Appunti di Geometria

Liam Ferretti

18 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:

$$X_i := \{m \in \mathbb{Z} \text{ t.c. } i|m\}$$

L'unione degli insiemi X_i è l'insieme X t.c. $x \in X \iff \exists i \in I$ t.c. $x \in X_i$

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

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:

$$X_i := \{m \in \mathbb{Z} \text{ t.c. } i|m\}$$

L'intersezione degli insiemi X_i è l'insieme X t.c. $x \in X \iff \forall i \in I, \exists x \in X_i$

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

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 $x \in X, y \in Y$.

$$X = Y = \mathbb{R} \to \mathbb{R} \times \mathbb{R} := \{(x, y) \text{ t.c. } x, y \in \mathbb{R}\}$$

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

Se si hanno più insiemi:

$$X_1 \times X_2 \times X_3 \times ... \times X_n := \{(x_1, x_2, x_3, ..., x_n) \text{ t.c. } x_n \in X_n \acute{I}\}$$

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 dall'insieme X all'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:

$$X \xrightarrow{f} Y$$

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

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

$$\text{Im}f := \{y \in Y \text{ t.c. } \exists x \in X \text{ t.c. } f(x) = y\}$$

OSS: f è suriettiva $\iff$ Im$f = Y$

2.6 Biettività

Presi due insiemi X, Y e una applicazione f:

$$X \xrightarrow{f} Y$$

$$f \text{ è biunivoca } \iff \forall y \in Y, \exists! x \in X \text{ t.c. } f(x) = y$$

(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:

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

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 $y \in Y \rightarrow f^{-1}(y) := \{x \in X \text{ t.c. } f(x) = y\}$, 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 t.c. $f(x) = y$ si otterrà come risultato l'insieme numerico che contiene tutte le x

3 Relazioni

Preso X un insieme, una relazione R su X, è un sottoinsieme definito come:

$$R \subset X^2 = X \times X$$

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

Es 1:

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

$$R = \{(x, y) \text{ t.c. x e y sono coetanei}\}$$

$$xRy \rightarrow (x, y) \in R \rightarrow \text{x e y sono coetanei}$$

Es 2:

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

$$R_n = \{(x, y) \text{ t.c. } n|(x - y), x, y \in X\} = x \equiv y \pmod{n}$$

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

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

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

fissato x, $[x]$ è l'insieme composto 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 2:

$$X/R_n := \{[0], [1], [2], ..., [n-1]\}$$

e ogni elemento ad esempio [1], ha la proprio classe di equivalenza:

$$[1] = \{y \in X \text{ t.c. } 1Ry, 1 \equiv y \pmod{n}\}$$

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:

$$P(S) := \{\{1,2,3\}, \{\{1,2\},\{3\}\}, \{1,\{2,3\}\}, \{\{1,3\},\{2\}\}, \{\{1\},\{2\},\{3\}\}\}$$

Partendo da una relazione di equivalenza R su X, $S := X/R$, con $x \in X$:

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

allora, una partizione di S è definita come:

$$P(S) := \{[x] \text{ t.c. } x \in X\}$$

quindi una partizione di S, l'insieme quoziente X/Rè l'insieme che contiene tutte le classi di equivalenza disgiunte.
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 $R \longrightarrow P_{R_{\{[x]\}}}$
Per ogni partizione $P \longrightarrow R_P$

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

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:

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

$$m * l = 0 \pmod{n}$$

se $\exists \frac{1}{m} \to \frac{1}{m} * m * l = 0 \Rightarrow l = 0$, 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:

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

Il termine py scompare in quanto applicando il modulo p all'insieme, rendendolo un insieme quoziente, py, è uguale a 0.

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:

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

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

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:

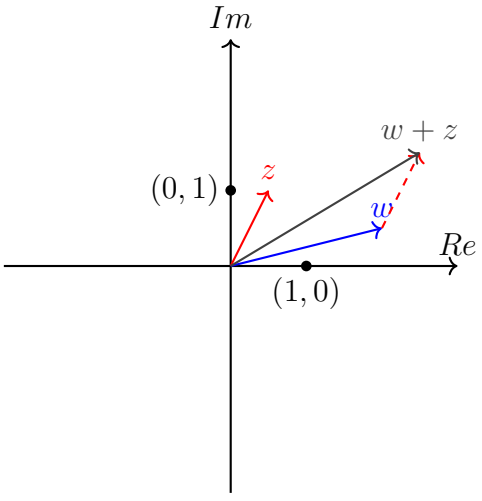
$$(a,b) * \left(\frac{a}{a^2 + b^2}, \frac{b}{a^2 + b^2}\right) = (1,0)$$

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, quindi esegui una normale somma tra le componenti:

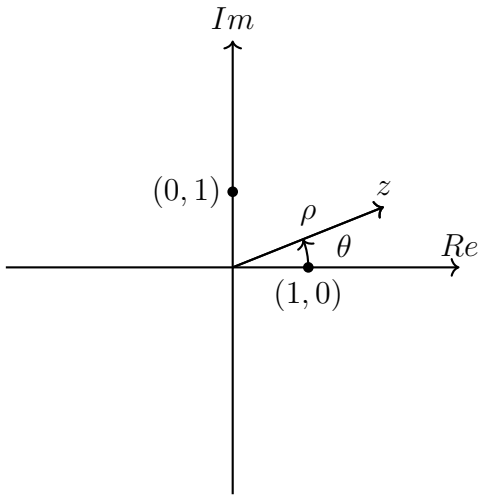
$$z = a + bi = (a, b), w = c + di = (c, d) \Rightarrow z + w = (a, b) + (c, d) = (a + c, b + d)$$

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 un numero complesso:

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



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

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

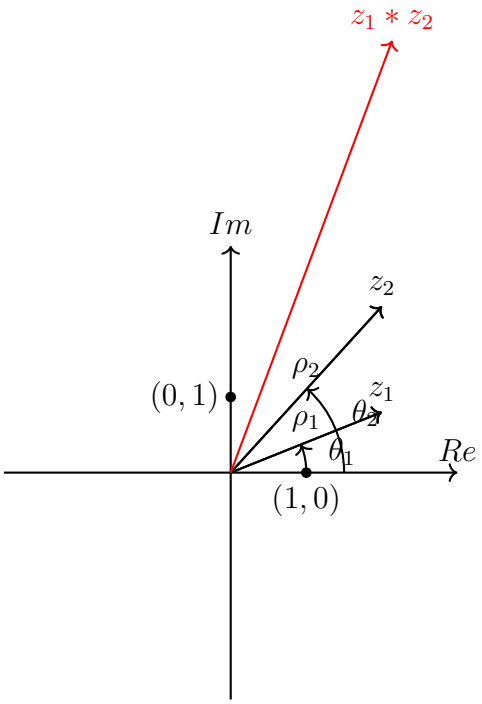
$$= \rho_1 * \rho_2(\cos\theta_1 * \cos\theta_2 - \sin\theta_1 * \sin\theta_2) + i(\cos\theta_1 * \sin\theta_2 + \sin\theta_1 * \cos\theta_2) =$$

