Orale sudatissimo algebra

(1) SPAZI VETTORIALI

1.1 Def. SV

É una strutt alg. su un campo F : $(V, F, +, \cdot)$
con somma e prodotto per uno scalare.

Prop. somma:

- Commutativa
- Associativa
- Elem. neutro
- Elem. opposto

(Elem. neutro ed elem. opposto: UNICI) $\Rightarrow$ $(V, +, 0, \cdot^{-1})$ forma un gruppo abeliano

Prop. prod:

- associativa
- Distributiva (a DX e SX)
- Elem. neutro

1.2 Def. Sottospazi vettoriali

Dato V SV, U é uno sottospazio vettoriale se:

- $U \subseteq V$
- $U \neq \emptyset$
- U é chiuso rispetto alla somma e al prodotto

Nota: $\underline{0} \in U$

1.3 Def. Combinazione lineare

$v \in V$ é comb. lineare di $v_1, \ldots, v_n \in V$ se $\exists \lambda_1, \ldots, \lambda_n \in \mathbb{R}$.

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

Dati n vettori, l'insieme delle loro combinazioni lineari è dato da:

$$\langle v_1, \dots, v_n \rangle = \{ \lambda_1 v_1 + \dots + \lambda_n v_n \mid \lambda_1, \dots, \lambda_n \in \mathbb{R} \}$$

1.3.1

- $v_1, \dots, v_n \in V \Rightarrow \langle v_1, \dots, v_n \rangle \leq V$ ①
- $Z \leq V.\ v_1, \dots, v_n \in Z \Rightarrow \langle v_1, \dots, v_n \rangle \subseteq Z$ ②

① L'insieme delle combinazioni lineari di vettori $\in$ SV formano un sottospazio di quello SV

② L'insieme delle combinazioni lineari di n vettori è il sottosp più piccolo che contiene tutti gli n vettori

$\boxed{1.4}$ Def. generatori

$v_1, \dots, v_n \in V$ SV generano V sse $V = \langle v_1, \dots, v_n \rangle$

1.4.1

v è comb. lin. di $v_1, \dots, v_n$ sse

$$\langle v_1, \dots, v_n \rangle = \langle v_1, \dots, v_n, v \rangle$$

$\boxed{1.5}$ Def. Indipendenza lineare

$v_1, \dots, v_n \in V$ SV sono lin. ind. sse

$$\lambda_1 v_1 + \dots + \lambda_n v_n = \underline{0} \Longrightarrow \lambda_1, \dots, \lambda_n = 0$$

↙

l'unica loro comb. lin. che dà il vettore nullo ha tutti gli scalari nulli

1.5.1 Dato un insieme S di vettori lin. ind., ogni suo sottoinsieme è anche lin. ind.

1.5.2 Dati n vettori, questi sono lin. dip. (NOT lin. ind.) sse uno di questi vettori è combinazione lin. degli altri

Dim

$(\lambda_1 \neq 0 \vee \lambda_2 \neq 0 \vee \dots) \to \lambda_i \neq 0$

$\Rightarrow)$ $\neg$(lin ind) $\Rightarrow \exists \lambda_1, \dots, \lambda_n \,.\, \lambda_1 v_1 + \dots + \lambda_n v_n = 0$, quindi

$$v_i = \left(-\frac{\lambda_1}{\lambda_i}\right) v_1 + \dots + \left(\frac{-\lambda_n}{\lambda_i}\right) v_n \Rightarrow v_i \text{ è comb. lin. degli altri}$$

$\Leftarrow)$ $v_i = \lambda_1 v_1 + \dots + \lambda_n v_n$, quindi:

$0 = \lambda_1 v_1 + \dots + \lambda_n v_n + (-1) v_i$, $-1 \neq 0 \Rightarrow v_1, \dots, v_n$ Non sono lin. ind.

$\boxed{1.6}$ Def. Base

V SV, $v_1, \dots, v_n \in V$, $B = \{v_1, \dots, v_n\}$ è una base di V sse:

- $\langle v_1, \dots, v_n \rangle = V$
- $v_1, \dots, v_n$ sono lin. ind.

