Quaderno di Antonio Lorenzin del corso di

Geometria I

Tenuto da Claudio Fontanari

SPAZIO VETTORIALE

Per poter dare la definizione di spazio vettoriale necessitiamo di un "campo", che informalmente definiamo come un insieme che contiene l′inverso moltiplicativo dei suoi elementi (tranne lo 0, che non ha inversi). Per indicare un campo useremo la lettera k. Degli esempi sono $k=\mathbb{R},\mathbb{Q},\mathbb{C}$.

DEFINIZIONE 1.1. Uno *spazio vettoriale* su k è un insieme V dotato delle seguenti due operazioni

- Somma: $+: V\times V\to V \quad (v,w)\to v+w$
- Prodotto scalare: $\cdot: k\times V\to V \quad (\lambda,v)\to\lambda v$

che soddisfa le seguenti proprietà:

S1.	$v+w=w+v$ per ogni $v,w\in V$	proprietà commutativa
S2.	$v+(w+z)=(v+w)+z$ per ogni $v,w,z\in V$	proprietà associativa
S3.	$\exists\, 0_V\in V$ tale che $v+0_V=0_V+v=v$ per ogni $v\in V$	esistenza dell′elemento neutro
S4.	$\forall v\in V\ \exists -v\in V$ tale che $v+(-v)=0_V=(-v)+v$	esistenza dell′opposto
P1.	$(ab)v=a(bv)=b(av)$ per ogni $a,b\in k$, $v\in V$	pseudo-associatività
P2.	$1\cdot v=v\cdot 1=v$ per ogni $v\in V$	neutralità di 1
D1.	$a(v+w)=av+bw$ per ogni $a\in k$, $v,w\in V$	prima proprietà
D2.	$(a+b)v=av+bv$ per ogni $a,b\in k$, $v\in V$	seconda proprietà

Si noti che le proprietà S,P,D sono rispettivamente riguardanti la somma, il prodotto per scalare e la distribuzione di esse.

ESEMPI 1.1.

1) $(\mathbb{R}^n,+,\cdot)$ è uno spazio vettoriale su $\mathbb{R}$ con la somma per componenti ed il prodotto scalare che moltiplica ogni componente per lo scalare.
2) Spazio dei polinomi. Il generico polinomi di grado k in una indeterminata a coefficienti reali ($a_i\in\mathbb{R}$) si scrive $\sum_{i=0}^{k} a_i x^i$. Lo spazio dei polinomi sarà perciò
$$\mathbb{R}[x]:=\left\{\sum_{i=0}^{k} a_i x^i,\ k\in\mathbb{N}, a_i\in\mathbb{R}\right\}$$
con la somma ed il prodotto per scalare definiti come naturale, ovvero
$$f(x)+g(x)=\sum_{i=0}^{h}(a_i+b_i)x^i+\sum_{i=h+1}^{k} a_i x^i,\quad \lambda\cdot f(x)=\sum_{i=0}^{k}\lambda a_i x^i$$
ove $f(x)=\sum_{i=0}^{k} a_i x^i$, $g(x)=\sum_{i=0}^{h} b_i x^i$ ed è stato supposto che $k\geq h$.

DEFINIZIONE 1.2. Preso V spazio vettoriale su k e W sottoinsieme di V, W è un *sottospazio vettoriale* se

1. $0_V\in W$
2. Per ogni $w_1,w_2\in W$, $w_1+w_2\in W$
3. Per ogni $\lambda\in k, w\in W$, $\lambda w\in W$

Si osservi che se W è un sottospazio vettoriale, allora $(W,+,\cdot)$ è uno spazio vettoriale su k.

OSSERVAZIONE 1.1. Vogliamo studiare l'intersezione e l'unione di sottospazi vettoriali. Prendiamo k campo, $(V,+,\cdot)$ spazio vettoriale su k e W_1, W_2 due sottospazi vettoriali di V. Si ricordi che

$$W_1 \cap W_2 := \{v \in V \mid v \in W_1 \text{ e } v \in W_2\}$$
$$W_1 \cup W_2 := \{v \in V \mid v \in W_1 \text{ o } v \in W_2\}$$

L'intersezione è un sottospazio vettoriale? Verifichiamo le tre proprietà:

1. $0_V \in W_1$, $0_V \in W_2$. Dunque $0_V \in W_1 \cap W_2$
2. $v_1, v_2 \in W_1$, perciò $v_1 + v_2 \in W_1$; analogamente per W_2. Quindi $v_1 + v_2 \in W_1 \cap W_2$
3. $v \in W_1 \cap W_2$, $\lambda \in k$: $\lambda v \in W_1$, $\lambda v \in W_2$. Perciò $\lambda v \in W_1 \cap W_2$

Dunque la risposta è sì: *l'intersezione di due spazi vettoriali è uno spazio vettoriale*.
Se invece considerassimo l'unione arriveremo alla stessa conclusione? No, vediamo un controesempio. Si prendano $V = \mathbb{R}^2$ spazio vettoriale, $W_1 = \{(a,0) : a \in \mathbb{R}\}$ e $W_2 = \{(0,b) : b \in \mathbb{R}\}$ sottospazi vettoriali. Proviamo a verificare le tre proprietà:

1. $0_{\mathbb{R}^2} = (0,0) \in W_1$. Perciò $0_{\mathbb{R}^2} \in W_1 \cup W_2$
2. Prendo $(1,0) \in W_1$, $(0,1) \in W_2$. $(1,0) + (0,1) = (1,1) \notin W_1 \cup W_2$

Dunque *l'unione di due sottospazi vettoriali non è sempre uno spazio vettoriale*, dato che non vale la seconda condizione.

OSSERVAZIONE 1.2. Vogliamo ora determinare "il più piccolo" sottospazio vettoriale di V che contiene $V_1 \cup V_2$ con V_1 e V_2 sottospazi vettoriali.
Sia W un sottospazio vettoriale di V che contiene $V_1 \cup V_2$. Allora vale che per ogni $v_1 \in V_1$ e $v_2 \in V_2$ si ha $v_1 + v_2 \in W$. Definiamo *la somma di due sottospazi vettoriali* come

$$V_1 + V_2 := \{v_1 + v_2 \mid v_1 \in V_1, v_2 \in V_2\}$$

Dunque se W è come detto precedentemente, $V_1 + V_2 \subseteq W$.

PROPOSIZIONE 1.1. $V_1 + V_2$ è un sottospazio vettoriale di V.

DIMOSTRAZIONE. Verifichiamo le tre proprietà:

1. $0_V \in V_1$, $0_V \in V_2$. Allora $0_V + 0_V = 0_V \in V_1 + V_2$
2. $v_1 + v_2$, $w_1 + w_2 \in V_1 + V_2$. Allora $(v_1 + v_2) + (w_1 + w_2) = (v_1 + w_1) + (v_2 + w_2) \in V_1 + V_2$
3. $\lambda \in k$, $(v_1 + v_2) \in V_1 + V_2$. Allora $\lambda(v_1 + v_2) = \lambda v_1 + \lambda v_2 \in V_1 + V_2$

Grazie ad osservazione 1.2 e proposizione 1.1, si ottiene che $V_1 + V_2$ è il più piccolo sottospazio vettoriale di V che contiene $V_1 \cup V_2$.

DEFINIZIONE 1.3. Sia V spazio vettoriale sul campo k. Prendiamo $v_1, v_2, \dots, v_n \in V$ e $a_1, a_2, \dots, a_n \in k$. Allora la *combinazione lineare* dei vettori $v_1, \dots, v_n$ a coefficienti $a_1, \dots, a_n$ è il vettore

$$a_1 v_1 + a_2 v_2 + \dots + a_n v_n \in V$$

Fissati $v_1, \dots, v_n \in V$, consideriamo l'insieme delle loro combinazioni lineari:

$$\mathcal{L}(v_1, v_2, \dots, v_n) := \{a_1 v_1 + a_2 v_2 + \dots + a_n v_n \mid a_i \in k \text{ per ogni } i\}$$

PROPOSIZIONE 1.2. Per ogni $v_1, v_2, \dots, v_n \in V$, $\mathcal{L}(v_1, v_2, \dots, v_n)$ è un sottospazio vettoriale di V.

DIMOSTRAZIONE. Dobbiamo vedere che valgano le tre proprietà:

1. $0_V=0v_1+0v_2+\ldots+0v_n\in\mathcal{L}(v_1,v_2,\ldots,v_n)$
2. $(a_1v_1+\ldots+a_nv_n)+(b_1v_1+\ldots+b_nv_n)=(a_1+b_1)v_1+\ldots+(a_n+b_n)v_n\in\mathcal{L}(v_1,v_2,\ldots,v_n)$
3. $\lambda\in k:\ \lambda(a_1v_1+\ldots a_nv_n)=\lambda a_1v_1+\ldots+\lambda a_nv_n\in\mathcal{L}(v_1,v_2,\ldots,v_n)$

DEFINIZIONE 1.4. $\mathcal{L}(v_1,v_2,\ldots,v_n)$ si dice il *sottospazio vettoriale generato* da $v_1,v_2,\ldots,v_n$. Se W è un sottospazio vettoriale di V e $W=\mathcal{L}(v_1,v_2,\ldots,v_n)$, i vettori $v_1,v_2,\ldots,v_n$ sono detti *generatori* di W.

Consideriamo $V=\mathbb{R}^n$. Posso prendere

$$e_1=(1,0,\ldots,0),\ e_2=(0,1,0,\ldots,0),\ \ldots,\ e_n=(0,\ldots,0,1)$$

Viene naturale pensare che il sottospazio generato copre in realtà tutto $\mathbb{R}^n$. Proviamolo.

PROPOSIZIONE 1.3. I vettori $e_1,e_2,\ldots,e_n$ generano $\mathbb{R}^n$.

DIMOSTRAZIONE. Verifichiamo che $\mathbb{R}^n=\mathcal{L}(e_1,e_2,\ldots,e_n)$.

$$\mathcal{L}(e_1,e_2,\ldots,e_n)=\{a_1e_1+\ldots+a_ne_n\mid a_i\in\mathbb{R}\}=\{a_1(1,0,\ldots,0)+\ldots+a_n(0,\ldots,0,1)\mid a_i\in\mathbb{R}\}=$$
$$=\{(a_1,0,\ldots,0)+\ldots+(0,\ldots,0,a_n)\mid a_i\in\mathbb{R}\}=\{(a_1,\ldots,a_n)\mid a_i\in\mathbb{R}\}=\mathbb{R}^n$$

DEFINIZIONE 1.5. Preso $(V,+,\cdot)$ spazio vettoriale su k, i vettori $v_1,\ldots,v_n\in V$ si dicono *linearmente indipendenti* se l'uguaglianza $a_1v_1+a_2v_2+\ldots+a_nv_n=0$ implica che $a_1=a_2=\ldots=a_n=0$.

Continuiamo a considerare $\mathbb{R}^n$ con i vettori $e_1,\ldots,e_n$. Si noti che essi sono linearmente indipendenti: infatti se $a_1e_1+\ldots+a_ne_n=0_{\mathbb{R}^n}$, allora $a_1(1,0,\ldots,0)+\ldots+a_n(0,\ldots,0,1)=0_{\mathbb{R}^n}$. Perciò $(a_1,a_2,\ldots,a_n)=0_{\mathbb{R}^n}$, da cui ricavo semplicemente che $a_1=\ldots=a_n=0$.

OSSERVAZIONE 1.3. Essere generatori ed essere linearmente indipendenti sono due proprietà diverse. Inoltre, se $v_1,\ldots,v_n$ non sono linearmente indipendenti, si dicono *linearmente dipendenti*.

DEFINIZIONE 1.6. Preso $(V,+,\cdot)$ spazio vettoriale su k, un insieme ordinato di vettori di V $(v_1,\ldots,v_n)$ si dice una *base* di V se

1. $V=\mathcal{L}(v_1,\ldots,v_n)$
2. $v_1,\ldots,v_n$ sono linearmente indipendenti.

Per quanto precedentemente visto, $(e_1,\ldots,e_n)$ è base di $\mathbb{R}^n$ e viene detta *base canonica*.

PROPOSIZIONE 1.4. Preso $(V,+,\cdot)$ spazio vettoriale su k e $(v_1,\ldots,v_n)$ base di V, allora per ogni $v\in V$ esistono unici $a_1,\ldots,a_n\in k$ tali che

$$v=a_1v_1+\ldots+a_nv_n$$

A livello terminologico, diremo che $a_1,\ldots,a_n$ sono le *componenti* di v nella base fissata.

DIMOSTRAZIONE. Per ogni $v\in V$ si ha $v=a_1v_1+\ldots+a_nv_n$ poichè $v_1,\ldots,v_n$ sono generatori di V. Verifichiamo l′unicità; si noti che basta provare che se $v=a_1 v_1+\ldots+a_n v_n=b_1 v_1+\ldots+b_n v_n$, allora $a_i=b_i$ per ogni i. Anzitutto, vale che $(a_1-b_1)v_1+\ldots+(a_n-b_n)v_n=0_V$. Poichè $v_1,\ldots,v_n$ sono linearmente indipendenti, $a_1-b_1=\ldots=a_n-b_n=0$, ovvero $a_i=b_i$ per ogni i.