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

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-tuple:

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

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

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

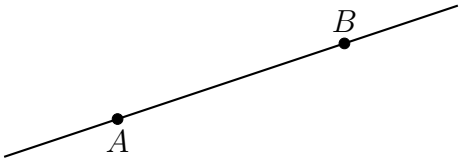
$$\underline{0}_1 + v = v \quad \wedge \quad \underline{0}_2 + v = v, \forall v \in \mathbb{V}$$

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

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 $\mathbb{E}^2$, il piano euclideo, allora un vettore nel piano è una classe di equivalenza di segmenti orientati nel piano, indipendenti dalla loro posizione. Presi $A, (x_a, y_a) \neq B, (x_b, y_b) \in \mathbb{E}^2, \overline{AB}$ è l'unica retta in $\mathbb{E}^2$ contenente contemporaneamente A e B.



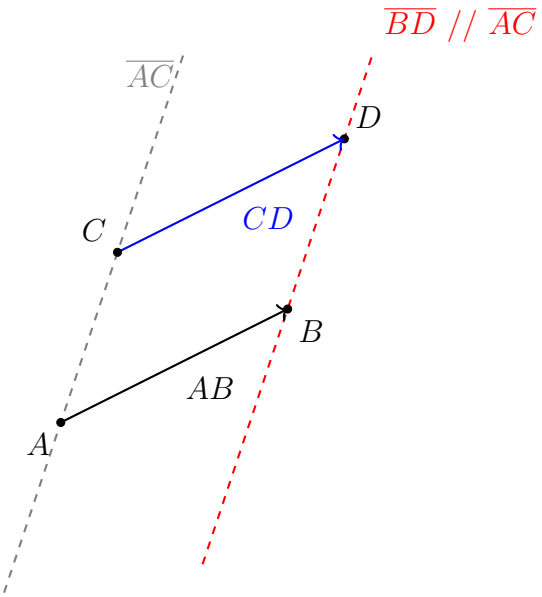
- Due rette R_1, R_2 in $\mathbb{E}^2$ sono parallele se: $\begin{cases} R_1 \cap R_2 = \emptyset \\ R_1 = R_2 \end{cases}$
- Presi i punti: $A, B, C, D \in \mathbb{E}^2, \overline{AB} \parallel \overline{CD}$, significa che:

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

Un segmento orientato in $\mathbb{E}^2$ è una coppia ordinata $(A, B) = ((x_a, y_a), (x_b, y_b)) = \mathbb{E}^2 \times \mathbb{E}^2$, con $A, B \in \mathbb{E}^2$ e si definisce per semplicità come $AB := (A, B)$

Due segmenti orientati AB, CD si dicono equipollenti se:

$$AB \parallel CB \text{ e } \overline{AC} \parallel \overline{BD}$$



- 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: $\sim$.

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

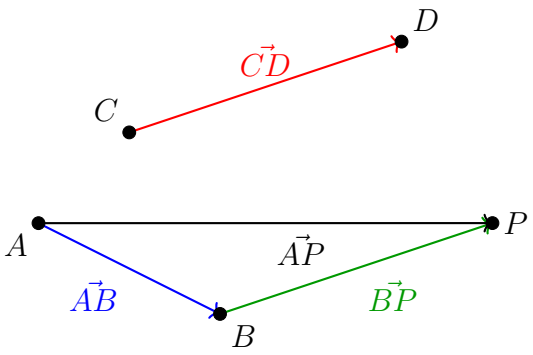
$$\vec{AB} := [AB]$$

quindi $V(\mathbb{E}^2)$ è l'insieme quoziente, definito dalla equipollenza, una relazione di equivalenza, perciò i suoi elementi sono tutte le classi di equivalenza contenenti tutti i possibili vettori con la stessa direzione e lunghezza, perciò l'insieme $V(\mathbb{E}^2)$ contiene tutti i possibili vettori nel piano euclideo, ed ogni classe di equivalenza si rappresenta come un rappresentate scelto con una freccia sopra, per definire la direzione.

Definisco la somma in $V(\mathbb{E}^2)$:

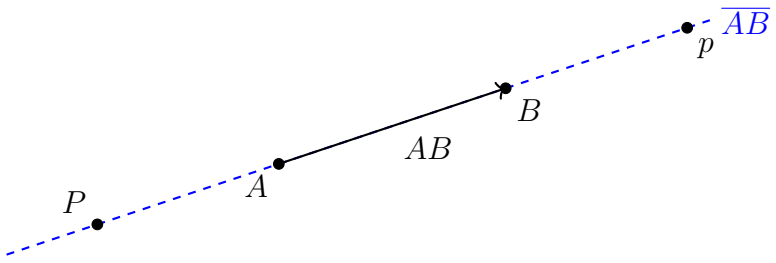
$$\begin{array}{ccc} \mathbb{V}(\mathbb{E}^2) \times \mathbb{V}(\mathbb{E}^2) & \xrightarrow{somma} & \mathbb{V}(\mathbb{E}^2) \\ (\vec{AB}, \vec{CD}) & \longmapsto & \vec{AP} \end{array}$$

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/$\mathbb{R}$

6.2 Sottospazi vettoriali

Preso $\mathbb{V}$ un sp.vett./$\mathbb{K}$, allora $\mathbb{W} \subset \mathbb{V}$ è un sottospazio vettoriale se:

- non è vuoto, quindi:

$$\mathbb{W} \neq \emptyset$$

- a) è chiuso per la somma:

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

- b) 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:

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

Sia $\mathbb{W} \subset \mathbb{K}^n$, un sottoinsieme, 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

allora $\mathbb{W}$ è un sottospazio.
Sia $\mathbb{U} \subset \mathbb{K}^n$, un sottoinsieme, 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 $\underline{0} \notin \mathbb{U}$

6.3 Polinomi su $\mathbb{K}$

Un polinomio su $\mathbb{K}$ nella variabile x è espresso come:

$$a_0x^d + a_1x^{d-1} + \cdots + a_{d-1}x + a_d, a_i \in \mathbb{K}$$

$$\mathbb{K}[x] := \{\text{polinomi in x a coefficienti in } \mathbb{K}\}$$

La somma tra polinomi in $\mathbb{K}$ si ottiene sommando i coefficienti:

$$(x^3 + x + 1) + (x^2 - 4x + 3) = x^3 + x^2 - 3x + 4$$

Il prodotto, moltiplicando i coefficienti e sommando i gradi delle x:

$$(x^3 + x + 1)(x^2 - 4x + 3) = x^5 - 4x^4 + 4x^3 - 3x^2 - x + 3$$

$\mathbb{K}[x]$ con le operazioni definite è un anello, in cui l'elemento neutro è il polinomio 0, e l'unità moltiplicativa è il polinomio 1.