1.6.1 Esistenza base

$\forall V$ SV finitamente generato, $\exists$ una base di V

Dim

Essendo finitamente generato, $\exists v_1, \dots, v_n \in V \,.\, V = \langle v_1, \dots, v_n \rangle$

1. se $v_1, \dots, v_n$ sono lin. ind., allora sono una base
2. altrimenti per 1.5.2 $\exists v \in \{v_1, \dots, v_n\}$ t.c. v è combinazione lineare degli altri, quindi per 1.4.1 possiamo rimuoverlo e rimane che $\langle v_1, \dots, v_n \rangle = \langle v_1, \dots, v_n \rangle \setminus v = V$. Torna al punto 1.

1.6.2 Teorema completamento

Data una base $B = \{v_1, \dots, v_n\}$ di V sv e un insieme $W = \{w_1, \dots, w_m\} \subseteq V$, con $w_1, \dots, w_m$ lin. ind. allora:

- $m \leq n$
- é possibile aggiungere $m-n$ vettori di B a W in modo che W sia una base

1.6.3 Dimensione

Grazie al teo. compl. possiamo dimostrare che tutte le basi di uno stesso sottospazio hanno lo stesso numero di vettori, che possiamo chiamare dimensione.

1.6.4 GEL

V sv, $\dim V = n$, allora sono equivalenti:

- $\{v_1, \dots, v_n\}$ é base di V — ovvio per def. base
- $v_1, \dots, v_n$ sono lin. ind.
- $v_1, \dots, v_n$ generano V

Dim

(2) => (1) Per teo. compl. possiamo aggiungere $n-n=0$ vettori a $v_1, \dots, v_n$ in modo che formino una base

(3) => (2) Per assurdo, se $v_1, \dots, v_n$ generano e sono lin. dip. potrei eliminarne uno o più finché non formano una base, ma questo significherebbe avere una base con meno di $\dim V$ elementi che é assurdo.

1.7 Gauss diretto

- Le righe non nulle di una matrice a scala sono lin. ind.
- Le operazioni elementari sulle righe non cambiano lo spazio generato dalle righe stesse

$\boxed{1.8}$ Coordinate rispetto una base

1.8.1 Unicità coordinate rispetto una base

$B = \{v_1, \dots, v_n\}$ base di V SV, $v \in V$, $\exists! \lambda_1, \dots, \lambda_n$.

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

Dim

Dato che $v_1, \dots, v_n$ generano V (def. base) e $v \in V$, $\exists \lambda_1, \dots, \lambda_n$.

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

Prendiamo altri scalari $\mu_1, \dots, \mu_n$:

$$v = \mu_1 v_1 + \dots + \mu_n v_n$$

Se valgono entrambe le equazioni:

$$(\mu_1 - \lambda_1) v_1 + \dots + (\mu_n - \lambda_n) v_n = 0$$

Dato che $v_1, \dots, v_n$ sono lin. ind. (def. base) si ha che (def. lin. ind.) $\forall i \in \{1, \dots, n\}$. $\mu_i - \lambda_i = 0 \Rightarrow \mu_i = \lambda_i$. Quindi i coefficienti sono unici.

$\boxed{1.9}$ Equazioni parametriche e cartesiane

Diversi modi per rappresentare un sottosp. $V = \langle v_1, \dots, v_k \rangle \leq \mathbb{R}^n$:

- PARAMETRICO

$$V = \{ v = \lambda_1 v_1 + \dots + \lambda_k v_k \mid \lambda_1, \dots, \lambda_k \in \mathbb{R} \}$$

- CARTESIANO

$$V = \{ v \in \mathbb{R}^n / A v = \underline{0} \} = \operatorname{Ker} A$$

$\rightarrow$ A lo dobbiamo ricavare dalla rappr. param.

② APPLICAZIONI LINEARI

2.1 Def. Applicazione lineare

Una funzione $F: V \to W$ con V e W sottosp. vett. é un' appl. lin. se:

- $F(0_V) = 0_W$ --- in realtà questa deriva dalle altre due
- $F(u+v) = F(u) + F(v)$
- $F(\lambda v) = \lambda F(v)$

MORFISMO

NT

Ogni matrice ha un' applicazione lin. associata

$$A \in M_{n \times m} \Rightarrow L_A : \mathbb{R}^m \to \mathbb{R}^n \quad L_A(x) = Ax$$