ESEMPIO 1.2. Supponiamo che $(p_1,\ldots,p_n)$ sia una base di $k[x]$ (spazio vettoriale che contiene tutti i polinomi, $k[x]=\{a_n x^n+\ldots+a_1 x+a_0 \mid a_i\in k\}$). Ogni polinomio p in x si può allora scrivere in modo unico come

$$p=a_1 p_1+\ldots+a_n p_n$$

con $a_i\in k$. Sia $d=max\{grado(p_i) \text{ per ogni } i\}$. Condieriamo $q\in k[x]$ con grado $d+1$. Se vale che

$$q=a_1 p_1+\ldots+a_n p_n$$

potrei avere una base di $k[x]$, ma ciò è impossibile in quanto q ha grado $d+1$, mentre $a_1 p_1+\ldots+a_n p_n$ ha al massimo grado d. Dunque $k[x]$ non ammette una base.

DEFINIZIONE 1.7. Se $(V,+,\cdot)$ spazio vettoriale su k ha una base $(v_1,\ldots,v_n)$ formata da n vettori, si dice che V ha *dimensione* n. Se invece V non ammette una base, diremo che esso ha *dimensione infinita*. Indicheremo la dimensione di V con $dim(V)$.

ESEMPI 1.3. Si ha che k^n ha dimensione n, mentre $k[x]$ ha dimensione infinita.

TEOREMA 1.1: Per l′unicità della dimensione di V. Se $(v_1,\ldots,v_n)$ e $(w_1,\ldots,w_m)$ sono basi di V, allora si ha $m=n$.

Abbiamo bisogno del seguente risultato:

LEMMA 1.1: Di Steinitz. Siano V uno spazio vettoriale su k e $v_1,\ldots,v_m\in V$ vettori linearmente indipendenti e $w_1,\ldots,w_n\in V$ vettori generatori. Allora $m\leq n$.

DIMOSTRAZIONE di Teorema 1.1. Grazie al lemma di Steinitz,

$(v_1,\ldots,v_n)$ base, in particolare	linearmente indipendenti	generatori
$(w_1,\ldots,w_m)$ base, in particolare	generatori	linearmente indipendenti
	$m\leq n$	$n\leq m$

Allora $m\leq n\leq m$, ovvero $m=n$.

PROPOSIZIONE 1.5. Sia V uno spazio vettoriale di dimensione finita e sia W un sottospazio vettoriale di V. Allora si ha $dim(W)\leq dim(V)$ e se $dim(W)=dim(V)$, allora $W=V$.

DIMOSTRAZIONE. Sia $(v_1,\ldots,v_m)$ una base di V ($dim(V)=m$) e $(w_1,\ldots,w_n)$ una base di W (dunque si ha $dim(W)=n$). Poichè $w_1,w_2,\ldots,w_n$ sono linearmente indipendenti e $v_1,\ldots,v_m$ sono generatori, si ottiene $n\leq m$.
Supponiamo che $n=m$. Se $w_1,\ldots,w_n$ sono generatori di V, si ha $V=\mathcal{L}(w_1,\ldots,w_n)\subseteq W\subseteq V$ e quindi ho dimostrato la seconda parte della proposizione, infatti $V=W$.
Supponiamo per assurdo che $w_1,\ldots,w_n$ non siano generatori di V. Allora esiste $v\in V$ tale che

$$v\notin\mathcal{L}(w_1,\ldots,w_n)$$

Affermo che $v, w_1, \dots, w_n$ sono linearmente indipendenti. Allora

$$av + a_1 w_1 + \dots + a_n w_n = 0$$

per qualche $a, a_i \in k$. Allora $a = 0$, altrimenti $v = (-a_1 w_1 - \dots - a_n w_n)/a \in \mathcal{L}(w_1, \dots, w_n)$. Dunque, poichè $w_1, \dots, w_n$ sono linearmente indipendenti, vale che $a_1 = a_2 = \dots = a_n = 0$. Tuttavia così avrei $n+1$ vettori linearmente indipendenti e $m = n$ vettori generatori, in contraddizione con il lemma di Steinitz.

TEOREMA 1.2: Formula di Grassmann. Sia $(V, +, \cdot)$ spazio vettoriale di dimensione finita. Siano U e W sottospazi di V. Allora

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

Dimostrazione del lemma di Steinitz (lemma 1.1)

Supponiamo per assurdo che $n > m$. Per ottenere una contraddizione basta verificare che $v_1, v_2, \dots, v_m$ sono generatori di V (si veda l'enunciato).
Infatti $v_1, \dots, v_m$ generatori significa che $V = \mathcal{L}(v_1, \dots, v_m) = \{a_1 v_1 + \dots + a_m v_m \mid a_i \in k\}$; in particolare,

$$v_{m+1} = a_1 v_1 + \dots + a_m v_m$$

da cui otterrei $a_1 v_1 + \dots + a_m v_m - v_{m+1} + 0 v_{m+2} + \dots + 0 v_n = 0$, che è una combinazione lineare nulla dei vettori $v_1, \dots, v_n$. Tuttavia, essendo questi ultimi linearmente indipendenti, la loro somma non può essere nulla se non quando tutti i coefficienti sono nulli. Perciò, se $v_1, \dots, v_m$ sono generatori, vale il lemma di Steinitz.
Per la dimostrazione della tesi ridotta ($v_1, \dots, v_m$ generatori), usiamo il *principio di induzione di Peano*:

"Data $P(n)$ proprietà che dipende da $n \in \mathbb{N}$, se $P(1)$ vale e
$P(s)$ implica $P(s+1)$, allora $P(n)$ vale per ogni $n \in N$."

$P(1)$ vale:
Dato che $w_1, \dots, w_m$ sono generatori, allora $v_1 = b_1 w_1 + \dots + b_m w_m$. Non è possibile che $b_i = 0$ per ogni i che va da 1 a m, altrimenti $v_1 = 0$ e dunque $v_1, \dots, v_n$ non sono linearmente indipendenti. A meno di riordinare, posso supporre che $b_1 \neq 0$. Dunque

$$w_1 = \frac{v_1}{b_1} - \frac{b_2}{b_1} w_2 - \dots - \frac{b_m}{b_1} w_m$$

Si noti quindi che $w_1 \in \mathcal{L}(v_1, w_2, \dots, w_m)$; naturalmente, $w_2, \dots, w_m \in \mathcal{L}(v_1, w_2, \dots, w_m)$ e perciò

$$V = \mathcal{L}(w_1, w_2, \dots, w_m) \subseteq \mathcal{L}(v_1, w_2, \dots, w_m) \subseteq V,$$

da cui $V = \mathcal{L}(v_1, w_2, \dots, w_m)$.
$P(s)$ implica $P(s+1)$:
Posso supporre che $A = v_1, \dots, v_s, w_{s+1}, \dots, w_m$ siano generatori. Verifichiamo che $v_1, \dots, v_{s+1}, w_{s+1}, \dots, w_m$ sono generatori. Anzitutto, si ha che

$$v_{s+1} = a_1 v_1 + \dots + a_s v_s + a_{s+1} w_{s+1} + \dots + a_m w_m$$

con $a_i \in k$. Non è possibile che $a_{s+1} = a_{s+2} = \dots = a_m = 0$, altrimenti $v_1, \dots, v_n$ non sarebbero linearmente indipendenti. Posso quindi supporre che $a_{s+1} \neq 0$.

$$w_{s+1} = -\frac{a_1}{a_{s+1}} v_1 - \dots - \frac{a_s}{a_{s+1}} v_s + \frac{1}{a_{s+1}} v_{s+1} - \frac{a_{s+2}}{a_{s+1}} w_{s+2} - \dots - \frac{a_m}{a_{s+1}} w_m$$

Allora $w_{s+1} \in \mathcal{L}(v_1, \ldots, v_{s+1}, w_{s+2}, \ldots, w_m)$. In più $v_1, \ldots, v_s, w_{s+2}, \ldots, w_m \in \mathcal{L}(v_1, \ldots, v_{s+1}, w_{s+2}, \ldots, w_m)$. Dunque ho

$$V = \mathcal{L}(v_1, \ldots, v_s, w_{s+1}, \ldots, w_m) \subseteq \mathcal{L}(v_1, \ldots, v_{s+1}, w_{s+2}, \ldots, w_m) \subseteq V$$

Allora $V = \mathcal{L}(v_1, \ldots, v_{s+1}, w_{s+2}, \ldots, w_m)$.
Perciò $v_1, \ldots, v_m$ sono generatori di V. Ho quindi dimostrato il lemma di Steinitz.

PROPOSIZIONE 1.6: Tecnica di completamento a una base. Sia $(V, +, \cdot)$ uno spazio vettoriale su k con $dim(V) = n$. Se $v_1, \ldots, v_k$ sono vettori linearmente indipendenti di V, allora esistono $v_{k+1}, \ldots, v_n$ tali che $(v_1, \ldots, v_n)$ è una base di V.

DIMOSTRAZIONE. Se $v_1, v_2, \ldots, v_k$ sono anche generatori, allora $v_1, \ldots, v_k$ è una base e $k = n$. Se invece $v_1, v_2, \ldots, v_k$ non sono generatori di V, si ha che $\mathcal{L}(v_1, \ldots, v_k) \subset V$ strettamente; esiste perciò $v \in V$ tale che $v \notin \mathcal{L}(v_1, \ldots, v_k)$. Sia $v_{k+1} := v$. Verifichiamo che $v_1, v_2, \ldots, v_{k+1}$ sono linearmente indipendenti:

$$a_1 v_1 + \ldots + a_{k+1} v_{k+1} = 0$$

con $a_i \in k$. Se $a_{k+1} \neq 0$, si avrebbe

$$v_{k+1} = -\frac{a_1}{a_{k+1}} - \ldots - \frac{a_k}{a_{k+1}} v_k$$

da cui si otterrebbe $v_{k+1} \in \mathcal{L}(v_1, \ldots, v_k)$, che contraddice la tesi. Perciò $a_{k+1} = 0$. Dato che $v_1, \ldots, v_k$, questo basta per avere che $a_1 = a_2 = \ldots = a_k = 0$. Se ne ricava che $v_1, \ldots, v_{k+1}$ sono linearmente indipendenti. Ripetendo la stessa procedura per $n-k$ passi, otteniamo che $v_1, \ldots, v_k, v_{k+1}, \ldots, v_n$ sono linearmente indipendenti e devono essere anche generatori di V, altrimenti riapplicando ancora una volta la procedura contraddiremmo il lemma di Steinitz (se $dim(V) = n$, V ha n generatori e quindi non possiamo avere più vettori linearmente indipendenti).

DIMOSTRAZIONE della formula di Grassmann (teorema 1.2). Sia $(z_1, \ldots, z-q)$ una base di $U \cap W$. Applicando la tecnica di completamento a una base, ottengo:

- $(z_1, \ldots, z_q, u_1, \ldots, u_t)$ base di U
- $(z_1, \ldots, z_q, w_1, \ldots, w_s)$ base di W

Quindi, se verifichiamo che $\mathcal{B}(U+W) = (z_1, \ldots, z_q, u_1, \ldots, u_t, w_1, \ldots, w_s)$ è una base di $U+W$, allora otteniamo la tesi. Infatti, in dato caso si avrebbe

$$\underbrace{q+t}_{dim(U)} + \underbrace{q+s}_{dim(W)} = \underbrace{q}_{dim(U \cap W)} + \underbrace{q+t+s}_{dim(U+W)}$$

Mostriamo che $\mathcal{B}(U+W)$ sono generatori di $U+W$. Sia $u+w \in U+W$. Poichè $u \in U$ e $w \in W$, allora

$$u = a_1 z_1 + \ldots + a_q z_q + b_1 u_1 + \ldots + b_t u_t, \quad w = c_1 z_1 + \ldots + c_q z_q + d_1 w_1 + \ldots + d_s w_s$$

Ne segue immediatamente che

$$u+w = (a_1 + c_1) u_1 + \ldots + (a_q + c_q) z_q + b_1 u_1 + \ldots + b_t u_t + d_1 w_1 + \ldots + d_s w_s \in \mathcal{L}(z_1, \ldots, z_q, u_1, \ldots, u_t, w_1, \ldots, w_s)$$

Dobbiamo vedere quindi che $\mathcal{B}(U+W)$ sono linearmente indipendenti di $U+W$.

$$a_1 z_1 + \ldots + a_q z_q + b_1 u_1 + \ldots + b_t u_t + c_1 w_1 + \ldots + c_s w_s = 0$$
$$a_1 z_1 + \ldots + a_q z_q + b_1 u_1 + \ldots + b_t u_t = -c_1 w_1 - \ldots - c_s w_s =: v$$

Si vede subito che $v \in U \cap W$, dato che abbiamo da una parte l'uguaglianza con dei vettori di U e dall'altra con dei vettori di W. Allora $v=d_1 z_1+\dots d_q z_q$. Si ricava quindi che

$$c_1 w_1+\dots+c_s w_s+d_1 z_1+\dots+d_q z_q=0$$

da cui ottengo $c_1=\dots=c_s=d_1=\dots=d_q=0$, dato che $(z_1,\dots,z_q,w_1,\dots,w_s)$ è base di W. Da questo, si ha che

$$a_1 z_1+\dots+a_q z_q+b_1 u_1+\dots+b_t u_t=0$$

per cui $a_1=\dots=a_q=b_1=\dots=b_t=0$, poichè $(z_1,\dots,z_q,u_1,\dots,u_t)$ è base di U.

Abbiamo quindi dimostrato che $\mathcal{B}(U+W)$ è una base di $U+W$ e quindi la formula è verificata.

MATRICI E SISTEMI LINEARI

DEFINIZIONE 2.1. Sia k un campo ed m,n dei numeri naturali non nulli. Allora

$$k^{m,n} := \left\{ \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} : a_{ij} \in k \right\}$$

è detto *spazio delle matrici*. I contatori i, j sono rispettivamente riferiti alla riga ed alla colonna. a_{ij} si dicono *coefficienti* della *matrice* A, che è un elemento di $k^{m,n}$.