Sia $p \in \mathbb{K}[x]$ un polinomio a coefficienti in $\mathbb{K}[x]$, del tipo $a_0x^d + a_1x^{d-1} + \cdots + a_{d-1}x + a_d, a_i \in \mathbb{K}$, definiamo una applicazione:

$$\begin{array}{ccc} \mathbb{K} & \xrightarrow{F_p(\text{ funzione polinomiale})} & \mathbb{K} \\ c & \longmapsto & p(c) \end{array}$$

$$p(c) = a_0c^d + a_1c^{d-1} + \cdots + a_{d-1}c + a_d, a_i \in \mathbb{K}$$

Dove $F_p := \mathbb{Z}/p$, è un campo.
Se $||\mathbb{K}|| = +\infty$ e si hanno due polinomi $p, q \in \mathbb{K}$, allora:

$$F_p = F_q \Longrightarrow p = q$$

Se $||\mathbb{K}|| < +\infty$ allora non è vero.

Esempio: consideriamo $F_2[x]$

$$F_2[x] := \{[0], [1]\}$$

$$\phi = (x^2 + x) \in F_2[x]$$

F_2	F_2
0	$\phi(0) = 0$
1	$\phi(0) = 0$

6.3.1 Anello polinomiale

Considerato l'anello polinomiale di un certo campo, $\mathbb{K}[x]$, con la somma tra polinomi:

$$\begin{array}{ccc} \mathbb{K}[x] \times \mathbb{K}[x] & \xrightarrow{\text{somma}} & \mathbb{K}[x] \\ (p, q) & \longmapsto & p + q \end{array}$$

e prodotto per costante:

$$\begin{array}{ccc} \mathbb{K} \times \mathbb{K}[x] & \xrightarrow{\text{prodotto}} & \mathbb{K}[x] \\ (\lambda, q) & \longmapsto & \lambda p \end{array}$$

con queste operazioni $\mathbb{K}[x]$ è uno sp. vett./$\mathbb{K}$, allora:

$$\mathbb{K}[x]_{\leq d \geq 0} := \{a_0x^d + a_1x^{d-1} + \cdots + a_d \text{ t.c. } a_i \in \mathbb{K}\} \subset \mathbb{K}[x]$$

è un sotto spazio vettoriale di $\mathbb{K}[x]$ in cui la somma tra due polinomi di grado al più d, da come risultato un polinomio di grado al più d, invece il prodotto tra una costante ed un polinomio mantiene il grado massimo.

Osservazione:

Sia $\{\mathbb{W}_i\}_{i \in I}$ una collezione di sottospazi di $\mathbb{V}$, allora :

$$\bigcap_{i \in I} \mathbb{W}_i$$

è un sottospazio vettoriale di $\mathbb{V}$
Dimostrazione:

- dato che $\underline{0} \in \mathbb{W}_i, \forall i \in I \Rightarrow 0 \in \bigcap_{i\in I} \mathbb{W}_i$
- se $w_1, w_2 \in \bigcap_{i\in I} \mathbb{W}_i \rightarrow w_1, w_2 \in \mathbb{W}_i, \forall i \in I$ quindi $(w_1 + w_2) \in \mathbb{W}_i, \forall i \in I \Rightarrow (w_1 + w_2) \in \bigcap_{i\in I} \mathbb{W}_i$

Esempio: Abbiamo visto che se $a_1, a_2, \ldots, a_n \in \mathbb{K}$, allora:

$$\{X \in \mathbb{K}^n \text{ t.c. } (a_1x_1 + a_2x_2 + ...a_nx_n) = 0\}$$

per la proposizione iniziale, l'insieme delle soluzioni $(x_1, x_2, \ldots, x_n)$ del sistema di equazioni lineari omogenee:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = 0 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = 0 \end{cases}$$

è un sottospazio vettoriale di $\mathbb{K}^n$, ed equivale all'intersezione tra le soluzioni delle singole equazioni.

7 Combinazioni lineari

Presi $v_1, v_2, \ldots, v_n \in \mathbb{V}$, allora $v \in \mathbb{V}$ è una combinazione lineare di $v_1, \ldots, v_n$, se esistono $\lambda_1, \ldots, \lambda_n$, tali per cui:

$$v = \lambda_1 v_1 + \cdots + \lambda_n v_n$$

Esempio 1: presi

$$\underline{e}_1 := (1, 0, 0, \ldots, 0) \in \mathbb{K}^n$$
$$\underline{e}_2 := (0, 1, 0, \ldots, 0) \in \mathbb{K}^n$$
$$\vdots$$
$$\underline{e}_n := (0, 0, 0, \ldots, n) \in \mathbb{K}^n$$

allora ogni vettore $X \in \mathbb{K}^n$ è una combinazione lineare di $\underline{e}_1, \underline{e}_2, \ldots, \underline{e}_n$, quindi:

$$X = \lambda_1\underline{e}_1 + \cdots + \lambda_n\underline{e}_n = (x_1, \ldots, x_n)$$

rendendo ogni $x_i = \lambda_i$:

$$X = x_1\underline{e}_1 + \cdots + x_n\underline{e}_n$$

Esempio 2: Quali vettori in $\mathbb{K}^3$ sono combinazioni lineari di $\underline{e}_1, \underline{e}_2$?

$$(x_1, x_2, x_3) = \lambda_1\underline{e}_1 + \lambda_2\underline{e}_2 = (\lambda_1, \lambda_2, 0) \Rightarrow x_1 = \lambda_1, x_2 = \lambda_2, x_3 = 0$$