2.2 Esistenza e unicità di applicazioni lin.

Data una base $B = \{v_1, \dots, v_n\}$ di V e $w_1, \dots, w_n$ vettori di W (non necess. distinti) $\exists! L_A . \forall i \in \{1, \dots, n\} . L_A(v_i) = w_i$

Dim

Per 1.8.1 $\exists! \lambda_1, \dots, \lambda_n . v = \lambda_1 v_1 + \dots + \lambda_n v_n$ $(\forall v \in V)$. Uso queste coordinate per definire:

$$L_A(v) = \lambda_1 w_1 + \dots + \lambda_n w_n \quad (\forall v \in V)$$

① Notiamo che $\forall i \in \{1, \dots, n\} . L_A(v_i) = w_i$ (quindi rispetta la condizione)

② $L_A(v+u) = (\lambda_1 + \mu_1) w_1 + \dots + (\lambda_n + \mu_n) w_n = \lambda_1 w_1 + \dots + \lambda_n w_n + \mu_1 w_1 + \dots + \mu_n w_n =$
$= L_A(v) + L_A(u)$

③ $L_A(\rho v) = \rho \lambda_1 w_1 + \dots + \rho \lambda_n w_n = \rho(\lambda_1 w_1 + \dots + \lambda_n w_n) =$
$= \rho L_A(v)$ * Manca la dimostrazione dell' unicità!

$\boxed{2.3}$ Nucleo e Immagine

Def. Data $L_A : V \to W$, definiamo:

- Nucleo $= \text{Ker}\, L_A = \{x \in V \mid L_A(x) = \underline{0}\}$ $(\leq V)$
- Immagine $= \text{Im}\, L_A = \{L_A(x) \mid x \in V\}$ $(\leq W)$

2.3.1 Generatori Immagine

Data $L_A : V \to W$, $\text{Im}\, L_A$ é generata dai vettori immagine di una qualunque base di V $(B = \{v_1, \dots, v_n\})$

$$\text{Im}\, L_A = \langle L_A(v_1), \dots, L_A(v_n) \rangle$$

Dim

① $\text{Im}\, L_A \subseteq \langle L_A(v_1), \dots, L_A(v_n) \rangle$

$$L_A(v) = L_A(\lambda_1 v_1 + \dots + \lambda_n v_n) = \lambda_1 L_A(v_1) + \dots + \lambda_n L_A(v_n) \in \langle L_A(v_1), \dots, L_A(v_n) \rangle$$

$$(\forall v \in V)$$

② $\langle L_A(v_1), \dots, L_A(v_n) \rangle \subseteq \text{Im}\, L_A$

$\text{Im}\, L_A \leq W$ e $L_A(v_1), \dots, L_A(v_n) \in W$ quindi per 1.3.1

$\langle L_A(v_1), \dots, L_A(v_n) \rangle \subseteq \text{Im}\, L_A$

① e ② valgono contemporaneamente $\Leftrightarrow$

$$\langle L_A(v_1), \dots, L_A(v_n) \rangle = \text{Im}\, L_A$$

2.3.2 Iniettività e nucleo

Una app. lin. L_A é iniettiva sse $\text{Ker}\, L_A = \{\underline{0}_V\}$

Dim

$\Rightarrow$) Assumo L_A iniettiva, $\forall v \in V$. $F(v) = \underline{0}_W = F(\underline{0}_V) \Rightarrow v = \underline{0}_V \Rightarrow \text{Ker}\, L_A = \{\underline{0}_V\}$

$\Leftarrow$) Assumo $\operatorname{Ker} L_A = \{\underline{0}_V\}$, prendo $v, u \in V$. $L_A(v) = L_A(u)$.
Per linearità $L_A(v-u) = L_A(v) - L_A(u) = \underline{0}_W$, quindi $v-u \in \operatorname{Ker} L_A \in \{\underline{0}_V\}$. Per singoletto $v - u = \underline{0}_V \Rightarrow v = u$ quindi L_A è iniettiva

2.4 Teorema dimensione

Data $L_A : V \to W$, V e W SV, $\dim V = n$:

$$\dim(\operatorname{Im} L_A) + \dim(\operatorname{Ker} L_A) = n$$

Dim

Sia $\dim(\operatorname{Ker} L_A) = r$ e $v_1, \dots, v_r$ una base di $\operatorname{Ker} L_A$, per teo. compl. posso aggiungere $n-r$ vettori di una base di V per formare una nuova base $B = \{v_1, \dots, v_r, v_{r+1}, \dots, v_n\}$.