Su $k^{m,n}$ definiamo due operazioni:

$$+ \text{ somma: } \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} + \begin{pmatrix} b_{11} & \dots & b_{1n} \\ \vdots & & \vdots \\ b_{m1} & \dots & b_{mn} \end{pmatrix} = \begin{pmatrix} a_{11}+b_{11} & \dots & a_{1n}+b_{1n} \\ \vdots & & \vdots \\ a_{m1}+b_{m1} & \dots & a_{mn}+b_{mn} \end{pmatrix}$$

$$\cdot \text{ prodotto per scalare con } \lambda \in k \text{: } \lambda \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} = \begin{pmatrix} \lambda a_{11} & \dots & \lambda a_{1n} \\ \vdots & & \vdots \\ \lambda a_{m1} & \dots & \lambda a_{mn} \end{pmatrix}$$

Si ha che $(k^{m,n}, +, \cdot)$ è uno spazio vettoriale su k.

DEFINIZIONE 2.2. Prendiamo $(a_{ij}) \in k^{m,n}$; si definiscano $R_i := (a_{i1}, \dots, a_{¿}) \in k^n$ *vettore riga* per ogni i e $C_j := (a_{1j}, \dots, a_{mj}) \in k^m$ *vettore colonna* per ogni j. Consideriamo lo *spazio delle righe* e lo *spazio delle colonne* rispettivamente

$$\mathcal{L}(R_1, \dots, R_m) \subseteq k^n, \quad \mathcal{L}(C_1, \dots, C_n) \subseteq k^m$$

A questo punto, possiamo considerare le seguenti due definizioni: il *rango per righe* di una matrice sarà $\rho := dim\, \mathcal{L}(R_1, \dots, R_m)$, mentre il *rango per colonne* è $\sigma := dim\, \mathcal{L}(C_1, \dots, C_n)$.

DEFINIZIONE 2.3. $A \in k^{m,n}$ è *ridotta (per righe)* se ogni riga non nulla di A contiene un elemento diverso da 0 al di sotto del quale compaiono soltanto zeri.

PROPOSIZIONE 2.1. Sia A una matrice ridotta in $k^{m,n}$. Allora il rango di A è uguale al numero di righe non nulle di A.

DIMOSTRAZIONE. Si consideri $A = (a_{ij})$ con $i = 1, \dots, m$ e $j = 1, \dots, n$. So che $\rho(A) = dim\, \mathcal{L}(R_1, \dots, R_m)$ con R_i come in definizione 2.2. Possiamo supporre che le eventuali righe nulle di A siano le ultime; perciò

$$\rho(A) = dim\, \mathcal{L}(R_1, \dots, R_s)$$

con $s \le n$. Se $R_1, \dots, R_s$ sono linearmente indipendenti, allora $(R_1, \dots, R_s)$ è una base di $\mathcal{L}(R_1, \dots, R_s)$ e dunque dell'intero spazio delle righe. Dunque, $\rho(A) = s$ (ovvero il numero di righe non nulle di A).
Prendiamo in esame la seguente situazione: $c_1 R_1 + c_2 R_2 + \dots c_s R_s = 0_{k^n}$. Poichè A è ridotta, esiste h con $1 \le h \le n$ tale che $a_{1h} \ne 0$ e $a_{rh} = 0$ con $r \ge 2$. Dunque, considerata la componente h-esima,

$$c_1 a_{1h} + c_2 a_{2h} + \dots + c_s a_{sh} = 0$$

da cui si ricava immediatamente che $c_1=0$. Poichè A ridotta, esiste t con $1\leq t\leq h$ tale che $a_{2t}\neq 0$ e $a_{pt}=0$ per ogni $p\geq 3$. Considero la componente t-esima ed ottengo $d_2 a_{2t}+d_3 a_{3t}+\ldots+d_s a_{st}=0$, perciò $d_2=0$. Ripetendo s volte questa procedura si ottiene che $R_1,\ldots,R_s$ sono linearmente indipendenti.

Presa una matrice $A\in k^{m,n}$, vogliamo trovare A' ridotta tale che $\rho(A)=\rho(A')$. Si considerino le seguenti *trasformazioni elementari*, ricordando che le righe della matrice sono indicate con R_i;

$E1$ $R_i\to aR_i (a\neq 0)$ $\mathcal{L}(R_1,\ldots,R_i,\ldots,R_m)=\mathcal{L}(R_1,\ldots,aR_i,\ldots,R_m)$

$E2$ $R_i\to R_j, R_j\to R_i$ $\mathcal{L}(R_1,\ldots,R_i,\ldots,R_j,\ldots,R_m)=\mathcal{L}(R_1,\ldots,R_j,\ldots,R_i,\ldots,R_m)$

$E3$ $R_i\to R_i+bR_j (j\neq i)$ $\mathcal{L}(R_1,\ldots,R_i,\ldots,R_j,\ldots,R_m)=\mathcal{L}(R_1,\ldots,R_i+bR_j,\ldots,R_j,\ldots,R_m)$

Grazie a quanto scritto a destra, si vede che queste trasformazioni sono ben definite.

DEFINIZIONE 2.4. Prese $A\in k^{m,n}$ e $B\in k^{n,q}$, definisco il *prodotto riga per colonna* come l'operatore che restituisce $A\cdot B=C\in k^{m,q}$ ove $c_{ij}=a_{i1}b_{1j}+a_{i2}b_{2j}+\ldots+a_{in}b_{nj}$.
In generale, si nota che $A\cdot B\neq B\cdot A$.

DEFINIZIONE 2.5. Si consideri la seguente terminologia:

1. $A\in k^{m,m}$ si dice *quadrata*
2. La *trasposta* di $A\in k^{m,n}$, indicata con $A^t={}^tA$, appartiene a $k^{n,m}$ è la matrice ottenuta da A scambiando le righe con le colonne.
3. A è *simmetrica* se $A=A^t$.

Si noti che se A è simmetrica, allora A è quadrata. Infatti presa $A\in k^{m,n}$, allora $A^t\in k^{n,m}$, ma $A=A^t$ implica che $m=n$.

DEFINIZIONE 2.6. Un sistema lineare di m equazioni in n incognite $(x_1,\ldots,x_n)$ è

$$\begin{cases} a_{11}x_1+a_{12}x_2+\ldots+a_{1n}x_n=b_1\\ a_{21}x_1+a_{22}x_2+\ldots+a_{2n}x_n=b_2\\ \vdots\\ a_{m1}x_1+a_{m2}x_2+\ldots+a_{mn}x_n=b_m\end{cases}$$

ove $a_{ij}\in k$ vengono detti *termini noti*, mentre $b_i\in k$ sono i *termini noti*. Una soluzione del sistema è una n-upla $(h_1,\ldots,h_n)\in k^n$ che soddisfa contemporaneamente tutte le equazioni del sistema.

OSSERVAZIONE 2.1. Un sistema lineare può essere scritto in forma matriciale nel seguente modo: presi $A\in k^{m,n}$ detta *matrice dei coefficienti*, $X\in k^{n,1}$ detto *vettore delle incognite* e $B\in k^{m,1}$ detto *vettore dei termini noti*,

$$AX=B$$

Si noti che quanto scritto è ben definito perchè posso fare il prodotto riga per colonna fra A ed X ed ottengo una matrice di $k^{m,1}$, che è lo spazio delle matrici che contiene B.
Da questo, se $B=0$, ovvero se $b_1=\ldots=b_m=0$, allora le soluzioni del sistema lineare

$$AX=0$$

sono le relazioni di dipendenza lineare fra le colonne di A. Per l'importanza di questo caso particolare, un sistema ove i termini noti sono tutti nulli ha un suo nome indentificativo: esso è un *sistema omogeneo*.

TEOREMA 2.1. Sia $A \in k^{m,n}$. Allora il rango per righe $\rho(A)$ e il rangono per colonne $\sigma(A)$ coincidono.

DIMOSTRAZIONE. Sia $\rho(A)=r=dim\,\mathcal{L}(R_1, R_2, \dots, R_m)$. Per quanto appena visto in osservazione 2.1, il rango per colonne di A dipende dalle soluzioni del sistema lineare omogeneo $AX=0$. Possiamo supporre che le prime r equazioni di $AX=0$ siano linearmente indipendenti e che le rimanenti $m-r$ siano combinazione lineare delle prime r. Sia $A^*=(R_1, R_2, \dots, R_r)^t \in k^{r,n}$. Poichè le soluzioni di $AX=0$ coincidono con le soluzioni di $A^* X=0$, allora

$$\sigma(A)=\sigma(A^*)\leq r=\rho(A)$$

Infatti le colonne di A^* sono vettori di k^r. Pertanto $\sigma(A)\leq\rho(A)$ per ogni matrice A. Consideriamo la trasposta di A: $\sigma(A^t)\leq\rho(A^t)$; si ottiene quindi che $\rho(A)\leq\sigma(A)$. Ottengo dunque $\rho(A)=\sigma(A)$.

LEMMA 2.1. Sia $A \in k^{m,n}$ e sia $M \in k^{m,n+1}$ ottenuta aggiungendo ad A una colonna. Allora A e M hanno lo stesso rango se e solo se la colonna aggiunta è una combinazione lineare delle colonne di A.

Si noti che $(b_1, \dots, b_m)$ è una combinazione lineare delle colonne di A se e solo se il sistema lineare

$$AX=(b_1, \dots, b_m)^t$$

ha soluzione. Da quanto appena detto, otteniamo il seguente risultato.

TEOREMA 2.2: Di Rouché-Capelli. Il sistema $AX=B$ è compatibile (ovvero ammette soluzione) se e solo se la matrice $(A \mid B)$, ottenuta aggiungendo ad A la colonna B, soddisfa $\rho(A \mid B)=\rho(A)$.

Studiamo i sistemi lineari ridotti, ovvero $AX=B$ con A ridotta per righe. Cambiando eventualmente l'ordine delle equazioni possiamo supporre che le prime r righe di A siano non nulle e le rimanenti $m-r$ siano nulle. Dalla riga r-esima, ricaviamo un'incognita in funzione delle rimanenti e sostituiamo nelle righe precedenti. Poichè A è ridotta, nella $(r-1)$-esima riga trovo un'incognita che non compare nell'ultima e ricavo in funzione delle rimanenti. Sostituisco nelle equazioni precedenti. Poichè A è ridotta, applico questo procedimento risalendo.
In conclusione, riesco ad esprimere r incognite (una per ciascuna riga non nulla di A) in funzione delle rimanenti $m-r$ incognite (queste ultime si chiamano *libere* perché possono assumere qualunque valore). In questo caso, si dice che il sistema lineare (ridotto) ha ∞^{m-r} soluzioni, con $m=$numero di incognite e r che vale $\rho(A)=\rho(A \mid B)$.

OSSERVAZIONE 2.2. Se $(A \mid B)$ può essere trasformato in $(A' \mid B')$ tramite trasformazioni elementari, allora i sistemi $AX=B$ e $A'X=B'$ sono *equivalenti*, cioè hanno le stesse soluzioni.

Vale il seguente *algoritmo per risolvere un sistema lineare arbitrario*:

1. Consideriamo la matrice completa $(A \mid B)$.
2. Effettuiamo trasformazioni elementari $(A \mid B)\rightarrow(A' \mid B')$ finchè A' non è ridotta per righe
3. Risolviamo il sistema ridotto $A'X=B'$ (che per l'osservazione precedente ha le stesse soluzioni).

Possiamo dunque riscrivere così l'enunciato di Rouché-Capelli.
Dato un sistema lineare $AX=B$ con $A \in k^{m,n}$ e $B \in k^{m,1}$,

1. $AX=B$ è risolubile se e solo se $\rho(A)=\rho(A \mid B)=r$
2. Se $AX=B$ è risolubile, allora ha ∞^{n-r} soluzioni.

Studiamo ora i sistemi lineari omogenei. Ovviamente, per $AX=0$, $X=0$ è sempre soluzione. Per il teorema di Rouché-Capelli, $\rho(A)=\rho(A\mid 0)$, perciò $AX=0$ è risolubile in ogni caso.

PROPOSIZIONE 2.2. L'insieme delle soluzioni di un sistema lineare omogeneo è un sottospazio vettoriale.

DIMOSTRAZIONE. Considero $AX=0$

1. $0_{k^n}=(0,0,\dots,0)$ è soluzione.
2. Se X_1 e X_2 sono soluzioni, allora $AX_1=0=AX_2$; si ha $A(X_1+X_2)=AX_1+AX_2=0$
3. Presi $\lambda\in k$ ed X soluzione, $A(\lambda X)=\lambda AX=0$

Dato un sistema $AX=0$, vogliamo trovare una base del suo spazio soluzioni. A meno di riordinare le incognite, posso supporre che le prime $n-r$ siano variabili libere.

$$(x_1,\dots,x_n)=(x_1,\dots,x_{n-r},f_1(x_1,\dots,x_{n-r}),\dots,f_r(x_1,\dots,x_{n-r}))$$

Per trovare una base dello spazio soluzioni basta sostituire alle variabili libere i valori della base canonica di k^{n-r}.

$$\begin{gathered}(1,0,\dots,0,f_1(1,0,\dots,0),\dots,f_r(1,0,\dots,0))\\ \vdots\\ (0,\dots,0,1,f_1(0,\dots,0,1),\dots,f_r(0,\dots,0,1))\end{gathered}$$

sono $n-r$ soluzioni di $AX=0$ linearmente indipendenti e lo spazio delle soluzioni ha dimensione $n-r$ per Rouché-Capelli. Allora esse formano una base dello spazio soluzioni.

