Dipartimento di Matematica "Guido Castelnuovo"

Sapienza Università di Roma

Esercizi e Complementi di Algebra Lineare 2006-2007

Enrico Arbarello e Marco Manetti

Indice

1.	Tutoraggio del 2 ottobre 2006	1
2.	Tutoraggio del 9 ottobre 2006	2
3.	Vettori linearmente indipendenti, generatori, basi, dimensione.	2
4.	La formula di Grassmann	5
5.	Tutoraggio del 16 ottobre 2006	11
6.	Matrici e combinazioni lineari di vettori	13
7.	Tutoraggio del 23 ottobre 2006	15
8.	Tutoraggio del 30 ottobre 2006	16
9.	Cambi di base e rango	18
10.	I numeri algebrici	24
11.	Tutoraggio del 6 novembre 2006	27
12.	Esonero del 13 novembre 2006	29
13.	Permutazioni ed incroci	32
14.	Permutazioni e cicli	35
15.	La matrice di Vandermonde	40
16.	La matrice aggiunta	42
17.	Il teorema di Cayley-Hamilton	43
18.	Tutoraggio del 27 novembre 2006	45
19.	Dualità	46
20.	Tutoraggio del 4 dicembre 2006	51
21.	Tutoraggio dell'11 dicembre 2006	52
22.	Polinomi in un endomorfismo	53
23.	Autovettori	55
24.	Il polinomio caratteristico	56
25.	Diagonalizzazione	59
26.	Polinomi in un endomorfismo (remix)	63
27.	Autovettori (remix)	64
28.	Il polinomio caratteristico (remix)	66
29.	La filtrazione dei nuclei	69
30.	Struttura delle applicazioni nilpotenti	70
31.	Molteplicità algebrica e geometrica di un autovalore	72
32.	Diagonalizzazione (remix)	73
33.	Variazioni su di un classico di algebra lineare	75
34.	Esercizi gentilmente offerti da Lidia Stoppino	78
35.	Tutoraggio dell'8 gennaio 2007	80
36.	Esonero del 17 gennaio 2007	81
37.	Appello del 24 gennaio 2007	83
38.	Appello del 6 febbraio 2007	84
39.	Appello del 26 giugno 2007	86

Nelle considerazioni che seguono $\mathbb{K}$ è un campo di numeri, ossia un insieme di numeri complessi che contiene $0, 1$, che è chiuso per somma, prodotto, esistenza dell'opposto e dell'inverso. In particolare ogni matrice a coefficienti in $\mathbb{K}$ può essere considerata come una matrice a coefficienti in $\mathbb{C}$. A volte ci restringeremo al caso in cui $\mathbb{K} = \mathbb{C}$, e diremo quando ciò è necessario, in modo da poter usare il seguente

Teorema 0.1 (Teorema fondamentale dell'algebra). *Ogni polinomio $p(t) \in \mathbb{C}[t]$ di grado $n > 0$ a coefficienti complessi è il prodotto di n polinomi di grado 1.*

Di norma utilizzeremo le abbreviazioni derivanti dalla lingua inglese; scriveremo quindi deg *per grado,* ker *per nucleo,* det *per determinante,* trace *per traccia,* rank *per rango eccetera.*
L'asterisco $*$ segnala gli esercizi più difficili della media.
Con **Lang** indicheremo il libro *Algebra Lineare* di Serge Lang.

1. Tutoraggio del 2 ottobre 2006

Esercizio 1.1. Dire quali delle seguenti coppie di vettori sono ortogonali?

(1) $(1, 2, 4)$, $(2, 3, -2)$.
(2) $(1, 2, 0, 4)$, $(1, 2, 3, -2)$.
(3) $(1, 2, 0, 4, 1)$, $(1, 2, 3, -2, 4)$.

Esercizio 1.2. Trovare i vettori di $\mathbb{R}^2$ ortogonali a $(1, 3)$ e di norma 5.

Esercizio 1.3. Trovare i vettori di $\mathbb{R}^3$ ortogonali ai vettori $(0, 2, -1)$ e $(-1, 2, 0)$.

Esercizio 1.4. Trovare la retta in $\mathbb{R}^2$ parallela al vettore $(1, -1)$ e passante per il punto $(0, -3)$; di tale retta si determinino i punti di intersezione con gli assi coordinati.

Esercizio 1.5. Dimostrare che per ogni coppia di vettori $A, B \in \mathbb{R}^n$ vale l'uguaglianza

$$\|A + B\|^2 + \|A - B\|^2 = 2\|A\|^2 + 2\|B\|^2.$$

Esercizio 1.6. Si considerino i punti $A = (1, 0)$, $B = (2, 1)$ e $C = (5, 4)$, contenuti nella retta di equazione $x - y = 1$. Calcolare

$$\frac{|(A - B) \cdot (A - C)|}{\|A - B\|\|A - C\|}.$$

Esercizio 1.7. Sia $P = (2, 0)$. Descrivere geometricamente il luogo dei punti $X \in \mathbb{R}^2$ tali che $X \cdot (P - X) = 0$.

Esercizio 1.8 ($*$). Verificare l'identità tra prodotti scalari di vettori di $\mathbb{R}^2$

$$(A - O) \cdot (B - C) - (A - C) \cdot (B - O) + (A - B) \cdot (C - O) = 0$$

e utilizzarla per dimostrare che le tre altezze di un triangolo ABC si incontrano in un punto O.

2. Tutoraggio del 9 ottobre 2006

Esercizio 2.1. Scrivere i seguenti numeri complessi nella forma $a + ib$

$$\frac{1-i}{1+2i}, \quad \frac{1-2i}{1-i}, \quad (1+i)^4.$$

Esercizio 2.2. Scrivere i seguenti numeri nella forma $a + b\sqrt{2}$, con $a, b \in \mathbb{Q}$.

$$\frac{1-\sqrt{2}}{1+\sqrt{2}}, \quad \frac{1-2\sqrt{2}}{1-\sqrt{2}}, \quad (1-\sqrt{2})^3(1+\sqrt{2})^3.$$

Esercizio 2.3. Trovare la distanza del punto $P = (1, 2, 1)$ dal piano π di equazione $3x - 2y + z = 1$.

Esercizio 2.4. Dati tre numeri complessi z_1, z_2, z_3 diversi da 0. Quanto vale la somma degli argomenti di

$$\frac{z_1}{z_2}, \quad \frac{z_2}{z_3}, \quad \frac{z_3}{z_1}.$$

Esercizio 2.5. Descrivere il luogo $H \subset \mathbb{C}$ dei numeri complessi z tali che $|z - i| < |z + i|$.

Esercizio 2.6. Descrivere il luogo $Q \subset \mathbb{C}$ dei numeri complessi $z = a + ib$ tali che $|z^2 - i| < |z^2 + i|$ e $b > 0$.

Esercizio 2.7. Dire, motivando la risposta, se l'applicazione $f\colon \mathbb{C} \to \mathbb{C}^2$, $f(z) = (z^2, z^3)$, è iniettiva.

Esercizio 2.8. Risolvendo un opportuno sistema lineare, si determinino tre numeri razionali x, y, z tali che

$$\frac{1}{1-\sqrt[3]{2}+\sqrt[3]{4}} = x + y\sqrt[3]{2} + z\sqrt[3]{4}.$$

Esercizio 2.9 ($*$). Siano A, B, C punti del piano non allineati. Mostrare che esistono tre vettori U, V, W di norma 1 e tali che:

(1) $(C - A) \cdot U = (C - B) \cdot U > 0$.
(2) $(B - A) \cdot V = (B - C) \cdot V > 0$.
(3) $(A - B) \cdot W = (A - C) \cdot W > 0$.

Mostrare che per ogni punto P vale la relazione

$$(P - A) \cdot (V - U) + (P - B) \cdot (U - W) + (P - C) \cdot (W - V) = 0$$

ed utilizzarla per dimostrare che le bisettrici di un triangolo si incontrano in un punto.

3. Vettori linearmente indipendenti, generatori, basi, dimensione.

Sia $\mathbb{K}$ un campo di numeri e V un $\mathbb{K}$-spazio vettoriale. Siano $v_1, \ldots, v_N$ vettori in V. Il *sottospazio vettoriale di V generato da $v_1, \ldots, v_N$* è l'insieme

$$L(v_1, \ldots, v_N) = \{v \in V \ : \ v = a_1v_1 + \cdots + a_Nv_N, \ a_i \in \mathbb{K}, \ i = 1, \ldots, N\}$$

Si dice che il vettore $v = a_1v_1 + \cdots + a_Nv_N$ è *una combinazione lineare (a coefficienti in $\mathbb{K}$) dei vettori $v_1, \ldots, v_N$*. Si verifica facilmente che $L(v_1, \ldots, v_N)$ è un sottospazio vettoriale di V. A volte si dice anche che $L(v_1, \ldots, v_N)$ *è il sottospazio lineare di V generato da $v_1, \ldots, v_N$*.