Esempio generale, quali vettori in $\mathbb{K}^3$ sono combinazioni lineari di:

$$v := (a_1, a_2, a_3), W := (b_1, b_2, b_3)$$

$(c_1, c_2, c_3) = C \in \mathbb{K}^3$ è combinazione lineare di V e $W \iff$ esiste una soluzione (λ_1, λ_2) del sistema di equazioni lineari:

$$\begin{cases} a_1\lambda_1 + b_1\lambda_2 = c_1 \\ a_2\lambda_1 + b_2\lambda_2 = c_2 \\ a_3\lambda_1 + b_3\lambda_2 = c_3 \end{cases}$$

dove λ_n sono le incognite. Posso quindi scrivere che $C = \lambda_1 v + \lambda_2 w$

8 Sottospazi generati

Preso $\mathbb{S} \subset \mathbb{V}$, allora il sottospazio di $\mathbb{V}$ generato da $\mathbb{S}$ è:

$$\langle \mathbb{S} \rangle := \{\lambda_1 v_1 + \dots \lambda_n v_n \text{ t.c. } v_1, \dots, v_n \in \mathbb{S}, \lambda_1, \dots, \lambda_n \in \mathbb{K}\}$$

ovvero, il sottospazio generato da $\mathbb{S}$ è l'insieme di tutte le combinazioni lineari di vettori presi da $\mathbb{S}$, è il più piccolo sottospazio di $\mathbb{V}$ che contiene i vettori da v_1 a v_n, e se l'insieme $\mathbb{S}$ è vuoto, allora, $\langle \emptyset \rangle = \{\underline{0}\}$
Dimostrazione che $\langle S \rangle$ sia effettivamente un sottospazio:

- $\underline{0} \in \mathbb{S}$ perchè?

  Se $\mathbb{S} = \emptyset \Rightarrow \langle \mathbb{S} \rangle = \{\underline{0}\}$

  se invece $\mathbb{S} \neq \emptyset$, allora $v \in \mathbb{S} \rightarrow v \in \mathbb{S} \rightarrow 0v = \underline{0} \in \mathbb{S} \Rightarrow \underline{0} \in \langle \mathbb{S} \rangle$

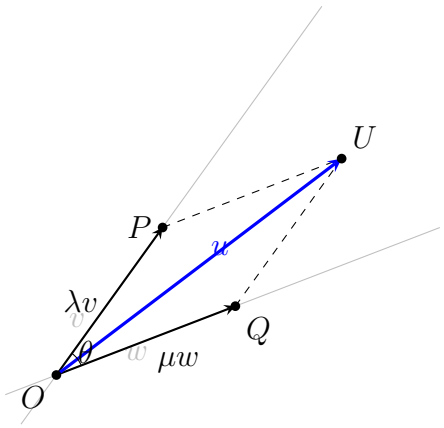
- siano $v, w \in \langle \mathbb{S} \rangle, v = \lambda_1 v_1 \cdots + \lambda_n v_n, w = \mu_1 w_1 + \cdots + \mu_n w_n$, con $v_1, \dots, v_n, w_1, \dots, w_n \in \mathbb{S}$

- verificare prodotto rispetto a scalare

Notazione:

- $S := \{v_1, v_2, \dots, v_n\}$
- $\langle v_1, \dots, v_n \rangle = \langle \{v_1, \dots, v_n\} \rangle$

Definito $V = V(\mathbb{E}^2)$, allora:



$$\vec{OP} = \lambda v, \quad \vec{OQ} = \mu w$$
$$u = \vec{OP} + \vec{OQ} = \vec{OU}$$

$\langle v \rangle = \lambda_1 v$ si intendono tutti i vettori paralleli alla retta r, e con origine in 0 .
$\langle v, w \rangle = \lambda_1 v + \lambda_2 w = V(\mathbb{E})$, se i due vettori sono linearmente indipendenti, ovvero non paralleli, quindi ogni vettore nel piano euclideo può essere rappresentato come una combinazione lineare tra v e w, se invece i due vettori fossero paralleli, il sottospazio generato sarebbe uguale al sottospazio generato da uno solo dei due vettori.

Osservazione:

$$S \subset T \subset V \Rightarrow \langle S \rangle \subset \langle T \rangle$$

8.1 Sottospazio finitamente generato

V è finitamente generato se:

$$\exists v_1, \ldots, v_n \text{ t.c. } \langle v_1, \ldots, v_n \rangle = V$$

quindi si dice che V è finitamente generato se esistono finiti vettori tali per cui il sottospazio generato dalle loro combinazioni lineari genera lo spazio vettoriale V.

Ad esempio $\mathbb{K}^n$ è finitamente generato perchè può essere ottenuto attraverso le combinazioni lineari di $\underline{e}_1, \ldots, \underline{e}_n$, quindi $\langle \underline{e}_1, \ldots, \underline{e}_n \rangle = \mathbb{K}^n$

Invece $\mathbb{K}[x]$, ovvero l'anello polinomiale, non è finitamente generato, infatti se $p_1, \ldots, p_n \in \mathbb{K}^n$, allora ogni $q \in \langle p_1, \ldots, p_n \rangle$ ha grado al più il massimo del $\deg p_1, \ldots, \deg p_n$

In quanto:

$$\langle p_1, \ldots, p_n \rangle = \lambda_1 p_1 + \lambda_2 p_2 + \cdots + \lambda_n p_n$$

sommando dei polinomi moltiplicati per una certa costante, non permette di aumentare il grado del polinomio.

Se $V(\mathbb{E}^2)$ è finitamente generato, allora ogni sottospazio di $V(\mathbb{E}^2)$ è finitamente generato.

Ad esempio: in sistema di m equazioni lineari omogenee in n incognite, l'insieme delle soluzioni è un sottospazio vettoriale di $\mathbb{K}^n$, allora W è finitamente generato.

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = 0 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = 0 \end{cases}$$

9 Lista di vettori

Per lista di vettori di $\mathbb{V}$ si intende un insieme ordinato di elementi univoci, e può essere descritta da una funzione:

$$f : \mathbb{I} \longrightarrow \mathbb{V}, \mathbb{I} = [n], n \in N$$
$$f : f(i) = \mathbb{V}_i$$
$$f : \{V_i\}_{i \in \mathbb{I}}$$

9.1 Lista di generatori

Una lista di vettori, $v_1, \ldots, v_n$, si dice generatrice se:

$$\forall v \in \mathbb{V}, \exists x_1, \ldots, x_n \text{ t.c. } v = \sum_{i=1}^{n} x_i v_i = x_1 v_1 + x_2 v_2 + \cdots + x_n v_n$$

Quindi i vettori di una lista si dicono generatori se ogni vettore di $\mathbb{V}$ può essere ottenuto per combinazione lineare dei vettori appartenenti alla lista.