DEFINIZIONE 2.7. Sia $A\in k^{n,n}$ una matrice quadrata. A è *invertibile* se esiste $X\in k^{n,n}$ tale che

$$AX=\begin{pmatrix}1 & 0 & 0 & \dots & 0\\ 0 & 1 & 0 & \dots & 0\\ \vdots & & \ddots & & \vdots\\ 0 & \dots & 0 & 1 & 0\\ 0 & \dots & 0 & 0 & 1\end{pmatrix}=:I_n$$

ove I_n è detta *matrice identica* o *identità*. In questo caso si dice che X è l'*inversa* di A e si scrive A^{-1}.

Siamo interessati al seguente problema: data A matrice, vogliamo calcolare (se esiste) A^{-1}. Il sistema lineare $AX=I_n$ è un sistema di n^2 equazioni in n^2 incognite. Per semplificare il problema, consideriamo le righe di X: avremo quindi un sistema lineare ad incognite vettoriali. Utilizzando il teorema di Rouché-Capelli diciamo che $A(X_1,X_2,\dots,X_n)^t=I_n$ è risolubile se e solo se $\rho(A)=\rho(A\mid I_n)=n$ (X_i indica l'i-esima riga), poichè le ultime n colonne sono vettori di k^n linearmente indipendenti. Quindi, data $A\in k^{n,n}$, A è invertibile se e solo se $\rho(A)=n$, cioè se A ha rango massimo.

DEFINIZIONE 2.8. Sia $A\in k^{n,n}$ (matrice quadrata). Per definire $det(A)$, ovvero il *determinante* di A, procediamo per induzione. La base dell'induzione è il caso $n=1$: $A\in k^{1,1}$ è semplicemente $(a)\in k$, quindi definisco $det(A):=a$. Supponiamo ora di aver definito $det(B)$ per ogni $B\in k^{n-1,n-1}$. Considero $A\in k^{n,n}$.

$$A=\begin{pmatrix}a_{11} & \dots & a_{1n}\\ \vdots & & \vdots\\ a_{n1} & \dots & a_{nn}\end{pmatrix}$$

Definisco $A_{ij}:=(-1)^{i+j}det(E_{ij})$, dove $E_{ij}\in k^{n-1,n-1}$ è la matrice ottenuta da A cancellando la i-esima riga e la j-esima colonna. Allora

$$det(A):=a_{11}A_{11}+a_{12}A_{12}+\ldots+a_{1n}A_{1n}$$

TEOREMA 2.3: Sviluppo di Laplace. Sia $A\in k^{n,n}$. Allora vale che

$$det(A)=a_{i1}A_{i1}+a_{i2}A_{i2}+\ldots+a_{in}A_{in}=a_{1j}A_{1j}+a_{2j}A_{2j}+\ldots+a_{nj}A_{nj}$$

per ogni $i,j=1,\ldots,n$.

TEOREMA 2.4: Di Binet. Siano $A,B\in k^{n,n}$. Allora

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

ovvero il determinante è moltiplicativo.

Valgono le seguenti proprietà:

1. $det(A)=0$ se A ha una riga o una colonna nulla.
2. Se B è ottenuta da A scambiando due righe o due colonne, allora $det(B)=-det(A)$.
3. $det(A)=0$ se A ha due righe o due colonne uguali.
4. Se $a,b\in k$ e $v,w\in k^n$, vale che

$$det\begin{pmatrix} R_1 \\ \vdots \\ av+bw \\ \vdots \\ R_n \end{pmatrix}=a\,det\begin{pmatrix} R_1 \\ \vdots \\ v \\ \vdots \\ R_n \end{pmatrix}+b\,det\begin{pmatrix} R_1 \\ \vdots \\ w \\ \vdots \\ R_n \end{pmatrix}$$

TEOREMA 2.5: Determinante ed invertibilità. A è invertibile se e solo se $det(A)\neq 0$.

DIMOSTRAZIONE.

1. A invertibile implica che esiste $A^{-1}\in k^{n,n}$ tale che $A A^{-1}=I_n$; allora $det(A)\cdot det(A^{-1})=det(I_n)=1$. Dunque $det(A)\neq 0$.
2. Supponiamo A non invertibile. Allora il rango $\rho(A)$ non è massimo e quindi le righe di A non sono linearmente indipendenti. Dunque esiste j tale che $R_j=c_1R_1+\ldots+c_{j-1}R_{j-1}+c_{j+1}R_{j+1}+\ldots+c_nR_n$:

$$det\begin{pmatrix} R_1 \\ \vdots \\ R_j \\ \vdots \\ R_n \end{pmatrix}=c_1\,det\begin{pmatrix} R_1 \\ \vdots \\ R_1 \\ \vdots \\ R_n \end{pmatrix}+\ldots+c_{j-1}\,det\begin{pmatrix} R_1 \\ \vdots \\ R_{j-1} \\ \vdots \\ R_n \end{pmatrix}+c_{j+1}\,det\begin{pmatrix} R_1 \\ \vdots \\ R_{j+1} \\ \vdots \\ R_n \end{pmatrix}+\ldots+c_n\,det\begin{pmatrix} R_1 \\ \vdots \\ R_n \\ \vdots \\ R_n \end{pmatrix}=c_1 0+\ldots+c_n 0=0$$

   grazie alle proprietà 3 e 4. Ho dimostrato la tesi.

TEOREMA 2.6: Sulle matrici invertibili. Sia $A\in k^{n,n}$. Allora sono equivalenti:

1. A è invertibile
2. $\rho(A)=n$
3. $det(A)\neq 0$

APPLICAZIONI LINEARI

DEFINIZIONE 3.1. Siano V, W spazi vettoriali su k. Una funzione $f: V \to W$ si dice *applicazione lineare* se:

1. Per ogni $u, v \in V$, $f(u+v) = f(u) + f(v)$
2. Per ogni $v \in V$ e $\lambda \in k$, $f(\lambda v) = \lambda f(v)$

OSSERVAZIONE 3.1. Se $f: V \to W$ è lineare, allora $f(0_V) = 0_W$. Infatti, $f(0_V) = f(0 \cdot 0_V) = 0 f(0_V) = 0_W$.

DEFINIZIONE 3.2. Sia $f: A \to B$ una funzione. Essa si dice *iniettiva* se, presi $a_1, a_2 \in A$ tali che $a_1 \neq a_2$, allora $f(a_1) \neq f(a_2)$. Analogamente, f è iniettiva se $f(a_1) = f(a_2)$ implica $a_1 = a_2$.

DEFINIZIONE 3.3. Sia $f: V \to W$ lineare; definiamo

$$Ker(f) := \{v \in V \mid f(v) = 0_W\}$$

come il *nucleo* (o kernel) di f.

PROPOSIZIONE 3.1. $Ker(f)$ è un sottospazio vettoriale di V.

DIMOSTRAZIONE.

1. $0_V \in Ker(f)$ grazie a osservazione 3.1.
2. $u, v \in Ker(f)$: $f(u+v) = f(u) + f(v) = 0_W + 0_W = 0_W$; $u + v \in Ker(f)$
3. $v \in Ker(f)$, $\lambda \in k$: $f(\lambda v) = \lambda f(v) = \lambda 0_W = 0_w$

TEOREMA 3.1. Sia $f: V \to W$ lineare. Sono equivalenti:

1. f è iniettiva
2. $Ker(f) = \{0_V\}$
3. $dim(Ker(f)) = 0$

DIMOSTRAZIONE.

$1 \Rightarrow 2$. Prendo f iniettiva e $v \neq 0_V$; allora $f(v) \neq f(0_V) = 0_W$. Quindi $v \notin Ker(f)$, da cui $Ker(f) = \{0_V\}$

$2 \Rightarrow 1$. Vogliamo dimostrare che $f(u) = f(v)$ implica $u = v$. Da $f(u) = f(v)$, ottengo $f(u) - f(v) = 0_W$.

$$f(u) + f(-v) = f(u - v) = 0_W$$

Dunque $u - v \in Ker(f) = \{0_V\}$. Allora $u - v = 0_V$; $u = v$.

Si noti che $2 \Leftrightarrow 3$ è ovvio. Abbiamo quindi dimostrato il teorema.

DEFINIZIONE 3.4. Sia $f: A \to B$ funzione. Essa è *suriettiva* se e solo se per ogni $b \in B$ esiste $a \in A$ tale che $f(a) = b$. Ovvero, l' *insieme delle immagini* di f

$$\mathrm{Im}(f) := \{b \in B \mid \exists a \in A \text{ con } f(a) = b\}$$

dev'essere uguale a B.

PROPOSIZIONE 3.2. Sia $f: V \to W$ lineare. Allora $\mathrm{Im}(f)$ è un sottospazio vettoriale di W.

DIMOSTRAZIONE.

1. $f(0_V)=0_W$; quindi $0_W \in \mathrm{Im}(f)$
2. $z, w \in \mathrm{Im}(f)$, per cui $z=f(u), w=f(v)$ con $u, v \in V$. $z+w=f(u)+f(v)=f(u+w) \in \mathrm{Im}(f)$
3. $\lambda \in k$ e $w \in \mathrm{Im}(f)$, per cui $w=f(v)$ con $v \in V$. $\lambda w=\lambda f(v)=f(\lambda v) \in \mathrm{Im}(f)$

Grazie a quanto detto in definizione 3.4 e proposizione 3.2, si ha che $f: V \to W$ lineare è suriettiva se e solo se $dim(\mathrm{Im}(f))=dim(W)$.

TEOREMA 3.2: Della dimensione. Sia $f: V \to W$ lineare con $dim(V)=n$. Allora
$$n=dim(Ker(f))+dim(\mathrm{Im}(f))$$

DIMOSTRAZIONE. Sia $(n_1, \dots, n_s)$ base del $Ker(f)$. Completandola a base di V otteniamo:
$$(n_1, \dots, n_s, v_{s+1}, \dots, v_n)$$
Vogliamo verificare che $(f(v_{s+1}), \dots, f(v_n))$ sia una base di $\mathrm{Im}(f)$
Generatori di $\mathrm{Im}(f)$. Sia $w \in \mathrm{Im}(f)$. Allora $w=f(v)$ con $v \in V$:
$$v=a_1 n_1+\dots+a_s n_s+a_{s+1} v_{s+1}+\dots+a_n v_n$$
Da cui
$$w=f(v)=f(a_1 n_1+\dots+a_s n_s+a_{s+1} v_{s+1}+\dots+a_n v_n)=a_1 f(n_1)+\dots+a_s f(n_s)+a_{s+1} f(v_{s+1})+\dots+a_n f(v_n)=$$
$$=a_{s+1} f(v_{s+1})+\dots+a_n f(v_n)$$
Linearmente indipendenti. Siano $c_i \in k$ tali che
$$0_W=c_{s+1} f(v_{s+1})+\dots+c_n f(v_n)=f(c_{s+1} v_{s+1})+\dots+f(c_n v_n)=f(c_{s+1} v_{s+1}+\dots+c_n v_n)$$
Si ha quindi che $c_{s+1} v_{s+1}+\dots+c_n v_n \in Ker(f)$:
$$c_{s+1} v_{s+1}+\dots+c_n v_n=c_1 n_1+\dots+c_s n_s$$
Ne ricavo che
$$c_{s+1} v_{s+1}+\dots+c_n v_n-c_1 n_1-\dots-c_n v_n=0_V$$
Poichè $(n_1, \dots, n_s, v_{s+1}, \dots, v_n)$ è base di V, otteniamo che $c_1=\dots=c_s=c_{s+1}=c_n=0$.
Dunque $(f(v_{s+1}), \dots, f(v_n))$ è base di $\mathrm{Im}(f)$.

COROLLARIO 3.1. Sia $f: V \to V$ lineare con $dim(V)$ finita. Allora f è iniettiva se e solo se è suriettiva.

DIMOSTRAZIONE. f iniettiva $\Leftrightarrow dim(Ker(f))=0 \Leftrightarrow dim(V)=dim(\mathrm{Im}(f)) \Leftrightarrow f$ suriettiva.

Sia $A \in k^{m,n}$ e si consideri $f_A: k^n \to k^m$ tale che $v \to A \cdot v$, con $v=(v_1, \dots, v_n) \in k^n$. Si noti che $Av=w \in k^m$.

PROPOSIZIONE 3.3. Per ogni $A \in k^{m,n}$, la funzione $f_A: k^n \to k^m$ è lineare.

DIMOSTRAZIONE.

1. $v, u \in k^n$. $f_A(v+u)=A(v+u)=Av+Au=f_A(v)+f_A(u)$
2. $\lambda \in k$, $v \in k^n$. $f_A(\lambda v)=A(\lambda v)=\lambda Av=\lambda f_A(v)$

TEOREMA 3.3. Sia $f: k^n \to k^m$ lineare. Allora esiste $A \in k^{m,n}$ tale che $f=f_A$.