Osservazione 3.1. Si osservi che $L(w_1, \dots, w_k) \subset L(v_1, \dots, v_s)$, se e solo se
$$w_i \in L(v_1, \dots, v_s), \quad i = 1, \dots, k.$$

Lo spazio vettoriale V si dice *di dimensione finita, o anche finitamente generato*, se esistono vettori $v_1, \dots, v_N$ in V
$$V = L(v_1, \dots, v_N)$$
In questo caso si dice che $\{v_1, \dots, v_N\}$ è un *sistema di generatori per V.*

Sia $\{w_1, \dots, w_k\} \subset V$ un sottoinsieme finito. I vettori $w_1, \dots, w_k$ si dicono *linearmente dipendenti* se se esiste una loro combinazione lineare, non banale, che dà il vettore nullo:
$$a_1 w_1 + \cdots + a_k w_k = 0 \qquad (*)$$
Dire che la combinazione è *non banale* vuol dire che non tutti i coefficienti a_i sono nulli:
$$(a_1, \dots, a_k) \neq (0, \dots, 0).$$
Si dice che la $(*)$ è una *relazione (lineare) tra i vettori $w_1, \dots, w_k$.*

I vettori $w_1, \dots w_k$ si dicono *lineramente indipendenti* se non sono linearmente indipendenti e cioè se *l'unica* loro combinazione lineare che dà il vettore nullo è la combinazione lineare banale:
$$0w_1 + \cdots + 0w_k = 0$$
Un sistema di generatori di V costituito da vettori linearmente indipendenti si dice *una base di V.*

Osservazione 3.2. Spesso capita che, i ragionamenti che si fanno a partire da un insieme finito di vettori $\{u_1, \dots, u_s\}$ siano completamente indipendenti dall'ordine in cui si prendono questi vettori. Con questo si vuole dire che se, per esempio, i vettori in esame sono i vettori A, B, C allora il ragionamento non cambia se si pone
$$u_1 = A,\ u_2 = B,\ u_3 = C,$$
oppure
$$u_1 = B,\ u_2 = A,\ u_3 = C,$$
oppure ancora
$$u_1 = C,\ u_2 = B,\ u_3 = A,$$
e così via.

Teorema 3.3. *Sia $V = L(v_1, \dots, v_N)$ e sia*
$$\{v_{i_1}, \dots, v_{i_n}\} \subset \{v_1, \dots, v_N\}$$
un sottoinsieme massimale di vettori linearmente indipendenti, allora $\{v_{i_1}, \dots, v_{i_n}\}$ è una base di V.

Dimostrazione. A meno di riordinare il sistema di generatori $\{v_1, \dots, v_N\}$ si può assumere che
$$v_{i_1} = v_1$$
$$\vdots$$
$$v_{i_n} = v_n$$

Dobbiamo mostrare che $V = L(v_1, \dots, v_n)$. Basta far vedere che $v_{n+k} \in L(v_1, \dots, v_n)$ per $k = 1, \dots, N - n$. Fissiamo un qualsiasi k con $1 \leq k \leq N - n$. Per la massimalità di $\{v_1, \dots, v_n\}$ i vettori dell'insieme $\{v_1, \dots, v_n, v_{n+k}\}$ sono linearmente dipendenti. Dunque c'è una relazione:

$$av_{n+k} + a_1 v_1 + \cdots + a_n v_n = 0\,.$$

Il coefficiente a è diverso da zero altrimenti $v_1, \dots, v_n$ sarebbero linearmente dipendenti. Quindi si può scrivere

$$v_{n+k} = -\frac{a_1}{a} v_1 - \cdots - \frac{a_n}{a} v_n\,,$$

come si voleva. □

Corollario 3.4. *Ogni spazio vettoriale finitamente generato ammette una base.*

Teorema 3.5. *Sia $\{v_1, \dots, v_n\}$ un insieme di generatori di V e sia $\{w_1, \dots, w_m\}$ un insieme di vettori linearmente indipendenti in V allora $m \leq n$*

Dimostrazione. Si supponga $m \geq n$. Scriviamo

$$w_1 = a_1 v_1 + \cdots + a_n v_n.$$

A meno di rinumerare l'insieme $\{v_1, \dots, v_n\}$, si può assumere che $a_1 \neq 0$. Dunque

$$v_1 = \frac{1}{a_1} w_1 - \frac{a_2}{a_1} v_2 - \cdots - \frac{a_n}{a_1} v_n.$$

Ne segue che $\{v_1, \dots, v_n\} \subset L(w_1, v_2 \dots, v_n)$ e dunque $V = L(w_1, v_2 \dots, v_n)$. Ora scriviamo

$$w_2 = b_1 w_1 + c_2 v_2 + c_3 v_3 + \cdots c_n v_n.$$

Poiché, w_1 e w_2 sono linearmente indipendenti, i c_i non possono essere tutti nulli. A meno di rinumerare l'insieme $\{v_2, \dots, v_n\}$, possiamo assumere che $c_2 \neq 0$. Dunque

$$v_2 = \frac{1}{c_2} w_2 - \frac{b_1}{c_2} w_1 - \frac{c_3}{c_2} v_3 - \cdots - \frac{c_n}{c_2} v_n.$$

Di conseguenza abbiamo $\{w_1, v_2, \dots, v_n\} \subset L(w_1, w_2, v_3, \dots, v_n)$ e dunque $V = L(w_1, w_2, v_3, \dots, v_n)$. Procedendo in questo modo, dopo r passi si dimostra che $V = L(w_1, w_2, \dots w_r, v_{r+1}, \dots, v_n)$. Facciamo il passo successsivo. Scriviamo

$$w_{r+1} = d_1 w_1 + \cdots + d_r w_r + e_{r+1} v_{r+1} + \cdots + e_n v_n\,.$$

Poiché, $w_1, \dots, w_{r+1}$ sono linearmente indipendenti, gli e_i non possono essere tutti nulli. A meno di rinumerare l'insieme $\{v_{r+1}, \dots, v_n\}$, possiamo assumere che $e_{r+1} \neq 0$. Dunque

$$v_{r+1} = \frac{1}{e_{r+1}} w_{r+1} - \frac{d_1}{e_{r+1}} w_1 - \cdots - \frac{d_r}{e_{r+1}} w_r - \frac{e_{r+2}}{e_{r+1}} v_{r+2} - \cdots - \frac{e_n}{e_{r+1}} v_n.$$

Ne segue che $\{w_1, w_2, \dots, w_r, v_{r+1}, \dots, v_n\} \subset L(w_1, \dots, w_{r+1}, v_{r+2}, \dots, v_n)$ e dunque $V = L(w_1, \dots, w_{r+1}, v_{r+2}, \dots, v_n)$. Alla fine si sostituiscono tutti i v_i con dei w_j e si ottiene che $w_1, \dots, w_n$ generano V:

$$V = L(w_1, \dots, w_n)\,.$$

Ma i vettori $w_1, \dots, w_n$ sono, per ipotesi, linearmente indipendenti e quindi, essendo anche dei generatori, formano una base di V. Ma allora $m = n$, altrimenti w_m potrebbe esprimersi come combinazione lineare di $w_1, \dots, w_n$, contro il supposto. □

Corollario 3.6. *Le basi di uno spazio vettoriale finitamente generato hanno tutte lo stesso numero di elementi.*

Si dice che V *ha dimensione* n *su* $\mathbb{K}$ e si scrive

$$\dim_{\mathbb{K}} V = n$$

se V possiede una base formata da n elementi. In virtù del Corollario 2, questa definizione è ben posta.

Teorema 3.7. *Sia V uno spazio n-dimensionale (su $\mathbb{K}$). Siano $v_1, \dots, v_k$ vettori di V linearmente indipendenti. Cosicché $k \leq n$. Allora è possibile trovare vettori $v_{k+1}, \dots, v_n$ tali che $\{v_1, \dots, v_n\}$ sia una base di V.*

Dimostrazione. Se $L(v_1, \dots, v_k) = V$, si ha $k = n$ e non vi è nulla da dimostrare. Altrimenti, sia $v_{k+1} \in V \setminus L(v_1, \dots, v_k)$. Allora $v_1, \dots, v_k, v_{k+1}$ sono linearmente indipendenti. Perché se vi fosse una relazione

$$a_1 v_1 + \cdots + a_k v_k + a_{k+1} v_{k+1} = 0\,,$$

per la lineare dipendenza di $\{v_1, \dots, v_k\}$, il coefficiente a_{k+1} dovrebbe essere non nullo e quindi si potrebbe esprimere v_{k+1} come combinazione lineare di $v_1, \dots, v_k$, contradicendo il fatto che $v_{k+1} \notin L(v_1, \dots, v_k)$. Procedendo in questo modo si costruisce la base $\{v_1, \dots, v_k, v_{k+1}, \dots, v_n\}$. □

4. La formula di Grassmann

La chiusura lineare.

Definizione 4.1. Sia A un sottoinsieme di uno spazio vettoriale V. Chiameremo *chiusura lineare* di A in V, in simboli $L(A)$, il più piccolo sottospazio vettoriale di V che contiene A.

Ma cosa intendiamo dire esattamente quando diciamo che $L(A)$ è il più piccolo sottospazio vettoriale che contiene A? Vogliamo dire che valgono le seguenti tre proprietà:

- **L1:** $A \subseteq L(A)$.
- **L2:** $L(A)$ è un sottospazio vettoriale di V.
- **L3:** Se $W \subseteq V$ è un sottospazio vettoriale che contiene A, allora $L(A) \subseteq W$.