1. Sappiamo che $\operatorname{Im} L_A = \langle L_A(v_1), \dots, L_A(v_n) \rangle$, ma $L_A(v_1) = \dots = L_A(v_r) = \underline{0}_W$ per def. nucleo. Quindi, dato che vettori nulli sono sempre comb. lin. possiamo rimuoverli dai generatori senza cambiare il sottosp. generato: $\operatorname{Im} L_A = \langle L_A(v_{r+1}), \dots, L_A(v_n) \rangle$

2. Ora dimostriamo che $L_A(v_{r+1}), \dots, L_A(v_n)$ sono lin. ind.
Assumo $\lambda_{r+1} L_A(v_{r+1}) + \dots + \lambda_n L_A(v_n) = \underline{0}_W$, dimostriamo che $\lambda_{r+1}, \dots, \lambda_n = 0$.
Per linearità $L_A(\lambda_{r+1} v_{r+1} + \dots + \lambda_n v_n) = \underline{0}_W$, quindi:

$$v = \lambda_{r+1} v_{r+1} + \dots + \lambda_n v_n \in \operatorname{Ker} L_A .$$

Quindi

$$v = \lambda_1 v_1 + \dots + \lambda_r v_r$$

Se sono vere entrambe le eq:

$$\lambda_1 v_1 + \dots + \lambda_r v_r - \lambda_{r+1} v_{r+1} - \dots - \lambda_n v_n = \underline{0}_V$$

Ma dato che $v_1, \dots, v_n$ formano una base, sono lin. ind., quindi $\lambda_1, \dots, \lambda_n = 0$.

Dato che $L_A(v_{r+1}), \dots, L_A(v_n)$ sono lin. ind e generano $\mathrm{Im}\, L_A$, sono anche una sua Base, quindi

$$\dim(\mathrm{Im}\, L_A) = n - r$$

Ovvero

$$\dim(\mathrm{Im}\, L_A) + \dim(\mathrm{Ker}\, L_A) = \dim V$$

$\square$

2.4.1

Due SV V e W sono isomorf. ($\exists$ una biezione $T: V \to W$)

sse $\dim V = \dim W$

Oss. $\mathbb{R}_n[x] \cong \mathbb{R}^{n+1}$, $M_{n \times m} \cong \mathbb{R}^{n \times m}$

2.4.2 Rango Righe = Rango Colonne

$A \in M_{n \times m}(\mathbb{R})$, si ha che $rr(A) = rr(A^T)$

Dim ($\dim V = m$)

$L_A : V \to W$ è l'app. lin. associata ad A. Per metodi di calcolo:

- $\dim(\mathrm{Ker}\, L_A) = m - rr(A)$
- $\dim(\mathrm{Im}\, L_A) = rr(A^T)$

Per teo. dim. $m - rr(A) + rr(A^T) = m$, quindi

$$rr(A) = rr(A^T)$$

2.5 Controimmagine

Def. $L_A : V \to W$ app. lin., $w \in W$, la controimmagine di w è:

$$L_A^{-1}(w) = \{v \in V \mid L_A(v) = w\}$$

- $w \notin \mathrm{Im}\, L_A \iff L_A^{-1}(w) = \emptyset$
- $L_A^{-1}(w) \leq V \iff w = 0_W$ (e quindi $L_A^{-1}(w) = \mathrm{Ker}\, L_A$)

Risolvere $A\underline{x} = b$ equivale a trovare gli elementi di $L_A^{-1}(b)$

2.5.1 Struttura dei sistemi lineari

Dato un sistema lineare $A\underline{x} = b$ di m equazioni in n incognite t.c. esiste almeno una soluzione v, si ha che l'insieme delle soluzioni é dato da

$$S = \{v + z \,/\, z \in \operatorname{Ker} A\}$$

2.5.2 Rouché - Capelli

Dato un sistema lineare $A\underline{x} = b$ di m equazioni in n incognite, se $rk(A) \neq rk(A|b)$ allora non esistono soluzioni, altrimenti:

- se $rk(A|b) = n$ esiste una sola soluzione
- se $rk(A|b) < n$ esistono infinite soluzioni che dipendono da $n - rk(A|b)$ parametri