DIMOSTRAZIONE. Costruiamo A come segue: sia $(e_1, e_2, \dots, e_n)$ la base canonica di k^n. Sia A la matrice avente come colonne $f(e_1), \dots, f(e_n)$:

$$A=(f(e_1)\mid\ldots\mid f(e_n))\in k^{m,n}$$

Affermo che per ogni $v\in k^n$ si ha $f(v)=f_A(v)=A\cdot v$. Se

$$A=\begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \ldots & a_{mn} \end{pmatrix}$$

allora per costruzione, $f(e_1)=(a_{11},\ldots,a_{m1}),\ldots,f(e_n)=(a_{1n},\ldots,a_{mn})$. Inoltre, per ogni $v\in k^n$,

$$v=(v_1,\ldots,v_n)=v_1e_1+\ldots+v_ne_n$$

Dunque,

$$f(v)=f(v_1e_1+\ldots+v_ne_n)=f(v_1e_1)+\ldots+f(v_ne_n)=v_1f(e_1)+\ldots+v_nf(e_n)=$$
$$=v_1(a_{11},\ldots,a_{m1})+\ldots+v_n(a_{1n},\ldots,a_{mn})=(v_1a_{11}+\ldots+a_{1n}v_n,\ldots,a_{m1}v_1+\ldots+a_{mn}v_n)$$

Inoltre,

$$f_A(v)=\begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \ldots & a_{mn} \end{pmatrix}\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}=\begin{pmatrix} a_{11}v_1+\ldots+a_{1n}v_n \\ \vdots \\ a_{m1}v_1+\ldots+a_{mn}v_n \end{pmatrix}=f(v)$$

COROLLARIO 3.2. Grazie a teorema 3.3 e proposizione 3.3, si vede che esiste una corrispondenza biunivoca fra le funzioni lineari $f:k^n\rightarrow k^m$ e le matrici di $k^{m,n}$.

DEFINIZIONE 3.5. Data $f:k^n\rightarrow k^m$ lineare, la sua *matrice associata* $M_f=M(f)$ è la matrice A costruita come nella dimostrazione di teorema 3.3, ovvero

$$M_f=(f(e_1)\mid\ldots\mid f(e_n))$$

LEMMA 3.1. Sia $f:k^n\rightarrow k^m$ lineare. Allora $\mathrm{Im}(f)=\mathcal{L}(f(e_1),\ldots,f(e_n))$.

DIMOSTRAZIONE. Sia $w\in\mathrm{Im}(f)$. Allora $w=f(v)$ per $v\in k^n$; $v=(v_1,\ldots,v_n)=v_1e_1+\ldots+v_ne_n$.

$$w=f(v)=f(v_1e_1+\ldots+v_ne_n)=v_1f(e_1)+\ldots+v_nf(e_n)\in\mathcal{L}(f(e_1),\ldots,f(e_n))$$

Come conseguenza di questo lemma, si ottiene subito che

$$dim(\mathrm{Im}(f))=dim(\mathcal{L}(f(e_1),\ldots,f(e_n)))=dim(\text{spazio-colonne di } M_f)=\sigma(M_f)=\rho(M_f)$$

per questo motivo $dim(\mathrm{Im}(f))$ viene chiamata *rango*.
Considero una funzione lineare $f:k^n\rightarrow k^m$.
Per determinare una base di $Ker(f)=\{v\in k^n\mid f(v)=0\}$, basta considerare la matrice M_f associata di f:

$$Ker(f)=\{v\in k^n\mid M_fv=0\}$$

Infatti l'insieme delle soluzioni del sistema lineare omogeneo $M_fX=0$ è il nucleo di f.
Per determinare una base di $\mathrm{Im}(f)$, grazie a lemma 3.1, posso vedere lo spazio delle colonne di M_f. Perciò prendo $M(f)^t$, la riduco ed ottengo la base di $\mathrm{Im}(f)$ sulle righe.

DEFINIZIONE 3.6. Sia $f:V\rightarrow W$ lineare, B base di V e B' base di W. La matrice associat a f nelle basi B e B' è la matrice $M_{B',B}(f)=(a_{ij})\in k^{m,n}$ tale che

$$f(b_1)=a_{11}b'_1+a_{21}b'_2+\ldots+a_{m1}b'_m$$
$$\vdots$$
$$f(b_n)=a_{1n}b'_1+a_{2n}b'_2+\ldots+a_{mn}b'_m$$

ove $B=(b_1,\ldots,b_n)$ e $B'=(b'_1,\ldots,b'_m)$.
Si noti che se $f:k^n\to k^n$, $M_f=M(f)=M_{c_m,c_n}$, dove $c_n=(e_1,\ldots,e_n)$ e $c_m=(e_1,\ldots,e_m)$.

PROPOSIZIONE 3.4. Sia $f:V\to W$ lineare e $M_{B',B}(f)$ la sua matrice associata nelle basi B di V e B' di W. Sia $v\in V$; posso scrivere che $v=x_1b_1+\ldots+x_nb_n$ e $f(v)=y_1b'_1+\ldots+y_mb'_m$. Allora

$$\begin{pmatrix} y_1\\ \vdots\\ y_m\end{pmatrix}=M_{B',B}(f)\begin{pmatrix} x_1\\ \vdots\\ x_n\end{pmatrix}$$

DIMOSTRAZIONE. $f(v)=f(x_1b_1+\ldots+x_nb_n)=x_1f(b_1)+\ldots+x_nf(b_n)=x_1(a_{11}b'_1+\ldots+a_{m1}b'_m)+\ldots+$ $+x_n(a_{1n}b'_1+\ldots+a_{mn}b'_m)=(x_1a_{11}+\ldots+x_na_{1n})b'_1+\ldots+(a_{m1}x_1+\ldots+a_{mn}x_n)b'_m=y_1b'_1+\ldots+y_mb'_m$.
Quanto risultato è equivalente a fare

$$\begin{pmatrix} y_1\\ \vdots\\ y_m\end{pmatrix}=\begin{pmatrix} a_{11} & \ldots & a_{1n}\\ \vdots & & \vdots\\ a_{m1} & \ldots & a_{mn}\end{pmatrix}\begin{pmatrix} x_1\\ \vdots\\ x_n\end{pmatrix}$$

ove $M_{B',B}=(a_{ij})$ per $1\le i\le m$, $1\le j\le n$.

OSSERVAZIONE 3.2. $M_{B',B}(f)$ non dipende solo da f ma anche dalla scelta di B e B'.

LEMMA 3.2. Siano U,V,W spazi vettoriale su k e

$$\begin{array}{ll} B=(u_1,\ldots,u_s) & \text{base di } U\\ B'=(v_1,\ldots,v_n) & \text{base di } V\\ B^{II}=(w_1,\ldots,w_m) & \text{base di } W\end{array}$$

Siano inoltre $g:U\to V$ e $f:V\to W$ lineari. Presa l'applicazione lineare composta $f\circ g:U\to W$, allora

$$M_{B'',B}(f\circ g)=M_{B'',B'}(f)\cdot M_{B',B}(g)$$

DIMOSTRAZIONE. Sia $u\in U$: vale che $u=z_1u_1+\ldots+z_su_s$. $g(u)\in V$; $g(u)=x_1v_1+\ldots+x_nv_n$. Inoltre, $f\circ g(u)\in W$: $f\circ g(u)=y_1w_1+\ldots+y_mw_m$

$$\begin{pmatrix} x_1\\ \vdots\\ x_n\end{pmatrix}=M_{B',B}(g)\begin{pmatrix} z_1\\ \vdots\\ z_s\end{pmatrix},\quad \begin{pmatrix} y_1\\ \vdots\\ y_m\end{pmatrix}=M_{B'',B}(f\circ g)\begin{pmatrix} z_1\\ \vdots\\ z_s\end{pmatrix}=M_{B'',B'}(f)\begin{pmatrix} x_1\\ \vdots\\ x_n\end{pmatrix}=M_{B'',B'}(f)\,M_{B',B}(g)\begin{pmatrix} z_1\\ \vdots\\ z_s\end{pmatrix}$$

Grazie a quanto scritto, ottengo la tesi.

ESEMPI 3.1. Grazie a lemma 3.2, si ottengono i seguenti risultati.

1. Prendo $U=V=W$, $g=f=i$ identità e B,E due basi di V.

$$M_{B,B}(i)=M_{B,B}(i\circ i)=M_{B,E}(i)\cdot M_{E,B}(i)$$

   Se $B=(v_1,\ldots,v_n)$, allora $M_{B,B}(i)=I_n$, infatti

$$\begin{gathered} i(v_1)=v_1=1v_1+0v_2+\ldots+0v_n\\ \vdots\\ i(v_n)=v_n=0v_1+\ldots+0v_{n-1}+1v_n\end{gathered}$$

   Dunque $M_{B,E}(i)\cdot M_{E,B}(i)=I_n$. Quindi $M_{B,E}(i)=(M_{E,B}(i))^{-1}$ è detta *matrice di cambiamento di base*.

2. Prendo $U=V=W$, B,E basi di V, $f:V\to V$ lineare e considero $f=i\circ f\circ i$. Considerate

$$M_{E,E}(i\circ f\circ i)=M_{E,E}(f),\quad P=M_{B,E}(i)$$

è facile vedere che
$$M_{E,E}(f)=P^{-1}M_{B,B}(f)P$$

DEFINIZIONE 3.7. $A,B\in k^{n,n}$ si dicono *simili* se esiste $P\in k^{n,n}$ invertibile tale che $B=P^{-1}AP$.

Vogliamo ora analizzare le funzioni lineari del tipo $f:V\to V$.

DEFINIZIONE 3.8. Un'applicazione lineare $f:V\to V$ si dice *endomorfismo* o *operatore lineare*.

DEFINIZIONE 3.9. $f:V\to V$ operatore lineare si dice *diagonalizzabile* se esiste una base B di V tale che
$$M_{B,B}(f)=\begin{pmatrix}\lambda_1 & 0 & \dots & & 0\\ 0 & \lambda_2 & 0 & \dots & 0\\ \vdots & & \ddots & & \\ 0 & \dots & 0 & \lambda_{n-1} & 0\\ 0 & \dots & & 0 & \lambda_n\end{pmatrix}$$
ovvero $M_{B,B}(f)$ è diagonale.
Si noti che $B=(b_1,\dots,b_n)$ è diagonale se ha il seguente comportamento
$$f(b_1)=\lambda_1 b_1+0b_2+\dots+0b_n$$
$$\vdots$$
$$f(b_n)=0b_1+\dots+0b_{n-1}\lambda_n b_n$$

DEFINIZIONE 3.10. Data $f:V\to V$ lineare con V spazio vettoriale su k,

1. $\lambda\in k$ si dice *autovalore* di f se esiste $v\in V\setminus\{0_V\}$ tale che $f(v)=\lambda v$
2. $v\in V$ si dice *autovettore* di f relativo all'autovalore λ se $f(v)=\lambda v$
3. $V_\lambda=\{v\in V \mid f(v)=\lambda v\}$ si dice *autospazio*.

LEMMA 3.3. V_λ è un sottospazio vettoriale di V.

DIMOSTRAZIONE.

1. $f(0_V)=\lambda 0_V=0_V$
2. Siano $v,w\in V$ tali che $f(v)=\lambda v$, $f(w)=\lambda w$; $f(v+w)=f(v)+f(w)=\lambda v+\lambda w=\lambda(v+w)$
3. Siano $a\in k$ e $v\in V$ tale che $f(v)=\lambda v$; $f(av)=af(v)=a\lambda v=\lambda av$

PROPOSIZIONE 3.5. Sia $f:V\to V$ lineare. f è diagonalizzabile se e solo se V ammette una base formata da autovettori di f.

LEMMA 3.4. Sia $f:V\to V$ lineare; siano $v_1,\dots,v_k\in V$ autovettori non nulli relativi agli autovalori $\lambda_1,\dots,\lambda_k$. Se $\lambda_1,\dots,\lambda_k$ sono tutti distinti, allora $v_1,\dots,v_k$ sono linearmente indipendenti.

DIMOSTRAZIONE. Procediamo per induzione su k.
1. Base dell'induzione: $k=1$; questo caso è banalmente vero.
2. Passo induttivo: $k\Rightarrow k+1$. Prendiamo c_i tali che
$$c_1v_1+\dots+c_kv_k+c_{k+1}v_{k+1}=0$$

Applichiamo f:

$$f(c_1 v_1+\ldots+c_k v_k+c_{k+1} v_{k+1})=f(0)=0$$

Da cui $c_1 f(v_1)+\ldots+c_k f(v_k)+c_{k+1} f(v_{k+1})=0$ e per ipotesi vale

$$c_1 \lambda_1 v_1+\ldots+c_k \lambda_k v_k+c_{k+1} \lambda_{k+1} v_{k+1}=0$$

Moltiplichiamo $c_1 v_1+\ldots+c_k v_k+c_{k+1} v_{k+1}=0$ per λ_{k+1} e sottraiamo il risultato a quanto appena trovato:

$$c_1(\lambda_1-\lambda_{k+1}) v_1+\ldots+c_k(\lambda_k-\lambda_{k+1}) v_k=0$$

Per ipotesi induttiva, $v_1,\ldots,v_k$ sono linearmente indipendenti. Dunque, avendo per ipotesi che gli autovalori sono tutti diversi, ho che

$$c_1=\ldots=c_k=0$$

Da cui si vede anche che $c_{k+1} v_{k+1}=0$, per cui $c_{k+1}=0$. $v_1,\ldots,v_{k+1}$ sono quindi linearmente indipendenti.