Mostreremo tra breve che la chiusura lineare esiste sempre. Per il momento dimostriamo che se esiste allora essa è unica, ossia che le tre proprietà L1,L2 e L3 determinano univocamente $L(A)$. Se infatti $L(A)$ e $L(A)'$ soddisfano entrambi L1,L2,L3, allora ponendo $W = L(A)'$ nella L3 si ottiene $L(A) \subseteq L(A)'$. Similmente, ponendo $W = L(A)$ si ottiene $L(A)' \subseteq L(A)$ e quindi $L(A) = L(A)'$. Prima di passare alla dimostrazione dell'esistenza in generale, consideriamo alcuni casi particolari.
Se $A = \emptyset$ è il sottoinsieme vuoto, allora $L(A) = 0$ soddisfa le tre condizioni

L1,L2,L3.
Se $A = \{v\}$ è formato da un solo vettore, allora

$$L(A) = L(v) = \{tv \mid t \in \mathbb{K}\}$$

è il sottospazio vettoriale formato da tutti i multipli scalari di v.
Se $A = \{v_1, \ldots, v_n\}$ è un insieme finito di vettori, allora

$$L(A) = L(v_1, \ldots, v_n) = \{t_1v_1 + \cdots + t_nv_n \mid t_1, \ldots, t_n \in \mathbb{K}\}$$

è l'insieme di tutte le combinazioni lineari di $v_1, \ldots, v_n$: per la dimostrazione che $L(v_1, \ldots, v_n)$ è un sottospazio vettoriale, ossia che soddisfa L2, rimandiamo al Lang, pagina 40.
Verifichiamo in dettaglio che $L(v_1, \ldots, v_n)$ soddisfa anche L1 e L3. Per ogni indice i possismo scrivere

$$v_i = 0v_1 + \cdots + 0v_{i-1} + 1v_i + 0v_{i+1} + \cdots + 0v_n \in L(v_1, \ldots, v_n)$$

e quindi vale L1. Se W è un sottospazio vettoriale che contiene $v_1, \ldots, v_n$, allora siccome W è chiuso per le operazioni di somma e prodotto per scalare, ed ogni combinazione lineare può essere pensata come una composizione di somme e prodotti per scalare, ne segue che ogni combinazione lineare di $v_1, \ldots, v_n$ appartiene a W e quindi $L(v_1, \ldots, v_n) \subset W$.

Se A è un sottoinsieme qualsiasi (possibilmente infinito) possiamo costruire $L(A)$ nei due modi seguenti: alcune verifiche sono lasciate per esercizio al lettore.

Primo metodo:

$$\begin{aligned} L(A) &= \{\text{combinazioni lineari di sottoinsiemi finiti di } A\} \\ &= \bigcup\{L(B) \mid B \subseteq A,\ B \text{ finito}\}. \end{aligned}$$

Secondo metodo: $L(A)$ =intersezione di tutti i sottospazi vettoriali che contengono A.

Il secondo metodo richiede qualche commento aggiuntivo. Indichiamo con $\mathcal{A}$ la famiglia di tutti i sottospazi vettoriali che contengono A; notiamo che essa non è vuota poiché contiene V. Consideriamo adesso l'insieme intersezione di tutti i sottospazi appartenenti a $\mathcal{A}$,

$$H = \bigcap\{W \mid W \in \mathcal{A}\}.$$

Notiamo che H soddisfa tutte le condizioni di sottospazio vettoriale ed è evidente che $A \subseteq H$. D'altronde se W è un sottospazio che contiene A, allora $W \in \mathcal{A}$ e segue quindi dalla definizione di H che $H \subseteq W$, ossia H soddisfa la condizione L3.
Spesso $L(A)$ viene detto **sottospazio vettoriale generato da** A.

Esempio 4.2. Sia V lo spazio vettoriale dei polinomi di grado ≤ 2 su $\mathbb{K}$ nella indeterminata x e sia $A = \{x, x^2\} \subset V$. Allora $L(A)$ è l'insieme dei polinomi di grado ≤ 2 senza termine noto.

Diremo che A è un **insieme di generatori** di V se vale $V = L(A)$.

Esempio 4.3. Gli n vettori di $\mathbb{R}^n$:

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad e_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \dots, e_n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

generano $\mathbb{R}^n$. Infatti ogni vettore di coordinate $x_1, \dots, x_n$ può essere pensato come la combinazione lineare dei vettori e_i con coefficienti x_i:

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = x_1 e_1 + x_2 e_2 + \cdots + x_n e_n.$$

Notiamo che se A, B sono due sottoinsiemi finiti di uno spazio vettoriale V, se A genera V ed ogni elemento di A può essere scritto come combinazione lineare di elementi di B, allora anche B genera V. Infatti se $V = L(A)$ e $A \subset L(B)$, segue dalla proprietà L3 che $L(A) \subseteq L(B)$ e quindi $V = L(B)$.
In particolare, se A è un insieme finito di vettori, se B è ottenuto da A aggiungendo un numero finito di combinazioni lineari di elementi di A, e se B è un insieme di generatori, allora anche A è un insieme di generatori.

Esempio 4.4. Mostriamo che i vettori $u = (1, 1, 1)$, $v = (1, 2, 3)$ e $w = (1, 3, 4)$ generano $\mathbb{R}^3$. Per le osservazioni viste sopra non è restrittivo aggiungere ai tre vettori u, v, w alcune combinazioni lineari dei medesimi. Ad esempio

$$a = v - u = (0, 1, 2), \quad b = w - u = (0, 2, 3), \quad c = b - 2a = (0, 0, -1).$$

(L'idea è chiara: far comparire quanti più zeri è possibile.)

$$d = a + 2c = (0, 1, 0), \qquad e = u - d + c = (1, 0, 0).$$

Abbiamo già osservato che i vettori $e_1 = e$, $e_2 = d$ e $e_3 = -c$ generano $\mathbb{R}^3$ e quindi anche u, v, w sono generatori.

Diremo che V ha **dimensione finita** se V posside un insieme finito di generatori.

Esercizio 4.5. Sia $\mathbb{K}$ un campo di numeri, ossia un sottoinsieme di $\mathbb{C}$ che contiene $0, 1$ ed è chiuso per le quattro operazioni (somma-differenza-prodotto-divisione). Dimostrare che che i vettori $u = (1, 2, 1)$, $v = (2, 1, 3)$ e $w = (3, 3, 3)$ generano $\mathbb{K}^3$.

Esercizio 4.6. Siano A, B sottoinsiemi finiti di uno spazio vettoriale V. Provare che in generale vale $L(A \cap B) \subseteq L(A) \cap L(B)$ e trovare un esempio in cui $L(A \cap B) \neq L(A) \cap L(B)$.

Esercizio 4.7. Determinare il luogo dei vettori $(b, c) \in \mathbb{R}^2$ tali che le radici di $x^2 + bx + c = 0$ generano $\mathbb{C}$ come spazio vettoriale su $\mathbb{R}$.

Indipendenza lineare.

Lemma 4.8. *Siano $v_1, \dots, v_n$ vettori di uno spazio vettoriale. Le seguenti condizioni sono equivalenti:*

(1) *$v_1, \dots, v_n$ sono linearmente indipendenti.*

(2) $v_1, \ldots, v_{n-1}$ *sono linearmente indipendenti e* $v_n \notin L(v_1, \ldots, v_{n-1})$.

Dimostrazione. Dimostriamo che 1. implica 2., ossia supponiamo per ipotesi che $v_1, \ldots, v_n$ siano linearmente indipendenti. È chiaro che $v_1, \ldots, v_{n-1}$ sono linearmente indipendenti, mentre se per assurdo $v_n \in L(v_1, \ldots, v_{n-1})$ esisterebbero $n-1$ scalari $a_1, \ldots, a_{n-1} \in \mathbb{K}$ tali che

$$v_n = a_1 v_1 + \cdots + a_{n-1} v_{n-1}.$$

In tal caso si avrebbe

$$a_1 v_1 + \cdots + a_{n-1} v_{n-1} + (-1) v_n = 0$$

in contraddizione con la lineare indipendenza di $v_1, \ldots, v_n$.
Dimostriamo adesso il viceversa, ossia che 2. implica 1.: sia

$$a_1 v_1 + \cdots + a_{n-1} v_{n-1} + a_n v_n = 0$$

una relazione lineare tra i vettori v_i. Se $a_n = 0$ allora l'espressione precedente si riduce ad una relazione tra i vettori indipendenti $v_1, \ldots, v_{n-1}$ e quindi anche $a_1 = a_2 = \cdots = a_{n-1} = 0$.
Se invece $a_n \neq 0$, allora si ha

$$v_n = -\frac{a_1}{a_n} v_1 - \cdots - \frac{a_{n-1}}{a_n} v_{n-1}$$

e quindi $v_n \in L(v_1, \ldots, v_{n-1})$, contrariamente a quanto ipotizzato. □

(**Nota:** il quadratino bianco è il simbolo che denota la conclusione di una dimostrazione. Sebbene sia il simbolo più comune vi sono in letteratura alcune varianti (CVD, QED, quadratini neri ecc.)

Il Teorema 2 del Paragrafo 10 (pagina 47) del **Lang** viene talvolta detto *teorema di scambio* (più raramente teorema di Steinitz) e può essere enunciato nel modo seguente.

Teorema 4.9. *Sia A un insieme finito di generatori di uno spazio vettoriale V sul campo $\mathbb{K}$ e sia $B \subset V$ un insieme di vettori linearmente indipendenti. Allora vale $|A| \geq |B|$.*

Tanto per capirci, se S è un insieme finito, il simbolo $|S|$ indica la sua *cardinalità*, ossia il numero di elementi di cui S è composto. Ad esempio $|\{\text{dita di una mano}\}| = 5$. Chiaramente se $S \subseteq T$ allora $|S| \leq |T|$. Proponiamo adesso una dimostrazione del teorema di scambio diversa da quella del Lang.

Dimostrazione del Teorema 4.9. Sia $m = |B|$ la cardinalità di B; vogliamo dimostrare che esiste un sottoinsieme di A formato da m vettori linearmente indipendenti. Fra tutti i possibili sottoinsiemi $C \subseteq A \cup B$, consideriamo quelli che soddisfano le seguenti tre proprietà:

(1) $|C| = m$,
(2) $A \cap B \subseteq C$,
(3) i vettori di C sono linearmente indipendenti.