Ad esempio, in $\mathbb{R}^2$:

- $\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix} \to \begin{pmatrix}a\\b\end{pmatrix} = a\begin{pmatrix}1\\0\end{pmatrix} + b\begin{pmatrix}0\\1\end{pmatrix}$

  quindi in questo caso ho solo un modo per scrivere un vettore $\begin{pmatrix}a\\b\end{pmatrix}$, la lista quindi è generatrice e genera i vettori in modo univoco

- $\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}-1\\1\end{pmatrix} \rightarrow \begin{pmatrix}a\\b\end{pmatrix} = (a-b)\begin{pmatrix}1\\0\end{pmatrix} + b\begin{pmatrix}1\\1\end{pmatrix} = (a+b)\begin{pmatrix}1\\0\end{pmatrix} + b\begin{pmatrix}-1\\1\end{pmatrix}$

  in questo caso la lista è sempre generatrice, ma ho più modi per scrivere lo stesso vettore, e ciò deriva dal fatto che non sono **linearmente indipendenti**, infatti:

$$\begin{pmatrix}-1\\1\end{pmatrix} = \begin{pmatrix}1\\1\end{pmatrix} - 2\begin{pmatrix}1\\0\end{pmatrix}$$

Quindi una lista è generatrice se per ogni vettore v, esiste almeno una scelta di $x_1, \ldots, x_n$, che soddisfa la relazione di dipendenza lineare di indice v.

9.2 Lista di vettori linearmente indipendenti

Una lista di vettori, $v_1, \ldots, v_n$, si dice **linearmente indipendente** se l'unica soluzione dell'equazione di dipendenza lineare:

$$x_1 v_1 + \cdots + x_n v_n = 0$$

è la soluzione banale, cioè quella in cui tutti i coefficienti sono nulli:

$$x_1 = x_2 = \cdots = x_n = 0$$

In tal caso:

$$0v_1 + 0v_2 + \cdots + 0v_n = 0$$

che rappresenta l'**equazione banale**.

Se invece esiste una combinazione non banale (cioè con almeno un coefficiente $x_i \neq 0$) che dà lo zero vettoriale, allora la lista si dice linearmente dipendente.

Ad esempio, in $\mathbb{R}^3$

- $\begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\end{pmatrix} \rightarrow \begin{pmatrix}0\\0\\0\end{pmatrix} = x_1\begin{pmatrix}1\\0\\0\end{pmatrix} + x_2\begin{pmatrix}0\\1\\0\end{pmatrix} + x_3\begin{pmatrix}0\\0\\1\end{pmatrix} \Rightarrow x_1 = x_2 = x_3 = 0$

  Sono quindi linearmente indipendenti, ed inoltre sono generatori, in quanto è possibile ottenere ogni vettore di $\mathbb{R}^3$ attraverso una combinazione lineare di questi 3 vettori.

  Questa lista di vettori è detta la forma canonica/standard di $\mathbb{R}^3$, in quanto è la lista più "semplice" a generare tutto l'insieme.

- $\begin{pmatrix}1\\0\\1\end{pmatrix}, \begin{pmatrix}1\\2\\1\end{pmatrix}, \begin{pmatrix}1\\1\\1\end{pmatrix} \rightarrow \begin{pmatrix}0\\0\\0\end{pmatrix} = 2\begin{pmatrix}1\\1\\1\end{pmatrix} - \begin{pmatrix}1\\0\\1\end{pmatrix} - \begin{pmatrix}1\\2\\1\end{pmatrix} \Rightarrow x_1 = 2, x_2 = x_3 = -1.$

  Quindi questa lista di vettori non è linearmente indipendente, ed inoltre è possibile scrivere il secondo vettore come combinazione lineare degli altri due:

$$\begin{pmatrix}1\\2\\1\end{pmatrix} = 2\begin{pmatrix}1\\1\\1\end{pmatrix} - \begin{pmatrix}1\\0\\1\end{pmatrix}$$

  In questo caso, i vettori $(1,1,1), (1,0,1)$, generano un piano, che contiene il vettore $(1,2,1)$.

Quindi una lista è linearmente indipendente se per ogni vettore v, esiste al massimo una scelta di $x_1, \ldots, x_n$, che soddisfa la relazione di dipendenza lineare di indice v.

Se una lista di vettori è linearmente indipendente, allora ogni sottolista è linearmente indipendente.

9.3 Lista di vettori base

Una lista di vettori, $v_1, \ldots, v_n$, è una base se la lista è allora stesso tempo:

(i) composta da vettori generatori.

(ii) linearmente indipendente.

Esempio:

- $\begin{pmatrix}1\\0\\1\end{pmatrix}, \begin{pmatrix}1\\1\\1\end{pmatrix}$

  Controllo che siano linearmente indipendenti:

  $$\begin{pmatrix}0\\0\\0\end{pmatrix} = x_1 \begin{pmatrix}1\\0\\1\end{pmatrix} + x_2 \begin{pmatrix}1\\1\\1\end{pmatrix} = \begin{pmatrix}x_1 + x_2\\x_2\\x_1 + x_2\end{pmatrix} \Rightarrow x_2 = 0, x_1 + x_2 = 0 \Rightarrow x_1 = x_2 = 0$$

  L'unico modo in cui si può ottenere il vettore 0 è se $x_1 = x_2 = 0$, quindi la soluzione all'equazione di dipendenza lineare è l'equazione banale, quindi sono linearmente indipendenti.

  Controllo che sia una lista generatrice:

  $$\begin{pmatrix}1\\0\\0\end{pmatrix} = x_1 \begin{pmatrix}1\\0\\1\end{pmatrix} + x_2 \begin{pmatrix}1\\1\\1\end{pmatrix} = \begin{pmatrix}x_1 + x_2\\x_2\\x_1 + x_2\end{pmatrix}$$

  Da cui deriva:

  $$\begin{cases}x_1 + x_2 = 1\\x_2 = 0\\x_1 + x_2 = 0\end{cases}$$

  Il sistema è inconsistente in quanto $x_1 + x_2$ deve fare 1 e 0 allo stesso tempo, quindi questo vettore non è ottenibile come combinazione lineare degli elementi nella lista, quindi:

  $$\begin{pmatrix}1\\0\\0\end{pmatrix} \notin \langle \begin{pmatrix}1\\0\\1\end{pmatrix}, \begin{pmatrix}1\\1\\1\end{pmatrix} \rangle$$

- $\begin{pmatrix}1\\0\\1\end{pmatrix}, \begin{pmatrix}1\\1\\1\end{pmatrix}, \begin{pmatrix}1\\2\\1\end{pmatrix}, \begin{pmatrix}1\\0\\0\end{pmatrix}$