3 DETERMINANTE

Def. Data una matrice quadrata $A \in M_{n\times n}(\mathbb{R})$, si chiama determinante di A la funzione det : $M_{n\times n} \to \mathbb{R}$ t.c.:

- Se la j-esima riga di $A = U + V$, allora il suo det è dato dalla somma dei due det di A con la j-esima riga $= U$ e con la j-esima riga $= V$
- Se la j-esima riga di $A = \lambda U$, allora il suo det è λ per il det di A con j-esima riga $= U$
- Se due righe sono uguali, allora $\det A = 0$
- $\det(I) = 1$

3.1 Proprietà determinante

Dalla definizione, possiamo ricavare le seguenti prop. che ci possono aiutare a calcolare il det:

- Se B si ottiene da A scambiando due righe:

$$\det(B) = -\det(A)$$

- Se B si ottiene da A sommando a una riga di A una qualunque comb. lin. delle altre, allora

$$\det(B) = \det(A)$$

- Se A è triangolare, allora $\det(A) =$ prodotto dei valori sulla diagonale

3.2 METODI DI CALCOLO

3.2.1 Binet

$$\det(AB) = \det(A)\det(B) \quad (\text{se } A, B \in M_n)$$

3.3 Matrici Invertibili

Def. Data $A \in M_n$, si chiama inversa di A la matrice $B \in M_n$ t.c.

$$AB = BA = I$$

3.3.1 Determinante e inversa

$A \in M_n$ è invertibile $\iff \det A \neq 0$

Dim

$\Rightarrow)$ $\exists B \in M_n .\ AB = I.$ $\det(AB) = \det(I) = 1$ (def. det)

Per Binet $\det(AB) = \det(A)\det(B) = 1 \Rightarrow \begin{cases} \det A \neq 0 \\ \det B \neq 0 \end{cases}$

Calcolo inversa e riassuntiva

Regola di Lagrange ??

4 CAMBIO DI BASE

$$I_{ee} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \vdots \end{pmatrix} \quad I_{Be} = \left(\begin{pmatrix} v_1 \end{pmatrix} \begin{pmatrix} v_2 \end{pmatrix} \dots \right) \quad I_{BB} = \left(\begin{pmatrix} v_1 \end{pmatrix}_B \begin{pmatrix} v_2 \end{pmatrix}_B \dots \right)$$

$$= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ & & & \ddots \end{pmatrix}$$

$$I_{eB} \circ I_{Be} = I_{BB} = I$$

$$I_{Be}^{-1} \circ I_{Be} = I_{BB}$$

5 DIAGONALIZZABILITÁ

<u>Def.</u> applicazione lineare diagonalizzabile

$L_A : \mathbb{R}^n \to \mathbb{R}^n$ é diag. se $\exists$ base B di $\mathbb{R}^n$ t.c.

A_{BB} é diag.

<u>Def.</u> Matrice diagonalizz.

Una matrice quadrata $A \in M_n$ é diag. se é simile a una matrice diagonale, ovvero se $\exists\, P \in M_n$.

$$P^{-1} A P = D = \text{matrice diagonale}$$

5.1 Diag. matrice e app. lin.

$L_A : \mathbb{R}^n \to \mathbb{R}^n$ é diag. $\iff$ A é diag.

<u>Dim</u>

$\Rightarrow$) $\exists B$. A_{BB} é diagonale. $A_{BB} = I_{BE}^{-1} A I_{BE}$, quindi A é simile a una matrice diagonale $\Rightarrow$ A é diag.

$\Leftarrow$) $\exists P$. $P^{-1} A P = D$. Se considero B una base formata dalle colonne di P, allora $P = I_{BE}$ e A_{BB} é diagonale.

5.2 AUTOVETTORI e AUTOVALORI

<u>Def.</u> Data un app. lin $L_A : \mathbb{R}^n \to \mathbb{R}^n$, $v \in \mathbb{R}^n$ si dice autovettore se $L_A(v) = \lambda v$, dove $\lambda \in \mathbb{R}$ si chiama autovalore

5.2.1 Autovettori e diagonalizzabilitá

Dato un endomorfismo di $\mathbb{R}^n$ L_A, é diagonalizzabile sse $\exists$ una base di autovettori di L_A

Dim

$\Rightarrow$) L_A é diagonalizz. $\Rightarrow \exists B .\ A_{BB}$ é diag. $B=\{v_1, \dots, v_n\}$

$A_{BB} = \begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \ddots \ \lambda_n \end{pmatrix}$ $\quad A_{BB} v_i = \lambda_i v_i$ quindi B é base di autovettori

$\Leftarrow$) $B=\{v_1, \dots, v_n\}$ é base di autovett.