Notiamo che la famiglia, che indicheremo con la lettera $\mathcal{F}$, dei sottoinsiemi che soddisfano tali proprietà non è vuota poiché $B \in \mathcal{F}$ (B, pensato come sottoinsieme di $A \cup B$ soddisfa per ipotesi le tre proprietà). Scegliamo adesso un

sottoinsieme C della famiglia $\mathcal{F}$ tale che $A \cap C$ ha cardinalità massima: ciò significa che per ogni altro $D \in \mathcal{F}$ vale $|A \cap C| \geq |A \cap D|$.
Per dimostrare il teorema è sufficiente dimostrare che $C \subset A$; per fare questo supporremo che esista $v \in C$ con $v \notin A$ e proveremo che questa assunzione porta ad una contraddizione.
Scriviamo quindi $C = \{v, v_2, \ldots, v_m\}$ con $v \notin A$; in particolare $v \notin A \cap B$ e quindi $A \cap B \subset \{v_2, \ldots, v_m\}$.
Siccome i vettori $v, v_2, \ldots, w_m$ sono linearmente indipendenti vale $v \notin L(v_2, \ldots, v_m)$ e quindi $L(v_2, \ldots, v_m)$ è strettamente contenuto in $V = L(A)$. Ne consegue che esiste un vettore $w \in A$ che non appartiene al sottospazio $L(v_2, \ldots, v_m)$ e di conseguenza l'insieme

$$D = \{w, v_2, \ldots, v_m\}$$

è formato da m vettori linearmente indipendenti. È dunque chiaro che $D \in \mathcal{F}$ e che $A \cap D = (A \cap C) \cup \{w\}$; quindi $|A \cap D| = |A \cap C| + 1$ e questo **contraddice** la massimalità di $|A \cap C|$. $\square$

Corollario 4.10. *Uno spazio vettoriale V ha dimensione finita se e solo se esiste un intero positivo n tale che, presi comunque $n+1$ vettori $v_0, \ldots, v_n \in V$, essi risultano linearmente dipendenti.*

Dimostrazione. Per definizione, uno spazio ha dimensione finita se possiede un insieme finito di generatori. Se $w_1, \ldots, w_n$ generano V allora, per il teorema di scambio, non è possibile trovare $n+1$ vettori linearmente indipendenti.
Viceversa supponiamo che esista un limite superiore al numero di vettori linearmente indipendenti e denotiamo con r il massimo numero di vettori linearmente indipendenti che possiamo trovare in V. Basta dimostrare che presi comunque r vettori $v_1, \ldots, v_r$ linearmente indipendenti si ha $L(v_1, \ldots, v_r) = V$.
Se fosse $L(v_1, \ldots, v_r) \neq V$, allora per ogni vettore $v_0 \notin L(v_1, \ldots, v_r)$ si avrebbe che $v_0, v_1, \ldots, v_r$ sarebbero indipendenti, in contraddizione con la definizione di r. $\square$

Esempio 4.11. Lo spazio $\mathbb{R}$ ha dimensione infinita (=non finita) come spazio vettoriale su $\mathbb{Q}$. La dimostrazione di questo fatto segue facilmente dall'esistenza dei numeri trascendenti. Un numero reale si dice *trascendente* se non è radice di alcun polinomio a coefficienti razionali. Se t è un numero trascendente, allora per ogni $n > 0$ i numeri reali $1, t, t^2, t^3, \ldots, t^n$ sono linearmente indipendenti su $\mathbb{Q}$ (Esercizio: perché?). Siccome esistono numeri trascendenti (i numeri e, π sono trascendenti) non esiste alcun limite superiore al numero dei vettori indipendenti su $\mathbb{Q}$.

Esercizio 4.12. Dimostrare che i numeri $1, \sqrt{2}, \sqrt{3}$ e $\sqrt{6}$ sono linearmente indipendenti su $\mathbb{Q}$.

Esercizio 4.13 ($*$). Dimostrare che le radici quadrate dei numeri primi sono linearmente indipendenti su $\mathbb{Q}$. (più avanti daremo qualche suggerimento).

Esercizio 4.14. Dimostrare che $\mathbb{R}$ non ha dimensione finita come spazio vettoriale su $\mathbb{Q}[\sqrt{2}]$. ($\mathbb{Q}[\sqrt{2}]$ è il campo dei numeri della forma $a + b\sqrt{2}$, con $a, b \in \mathbb{Q}$.)

Corollario 4.15. *Ogni sottospazio vettoriale di uno spazio di dimensione finita ha dimensione finita.*

Dimostrazione. Sia $W \subseteq V$ un sottospazio vettoriale e assumiamo V di dimensione finita. Siccome esiste un limite superiore al numero di vettori linearmente indipendenti di V, a maggior ragione tale limite esiste anche per i vettori di W. $\square$

Esercizio 4.16. Un insieme possibilmente infinito di vettori A di uno spazio vettoriale si dice indipendente se per ogni sottoinsieme proprio $B \subset A$, $B \neq A$, vale $L(B) \neq L(A)$. Dimostrare che A è indipendente se e solo se ogni sottoinsieme finito di vettori di A sono linearmente indipendenti (nel senso usuale del termine).

La formula di Grassmann.
Se U e W sono sottospazi vettoriali di uno spazio vettoriale V di dimensione finita, si indica con $U + W$ il sottospazio vettoriale di V formato dai vettori v che si possono scrivere nella forma

$$v = u + w,$$

al variare di $u \in U$ e $w \in W$. Osserviamo che $U \subseteq U + W$ (U è l'insieme dei vettori $u + 0$) e $W \subseteq U + W$.

Lemma 4.17. *Siano A, B sottoinsiemi finiti di uno spazio vettoriale V. Allora vale*

$$L(A \cup B) = L(A) + L(B).$$

Dimostrazione. Siccome il sottospazio vettoriale $L(A) + L(B)$ contiene sia A che B, esso contiene l'unione $A \cup B$ e quindi contiene il sottospazio da essa generato, ossia $L(A \cup B) \subseteq L(A) + L(B)$. Viceversa se $v \in L(A) + L(B)$, per definizione esistono $u \in L(A)$ e $w \in L(B)$ tali che $v = u + w$. Siccome u è una combinazione lineare di elementi di A e w è una combinazione lineare di elementi di B, la loro somma $u + w$ è una combinazione lineare di elementi di $A \cup B$. $\square$

Vogliamo adesso dimostrare la **formula di Grassmann**

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

Denotiamo con $n = \dim U$, $m = \dim W$ e con $p = \dim(U \cap W)$; siccome $U \cap W$ è un sottospazio di U vale $p \leq n$ e similmente $p \leq m$. Consideriamo una base $e_1, \ldots, e_p$ di $U \cap W$; i vettori $e_1, \ldots, e_p$ sono linearmente indipendenti in U e quindi possono essere completati ad una base $e_1, \ldots, e_p, u_{p+1}, \ldots, u_n$ di U. Similmente i vettori $e_1, \ldots, e_p$ possono essere completati ad una base $e_1, \ldots, e_p, w_{p+1}, \ldots, w_m$ di W. Basta adesso dimostrare che gli $n + m - p$ vettori

$$e_1, \ldots, e_p, u_{p+1}, \ldots, u_n, w_{p+1}, \ldots, w_m$$

formano una base di $U+W$. Il lemma precedente implica che tali vettori generano $U + W$; resta quindi da dimostrare che sono linearmente indipendenti. Siano dunque $a_1, \ldots, a_p, b_{p+1}, \ldots, b_n, c_{p+1}, \ldots, c_m \in \mathbb{K}$ tali che

$$a_1e_1 + \cdots + a_pe_p + b_{p+1}u_{p+1} + \cdots + b_nu_n + c_{p+1}w_{p+1} + \cdots + c_mw_m = 0;$$

dobbiamo dimostrare che $a_i = b_j = c_k = 0$ per ogni i, j, k.
Consideriamo il vettore di W

$$w = -(c_{p+1}w_{p+1} + \cdots + c_mw_m).$$

Dalla relazione precedente segue che

$$w = a_1e_1 + \cdots + a_pe_p + b_{p+1}u_{p+1} + \cdots + b_nu_n \in U$$

e quindi $w \in U \cap W$. Se indichiamo con $d_1, \ldots, d_p$ i coefficienti di w nella base $e_1, \ldots, e_p$ si ha

$$0 = w - w = d_1 e_1 + \cdots + d_p e_p + c_{p+1} w_{p+1} + \cdots + c_m w_m$$

e siccome $e_1, \ldots, e_p, w_{p+1}, \ldots, w_m$ è una base di W deve essere $d_i = c_j = 0$ per ogni i, j e quindi $w = 0$, ossia

$$w = a_1 e_1 + \cdots + a_p e_p + b_{p+1} u_{p+1} + \cdots + b_n u_n = 0.$$

Siccome $e_1, \ldots, e_p, u_{p+1}, \ldots, u_n$ è una base di U deve essere $a_i = b_j = 0$ per ogni i, j, come volevasi dimostrare.

Terminiamo con un po' di notazioni. Il sottospazio $U+W$ viene detto la **somma** di U, W. Diremo che $U + W$ è una **somma diretta interna** se $U \cap W = 0$, o equivalentemente se $\dim(U + W) = \dim U + \dim W$. Quando la somma risulta essere diretta, lo segnaleremo graficamente mettendo un cerchio intorno alla croce. Quindi se U, W sono sottospazi di V il simbolo $U \oplus W$ indica il sottospazio $U + W$ ed in più ci avverte che $U \cap W = 0$:

$$U \oplus W = \begin{cases} U + W & \text{se } U \cap W = 0 \\ \text{non è definito} & \text{se } U \cap W \neq 0 \end{cases}$$

Notiamo che $U + W = W + U$ e quindi, $U \oplus W = W \oplus U$ quando sono definite.