  Controllo che siano linearmente indipendenti, e non lo sono in quanto posso scrivere il terzo vettore come combinazione lineare dei primi 2:

  $$\begin{pmatrix}1\\2\\1\end{pmatrix} = 2 \begin{pmatrix}1\\1\\1\end{pmatrix} - \begin{pmatrix}1\\0\\1\end{pmatrix}$$

Dato che il vettore $\begin{pmatrix}1\\2\\1\end{pmatrix}$ può essere scritto come combinazione lineare, allora lo spazio generato dalla lista iniziale è equivalente a:

$$\langle \begin{pmatrix}1\\0\\1\end{pmatrix}, \begin{pmatrix}1\\1\\1\end{pmatrix}, \begin{pmatrix}1\\2\\1\end{pmatrix}, \begin{pmatrix}1\\0\\0\end{pmatrix} \rangle = \langle \begin{pmatrix}1\\0\\1\end{pmatrix}, \begin{pmatrix}1\\1\\1\end{pmatrix}, \begin{pmatrix}1\\0\\0\end{pmatrix} \rangle$$

Ora controllo che siano generatori, verificando se un vettore generico possa essere scritto come combinazione lineare degli elementi della lista:

$$\begin{pmatrix}b_1\\b_2\\b_3\end{pmatrix} = x_1 \begin{pmatrix}1\\0\\1\end{pmatrix} + x_2 \begin{pmatrix}1\\1\\1\end{pmatrix} + x_3 \begin{pmatrix}1\\0\\0\end{pmatrix} = \begin{pmatrix}x_1 + x_2 + x_3\\x_2\\x_1 + x_2\end{pmatrix}$$

$$\begin{cases} x_1 + x_2 + x_3 = b_1 \\ x_2 = b_2 \\ x_1 + x_2 = b_3 \end{cases} \Rightarrow \begin{cases} x_3 = b_1 - b_3 \\ x_2 = b_2 \\ x_1 = b_3 - b_2 \end{cases}$$

$$\forall b_1, b_2, b_3, \exists x_1, x_2, x_3 \text{ t.c. } \begin{pmatrix}b_1\\b_2\\b_3\end{pmatrix} \in \langle \begin{pmatrix}1\\0\\1\end{pmatrix}, \begin{pmatrix}1\\1\\1\end{pmatrix}, \begin{pmatrix}1\\0\\0\end{pmatrix} \rangle$$

Quindi la lista è generatrice ma non linearmente indipendente.

- $\begin{pmatrix}1\\0\\1\end{pmatrix}, \begin{pmatrix}1\\1\\1\end{pmatrix}, \begin{pmatrix}1\\0\\0\end{pmatrix}$

  Ora basta controllare che siano linearmente indipendenti in quanto abbiamo già dimostrato sopra che sono generatori, quindi controllo che l'unica soluzione possibile per l'equazione di dipendenza lineare sia quella in cui tutti i coefficienti sono uguali a 0:

$$\begin{pmatrix}0\\0\\0\end{pmatrix} = x_1 \begin{pmatrix}1\\0\\1\end{pmatrix} + x_2 \begin{pmatrix}1\\1\\1\end{pmatrix} + x_3 \begin{pmatrix}1\\0\\0\end{pmatrix} = \begin{pmatrix}x_1 + x_2 + x_3\\x_2\\x_1 + x_2\end{pmatrix}$$

$$\begin{cases} x_1 + x_2 + x_3 = 0 \\ x_2 = 0 \\ x_1 + x_2 = 0 \end{cases} \Rightarrow x_1 = x_2 = x_3 = 0$$

  Quindi la lista è linearmente indipendente.

Quindi una lista è base se per ogni vettore v, esiste ed è unica la scelta di $x_1, \ldots, x_n$, che soddisfa la relazione di dipendenza lineare di indice v.

9.4 Lemma di unicità della rappresentazione

Sia $v_1, \ldots, v_n$ una lista di vettori indipendenti, allora:

$$v = x_1 v_1 + \ldots x_n v_n = y_1 v_1 + \ldots y_n v_n$$

$$\Rightarrow x_1 = y_1, \dots, x_n = y_n$$

Dimostrazione:

$$v - v = x_1 v_1 + \cdots + x_n v_n - y_1 v_1 - \dots y_n v_n$$
$$\Rightarrow 0 = (x_1 - y_1)v_1 + \cdots + (x_n - y_n)v_n$$
$$\Rightarrow x_1 = y_1, \dots x_n = y_n$$

Quindi se si ha una lista indipendente allora ho un solo modo univoco per rappresentare un vettore come combinazione lineare di altri vettori.

9.5 Lista polinomiale

Preso l'insieme dei polinomi in x di grado massimo d a coefficienti in $\mathbb{K}$:

$$\mathbb{K}_{\leq d}[x] = \{a_0 + a_1 x + \cdots + a_d x^d \text{ t.c. } a_i \in \mathbb{K}\}$$

Allora:

$$1, x, x^2, \dots, x^d$$

è una base, nello specifico la base canonica di $\mathbb{K}_{\leq d}[x]$, preso $v \in \mathbb{K}_{\leq d}[x]$, allora:

$$v = a + a_1 x + \cdots + a_d x^d = \lambda_0 + \lambda_1 x + \cdots + \lambda_d x^d$$

L'unica soluzione è che $\lambda_i = a_i$, allora dato che se due polinomi sono uguali, la differenza tra i coefficienti è nulla:

$$a_0 + \cdots + a_d x^d = b_0 + \cdots + b_d x^d \iff a_i = b_i$$
$$(a_0 - b_0) + \cdots + (a_d - b_d)x^d = 0$$

10 Matrici

Presa una matrice 2x2:

$$Mat_{2x2}(\mathbb{K}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ t.c. } a, b, c, d \in \mathbb{K} \right\}$$

Con le operazioni di somma e prodotto per scalare:

- Somma:
$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{pmatrix}$$
- Prodotto per scalare:
$$k \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ka & kb \\ kc & kd \end{pmatrix}$$

è uno spazio vettoriale in quanto contiene l'elemento neutro della somma, è chiuso per la somma e per il prodotto per uno scalare.