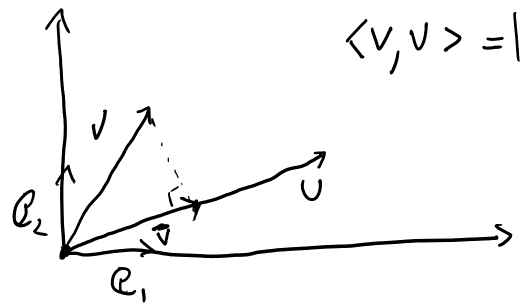
$$A_{BB} = \left(\left(L_A(v_1)\right)_B \dots \left(L_A(v_n)\right)_B \right) = \left(\left(\lambda_1 v_1\right)_B \dots \left(\lambda_n v_n\right)_B \right) = \begin{pmatrix} \lambda_1 & 0 & \\ 0 & \lambda_2 & \\ 0 & 0 & \ddots \\ \vdots & \vdots & \end{pmatrix}$$

é diag

$$Av = \lambda v \qquad (A - \lambda I)v = 0 \qquad \exists v \neq \underline{0} \Leftrightarrow \det(A - \lambda I) = 0$$

6 ORTOGONALITÁ

$$\text{proj}_u(v) = \frac{\langle v, u \rangle}{\|u\|^2} u$$



$$\langle v, u \rangle = \|\text{proj}_u(v)\| \|u\|$$

$$= \frac{|\langle v, u \rangle|}{\cancel{\|u\|^2}} \cancel{\|u\|^2} = |\langle v, u \rangle|$$

$u = \begin{pmatrix} 4 \\ 1 \end{pmatrix} \Rightarrow A = \begin{pmatrix} 4 & 1 \end{pmatrix} \quad L_A : \mathbb{R}^2 \to \mathbb{R} \qquad v = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$

$$\begin{pmatrix} 4 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \end{pmatrix} = 6$$

6.1 Disuguaglianza di Schwarz

$$|\langle v, w \rangle| \leq \|v\| \|w\|$$

6.2 Ortogonalità e indipendenza

$(\underline{0} \neq) v_1, \dots, v_K \in \mathbb{R}^n$ t.c. sono tutti ortogonali, allora $v_1, \dots, v_K$ sono lin. ind.

Dim

assumo $v_1, \dots, v_K$ ortogonali non nulli, d.d.

$\lambda_1 v_1 + \dots + \lambda_K v_K = \underline{0} \Rightarrow \lambda_1 = \dots = \lambda_K = 0$, assumo la parte a sx

quindi $\forall i \in \{1, \dots, K\}$. $\langle \underbrace{\lambda_1 v_1 + \dots + \lambda_K v_K}_{\underline{0}}, v_i \rangle = 0$. Per bilinearità

$\lambda_1 \langle v_1, v_i \rangle + \dots + \lambda_i \|v_i\|^2 + \dots + \lambda_n \langle v_n, v_i \rangle = 0$ per ortogonalità

$\lambda_i \|v_i\|^2 = 0$, $v_i \neq \underline{0}$ quindi $\lambda_i = 0$

$\boxed{6.3}$ Sottosp. ortogonale

Dato $W \leq \mathbb{R}^n$, $W^\perp$ è il sottosp. di $\mathbb{R}^n$ t.c.

$$W^\perp = \{ v \in \mathbb{R}^n / \forall w \in W . \langle v, w \rangle = 0 \}$$

6.3.1 Dimensione sottosp. ortogonale

Dato $W, W^\perp \leq \mathbb{R}^n$:

$$\dim W + \dim W^\perp = \dim \mathbb{R}^n = n$$

E $W \cap W^\perp = \{\underline{0}\}$

Dim

Possiamo definire $W^\perp = \{ v \in \mathbb{R} / Av = \underline{0} \}$ dove A ha per righe i vettori della base $\mathcal{B}$ di W. Quindi possiamo dire che $W^\perp = \mathrm{Ker} L_A$ e per il teo. dimensione $\dim(\mathrm{Ker}\, L_A) + \dim(\mathrm{Im}\, L_A) = n$