Definizione 4.18. Siano U, W due sottospazi di V. Diremo che W è un **complementare di** U **in** V se vale $V = U \oplus W$.

Segue dalla formula di Grassmann che se W è un complementare di U in V allora $\dim U + \dim W = \dim V$.

Esercizio 4.19. Trovare una bigezione (=applicazione bigettiva) tra l'insieme dei sottospazi complementari in $\mathbb{R}^3$ al piano π di equazione $x + y + z = 0$ e l'insieme dei vettori $(a, b, c) \in \mathbb{R}^3$ tali che $a + b + c = 1$.

Esercizio 4.20. Siano A, B, C tre sottospazi vettoriali di V. Dimostrare che le seguenti tre condizioni sono equivalenti:

(1) $V = (A \oplus B) \oplus C$.
(2) $V = A \oplus (B \oplus C)$.
(3) Per ogni vettore $v \in V$ esistono unici tre vettori $a \in A$, $b \in B$ e $c \in C$ tali che $v = a + b + c$.

5. Tutoraggio del 16 ottobre 2006

Esercizio 5.1. Dati i seguenti 4 vettori di $\mathbb{R}^3$: $e_1 = (1, 0, 0)$, $e_2 = (0, 1, 0)$, $u = (3, 4, 2)$ e $v = (2, 5, 0)$, eliminatene uno tra u e v in modo che i rimanenti 3 formino una base.

Esercizio 5.2. Per quali valori del parametro reale t, i tre vettori $u = (1, 0, 1)$, $v = (0, 1, 1)$, $w = (3, 4, t)$ sono linearmente indipendenti in $\mathbb{R}^3$?

Esercizio 5.3. Determinare le coordinate del vettore $(2, 5) \in \mathbb{R}^2$ rispetto alla base $u_1 = (1, 1)$, $u_2 = (1, -1)$.

Esercizio 5.4. Trovare una base e_1, e_2 di $\mathbb{R}^2$ tale che $(1,0) = e_1 + e_2$, $(0,1) = e_1 - e_2$.

Esercizio 5.5. Trovare una base e_1, e_2 di $\mathbb{R}^2$ tale che i tre vettori $v_1 = e_1$, $v_2 = e_1 + e_2$ e $v_3 = e_1 - e_2$ siano multipli di $u_1 = (1,1)$, $u_2 = (1,-1)$ e $u_3 = (0,1)$ rispettivamente. (In altri termini, si chiede che per ogni indice i i due vettori v_i, u_i siano linearmente dipendenti.)

Esercizio 5.6. Dire se esistono tre sottospazi vettoriali U, V, W di $\mathbb{R}^2$ tali che

$$\mathbb{R}^2 = U \oplus V = U \oplus W = V \oplus W.$$

Esercizio 5.7. Vero o falso? Il sottospazio vettoriale generato da tre vettori linearmente indipendenti u, v, w è uguale al sottospazio generato da $u - v, v - w, w - u$.

Esercizio 5.8. Vero o falso? Il sottospazio vettoriale generato da tre vettori linearmente indipendenti u, v, w è uguale al sottospazio generato da $u + v, v + w, w + u$.

Esercizio 5.9. Sia V lo spazio vettoriale dei polinomi reali di grado minore o eguale a 9. Sia W il sottospazio vettoriale formato dei polinomi $p(x)$ tali che $p(x) = p(-x)$. Trovare un complementare di W in V. Trovare le varie dimensioni.

Esercizio 5.10. Sia V lo spazio vettoriale dei polinomi reali di grado minore o eguale a 9. Sia W il sottospazio vettoriale formato dei polinomi $p(x)$ tali che $p(1) = p(0)$. Trovare un complementare di W in V. Trovare le varie dimensioni.

Esercizio 5.11. Nello spazio vettoriale dei polinomi reali di grado minore od uguale a 350, dire se il polinomio $(x+1)^{350}$ si può scrivere come combinazione lineare dei cinque polinomi

$$(x-1)^{350}, \quad (x-1)(x+1)^{349}, \quad (x-1)^2(x+1)^{348}, \quad (x-1)^3(x+1)^{347}, \quad x^{350} - 1.$$

Esercizio 5.12 ($*$). Sia $\mathbb{K} \subset \mathbb{R}$ un campo di numeri che ha dimensione 2 come spazio vettoriale su $\mathbb{Q}$. Dimostrare che esiste un intero positivo p tale che ogni elemento di $\mathbb{K}$ si può scrivere come $a + b\sqrt{p}$, con $a, b \in \mathbb{Q}$.

Esercizio 5.13 ($*$). Si assuma come noto a priori che il polinomio di terzo grado $x^3 - 3x - 1$ possiede tre radici reali distinte.

(1) Trovare due numeri complessi a, b tali che

$$\frac{a}{a-b}(x-b)^3 - \frac{b}{a-b}(x-a)^3 = x^3 - 3x - 1.$$

(2) Mostrare che per ogni radice cubica z di $\dfrac{a}{b}$ il numero $\dfrac{a-bz}{1-z}$ è reale ed è una radice del polinomio $x^3 - 3x - 1$.

(3) Sia u il seno di $2\pi/9$. Descrivere le tre radici di $x^3 - 3x - 1$ in funzione di u.

(4) Sostituite $x^3 - 3x - 1$ con un qualsiasi polinomio della forma $p(x) = x^3 - 3px - q$ con p, q numeri reali tali che $4p^3 \neq q^2$. Dimostrare che esistono a, b come al punto 1 e che, se $p(x)$ ha almeno due radici reali distinte, allora a, b non sono reali.

6. Matrici e combinazioni lineari di vettori

Sia $\mathbb{K}$ un campo di numeri e sia V un $\mathbb{K}$-spazio vettoriale. Chiameremo matrice di n vettori di V qualunque successione ordinata di $v_1, \dots, v_n$ di n vettori di V. Per le matrici si utilizza la notazione orizzontale (ricordiamo che i vettori di $\mathbb{K}^n$ si scrivono in verticale), e quindi

$$\mathbf{v} = (v_1, \dots, v_n), \qquad v_i \in V$$

indica una matrice di n vettori di V.

Se $V = \mathbb{K}^m$, esiste una naturale bigezione tra le matrici $m \times n$ a coefficienti in $\mathbb{K}$ e le matrici di n vettori di V.

Data una matrice di n vettori $\mathbf{v} = (v_1, \dots, v_n)$ ed un vettore

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{K}^n$$

Definiamo il prodotto *matrice-vettore* (detto anche *riga per colonna*) come

$$\mathbf{v}x = (v_1, \dots, v_n) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = x_1 v_1 + \cdots + x_n v_n \in V.$$

Notiamo che, se $\mathbf{v} = (v_1, \dots, v_n)$, allora il sottospazio vettoriale $L(v_1, \dots, v_n)$ coincide con l'insieme di tutti i prodotti $\mathbf{v}x$, al variare di x tra tutti i possibili vettori di $\mathbb{K}^n$.

Esercizio 6.1. Sia $\mathbf{v}$ una matrice di n vettori. Provare che $K = \{x \in \mathbb{K}^n \mid \mathbf{v}x = 0\}$ è un sottospazio vettoriale di $\mathbb{K}^n$. Inoltre $K = 0$ se e solo se i vettori di $\mathbf{v}$ sono linearmente indipendenti.

Sia $\mathbb{K}$ un campo di numeri e sia V un $\mathbb{K}$-spazio vettoriale. Siano $v_1, \dots, v_n$ dei vettori in V. Consideriamo la matrice $1 \times n$ di vettori

$$\mathbf{v} = (v_1, \dots, v_n)$$

Sia B una matrice $n \times n$ a cefficienti in $\mathbb{K}$. Consideriamo il prodotto di matrici $\mathbf{v}B$. Si ottiene una matrice $1 \times n$ di vettori:

$$\mathbf{v}B = (v_1, \dots, v_n) \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{pmatrix} =$$

$$(b_{11}v_1 + b_{21}v_2 + \cdots + b_{n1}v_n, b_{12}v_1 + b_{22}v_2 + \cdots + b_{n2}v_n, \cdots, b_{1n}v_1 + b_{2n}v_2 + \cdots + b_{nn}v_n)$$

Osservazione 6.2. Gli n vettori della matrice $\mathbf{v}B$ sono combinazioni lineari degli n vettori colonna della matrice $\mathbf{v}$.

In particolare:

Osservazione 6.3. Se i vettori $v_1, \dots, v_n$ sono linearmente dipendenti lo sono anche gli n vettori della matrice $\mathbf{v}B$.

In seguito dimostreremo il seguente teorema.

TEOREMA 6.4. *Siano Siano $v_1, \dots, v_n$ dei vettori linearmente indipendenti in V. Sia $\mathbf{v} = (v_1, \dots, v_n)$ e sia B una matrice $n \times n$. Allora gli n vettori della matrice $\mathbf{v}B$ sono linearmente indipendenti $\iff$ B è invertibile.*

DIMOSTRAZIONE. Per il momento possiamo solo dimostrare l'implicazione $\Leftarrow$). Se i vettori di $\mathbf{v}B$ fossero linearmente dipendenti, allora per l'Osservazione 6.3, si avrebbe che i vettori di $\mathbf{v}BB^{-1}$ sarebbero linearmente dipendenti. Ma $\mathbf{v}BB^{-1} = \mathbf{v}$, da cui la contraddizione. $\square$

Possiamo enunciare l'implicazione che abbiamo appena dimostrato in questo modo.