Studiamo un caso particolare: sia $f: V \to V$ con V spazio vettoriale su k. Prendiamo $V=k^n$. Sia M_f la matrice associata a f tale che $f(v)=M_f v$ per ogni $v \in k^n$. In questo caso,

$$M_f v=f(v)=\lambda v$$

Per cui $M_f v-\lambda I_n v=(M_f-\lambda I_n) v=0$ se e solo se v è soluzione del sistema lineare omogeneo

$$(M_f-\lambda I_n) X=0$$

Se ne deduce che λ è un autovalore di f se e solo se $\rho(M_f-\lambda I_n)$ non è massimo, ovvero se e solo se

$$det(M_f-\lambda I_n)=0$$

Pertanto gli autovalori di f sono esattamente le soluzioni dell'equazione in λ

$$det(M_f-\lambda I_n)=0$$

In generale, se $f: V \to V$ è lineare con $dim(V)=n$, $B=(b_1,\ldots,b_n)$ base qualunque di V, $M_{B,B}(f)$ matrice associata.

$$v=v_1 b_1+\ldots+v_n b_n, \quad f(v)=w_1 b_1+\ldots+w_n b_n$$

Poichè $f(v)=\lambda v$, si ha

$$\lambda \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}=\begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix}=M_{B,B}(f)\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$$

Ciò vale se e solo se $(M_{B,B}(f)-\lambda I_n)(v_1,\ldots,v_n)^t=0$, ovvero se e solo se $v_1,\ldots,v_n$ è soluzione del sistema lineare omogeneo

$$(M_{B,B}(f)-\lambda I_n) X=0$$

In maniera del tutto analoga al caso di $V=k^n$, si vede che se $f: V \to V$ lineare e $\lambda \in k$ è autovalore di f, allora λ è soluzione dell'equazione

$$det(M_{B,B}(f)-\lambda I_n)=0$$

OSSERVAZIONE 3.3. $det(M_{B,B}(f)-\lambda I_n)$ è un polinomio in λ di grado n.

OSSERVAZIONE 3.4. $det(M_{B,B}(f)-\lambda I_n)$ non dipende dalla scelta di B.

Dimostriamolo: sia B' un'altra base di V. Allora $M_{B',B'}(f)$ e $M_{B,B}(f)$ sono *simili*, ovvero esiste $P \in k^{n,n}$ invertibile tale che $M_{B',B'}(f)=P^{-1} M_{B,B}(f) P$.

$$det(M_{B',B'}(f)-\lambda I_n)=det(P^{-1} M_{B,B}(f) P-P^{-1} \lambda I_n P)=det(P^{-1}(M_{B,B}(f)-\lambda I_n) P)=$$

$$=det(P^{-1})det(M_{B,B}(f)-\lambda I_n)det(P)=det(P)^{-1}det(P)det(M_{B,B}(f)-\lambda I_n)=det(M_{B,B}(f)-\lambda I_n)$$

DEFINIZIONE 3.11. $f:V\to V$ lineare; $p(\lambda)=det(M_{B,B}(f)-\lambda I_n)$, dove B è una qualunque base di V, si dice *polinomio caratteristico* di f.

PROPOSIZIONE 3.6. λ è un autovalore di f se e solo se è radice del polinomio caratteristico di f.

DEFINIZIONE 3.12. Si dice che la *molteplicità* di x_0 come radice di $p(x)\in k[x]$ è $m\geq 1$ se

$$p(x)=(x-x_0)^m g(x)$$

con $g(x)\in k[x]$ e non esiste $h(x)\in k[x]$ tale che $p(x)=(x-x_0)^{m+1}h(x)$.

DEFINIZIONE 3.13. Siano $f:V\to V$ lineare, $\lambda\in k$ autovalore, $p(t)$ polinomio caratteristico, V_λ autospazio relativo a λ.

1. La *molteplicità algebrica* di λ $m_a(\lambda)$ è la molteplicità di λ come radice di $p(t)$
2. La *molteplicità geometrica* di λ $m_g(\lambda)$ è $m_g(\lambda):=dim(V_\lambda)$

PROPOSIZIONE 3.7. Per ogni λ autovalore si ha $1\leq m_g(\lambda)\leq m_a(\lambda)$.

DIMOSTRAZIONE. Poichè λ è un autovalore esiste $v\neq 0_V$ con $v\in V_\lambda$. Dunque $dim(V_\lambda)\geq 1$. Siano

$$m=m_g(\lambda),\ \ B_\lambda=(v_1,\dots,v_m)$$

ove quest'ultimo elemento è una base di V_λ. Completiamo B_λ a una base B di V.

$$B=(v_1,\dots,v_m,v_{m+1},\dots,v_n)$$

Considero il polinomio caratteristico $p(t)=det(M_{B,B}(f)-tI_n)$. Grazie al fatto che B_λ è base di V_λ,

$$p(t)=det\begin{pmatrix}\lambda-t & 0 & 0 & \dots & ?\\ 0 & \lambda-t & 0 & \dots & ?\\ \vdots & & \ddots & & ?\\ 0 & \dots & 0 & \lambda-t & ?\\ \vdots & & & & ?\\ 0 & 0 & \dots & 0 & ?\end{pmatrix}=(\lambda-t)^m det(?)$$

Dunque $m_a(\lambda)\geq m=m_g(\lambda)$.

OSSERVAZIONE 3.5. Un polinomio $p(x)\in k[x]$ di grado n ha un numero di radici (considerando anche quelle uguali) mai superiore ad n.

TEOREMA 3.4: Teorema fondamentale dell'algebra. Sia $p(x)\in\mathbb{C}[x]$ di grado n. Allora $p(x)$ ha n radici complesse.

Vediamo ora la *costruzione di una base di autovettori*. Siano $\lambda_1,\dots,\lambda_n$ le radici del polinomio caratteristico $p(\lambda)$ associato a $f:V\to V$ lineare. Consideriamo le basi dei relativi autospazi

$$V_{\lambda_1}:B_1,\ V_{\lambda_2}:B_2,\dots,\ V_{\lambda_n}:B_n$$

Sia $B:=B_1\cup B_2\cup\dots\cup B_n$. Infatti, poichè autovettori non nulli relativi ad autovalori distinti sono linearmente indipendenti, B è formata da vettori linearmente indipendenti. Pertanto B è una base di V se e solo se $|B|=m$ ($|B|$ indica il numero di vettori di B, ovvero la sua cardinalità come insieme) dove $m=dim(V)$.

$$|B|=|B_1|+|B_2|+\ldots+|B_n|=m_g(\lambda_1)+m_g(\lambda_2)+\ldots+m_g(\lambda_n)\le m_a(\lambda_1)+\ldots m_a(\lambda_n)\le m$$

Dunque B è base di V se e solo se vale l'uguaglianza di tutti i termini nella disequazione appena scritta. Vale il seguente risultato.

TEOREMA 3.5: Criterio di diagonalizzabilità. $f:V\to V$ lineare è diagonalizzabile (cioè esiste una base B di V formata da autovettori di f) se e solo se

1. Il polinomio caratteristico ha tutte le sue radici nel campo k di definizione
2. $m_a(\lambda)=m_g(\lambda)$ per ogni λ

COROLLARIO 3.3. Sia V spazio vettoriale su $\mathbb{C}$. $f:V\to V$ lineare è diagonalizzabile se e solo se

$$m_a(\lambda)=m_g(\lambda)$$

per ogni autovalore λ.

COROLLARIO 3.4. $f:V\to V$ lineare. Se il polinomio caratteristico $p(\lambda)$ ha n radici distinte (dove n è la dimensione di V), allora f è diagonalizzabile.

DIMOSTRAZIONE. Usiamo teorema 3.5.

1. Soddisfatta per ipotesi.
2. Se ha n radici distinte, allora $1=m_a(\lambda)\ge m_g(\lambda)\ge 1$ per ogni λ, grazie a proposizione 3.7.

Vediamo il problema della diagonalizzazione per le matrici. Si nota facilmente che $A\in k^{n,n}$ è diagonalizzabile se è simile ad una matrice diagonale, cioè se esiste $P\in k^{n,n}$ invertibile tale che

$$P^{-1}A\,P=I_n$$

OSSERVAZIONE 3.6. $f_A:k^n\to k^n$ tale che $f_A(v)=A\,v$ è diagonalizzabile se e solo se esiste una base B di V tale che

$$M_{B,B}(f)=\begin{pmatrix}\lambda_1 & 0\ldots & 0\\ & \ddots & \\ 0 & \ldots 0 & \lambda_n\end{pmatrix}$$

Si ha che $M_{B,B}(f)=M_{B,C}(id)\,M_{C,C}(f)\,M_{C,B}(id)=[M_{C,B}(id)]^{-1}\cdot A\cdot(M_{C,B}(id))$. Perciò A è diagonalizzabile se e solo se $f_A:k^n\to k^n$, definita come $f_A(v)=Av$, è diagonalizzabile e ciò vale se e solo se

$$P^{-1}AP=\begin{pmatrix}\lambda_1 & 0\ldots & 0\\ & \ddots & \\ 0 & \ldots 0 & \lambda_n\end{pmatrix}$$

dove $P=(M_{C,B}(id))=(b_1\mid b_2\mid\ldots\mid b_n)$ con $B=(b_1,\ldots,b_n)$ base di autovettori di f_A.

TEOREMA SPETTRALE

Si consideri V spazio vettoriale sul campo $k=\mathbb{R},\mathbb{C}$.

DEFINIZIONE 4.1. Un *prodotto scalare* su V è una funzione

$$\underset{(u,v)\to\langle u,v\rangle}{V\times V\to k}$$

che verifica le seguenti proprietà:

1. $\langle a u_1+b u_2,v\rangle=a\langle u_1,v\rangle+b\langle u_2,v\rangle$ per $u_1,u_2,v\in V$, $a,b\in k$
2. $\langle u,v\rangle=\overline{\langle v,u\rangle}$ per $u,v\in V$; la linea superiore indica il coniugato
3. Se $\langle u,u\rangle\in\mathbb{R}$, allora $\langle u,u\rangle\geq 0$ per ogni $u\in V$ e $u=0_V$ se e solo se $\langle u,u\rangle=0$

Un esempio fondamentale è il prodotto scalare standard su $V=\mathbb{R}^n$, così definito

$$\langle(a_1,\dots,a_n),(b_1,\dots,b_n)\rangle:=a_1 b_1+\dots+a_n b_n$$

DEFINIZIONE 4.2. Se V è uno spazio vettoriale con un prodotto scalare su V, la coppia $(V,\langle,\rangle)$ si dice *spazio vettoriale euclideo*.
In questo tipo di spazio, $u,v\in V$ si dicono *ortogonali* se $\langle u,v\rangle=0$. La *norma* (indotta dal prodotto scalare) di v è (nel caso in cui $k=\mathbb{R}$) $\|v\|:=\sqrt{\langle v,v\rangle}\in\mathbb{R}$.
Una famiglia $\{v_1,\dots,v_m\}\subseteq V$ è un *insieme ortonormale* se

$$\langle v_i,v_j\rangle=\delta_{ij}:=\begin{cases}0 & \text{se } i\neq j\\ 1 & \text{se } i=j\end{cases}$$

ove δ_{ij} è detto *delta di Kronecker*. Questo tipo di insieme è quindi formato da vettori di norma 1 a due a due perpendicolari. Di fatto, si definisce ortonormale un insieme ortogonale di norma 1.

LEMMA 4.1. Se $\{v_1,\dots,v_m\}$ è ortonormale, allora $v_1,\dots,v_m$ sono linearmente indipendenti.

DIMOSTRAZIONE. Prendo $a_i\in k$ coefficienti tali che

$$a_1 v_1+\dots+a_m v_m=0_V$$

Allora si ha che, per ogni $i\in\{1,\dots,m\}\subset\mathbb{N}$

$$\langle a_1 v_1+\dots+a_m v_m,v_i\rangle=\langle 0_V,v_i\rangle=\langle 0\cdot 0_V,v_i\rangle=0$$

Inoltre,

$$0=a_1\langle v_1,v_i\rangle+\dots+a_i\langle v_i,v_i\rangle+\dots+a_m\langle v_m,v_i\rangle=a_i$$

Ne ricavo che $a_i=0$ per ogni $i\in\{1,\dots,m\}$.

TEOREMA 4.1: Teorema Spettrale (spettro indica l'insieme degli autovalori). Sia $(V,\langle,\rangle)$ spazio vettoriale euclideo reale e sia $f:V\to V$ un'applicazione lineare *autoaggiunta*, cioè tale che $\langle f(v),w\rangle=\langle v,f(w)\rangle$ per ogni $v,w\in V$.
Allora esiste una base ortonormale di V formata da autovettori di f, in particolare f è diagonalizzabile.

LEMMA 4.2. Siano $(V,\langle,\rangle)$ spazio vettoriale euclideo e $\{v_1,\dots,v_m\}$ insieme ortonormale. Si assuma che $dim(V)=n$. Allora si può completare l'insieme a una base ortonormale $B=(v_1,\dots,v_m,v_{m+1},\dots,v_n)$ di V.

DIMOSTRAZIONE per induzione retrograda con ortonormalizzazione di Gram-Schmidt.
Base dell'induzione: $m=n$, ovvia.
Passo induttivo: supposta vera la tesi per m, verifichiamola per $m-1$. Sia $\{v_1,\dots,v_{m-1}\}$ ortonormale. Esiste $v\in V$ tale che $v\notin\mathcal{L}(v_1,\dots,v_{m-1})$. Sia $w:=v-\langle v,v_1\rangle v_1-\langle v,v_2\rangle v_2-\dots-\langle v,v_{m-1}\rangle v_{m-1}$. Si vede che

$$\langle w,v_i\rangle=0$$

per ogni $i=1,\dots,m-1$, infatti

$$\langle w,v_i\rangle=\langle v-\langle v,v_1\rangle v_1-\langle v,v_2\rangle v_2-\dots-\langle v,v_{m-1}\rangle v_{m-1},v_i\rangle=$$
$$=\langle v,v_i\rangle-\langle v,v_i\rangle\langle v_1,v_i\rangle-\dots-\langle v,v_{m-1}\rangle\langle v_{m-1},v_i\rangle=\langle v,v_i\rangle-\langle v,v_i\rangle\langle v_i,v_i\rangle=0$$

Dunque w,v_i sono ortogonali. Sia ora $v_m=w/\|w\|$. Noto che, ovviamente, $\langle v_m,v_i\rangle=0$. In più,

$$\|v_m\|=\sqrt{\langle v_m,v_m\rangle}=\sqrt{\left\langle\frac{w}{\|w\|},\frac{w}{\|w\|}\right\rangle}=\sqrt{\frac{1}{\|w\|}\langle w,\frac{1}{\|w\|}w\rangle}=\sqrt{\frac{1}{\|w\|}\langle\frac{1}{\|w\|}w,w\rangle}=\sqrt{\frac{1}{\|w\|^2}\langle w,w\rangle}=\sqrt{1}=1$$

Pertanto, $\{v_1,\dots,v_m\}$ è un insieme ortonormale. Per ipotesi induttiva si completa quindi a una base ortonormale $B=(v_1,\dots,v_{m-1},v_m,\dots,v_n)$ di V.