Sappiamo che $\dim(\mathrm{Im}\, L_A) = rk(A) = $ rango righe $A = \underbrace{\dim W}_{L_S(\text{Base di } W)}$ $\square$

6.3.2 Coordinate rispetto a base ortonormale

Data una base ortonormale $B = \{v_1, \dots, v_n\}$, un vettore v appartenente al sottosp. ha coordinate rispetto a B date da:

$$(v)_B = (\langle v, v_1 \rangle, \dots, \langle v, v_n \rangle)$$

Dim

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

$$\langle v, v_i \rangle = \langle \lambda_1 v_1 + \dots + \lambda_n v_n, v_i \rangle = \lambda_1 \langle v_1, v_i \rangle + \dots + \lambda_i \langle v_i, v_i \rangle + \dots$$
$$+ \lambda_n \langle v_n, v_i \rangle = \lambda_i$$

6.3.3 Gram-Schmidt

Data una base $B = \{v_1, \dots, v_n\}$ di un sottosp. W, si può trovare una base ortonormale $\overline{B}$ usando il seguente algoritmo:

1. $\overline{v}_1 = v_1$
2. $\overline{v}_i = v_i - \mathrm{proj}_{v_{i-1}}(v_i) - \dots - \mathrm{proj}_{v_1}(v_i)$
3. $\overline{v}_i = \dfrac{\overline{v}_i}{\|\overline{v}_i\|}$

6.4 Matrici e applicazioni ortogonali

Def. APP. LIN. ORTOGONALE

$$\langle F(v), F(v) \rangle = \langle v, v \rangle$$

Def. MATRICE ORTOGONALE

$A \in M_n$ é ortogonale sse $A^T = A^{-1}$

6.4.1

Sia $A \in M_n$, é equivalente:

- $\forall u, v \in \mathbb{R}^n$ $\langle Au, Av \rangle = \langle u, v \rangle$ $\Rightarrow$ L_A é ortogonale
- $\forall v \in \mathbb{R}^n$ $\langle Av, Av \rangle = \langle v, v \rangle$
- $A^T = A^{-1}$
- Le colonne (e le righe) di A sono una base ortonormale di $\mathbb{R}^n$

Dim ③ $\Leftrightarrow$ ④

$\Rightarrow$) $A^T A = I$ $\Rightarrow$ $\langle$ j-esima colonna di A, i-esima colonna di A $\rangle$

$= \begin{cases} 0 & \text{se } i \neq j \\ 1 & \text{se } i = j \end{cases}$ $\rightarrow$ delta di Kroneker (definizione di base ortonormale)

$\Leftarrow$) Sappiamo che $\forall i, j \in \{1, \dots, n\}$ $\langle v_i, v_j \rangle = \begin{cases} 0 & \text{se } i \neq j \\ 1 & \text{se } i = j \end{cases}$

Quindi $A = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$ o $A = \begin{pmatrix} v_1 & \cdots & v_n \end{pmatrix}$ $\Rightarrow$ $AA^T = I$

6.5 MATRICI e APP. LIN. SIMMETRICHE

Def. APP. LIN. SIMMETRICA

$\langle F(v), v \rangle = \langle v, F(v) \rangle$ $\forall u, v \in \mathbb{R}^n$

Def. MATRICE SIMMETRICA

$\forall i, j \in \{1, \dots, n\}$ $a_{ij} = a_{ji}$

6.5.1 Teorema spettrale

Data L_A APP. LIN. simmetrica, si ha:

- L_A é diagonalizzabile
- Dati due autovalori $\lambda_1\ \lambda_2$ distinti, V_{λ_1} e V_{λ_2} sono ortogonali
- Esiste una matrice ortogonale P. $P^T A P = D$, dove D é diagonale.

