overline{AC} \parallel \overline{BD}$$





- ogni segmento orientato è equipollente a se stesso
- se S_1 è equipollente a $S_2 \Rightarrow S_2$ è equipollente S_1
- se S_1 è equipollente a S_2 e S_2 è equipollente a S_3, allora S_1 è equipollente a S_3

Perciò l'equipollenza è una relazione di equivalenza, definita da: $\sim$.

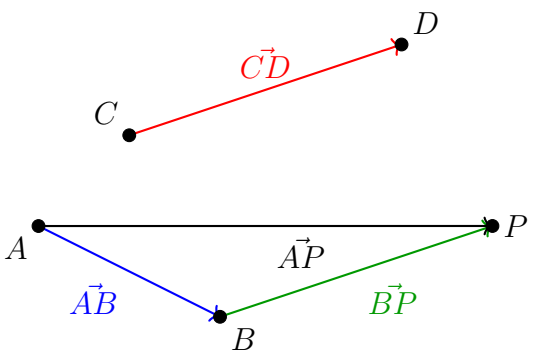
$$V(\mathbb{E}^2) := (\mathbb{E}^2 \times \mathbb{E}^2)/\sim$$
$$\vec{AB} := [AB]$$

quindi vuol dire il prodotto cartesiano tra i segmenti ordinati equipollenti, rappresentati dalle coppie ordinate.

Definisco la somma:

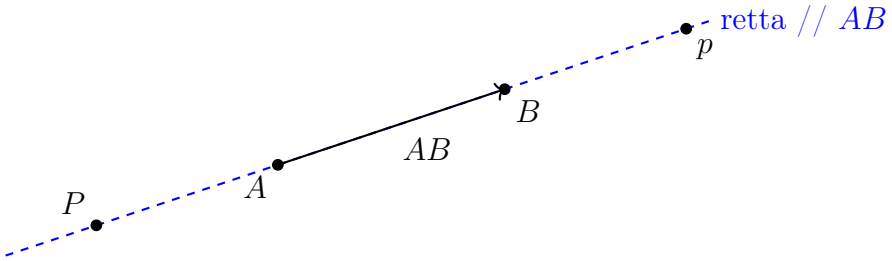
$$\begin{array}{ccc} \mathbb{V}(\mathbb{E}^2) \times \mathbb{V}(\mathbb{E}^2) & \xrightarrow{somma} & \mathbb{V}(\mathbb{E}^2) \\ (\vec{AB}, \vec{CD}) & \longmapsto & \vec{AP} \end{array}$$

Presi due vettori $\vec{AB}, \vec{CD}, \exists P \in \mathbb{E}^2$ t.c. $\vec{BP} \sim \vec{CD}$



Definisco il prodotto per uno scalare $\mathbb{R}$:

$$\begin{array}{ccc} \mathbb{R} \times \mathbb{V}(\mathbb{E}^2) & \xrightarrow{prodotto} & \mathbb{V}(\mathbb{E}^2) \\ (\lambda, \mathbb{V}(\mathbb{E}^2)) & \longmapsto & \vec{AP} \end{array}$$



$$\vec{AP} = \lambda * \vec{AB}, \lambda < 0$$
$$\vec{Ap} = \lambda * \vec{AB}, \lambda > 0$$

Con queste operazioni $V(\mathbb{E}^2)$ è uno spazio vettoriale/$\mathbb{R}$

7 V sp.vett/$\mathbb{K}$

Un sottoinsieme $\mathbb{W} \subset \mathbb{V}$ è un sottospazio se non è vuote e se:

- a) è chiuso per la somma:

$$v_1, v_2 \in \mathbb{W} \Rightarrow v_1 + v_2 \in \mathbb{W}$$

- a) è chiuso per il prodotto per scalare:

$$w \in \mathbb{W}, \lambda \in \mathbb{K} \Rightarrow \lambda w \in \mathbb{W}$$

Osservazione: Sia $\mathbb{W} \subset \mathbb{V}$ è un sottospazio:

- $\underline{0} \in \mathbb{W}$
- $w \in \mathbb{W} \Rightarrow (-1)w \in \mathbb{W}$, per la proposizione b
- $w \in \mathbb{W}, (-1)w \in \mathbb{W} \Rightarrow 1w + (-1)w = w(1-1) = 0w = \underline{0}$, per la proposizione a

Sia $\mathbb{W} \subset \mathbb{K}^n$, un sottospazio, dato da:

$$\mathbb{W} := \{X \in \mathbb{K}^n \text{ t.c. } x_1 + \cdots + x_n = 0\}$$

allora:

- $\underline{0} \in \mathbb{W}$
- $\mathbb{W}$ è chiuso per la somma
- $\mathbb{W}$ è chiuso per il prodotto per uno scalare

Sia $\mathbb{U} \subset \mathbb{K}^n$, un sottospazio, dato da:

$$\mathbb{U} := \{X \in \mathbb{K}^n \text{ t.c. } x_1 + \cdots + x_n = 1\}$$

allora non è un sottospazio di $\mathbb{K}$, perchè $\underline{0} \notin \mathbb{V}$