TEOREMA 6.5. *Siano $v_1, \dots, v_n$ dei vettori in V. Sia $\mathbf{v} = (v_1, \dots, v_n)$ e sia B una matrice $n \times n$. Supponiamo che B sia invertibile. Allora i vettori di $\mathbf{v}$ sono linearmente indipendenti se e solo se lo sono quelle di $\mathbf{v}B$.*

ESERCIZIO 6.6. Sia $\mathbf{v} = (v_1, \dots, v_n)$ e siano B, C due matrici $n \times n$. Provare che se $v_1, \dots, v_n$ sono linearmente indipendenti e $\mathbf{v}B = \mathbf{v}C$, allora $B = C$.

Occupiamoci ora delle matrici triangolari. Le *matrici triangolari superiori* sono quelle del tipo:

$$B = \begin{pmatrix} b_{11} & b_{12} & b_{13} & \cdots & b_{1\ n-1} & b_{1n} \\ 0 & b_{22} & b_{23} & \cdots & b_{2\ n-1} & b_{2n} \\ 0 & 0 & b_{33} & \cdots & b_{3\ n-1} & b_{2n} \\ . & . & . & \cdots & . & \\ . & . & . & \cdots & . & \\ . & . & . & \cdots & . & \\ 0 & 0 & 0 & \cdots & b_{n-1n-1} & b_{n-1n} \\ 0 & 0 & 0 & \cdots & 0 & b_{nn} \end{pmatrix}$$

Dimostreremo in seguito che non appena

$$\prod_{i=1}^{n} = b_{ii} \neq 0, \tag{1}$$

allora la matrice triangolare B è invertibile. Però, senza usare questo fatto possiamo comunque dimostrare che

TEOREMA 6.7. *Siano $v_1, \dots, v_n$ dei vettori in V. Sia $\mathbf{v} = (v_1, \dots, v_n)$ e sia B una matrice $n \times n$. Supponiamo che B sia triangolare e che valga la condizione (1). Allora i vettori di $\mathbf{v}$ sono linearmente indipendenti se e solo se lo sono quelli di $\mathbf{v}B$.*

DIMOSTRAZIONE. Se i vettori di $\mathbf{v}B$ sono linearmente indipendenti lo sono anche quelli di $\mathbf{v}$ per la Osservazione 6.3. Supponiamo ora che i vettori di $\mathbf{v}$ siano indipendenti. Si consideri una relazione tra i vettori di $\mathbf{v}B$:

$$\alpha_1(b_{11}v_1) + \alpha_2(b_{12}v_1 + b_{22}v_2) + \cdots + \alpha_{n-1}(b_{1\ n-1}v_1 + b_{2\ n-1}v_2 + \cdots + b_{n-1\ n-1}v_{n-1}) + \\ + \alpha_n(b_{1n}v_1 + b_{2n}v_2 + \cdots + b_{nn}v_n) = 0\,.$$

Il coefficiente di v_n in questa espressione è $\alpha_n b_{nn}$. Poiché $b_{nn} \neq 0$ si deve avere $\alpha_n = 0$. Il coefficiente di v_{n-1} nella nuova espressione (con $\alpha_n = 0$) è

$\alpha_{n-1}b_{n-1\,n-1}$. Poiché $b_{n-1\,n-1} \neq 0$ si deve avere $\alpha_{n-1} = 0$. Procedendo in questo modo si dimostra che tutti gli α_i sono nulli. $\square$

Nelle applicazioni sappiamo che un procedimento molto utile è il seguente. Dati n vettori $v_1, v_2, \dots, v_n$, per verificare la loro dipendenza o indipendenza lineare, si può fissare un indice j e sostituire il vettore v_j con il vettore $v_j + av_i$, lasciando gli altri vettori invariati. In effetti si ha

$$(v_1, v_2, \dots, v_{j-1}, v_j + av_i, v_{j+1} \dots v_n) = (v_1, v_2, \dots, v_{j-1}, v_j, v_{j+1} \dots v_n)C^{(ij)}(a)\,,$$

dove $C^{(ij)}(a)$ è la matrice triangolare superiore che ha tutti i coefficienti della diagonale uguli ad 1 e tutti gli altri coefficienti uguali a zero tranne il coefficiente di posto ij che è uguale ad a.

7. Tutoraggio del 23 ottobre 2006

Esercizio 7.1. Sia B una matrice $n \times n$. Dimostrare che $V = \{A \in M_{n,n} : AB = BA\}$ è un sottospazio di $M_{n,n}$. Descrivere V nel caso in cui $n = 2$ e

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

Esercizio 7.2. Per ogni numero complesso $z = a + ib$ si consideri la matrice reale $M(z) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$.
Verificare che per ogni coppia di numeri complessi z, w vale

$$M(z + w) = M(z) + M(w), \qquad M(zw) = M(z)M(w).$$

Esercizio 7.3. Siano

$$v = \begin{pmatrix} a \\ b \end{pmatrix} \qquad w = \begin{pmatrix} b \\ c \end{pmatrix}$$

due vettori in $\mathbb{R}^2$. Si consideri la matrice

$$A = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

Si dimostri che il coseno dell'angolo tra v e w è uguale a quello tra i vettori Av e Aw.

Esercizio 7.4. Si descriva, al variare di θ il luogo dei vettori $(x, y) \in \mathbb{R}^2$ definiti da:

$$(x, y) = \begin{pmatrix} \cos\frac{\pi}{7} & -\sin\frac{\pi}{7} \\ \sin\frac{\pi}{7} & \cos\frac{\pi}{7} \end{pmatrix} \cdot \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix}$$

Esercizio 7.5. Sia

$$A = \begin{pmatrix} 1 & -1 & 3 \\ 2 & 0 & -1 \\ -1 & -1 & 4 \end{pmatrix}$$

Si dimostri che

$$V = \left\{ (x, y, z) \in \mathbb{R}^3 \ : \ A \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 0 \right\}$$

è un sottospazio di $\mathbb{R}^3$. Se ne calcoli la dimensione e se ne trovi una base.

Esercizio 7.6. I polinomi $(t-1)(t-2)$, $(t-2)(t-3)$, $(t-3)(t-1)$ sono linearmente indipendenti?

Esercizio 7.7. Sia V l'insieme delle successioni reali

$$V = \{s = \{a_n\} \ : \ n = 0, 1, 2, \dots\}$$

V è in modo naturale uno spazio vettoriale. Si consideri l'insieme

$$W = \{s = \{s_n\} \ : \ s_n = s_{n-1} + s_{n-2}\,,, \, n = 3, 4, \dots\}$$

W è un sottospazio? ha dimensione finita?

Esercizio 7.8. Sia

$$A = \begin{pmatrix} 0 & 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Calcolare A^2

Esercizio 7.9. Calcolare AB, dove

$$A = \begin{pmatrix} 0 & \sqrt{2} & \sqrt{3} \\ -\sqrt{2} & 0 & \sqrt{5} \\ -\sqrt{3} & -\sqrt{5} & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} \sqrt{5} \\ -\sqrt{3} \\ \sqrt{2} \end{pmatrix}$$

Dire inoltre se i vettori colonna di A^{350} sono linearmente indipendenti.

Esercizio 7.10. Dimostrare che ogni matrice antisimmetrica 3×3 non è invertibile.

Esercizio 7.11. Sia $A \in M_{n,n}(\mathbb{K})$ una matrice i cui vettori colonna generano un sottospazio vettoriale di dimensione 1.
Dimostrare che esistono $B \in M_{n,1}(\mathbb{K})$ e $C \in M_{1,n}(\mathbb{K})$ tali che $BC = A$. Dedurre che $A^2 = \text{Traccia}(A)A$, dove $\text{Traccia}(A)$ indica la traccia di A, e che $A - tI$ è invertibile per ogni $t \neq 0, \text{Traccia}(A)$. (Suggerimento: calcolare il prodotto $(A - tI)(A - (\text{Traccia}(A) - t)I)$.)

8. Tutoraggio del 30 ottobre 2006

Esercizio 8.1. Vero o falso? L'applicazione $f\colon \mathbb{R} \to \mathbb{R}$ definita da $f(x) = 3^x - 2^x$ è lineare.

Esercizio 8.2. Si consideri l'applicazione lineare $F\colon \mathbb{R}^3 \to \mathbb{R}^3$ definita da

$$F(x, y, z) = (x - z, y, x - z).$$

Calcolare il rango di F ed F^2 e trovare le basi dei rispettivi nuclei.

Esercizio 8.3. Siano A, B due matrici $n \times n$ tali che $AB = BA$; dimostrare che $A^2B^2 = B^2A^2$. Trovare un esempio in cui il viceversa non vale (sugg.: provare con le matrici triangolari 2×2).

Esercizio 8.4. Sia $F\colon V \to V$ un'applicazione lineare. Dimostrare che
$$\ker(F) \subseteq \ker(F^2), \qquad F(\ker(F^2)) \subseteq \ker(F).$$
Considerare poi la restrizione di F al nucleo di F^2 e utilizzare la formula delle dimensioni di nucleo ed immagine per provare la formula.
$$\dim\ker(F^2) \leq 2\dim\ker(F).$$

Esercizio 8.5. Sia $P : \mathbb{K}^n \to \mathbb{K}^n$ l'applicazione lineare definita da $P(x_1,\ldots,x_n) = (0,0,\ldots,0,x_{k+1},\ldots,x_n)$. Dimostrare che $P^2 = P$. Trovare una matrice A tale che $P = L_A$ ($P = L_A$ vuol dire che $P(x) = Ax$ per ogni x).