7 ARITMETICA MODULARE

NT

$\forall a,b \in \mathbb{Z}.\ b \neq 0.\ \exists!\ q,r \in \mathbb{Z}.\quad a = qb + r \quad 0 \leq r < |b|$

Dfn DIVISIBILITÁ

$a,b \in \mathbb{Z}$. b divide a $(b|a)$ se $\exists c \in \mathbb{Z}.\ a = bc$

$d = gcd(a,b)$ é il massimo valore intero che divide sia a che b

$(d|b \wedge d|a)$

7.1 Algoritmo di Euclide

$gcd(a,b) = ? \longrightarrow \exists q, r_0 \in \mathbb{Z}.\quad a = qb + r_0 \quad 0 \leq r_0 < |b|$

$$b = q_0 r_0 + r_1 \quad 0 \leq r_1 < r_0$$

$$r_0 = q_1 r_1 + r_2 \quad 0 \leq r_2 < r_1$$

$$\vdots$$

$$r_{n-2} = q_{n-1} r_{n-1} + r_n$$

$$r_{n-1} = q_n r_n = gcd(a,b)$$

7.2 Identitá di Bezout

$gcd(a,b) = d \quad \Rightarrow \exists u,v \in \mathbb{Z}.\ d = va + ub$

7.3 Classi di congruenza

Dfn Dati $a, b, n \in \mathbb{Z}$ $(n > 0)$, a é congruente a b modulo n $(a \equiv_n b)$ se $n \mid a - b$

Prop:

1. riflessiva 2. simmetrica 3. transitiva

quindi é una relazione di equivalenza

↓

Se $a, b, c, d, n \in \mathbb{Z}$ e $n > 0$, $a \equiv_n b$ e $c \equiv_n d$, allora:

4. $a + d \equiv_n b + c$
5. $da \equiv_n cb$

→ sono le operazioni elementari che possiamo fare sulle equazioni normali!

Dfn Classi di congruenza

Dati $a, n \in \mathbb{Z}$, $[a]_n$ é l'insieme degli interi congrui ad a modulo n:

$$[a]_n = \{b \in \mathbb{Z} \mid b \equiv_n a\} = \{a + kn \mid k \in \mathbb{Z}\}$$

Dfn Interi modulo n

Si chiama insieme degli interi modulo n l'insieme

$$\mathbb{Z}_n = \{[a]_n \mid a \in \mathbb{Z}\}$$

Prop:

1. Sia r il resto di a diviso n, allora $[a]_n = [r]_n$
2. Le classi $[0]_n \dots [n-1]_n$ sono distinte
3. $\mathbb{Z}_n = \{[0]_n, \dots, [n-1]_n\}$

Dim

1. $a=qn+r$ D.d. $n|a-r$, ovvero $n|qn$ □

2. D.d. $\forall i,j\in\{1,\dots,n-1\}.\ [i]_n=[j]_n \Rightarrow i=j$. Assumiamo $i\geq j$,
$[i]_n=[j]_n$, $i-j<n$, $[i]_n-[j]_n=[0]_n$ $[i-j]_n=[0]_n$
quindi $n|i-j$ ma $i-j<n$, quindi $i-j=0$ e $i=j$

3. Uso ax. ext. $\Leftarrow$ è ovvio per def. $\mathbb{Z}_n$.
$\Rightarrow$) D.d. $\forall a\in\mathbb{Z}.\ [a]_n\in\{[0]_n,\dots,[n-1]_n\}$. $a=qn+r$,
per ① sappiamo che $[a]_n=[r]_n$ e $0\leq r<n$, quindi
$[r]_n\in\{[0]_n,\dots,[n-1]_n\}$

Dfn Invertibile

$[a]_n\in\mathbb{Z}_n$ è invertibile se $\exists [b]_n\in\mathbb{Z}_n.\ [b]_n[a]_n=[1]_n$

Prop.

$[a]_n\in\mathbb{Z}_n$ ha un inverso in $\mathbb{Z}_n$ sse $\gcd(a,n)=1$

Dim

$\Leftarrow$) $d=\gcd(a,n)=1$. Per Bezout $\exists b,c.\ ab+nc=1$

$[a]_n[b]_n \cancel{+[0]_n} = 1$ $[b]_n$ è l'inverso!

$\Rightarrow$) $[b]_n[a]_n=[1]_n$, quindi $n|ba-1$, quindi $\exists r$.
$ba-1=nr$. Se $d=\gcd(a,n)$, sappiamo che
$d|a$ e $d|n$, quindi $d|ac+nr$ (???) ovvero $d|1$
quindi $d=1$ □

Se $a|b$ e $a|c$ allora
$a|b+c$ e $a|b-c$