La base canonica di una matrice 2x2 è:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

infatti, ogni matrice 2x2 può essere scritta come combinazione lineare della base canonica:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = x_1 \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + x_2 \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + x_3 \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + x_4 \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$
$$\Rightarrow x_1 = a, x_2 = b, x_3 = c, x_4 = d$$

11 Dimensione di uno spazio vettoriale

Per dimensione di un certo spazio vettoriale $\mathbb{V}$, si intende il numero degli elementi di una base di $\mathbb{V}$, e si denota con:

$$\dim \mathbb{V}$$

Ad esempio:

- $\dim \mathbb{R}^3 = 3$
- $\dim \mathbb{R}^n = n \longrightarrow n = \left|\left\{e_1 = \begin{pmatrix}1\\0\\\cdot\\0\end{pmatrix}, e_2 = \begin{pmatrix}0\\1\\\cdot\\0\end{pmatrix}, \ldots, e_n = \begin{pmatrix}0\\\cdot\\0\\1\end{pmatrix}\right\}\right|$, ovvero la base canonica di ogni vettore in $\mathbb{R}^n$
- $\dim(\mathbb{K}_{\leq d}[x]) = d + 1 \longrightarrow (1 + x + x^2 + \cdots + x^d)$, ovvero la base canonica di ogni polinomio di grado massimo d
- Presa una matrice 2x2 del tipo:

  $$M_{2x2} = \{\begin{pmatrix}a & b\\c & d\end{pmatrix} \text{ t.c. } a, b, c, d \in \mathbb{K}\}$$

  allora la base canonica di una matrice due per due è:

  $$\begin{pmatrix}1 & 0\\0 & 0\end{pmatrix}, \begin{pmatrix}0 & 1\\0 & 0\end{pmatrix}, \begin{pmatrix}0 & 0\\1 & 0\end{pmatrix}, \begin{pmatrix}0 & 0\\0 & 1\end{pmatrix}$$

  quindi:

  $$\dim M_{2x2} = 4$$

Ogni lista **linearmente indipendente**, ha al massimo $\dim \mathbb{V}$ elementi, dove $\mathbb{V}$ è uno spazio vettoriale.

Invece ogni lista di **generatori**, ha almeno $\dim \mathbb{V}$ elementi.

12 Teorema di Steinitz / dello scambio

Se $v_1, \ldots, v_n = (\{v_i\}_{i \in \mathbb{I}})$, è una lista indipendente, e $w_1, \ldots, w_m = (\{w_j\}_{j \in \mathbb{G}})$ è una lista di generatori, allora:

- $n \leq m \Rightarrow |\mathbb{I}| \leq |\mathbb{G}|$
- Dopo aver riordinato, è possibile cambiare n vettori di w_j, con $v_1, \ldots, v_n$ e il risultato genera ancora

Ad esempio:

$$\exists \mathbb{G}' \subset \mathbb{G}, |\mathbb{G}'| = n * m \text{ t.c.}$$

$$\{v_i, w_j\}_{i \in \mathbb{I}, j \in \mathbb{G}}$$

$$\mathbb{I} := \left\{ \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \right\}$$

$$\mathbb{G} := \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\}$$

Posso mettere $\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$ al posto di $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, e $\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$ al posto di $\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$, ottenendo:

$$\mathbb{G} := \left\{ \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\}$$

Ma questa cosa non vale sempre, infatti bisogna scegliere con cura i vettori.

12.1 Dimostrazione teorema di Steinitz

INSERIRE DIMOSTRAZIONE PER INDUZIONE DAL MANUALE.

12.2 Conseguenze del teorema

- Ogni base ha lo stesso numero di elementi.

  Dimostrazione:

  $$\{v_i\}_{i\in\mathbb{B}} \wedge \{w_j\}_{j\in\mathbb{B}'}$$

  Supponendo che siano basi, dove $\mathbb{V}_i$ è indipendente e anche generatrice, e $\mathbb{W}_i$ è generatrice e anche indipendente.

  Quindi la cardinalità di $\mathbb{B}$ è minore o uguale a quella di $\mathbb{B}'$, oppure $\mathbb{B}'$ è minore o uguale a quella di $\mathbb{B}$, ciò implica che le due cardinalità siano uguali.

  $$\left.\begin{matrix} |\mathbb{B}| \leq |\mathbb{B}'| \\ |\mathbb{B}'| \leq |\mathbb{B}| \end{matrix}\right\} \Rightarrow |\mathbb{B}| = |\mathbb{B}'|$$

- Lemma: Ogni lista $\{v_i\}_{i\in\mathbb{I}}$ indipendente massima (quindi con cardinalità uguale alla $\dim \mathbb{V}$) è una base:

  $$|\mathbb{I}| = \dim \mathbb{V}$$

  Ogni lista $\{w_j\}_{j\in\mathbb{G}}$ generatori minima, (quindi con cardinalità uguale alla $\dim \mathbb{V}$) è una base:

  $$|\mathbb{G}| = \dim \mathbb{V}$$

  La dimensione è il più importante invariante di uno spazio vettoriale.

  Dimostrazione del primo punto del lemma:

  $$\langle v_i \rangle_{i\in I} \subset \mathbb{V}$$

  per definizione è un sottospazio.

- Se $\langle v_i \rangle_{i \in I} = \mathbb{V}$, allora i vettori sono una base.
- Se $\langle v_i \rangle_{i \in I} \neq \mathbb{V}$, allora $\exists v \notin \langle v_i \rangle_{i \in I}$

Presa la lista:

$$\{v_i, v\}_{i \in \mathbb{I}}$$

allora se si vuole dimostrare la seconda definizione:

$$\sum_{i \in \mathbb{I}} x_i v_i + xv = 0$$

con $x \neq 0$, però:

$$v = \frac{1}{x}(-\sum_{i \in \mathbb{I}} x_i v_i)$$

Si arriva ad una contraddizione in quanto si era posto che la lista indipendente fosse massima, perciò deve per forza essere indipendente.

Dimostrazione del secondo punto del lemma:

- $\{w_j\}_{j \in \mathbb{G}}$ è indipendente.
- $\{w_j\}_{j \in \mathbb{G}}$ non è indipendente.

Posso allora scrivere l'equazione di dipendenza lineare:

$$\sum_{j \in \mathbb{G}} y_j w_j = 0$$

con almeno un $y_j \neq 0$, e lo chiameremo y_k

$$\Rightarrow w_k = \frac{1}{y_k}(-\sum_{j \in \mathbb{G}} \setminus \{k\}) y_j w_j \Rightarrow w_k \in \langle w_j \rangle_{j \in \mathbb{G} \setminus \{k\}}$$

e questo contraddice il fatto che la lista $\{w_j\}_{j \in \mathbb{G}}$ sia minima.