Esercizio 8.6. Vero o falso? Sia $W \subset \mathbb{K}^5$ un sottospazio di dimensione 2. Allora possiamo scrivere W come intersezione di due sottospazi di dimensione 4 (sugg.: formula di Grassmann).

Esercizio 8.7. Vero o falso? Sia $W \subset \mathbb{K}^6$ un sottospazio di dimensione 2. Allora possiamo scrivere W come intersezione di tre sottospazi di dimensione 5.

Esercizio 8.8. Sia V lo spazio vettoriale delle funzioni continue a valori reali definite nell'intervallo $[0,1]$. Sia $P\colon V \to V$ l'applicazione lineare definita da
$$P(f(x)) = \frac{f(x)+f(-x)}{2}$$
Dimostrare che $P^2 = P$

Esercizio 8.9. Una applicazione lineare $P\colon V \to V$ tale che $P^2 = P$ si dice una **proiezione**. Dimostrare che una proiezione P non è invertibile, a meno che $P = I$. Cosa si può dire di $P - I$?

Esercizio 8.10. Sia V uno spazio vettoriale di dimensione finita e sia $f\colon V \to V$ un'applicazione lineare. Dimostrare che se $f(U) \subseteq U$ per ogni sottospazio vettoriale U, allora f è un multiplo dell'identità. (Suggerimento: se $(v_1,\ldots,v_n)$ è una base, considerare come sottospazi le $n+1$ rette generate dagli $n+1$ vettori $v_1, v_2, \ldots, v_n, v_1 + v_2 + \cdots + v_n$.)

Esercizio 8.11. Sia $(v_1,\ldots,v_n)$ una base di uno spazio vettoriale V. Per ogni sottoinsieme $I \subseteq \{1,\ldots,n\}$ indichiamo con $U_I \subseteq V$ il sottospazio vettoriale generato dai vettori v_i, con $i \in I$. Ad esempio se $I = \{1,2,4\}$ allora $U_I = L(v_1,v_2,v_4)$. Dimostrare:

(1) $\dim U_I = |I|, \qquad U_I \cap U_J = U_{I\cap J}, \qquad U_I + U_J = U_{I\cup J}$
(2) Sia $W \subseteq V$ un sottospazio vettoriale e sia $I \subseteq \{1,\ldots,n\}$ tale che $U_I \cap W = 0$. Se $U_J \cap (W + U_I) = 0$, allora vale $W \cap U_{I\cup J} = 0$.
(3) Sia $W \subseteq V$ un sottospazio vettoriale e sia $I \subseteq \{1,\ldots,n\}$ di cardinalità massima tra quelli che $U_I \cap W = 0$. Allora vale $V = W \oplus U_I$.

Esercizio 8.12 (∗). Sia V lo spazio vettoriale dei polinomi a coefficienti reali di grado $\leq n$. Siano $a_1,\ldots a_{n+1}$ numeri reali distinti. Sia $L_i : V \to \mathbb{R}$ l'applicazione lineare definita da
$$L_i(p(x)) = p(a_i) \quad p(x) \in V\,, \quad i = 1,\ldots,n\,.$$
Dimostrare che $L_1,\ldots,L_{n+1}$ è una base di $\mathcal{L}(V,\mathbb{R})$. (Suggerimento: considerare i polinomi $p_k(x) = \prod_{j\neq k}(x - a_j)$, per $k = 1,\ldots n+1$.)

Esercizio 8.13 ($*$). Siano $a_1, \dots, a_{n+1}$ numeri reali distinti. Dimostrare che esistono numeri reali $c_1, \dots, c_n$ tali che, per ogni polinomio $p(x) \in \mathbb{R}[x]$ di grado minore o uguale a n, valga la formula di quadratura:

$$\int_0^1 p(x)dx = c_1 p(a_1) + c_2 p(a_2) + \cdots + c_{n+1} p(a_{n+1}) \,.$$

9. Cambi di base e rango

Sia $\mathbb{K}$ un campo di numeri e sia V un $\mathbb{K}$-spazio vettoriale.
Anche se a prima vista può sembrare eccessivamente pedante, è necessario sottolineare che, mentre si parla di insiemi generatori e di insiemi di vettori linearmente indipendenti, nella definizione di base non si parla di insieme di vettori ma di **successione** di vettori.
Questo significa che se $v_1, \dots, v_n$ sono vettori linearmente indipendenti che generano V, non è l'insieme $\{v_1, \dots, v_n\} \subset V$ ad essere una base, ma è la successione

$$(v_1, \dots, v_n)$$

che viene definita come base. Naturalmente, siccome le proprietà di essere generatori e lineramente indipendenti non dipendono dall'ordine dei vettori, ne segue che se $(v_1, \dots, v_n)$ è una base di V, allora ogni altra successione dei vettori v_i ottenuta permutando gli indici è una base.
Ad esempio, se $\dim V = 2$, allora con due vettori linearmente indipendenti v_1, v_2 si possono costruire due basi

$$(v_1, v_2), \qquad (v_2, v_1).$$

Se $\dim V = 3$, allora con tre vettori linearmente indipendenti v_1, v_2, v_3 si possono costruire sei basi

$$\begin{array}{ccc} (v_1, v_2, v_3), & (v_2, v_1, v_3), & (v_3, v_1, v_2), \\ (v_1, v_3, v_2), & (v_2, v_3, v_1), & (v_3, v_2, v_1). \end{array}$$

In generale, se $\dim V = n$, allora con n vettori linearmente indipendenti si possono costruire $n!$ basi.

Utilizzando l'ormai familiare regola del prodotto righe per colonne, data una successione di n vettori di V

$$\mathbf{v} = (v_1, \dots, v_n), \qquad v_i \in V$$

ed un vettore

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{K}^n$$

Definiamo

$$\mathbf{v}x = (v_1, \dots, v_n) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = x_1 v_1 + \cdots + x_n v_n \in V.$$

Notiamo in proposito che $\mathbf{v}$ è una base di V se e soltanto se per ogni $w \in V$ esiste un unico vettore $x \in \mathbb{K}^n$ tale che $\mathbf{v}x = w$.

Il cambio di base.

Siano $\mathbf{v} = (v_1, \dots, v_n)$ e $\mathbf{w} = (w_1, \dots, w_n)$ due basi di uno stesso spazio vettoriale V. Per quanto osservato prima, esiste un unico vettore

$$a_{*1} = \begin{pmatrix} a_{11} \\ \vdots \\ a_{n1} \end{pmatrix} \in \mathbb{K}^n$$

tale che $\mathbf{v}a_{*1} = w_1$. Similmente esiste un unico $a_{*2} \in \mathbb{K}^n$ tale che $\mathbf{v}a_{*2} = w_2$ e più in generale, per ogni indice j esiste un unico $a_{*j} \in \mathbb{K}^n$ tale che $\mathbf{v}a_{*j} = w_j$. Se indichiamo con $A \in M_{n,n}(\mathbb{K})$ la matrice di vettori colonna $a_{*1}, a_{*2}, \dots, a_{*n}$ possiamo scrivere

$$\mathbf{v}A = \mathbf{v}(a_{*1}, a_{*2}, \dots, a_{*n}) = \mathbf{w},$$

che, guardando con la lente di ingrandimento diventa

$$(v_1, \dots, v_n) \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} = (w_1, \dots, w_n).$$

La matrice A che abbiamo costruito è l'unica matrice tale che

$$\mathbf{v}A = \mathbf{w}$$

che chiameremo *matrice di cambiamento di base.*

TEOREMA 9.1. *Nelle notazioni precedenti la matrice A è invertibile e vale*

$$\mathbf{w}A^{-1} = \mathbf{v}.$$

DIMOSTRAZIONE. Ripetendo il ragionamento con $\mathbf{w}$ al posto di $\mathbf{v}$ e viceversa, troviamo una matrice $B \in M_{n,n}(\mathbb{K})$ tale che

$$\mathbf{w}B = \mathbf{v}.$$

Moltiplicando entrambi i membri dell'equazione $\mathbf{v}A = \mathbf{w}$ per B e ricordando la proprietà associativa del prodotto righe per colonne si ottiene

$$\mathbf{v}AB = \mathbf{w}B = \mathbf{v}.$$

D'altra parte se I indica la matrice identità vale $\mathbf{v}I = \mathbf{v}$ e dall'unicità della matrice di cambiamento di base segue che $AB = I$. In maniera del tutto simile si prova che $BA = I$ e quindi $B = A^{-1}$. $\square$

Ricordiamo che le coordinate di un vettore v rispetto ad una base $\mathbf{v} = (v_1, \dots, v_n)$ sono per definizione gli n numeri $x_1, \dots, x_n$ tali che

$$v = x_1v_1 + \cdots + x_nv_n.$$

È chiaro che se cambia base, allora cambiano anche le coordinate di v. Se indichiamo con $y_1, \dots, y_n$ le coordinate dello stesso vettore v rispetto alla base $\mathbf{w} = (w_1, \dots, w_n)$ e consideriamo i due vettori colonna

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \quad y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \in \mathbb{K}^n$$

possiamo scrivere
$$v = \mathbf{v}x = \mathbf{w}y = \mathbf{v}Ay.$$
In particolare $\mathbf{v}x = \mathbf{v}Ay$ da cui si deduce
$$x = Ay.$$

Esercizio 9.2. Sia $\mathbf{v} = (v_1, v_2)$ una base. Determinare la matrice A tale che
$$(v_1, v_2)A = (v_2, v_1).$$
Sapete dire quanto vale A^2 senza bisogno di fare il conto?

Esercizio 9.3. Scrivere una matrice A 3×3 a coefficienti interi, diversa dall'identità e tale che $A^3 = I$.