DEFINIZIONE 4.3. Sia V spazio vettoriale su k; $b:V\times V\to k$ funzione è una *forma bilineare* se

1. $b(u+v,w)=b(u,w)+b(v,w)$ per ogni $u,v,w\in V$
2. $b(u,v+w)=b(u,v)+b(u,w)$ per ogni $u,v,w\in V$
3. $b(\lambda u,v)=b(u,\lambda v)=\lambda b(u,v)$ per ogni $u,v\in V$, $\lambda\in k$

Inoltre, b è bilineare *simmetrica* se $b(u,v)=b(v,u)$ per ogni $u,v\in V$.

DEFINIZIONE 4.4. Siano V spazio vettoriale su k, $b:V\times V\to k$ forma bilineare simmetrica, W sottospazio vettoriale di V. Il *complemento ortogonale* di W è

$$W^{\perp}:=\{v\in V\mid b(v,w)=0 \text{ per ogni } w\in W\}$$

LEMMA 4.3. Con le ipotesi di definizione 4.4 valgono i seguenti fatti:

1. $W^{\perp}$ è un sottospazio vettoriale di V.
2. $V=W+W^{\perp}$ se b è un prodotto scalare su $\mathbb{R}$
3. $W\cap W^{\perp}=\{0_V\}$ se b è un prodotto scalare su $\mathbb{R}$

DIMOSTRAZIONE.
1. Devo dimostrare i classici tre punti ($w\in W$):
   - (i) $0_V\in W^{\perp}$ se e solo se $b(0_V,w)=0$. $b(0\cdot 0_V,w)=0\,b(0_V,w)=0$
   - (ii) $v_1,v_2\in W^{\perp}$. $b(v_1,w)=0=b(v_2,w)$. Allora $b(v_1+v_2,w)=b(v_1,w)+b(v_{2},w)=0$
   - (iii) $b(v,w)=0$; allora $b(\lambda v,w)=\lambda b(v,w)=\lambda 0=0$ con $v\in W^{\perp}$
2. Sia $(w_1,\dots,w_m)$ una base di W e $B=(w_1,\dots,w_m,v_{m+1},\dots,v_n)$ base di V ottenuta completando quella di W. Applichiamo a B il procedimento di Gram-Schmidt (dimostrazione lemma 4.2). Otteniamo una base ortonormale di V
$$B'=(w'_1,\dots,w'_m,v'_{m+1},\dots,v'_n)$$
con $(w'_1,\dots,w'_m)$ base di W e $b(v_i,w_j)=0$ per ogni i,j. Sia $v\in V$:
$$v=a_1w'_1+\dots+a_mw'_m+a_{m+1}v'_{m+1}+\dots+a_nv'_n$$
ove $a_1w'_1+\dots+a_mw'_m\in W$ e $a_{m+1}v'_{m+1}+\dots+a_nv'_n\in W^{\perp}$. Dunque $v\in W+W^{\perp}$. $V=W+W^{\perp}$.
3. Sia $v\in W\cap W^{\perp}$; allora $b(v,w)=0$ per ogni $w\in W$ dato che $v\in W^{\perp}$ e $b(v,v)=0$ poichè $v\in W$.

Allora $v=0_V$.

COROLLARIO 4.1. Sia V spazio vettoriale su $\mathbb{R}$ di dimensione n con $\langle , \rangle$ prodotto scalare. Considerato W sottospazio vettoriale con $dim(W)=m$, allora $dim(W^{\perp})=n-m$.

DIMOSTRAZIONE. Grazie alla formula di Grassmann,

$$dim(W)+dim(W^{\perp})=dim(W+W^{\perp})+dim(W\cap W^{\perp})=dim(V)+0=n$$

Quindi $dim(W^{\perp})=n-m$.

LEMMA 4.4. Sia $\lambda\in\mathbb{C}$ una radice del polinomio caratteristico di f. Se f è autoaggiunto, allora $\lambda\in\mathbb{R}$.

DIMOSTRAZIONE. λ è autovalore di f, pertanto esiste $v\in V$, $v\neq 0_V$ tale che $f(v)=\lambda v$.

$$\lambda\langle v,v\rangle=\langle \lambda v,v\rangle=\langle f(v),v\rangle=\langle v,f(v)\rangle=\langle v,\lambda v\rangle=\overline{\langle \lambda v,v\rangle}=\bar{\lambda}\langle v,v\rangle$$

Poichè $v\neq 0_V$, si ha $\langle v,v\rangle>0$, dunque $\lambda=\bar{\lambda}$. Perciò $\lambda\in\mathbb{R}$.

DIMOSTRAZIONE del teorema spettrale (4.1) per induzione. Sia $n=dim(V)$.
Base dell'induzione: $n=1$; non abbiamo nulla da dimostrare.
Passo induttivo: supponendo vera la tesi per n, dobbiamo dimostrarla per $n+1$. Sia $f:V\to V$ autoaggiunto e $dim(V)=n+1$.
Per lemma 4.4, esiste $\lambda\in\mathbb{R}$ autovalore di f, dunque esiste $v\in V$, $v\neq 0$ tale che $f(v)=\lambda v$. Sia

$$W=\mathcal{L}(v)$$

($v\neq 0_V$, dunque $dim(W)=1$) e $W^{\perp}$ il suo complemento ortogonale. Per corollario 4.1, $dim(W^{\perp})=n$.
Considero la restrizione di f a $W^{\perp}$ ed affermo che se $u\in W^{\perp}$, allora $f(u)\in W^{\perp}$. Infatti, preso $w\in W$,

$$\langle f(u),w\rangle=\langle f(u),av\rangle=\langle u,f(av)\rangle=\langle u,\lambda av\rangle=\langle u,w'\rangle=0$$

La restrizione $f:W^{\perp}\to W^{\perp}$ è quindi lineare autoaggiunta; dunque per ipotesi induttiva esiste una base

$$(b_1,\dots,b_n)$$

di $W^{\perp}$ ortonormale formata da autovettori di f. Sia $b_{n+1}=v/\|v\|$. Allora $(b_1,\dots,b_n,b_{n+1})$ è una base ortonormale di V formata da autovettori di f.

Vogliamo ora formalizzare un teorema spettrale anche per le matrici.

LEMMA 4.5. Sia $(V,\langle , \rangle)$ spazio euclideo reale con $\mathcal{E}=(e_1,\dots,e_n)$ base ortonormale di V. Valgono i seguenti fatti:

1. $v=\langle v,e_1\rangle e_1+\langle v,e_2\rangle e_2+\dots+\langle v,e_n\rangle e_n$
2. $f:V\to V$ lineare, $A=M_{\mathcal{E},\mathcal{E}}(f)=(a_{ij})$ con $a_{ij}=\langle f(e_i),e_j\rangle$

DIMOSTRAZIONE.
1. $v=a_1e_1+\dots+a_ne_n$. Allora $\langle v,e_i\rangle=\langle a_1e_1+\dots+a_ne_n,e_i\rangle=a_1\langle e_1,e_i\rangle+\dots+a_i\langle e_i,e_i\rangle+\dots+a_n\langle e_n,e_i\rangle=a_i$
2. $f(e_i)=\langle f(e_i),e_1\rangle e_1+\langle f(e_i),e_2\rangle e_2+\dots+\langle f(e_i),e_n\rangle e_n$. Dunque

$$A=\begin{pmatrix}\langle f(e_1),e_1\rangle & \dots & \langle f(e_n),e_1\rangle\\ \vdots & & \vdots\\ \langle f(e_1),e_n\rangle & \dots & \langle f(e_n),e_n\rangle\end{pmatrix}$$

Da cui $a_{ij}=\langle f(e_i),e_j\rangle$.

Con le stesse ipotesi di lemma 4.5, consideriamo $f:V\to V$ autoaggiunto. Grazie a quanto appena dimostrato,

$$a_{ij}=\langle f(e_i),e_j\rangle=\langle e_i,f(e_j)\rangle=\langle f(e_j),e_i\rangle=a_{ji}$$

Pertanto, se f è autoaggiunto, la sua matrice associata A rispetto a una base ortonormale è simmetrica, ovvero $A=A^t$, dato che $a_{ij}=a_{ji}$ per ogni i,j.
Viceversa, sia $f:V\to V$ lineare ed $M_{\mathcal{E},\mathcal{E}}(f)$ simmetrica. Allora voglio vedere che $\langle f(e_i),e_j\rangle=\langle f(e_j),e_i\rangle$ per ogni i,j, ovvero che f è autoaggiunto.

$$\langle f(v),w\rangle=\langle f(v_1e_1+\ldots+v_ne_n),w_1e_1+\ldots+w_ne_n\rangle=\langle v_1f(e_1)+\ldots+v_nf(e_n),w_1e_1+\ldots+w_ne_n\rangle=$$
$$=\sum_{i,j=1}^{n}v_iw_j\langle f(e_i),e_j\rangle=\sum_{i,j=1}^{n}v_iw_j\langle f(e_j),e_i\rangle=\langle v_1e_1+\ldots+v_ne_n,w_1f(e_1)+\ldots+w_nf(e_n)\rangle=\langle v,f(w)\rangle$$

Dunque f è autoaggiunto.
Pertanto, se A è simmetrica, allora $f_A:k^n\to k^n$ è autoaggiunto. Dunque per il teorema spettrale c'è una base ortonormale di autovettori di f_A.

DEFINIZIONE 4.5. $M\in k^{n,n}$ è *ortogonale* se M è invertibile e $M^{-1}=M^t$, ovvero ($MM^t=I_n$).

OSSERVAZIONE 4.1. Sia $M\in k^{n,n}$. Se le righe di M sono una base ortonormale di k^n, allora M è una matrice ortogonale.
Di conseguenza, se $N\in k^{n,n}$ ha come colonne una base ortonormale di k^n, allora N^t è ortogonale. Dunque

$$N^t(N^t)^t=(NN^t)^t=N^tN=I_n$$

Da cui si deduce che N è ortogonale.

DEFINIZIONE 4.6. $A,B\in k^{n,n}$ si dicono *congruenti* se esiste $P\in k^{n,n}$ tale che $P^tAP=B$.

TEOREMA 4.2: Teorema Spettrale per matrici. Sia $A\in\mathbb{R}^{n,n}$ simmetrica. Allora esiste $P\in\mathbb{R}^{n,n}$ ortogonale tale che $P^{-1}AP=P^tAP$ è diagonale (dunque A è sia simile che congruente ad una matrice diagonale).

DEFINIZIONE 4.7. Sia b una forma bilineare $b:V\times V\to k$ simmetrica su V. $v\in V$ si dice *isotropo* (rispetto a b) se $b(v,v)=0$.
Si noti che se $b(v,v)=\langle v,v\rangle$ è un prodotto scalare, allora v è isotropo se e solo se $v=0_V$.

OSSERVAZIONE 4.2. Sia $v\in V$ non isotropo. Allora per ogni $w\in V$,

$$b\left(v,w-\frac{b(v,w)}{b(v,v)}v\right)=b(v,w)-\frac{b(v,w)}{b(v,v)}b(v,v)=0$$

OSSERVAZIONE 4.3. Sia $v\in V$ non isotropo. Valgono i seguenti due fatti:

$$V=\mathcal{L}(v)+(\mathcal{L}(v))^{\perp},\quad \mathcal{L}(v)\cap(\mathcal{L}(v))^{\perp}=\{0_V\}$$

Infatti, per la prima affermazione, basta notare che $w\in V$ può essere scritto nel seguente modo:

$$w=\frac{b(v,w)}{b(v,v)}v+\left(w-\frac{b(v,w)}{b(v,v)}v\right)$$

Mentre per la seconda, $w \in (\mathcal{L}(v))^{\perp}$, allora $b(w, av)=0$ e $w \in \mathcal{L}(v)$, allora $w=cv$; da cui $b(cv, av)=0$. Dunque $ac\, b(v, v)=0$ per ogni $a \in \mathbb{R} \setminus \{0\}$; $c=0$ e $w=0_V$.

FORME BILINEARI E QUADRATICHE

Per la definizione di forma bilineare si faccia riferimento a definizione 4.3.

ESEMPI 5.1.
1. Sia V spazio vettoriale su $\mathbb{R}$. $\langle , \rangle$ prodotto scalare su V è una forma bilineare simmetrica.
2. Sia $A \in k^{n,n}$. Allora $b_A : k^n \times k^n \to k^n$ definita come $b_A(x,y) := x^t A y$ è una forma bilineare che può non essere simmetrica perché il prodotto di matrici non è commutativo.