Conseguenze del lemma:

- Ogni lista $\{v_i\}_{i \in \mathbb{I}}$ di vettori indipendenti si può estendere a una base, aggiungendo vettori indipendente finché la lista non diventa massima
- Ogni lista $\{w_j\}_{j \in \mathbb{G}}$ di generatori contiene una base, è sempre presenta una sottolista di generatori minima

- Corollario: Se $\mathbb{W} \subset \mathbb{V}$, $\dim \mathbb{W} <= \dim \mathbb{V}$ è in realtà $\dim \mathbb{W} = \dim \mathbb{V} \iff \mathbb{V} = \mathbb{W}$

  Dimostrazione: presa una base di $\mathbb{W}$:

  $$\langle \{v_i\}_{i \in \mathbb{B}_w} \rangle = \mathbb{W}$$

  quindi $|\mathbb{B}_w| = \dim \mathbb{W}$ Allora i v_i sono per definizione indipendenti, quindi:

  $$|\mathbb{B}_w| \leq \dim \mathbb{V}$$

  se $\mathbb{W} \subset \mathbb{V}$, allora è possibile estendere $\{v_i\}_{i \in \mathbb{I}}$ ad una base di $\mathbb{V}$ e quindi $|\mathbb{B}_w| < \dim \mathbb{V}$

13 Formula di Grassman

Sia $\mathbb{V}$ uno spazio vettoriale su $\mathbb{K}$, e $\mathbb{U}, \mathbb{W} \subset \mathbb{V}$ sottospazi finitamente generati, allora:

$$\dim(U+W) = \dim U + \dim W - \dim(U \cap W)$$

Ad esempio:

- In $\mathbb{R}^3 = V$, allora siano U, W due piano, quindi $\dim U = \dim W = 2$, allora:

$$\dim U \cap W = \begin{cases} 1 \\ 2 \iff U = W \end{cases}$$

- In $\mathbb{R}^4$, con U, W piani, allora $U, W \leq W + U \leq \mathbb{R}^4$, allora:

$$\dim U \cap W = \dim U + \dim W - \dim(U+W) = \begin{cases} 0 \iff U + W = \mathbb{R}^4 \\ 1 \\ 2 \iff U = W \end{cases}$$

  Se $U = \langle v_1, v_2 \rangle$ e $W = \langle w_1, w_2 \rangle$, allora nel sistema otteniamo:

  - 0, se v_1, v_2, w_1, w_2 sono indipendenti
  - 1, se uno dei vettori che genera il piano W appartiene al piano U, o viceversa
  - 2, se v_1, v_2 generano lo stesso piano di w_1, w_2, quindi appartengono allo stesso piano

14 Risoluzione esercizi

14.1 Settimana due:

14.2 Esercizio 1

Sia $\mathbb{F}_p := \mathbb{Z}/p$, con p un numero primo:

Esercizio 1.1

$$x \in \mathbb{F}_p, x \neq 0$$

Dimostrare che:

$$\exists a > 0 \text{ t.c. } x^a = 1$$

Usare il suggerimento $\exists m \neq n$ t.c. $x^m = x^n$

$$\mathbb{F}_p := \{[0], [1], \dots, [p-1]\}$$

Allora stesso tempo:

$$I = \{x^m \text{ t.c. } m \in \mathbb{Z}\} := \{\dots, x^{-2}, x^{-1}, 1, x, x^2, \dots\}$$

Dato che $\mathbb{F}_p$ è un insieme finito, mentre l'insieme I è infinito, allora esistono almeno 2 elementi diversi di I, che fanno riferimento allo stesso elemento in $\mathbb{F}_p$, per via del principio di Dirichlet (teorema dei cassetti).

$$n \neq m \to x^n = x^m \xrightarrow{n>m} x^{n-m} = 1 \xrightarrow{a=n-m} x^a = 1$$

Questo è possibile solo se $x^m \neq 0, x \neq 0$, lo dimostro per contraddizione, ponendo che esiste $x^k = 0$, con $k = \min(k)$ t.c. $x^k = 0$, allora:

$$x^{k-1} \neq 0 \Rightarrow \exists(\frac{1}{x^{k-1}}) \Rightarrow x^k = x^{k-1}x \Rightarrow x = \frac{x^k}{x^{k-1}} = 0$$

Ma questo non è possibile in quanto $x \neq 0$, quindi non esiste k t.c. $x^k = 0, x \neq 0$

Esercizio 1.2

$$x \in \mathbb{F}_p, x \neq 0, a = \min a > 0 \text{ t.c. } x^a = 1$$

Dimostrare che la cardinalità dell'insieme delle potenze di x è uguale ad a:

$$|\{x^m \text{ t.c. } m \in \mathbb{Z}\}| = a$$

Allora affermo che:

$$\{x^m \text{ t.c. } m \in \mathbb{Z}\} \subseteq \{1, x, x^2, \dots, x^{a-1}\}$$

e bisogna dimostrare che:

$$\{x^m \text{ t.c. } m \in \mathbb{Z}\} \supseteq \{1, x, x^2, \dots, x^{a-1}\}$$

quindi che:

$$\{x^m \text{ t.c. } m \in \mathbb{Z}\} = \{1, x, x^2, \dots, x^{a-1}\}$$

per dimostrare questo parto da:

$$x^m = x^k, 0 \leq k \leq a-1 \Rightarrow m = a * q$$

ma se fosse così x^m sarebbe sempre uguale a 1, perciò bisogna aggiungere un termine r:

$$m = aq + r \Rightarrow x^m = x^{aq} \cdot x^r \Rightarrow x^m = x^r, 0 \leq r \leq a - 1$$

quindi:

$$\forall x^m, \exists r, 0 \leq r \leq a - 1 \text{ t.c. } x^m = x^r$$

La dimostrazione però non è ancora completa in quanto non ho ancora usato il fatto che a sia il minimo a possibile tale per cui $x^a = 1$, infatti se:

$$x^m = x^n, 0 \leq m \leq n \leq a - 1 \rightarrow x^{m-n} = 1$$

quindi $a = n - m, 0 \leq n - m \leq a - 1$, che va in contraddizione con il fatto che a sia minimo, perciò si è dimostrato che l'insieme delle potenze positive di x, ha cardinalità a.

15 Teoremi/Principi/Assiomi/Altro usati negli esercizi

15.1 Principio di Dirichlet

Afferma che:

> Se $n + 1$ oggetti, vengono distribuiti in n cassetti, allora almeno un cassetto deve contenere due oggetti

Esiste anche la versione generalizzata:

> Se si hanno m oggetti da distribuire in k cassetti, allora almeno un cassetto conterrà almeno $\lceil \frac{m}{k} \rceil$ oggetti

dove $\lceil \rceil$ rappresenta la parte intera superiore.