Siano V spazio vettoriale sul campo k con $dim(V)=n$, $(v_1, \dots, v_n)$ base di V e $b: V \times V \to k$ forma bilineare. Considero $b(u,w)$ per $u = u_1 v_1 + \dots + u_n v_n$, $w = w_1 v_1 + \dots + w_n v_n \in V$ con $u_i, w_j \in k$.

$$b(u,w) = b(u_1 v_1 + \dots + u_n v_n, w_1 v_1 + \dots + w_n v_n) =$$
$$= u_1 b(v_1, w_1 v_1 + \dots + w_n v_n) + \dots + u_n b(v_n, w_1 v_1 + \dots + w_n v_n) =$$
$$= \sum_{i=1}^{n} \sum_{j=1}^{n} u_i w_j b(v_i, v_j)$$

DEFINIZIONE 5.1. Sia $A = (a_{ij}) \in k^{n,n}$ tale che $a_{ij} = b(v_i, v_j)$. Allora A si dice la *matrice associata* alla forma bilineare b nella base $(v_1, \dots, v_n)$.

LEMMA 5.1. Con le notazioni precedenti, $b(u,w) = U^t A W$, ove U e W sono i vettori colonna dei coefficienti di u e w nella base $(v_1, \dots, v_n)$.

DIMOSTRAZIONE.

$$U^t A W = (u_1, \dots, u_n) \begin{pmatrix} b(v_1, v_1) & \dots & b(v_1, v_n) \\ \vdots & & \vdots \\ b(v_n, v_1) & \dots & b(v_n, v_n) \end{pmatrix} \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = (u_1, \dots, u_n) \begin{pmatrix} \sum_{j=1}^{n} w_j b(v_1, v_j) \\ \vdots \\ \sum_{j=1}^{n} w_j b(v_n, v_j) \end{pmatrix}$$
$$= \sum_{i,j=1}^{n} u_i w_j b(v_i, v_j) = b(u,w)$$

Siano V spazio vettoriale su k, $b: V \times V \to k$ forma bilineare, $u, w \in V$, B, B' due basi di V e A matrice associata a b nella base B. Grazie a lemma 5.1, $b(u,w) = U^t A W$ ove U e W sono come in enunciato. Se $P = M_{B,B'}(id)$, allora $U = PU'$, $W = PW'$, dove U' e W' sono i vettori colonna dei coefficienti di u e w in B'.

$$b(u,w) = U^t A W = (PU')^t A P W' = U'^t P^t A P W' = U'^t A' W'$$

dove $A' = P^t A P$ è la matrice associata a b nella base B'.
Ne ricavo che le matrici associate alla stessa forma bilineare in basi diverse sono congruenti.

Un'altra cosa che si può notare è che b è simmetrica se e solo se $b(u,w) = b(w,u)$ per $u, w \in V$ e dunque se e solo se la sua matrice associata in una base qualsiasi è simmetrica.

DEFINIZIONE 5.2. $b: V\times V\to k$ bilineare è *diagonalizzabile* se esiste una base B di V tale che la matrice associata a b in B è diagonale.
Si nota immediatamente che b diagonalizzabile implica b simmetrica; infatti, se b è diagonalizzabile, esiste una base $(v_1,\dots,v_n)$ di V tale che

$$b(v_i,v_j)=\begin{cases}\lambda_i & \text{se } i=j\\ 0 & \text{se } i\neq j\end{cases}$$

Se A è la matrice associata a b nella base $(v_1,\dots,v_n)$, allora $A=(b(v_i,v_j))$ è diagonale, quindi simmetrica.

TEOREMA 5.1. Siano V spazio vettoriale su k e $b: V\times V\to k$ forma bilineare simmetrica.
Se $dim(V)=n$, allora b è diagonalizzabile. Equivalentemente, ogni matrice simmetrica è congruente a una matrice diagonale.

DIMOSTRAZIONE. Se $b(v,w)=0$ per ogni $v,w\in V$ (cioè b è identicamente nulla), la tesi è ovvia. Pertanto possiamo assumere che esistano $v,w\in V$ tali che $b(v,w)\neq 0$.
Affermo che almeno uno fra i vettori $v,w,v+w$ non è isotropo. Infatti, se v e W fossero entrambi isotropi, allora

$$b(v+w,v+w)=b(v,v+w)+b(w,v+w)=b(v,v)+b(v,w)+b(w,v)+b(w,w)=2b(v,w)\neq 0$$

Sia e_1 un vettore non isotropo per b. Allora per osservazione 4.3,

$$V=\mathcal{L}(e_1)+(\mathcal{L}(e_1))^{\perp}$$

con $dim(\mathcal{L}(e_1))^{\perp}=n-1$. Ma allora $b:(\mathcal{L}(e_1))^{\perp}\times(\mathcal{L}(e_1))^{\perp}\to k$ è una forma bilineare simmetrica su uno spazio vettoriale di dimensione $n-1$; dunque per induzione su n, $b|_{(\mathcal{L}(e_1))^{\perp}}$ è diagonalizzabile, cioè esiste una base $B'=(e_2,\dots,e_n)$ di $(\mathcal{L}(e_1))^{\perp}$ tale che

$$b(e_i,e_j)=\begin{cases}\lambda_i & \text{se } i=j\\ 0 & \text{se } i\neq j\end{cases}$$

per ogni $i,j=2,\dots,n$. $B=(e_1,\dots,e_n)$ è base di V, perchè vale anche che $b(e_1,e_1)=\lambda\neq 0$ e $b(e_1,e_i)=0$ per $i\geq 2$. La matrice associata a b nella base B è diagonale.

ALGORITMO. Data $A\in k^{n,n}$ simmetrica, determinare B diagonale con $B=P^t A P$ e $P\in k^{n,n}$ invertibile.

1. Affiancare ad A la matrice I_n, $(A\mid I_n)\in k^{n,2n}$
2. Agire su $(A\mid I_n)$ con operazioni elementari per riga riportando ogni volta l'operazione corrispondente sulle colonne
3. Conclusione: trovo $(B\mid Q)$, con B diagonale e $P=Q^t$

Nel punto 2, per operazioni elementari si intendono $E1, E2, E3$ a pagina 10.
Infatti, presa e operazione elementare per riga, allora posso considerare la matrice associata E e per e', ovvero la stessa operazione per colonne, vale $e'(A)=A E^t$. Quindi

$$(A\mid I_n)\to(E_1 A\mid E_1 I_n)\to(E_1 A E_1^t\mid E_1 I_n)\to\dots\to(E_s\dots E_1 A E_1^t\dots E_s^t\mid E_s\dots E_1 I_n)$$

Perciò, se $Q=E_s\dots E_1 I_n=E_s\dots E_1$, allora ho $(Q A Q^t\mid Q)$. Vale quindi l'algoritmo.

Studiamo la diagonalizzazione di forme bilineare nel caso complesso e nel caso reale.

Sia $k=\mathbb{C}$. A meno di riordinare i vettori della base B, posso supporre che

$$b(v_i,v_i)=\begin{cases}\lambda_i\neq 0 & i=1,\dots,r\\ 0 & i=r+1,\dots,n\end{cases}$$

Sia $a_i\in\mathbb{C}$ tale che $(a_i)^2=\lambda_i$ per $i=1,\dots,r$. Prendo quindi

$$\widetilde{B}=\left(\frac{1}{a_1}v_1,\dots,\frac{1}{a_r}v_r,v_{r+1},\dots,v_n\right)$$

Si vede che

$$b\left(\frac{1}{a_i}v_i,\frac{1}{a_i}v_i\right)=\frac{1}{a_i}\frac{1}{a_1}b(v_i,v_i)=\frac{1}{\lambda_i}\lambda_i=1$$

Pertanto, se $k=\mathbb{C}$ e $b:V\times V\to\mathbb{C}$, esiste una base $\widetilde{B}$ di V tale che la matrice associata a b nella base $\widetilde{B}$ è

$$\begin{pmatrix} I_r & 0 & \dots & 0\\ 0 & 0 & & \vdots\\ \vdots & & \ddots & \\ 0 & \dots & & 0\end{pmatrix}$$

Sia $k=\mathbb{R}$. Allora,

$$b(v_i,v_i)=\begin{cases}\lambda_i>0 & i=1,\dots,p\\ \lambda_i<0 & i=p+1,\dots,p+q\\ 0 & i=p+q+1,\dots,n\end{cases}$$

Siano $a_i\in\mathbb{R}$ tali che $(a_i)^2=\lambda_i$ per $i=1,\dots,p$ e $(a_i)^2=-\lambda_i$ per $i=p+1,\dots,p+q$. Prendo

$$\widetilde{B}=\left(\frac{1}{a_1}v_1,\dots,\frac{1}{a_{p+q}}v_{p+q},v_{p+q+1},\dots,v_n\right)$$

In maniera quasi analoga al caso $k=\mathbb{C}$,

$$b\left(\frac{v_i}{a_i},\frac{v_i}{a_i}\right)=\begin{cases}1 & i=1,\dots,p\\ -1 & i=p+1,\dots p+q\end{cases}$$

Quindi, se V è spazio vettoriale su $\mathbb{R}$, $b:V\times V\to\mathbb{R}$ bilineare simmetrica, allora esiste $\widetilde{B}$ base di V tale che la matrice associata a b nella base $\widetilde{B}$ è della forma

$$\begin{pmatrix} I_p & 0 & \dots & 0\\ 0 & -I_q & \ddots & \vdots\\ \vdots & \ddots & 0 & 0\\ 0 & \dots & 0 & 0\end{pmatrix}$$

DEFINIZIONE 5.3. Siano V uno spazio vettoriale su k, $b:V\times V\to k$ forma bilineare simmetrica.
La *forma quadratica* associata a b è la funzione

$$q:\ \underset{v\to b(v,v)}{V\to k}$$

OSSERVAZIONE 5.1. Siano $b:V\times V\to k$ forma bilineare simmetrica e $q:V\to k$ quadratica associata a b.

$$q(v+w)=b(v+w,v+w)=b(v,v)+2b(v,w)+b(w,w)=q(v)+b(v,w)+q(w)$$

Ricavo la cosiddetta *forma polare*

$$b(v,w)=\frac{1}{2}(q(v+w)-q(v)-q(w))$$

che descrive la relazione fra forma bilineare simmetrica e forma quadratica associata.

Ne segue che c'è una corrispondenza biunivoca fra forme bilineari simmetriche e forme quadratiche: presa b, definisco $q(v)=b(v,v)$; presa q, definisco $b(v,w)=(q(v+w)-q(v)-q(w))/2$.

Riprendiamo lo studio del caso reale e complesso affrontato nelle pagine precedenti (28,29). Vogliamo verificare che i numeri r e (p,q) sono *intrinseci*, cioè dipendono dalla forma bilineare simmetrica e non dalla base.

LEMMA 5.2. Sia $Q \in k^{n,n}$ una matrice invertibile; allora per ogni matrice $M \in k^{n,n}$, $\rho(QM)=\rho(M)$.

DIMOSTRAZIONE. Notiamo che le righe della matrice prodotto QM sono combinazione lineare delle righe di M; pertanto $\rho(QM) \le \rho(M)$. D'altra parte, $\rho(M)=\rho(Q^{-1}QM) \le \rho(QM)$.

LEMMA 5.3. Sia $Q \in k^{n,n}$ invertibile. Allora per ogni $M \in k^{n,n}$, $\rho(MQ)=\rho(M)$.
La dimostrazione è analoga.

COROLLARIO 5.1. Se $A, B \in k^{n,n}$ sono congruenti, allora $\rho(A)=\rho(B)$.

DIMOSTRAZIONE. Per definizione, esiste P invertibile tale che $A=P^t B P$. Per lemma 5.2 e 5.3,
$$\rho(B)=\rho(P^t B)=\rho(P^t B P)=\rho(A)$$

Abbiamo le seguenti conclusioni.
1. Nel caso $k=\mathbb{C}$, r, che è il rango della matrice associata a b nella base $\widetilde{B}$, coincide con il rango di tutte le matrici associate a b in qualche base di V.
2. Nel caso $k=\mathbb{R}$, la somma $p+q$ (rango della matrice associata a b nella base $\widetilde{B}$) non dipende dalla scelta della base. Vorremmo vedere che p e q non cambiano valore.

DEFINIZIONE 5.4. La coppia (p,q) si dice la *segnatura* della forma bilineare simmetrica $b: V \times V \to \mathbb{R}$.

TEOREMA 5.2: Di Sylvester (legge di inerzia). La segnatura è intrinseca.

DIMOSTRAZIONE. Sia $B=(v_1,\dots,v_n)$ una base di V in cui la matrice associata a $b: V \times V \to \mathbb{R}$ è
$$\begin{pmatrix} I_p & 0 & \dots & 0 \\ 0 & -I_q & \ddots & \vdots \\ \vdots & \ddots & 0 & 0 \\ 0 & \dots & 0 & 0 \end{pmatrix}$$
Sia $B'=(w_1,\dots,w_n)$ un'altra base di V in cui la matrice associata a b è
$$\begin{pmatrix} I_{p'} & 0 & \dots & 0 \\ 0 & -I_{q'} & \ddots & \vdots \\ \vdots & \ddots & 0 & 0 \\ 0 & \dots & 0 & 0 \end{pmatrix}$$
Sappiamo già che $p+q=p'+q'$. Basta verificare che $p=p'$. Siano
$$U=\mathcal{L}(v_1,\dots,v_p) \subseteq V, \quad W=\mathcal{L}(w_{p'+1},\dots,w_n)$$

Valgono i seguenti fatti:

1. $dim(U)=p$
2. $dim(W)=n-p'$
3. $b(v,v)\geq 0$ per ogni $v\in U$, $b(w,w)\leq 0$ per $w\in W$: $U\cap W=\{0_V\}$

Usando Grassmann, ho quindi che

$$n\geq dim(U+W)=dim(U)+dim(W)-dim(U\cap W)=p+n-p'-0$$

Dunque ottengo $p\leq p'$. Ripetendo lo stesso ragionamento con i ruoli di B e B' invertiti, otteniamo anche $p\geq p'$. Dunque $p=p'$.