Esercizio 9.4. Sia $\mathbf{v} = (v_1, v_2, v_3)$ una base. Dimostrare che
$$\mathbf{w} = (v_1, v_2 + 2v_1, v_3 + v_2)$$
è ancora una base e calcolare la matrice A soggetta alla relazione $\mathbf{v}A = \mathbf{w}$. Infine calcolare, senza eseguire prodotti di matrici, la somma dei coefficienti della quarta colonna di A^2, A^3 e A^4. Fate una previsione sulla somma dei coefficienti delle prime tre righe della quarta colonna di A^n per ogni $n > 0$ e provate a dimostrarlo per induzione.

Il rango di un'applicazione lineare.
Richiamiamo il seguente risultato dimostrato sul **Lang**:

Teorema 9.5. *Sia $f\colon V \to W$ un'applicazione lineare. Allora il suo nucleo*
$$\ker(f) = \{v \in V \mid f(v) = 0\}$$
e la sua immagine
$$f(V) = \{f(v) \mid v \in V\}$$
sono sottospazi vettoriali (di V e W rispettivamente). Inoltre, se V ha dimensione finita vale la formula
$$\dim V = \dim \ker(f) + \dim f(V).$$

Definizione 9.6. Il **rango** di un'applicazione lineare $f\colon V \to W$ è la dimensione dell'immagine: $\text{rango}(f) = \dim f(V)$.

Esempio 9.7. Sia $(v_1, \ldots, v_n)$ una base di V e $w_1, \ldots, w_n$ vettori di W. Se denotiamo con $f\colon V \to W$ l'unica applicazione lineare tale che $f(v_i) = w_i$, allora $f(V) = L(w_1, \ldots, w_n)$ e quindi il rango di f è uguale al massimo numero di vettori w_i linearmente indipendenti.

Notiamo che il rango di un'applicazione $f\colon V \to W$ è minore od uguale al minimo tra le dimensioni di V e W. Infatti $f(V)$ è un sottospazio di W (quindi $r(f) \le \dim W$), mentre per il teorema si ha $\dim V - \dim f(V) = \dim \ker(f) \ge 0$.

Esercizio 9.8. Calcolare il rango dell'applicazione lineare
$$\mathbb{R}^3 \to \mathbb{R}^3, \qquad (x, y, z) \mapsto (x - y, y - z, z - x).$$

Esercizio 9.9. Siano $f, g\colon V \to W$ lineari. Dimostrare che

$$(f+g)(V) \subseteq f(V) + g(V)$$

e dedurre la diseguaglianza

$$\text{rango}(f+g) \leq \text{rango}(f) + \text{rango}(g).$$

Trovare un esempio dove $\text{rango}(f+g) = 2$ e $\text{rango}(f) = \text{rango}(g) = 1$.

La caratteristica di una matrice.

Sia $A = (a_{ij})$ una matrice $n \times m$ a coefficienti in un campo $\mathbb{K}$. Possiamo pensare A come una successione (verticale) di vettori riga oppure come una successione (orizzontale) di vettori colonna.

Chiameremo **rango** di A il rango dell'applicazione lineare

$$L_A\colon \mathbb{K}^m \to \mathbb{K}^n, \qquad L_A(x) = Ax.$$

Chiameremo **caratteristica per righe** di A il massimo numero di vettori riga di A linearmente indipendenti e **caratteristica per colonne** il massimo numero vettori colonna di A linearmente indipendenti.

Osservazione 9.10. La caratteristica per righe di una matrice A è uguale alla caratteristica per colonne della matrice trasposta ${}^tA$.

Obiettivo di questa sezione è quello di dimostrare il teorema.

Teorema 9.11. *In ogni matrice, la caratteristica per righe, la caratteristica per colonne ed il rango coincidono. In particolare ogni matrice ha lo stesso rango della propria trasposta.*

Dimostrazione. Consideriamo l'applicazione lineare

$$L_A\colon \mathbb{K}^m \to \mathbb{K}^n, \quad L_A(x) = Ax.$$

I vettori $Ax \in \mathbb{K}^n$ sono, al variare di $x \in \mathbb{K}^m$, tutte e sole le combinazioni lineari dei vettori colonna di A e quindi l'immagine dell'applicazione lineare L_A coincide con il sottospazio vettoriale generato dalle colonne di A. Ne deduciamo che il rango di A è uguale alla caratteristica per colonne.

Per ogni matrice A indichiamo con $r(A)$ la caratteristica per righe e con $c(A)$ la caratteristica per colonne. Naturalmente vale $c(A) \leq m$ e, siccome i vettori colonna appartengono allo spazio vettoriale $\mathbb{K}^n$, che ha dimensione n, vale anche $c(A) \leq n$. Lo stesso ragionamento si applica ai vettori riga e quindi

$$c(A) \leq \min(n, m), \qquad r(A) \leq \min(n, m).$$

Il resto della dimostrazione si articola in due passi: nel primo proveremo che per ogni matrice A vale $c(A) \leq r(A)$ e nel secondo che vale la disuguaglianza opposta $r(A) \leq c(A)$.

Consideriamo l'applicazione lineare

$$L_A\colon \mathbb{K}^m \to \mathbb{K}^n, \quad L_A(x) = Ax.$$

Per la formula delle dimensioni di nucleo ed immagine ne consegue che

$$\dim \ker(L_A) = m - \dim L_A(\mathbb{K}^m) = m - c(A).$$

Se $A = (a_{ij})$, allora $\ker(L_A) = V$, dove $V \subseteq \mathbb{K}^m$ è l'insieme dei vettori di coordinate $x_1, \ldots, x_m$ che risolvono il sistema lineare omogeneo di n equazioni

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1m}x_m = 0 \\ \vdots \qquad\quad \vdots \qquad\qquad\quad \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nm}x_m = 0 \end{cases}$$

Dimostriamo per induzione su n che vale $\dim(V) \geq m - r(A)$.
Se $n = 0$ allora $\dim(V) = m \geq r$. Se $r = n$, ricordando che $c(A) \leq n$ si ottiene

$$\dim(V) = m - c(A) \geq m - n = m - r(A).$$

Supponiamo adesso $r(A) < n$; scambiando l'ordine delle righe l'insieme V rimane chiaramente invariato. Possiamo quindi supporre che la prima riga della matrice sia una combinazione lineare delle successive.
Dal punto di vista del sistema lineare ciò significa che la prima equazione si può scrivere come combinazione lineare delle equazioni successive e quindi può essere omessa dal sistema senza che questo modifichi l'insieme V delle soluzioni. In altri termini V coincide con l'insieme delle soluzioni del sistema di $n - 1$ equazioni

$$\begin{cases} a_{21}x_1 + a_{22}x_2 + \cdots + a_{2m}x_m = 0 \\ \vdots \qquad\quad \vdots \qquad\qquad\quad \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nm}x_m = 0 \end{cases}$$

e per l'ipotesi induttiva applicata a questo nuovo sistema si ricava $\dim(V) \geq m - r(A)$.
In conclusione abbiamo dimostrato che $m - c(A) = \dim(V) \geq m - r(A)$ e quindi che per ogni matrice A vale $c(A) \leq r(A)$.
Per dimostrare che $r(A) \leq c(A)$ basta osservare che $r(A) = c({}^tA)$, $c(A) = r({}^tA)$ e quindi

$$r(A) = c({}^tA) \leq r({}^tA) = c(A).$$

□

Il teorema di Rouché-Capelli.
Supponiamo di avere un sistema lineare non omogeneo di n equazioni in m incognite

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1m}x_m = b_1 \\ \vdots \qquad\quad \vdots \qquad\qquad\quad \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nm}x_m = b_n \end{cases}$$

e associamo ad esso la matrice dei coefficienti

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nm} \end{pmatrix} \in M_{n,m}(\mathbb{K})$$

e la **matrice completa**

$$C = \begin{pmatrix} a_{11} & \cdots & a_{1m} & b_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{n1} & \cdots & a_{nm} & b_n \end{pmatrix} \in M_{n,m+1}(\mathbb{K}).$$

Teorema 9.12 (Rouché-Capelli). *Un sistema lineare ammette soluzione se e soltanto se la matrice completa e la matrice dei coefficienti hanno lo stesso rango.*

Dimostrazione. Nelle notazioni precedenti, il sistema ammette soluzione se e soltanto se l'ultimo vettore colonna di C appartiene al sottospazio vettoriale generato dai vettori colonna di A e quindi se e soltanto se l'immagine di L_C è uguale all'immagine di L_A. $\square$

Esercizio 9.13. Dimostrare che, nelle notazioni precedenti, il sistema lineare ammette un'unica soluzione se e solo se

$$\text{rango}(A) = \text{rango}(C) = m.$$

Esercizio 9.14. Ogni matrice a coefficienti reali può essere pensata anche come una matrice a coefficicnti complessi. Dimostrare che il rango non cambia. (Sugg.: mostrare che se $v_1, \ldots, v_r \in \mathbb{R}^n$ sono linearmente indipendenti su $\mathbb{R}$, lo sono anche su $\mathbb{C}$ quando li pensiamo come vettori di $\mathbb{C}^n$.)

Osservazione 9.15. Dimostreremo più avanti, con l'aiuto del determinante, che il rango di una matrice a coefficienti in un qualunque campo di numeri non cambia la consideriamo a coefficienti complessi.

Esercizi sui polinomi.

Si consiglia di risolvere gli esercizi nell'ordine proposto.
Nel seguito $\mathbb{K}$ indicherà un campo di numeri e $\mathbb{K}[x]_{\leq n}$ lo spazio vettoriale dei polinomi di di grado $\leq n$. Ricordiamo che $\mathbb{K}[x]_{\leq n}$ ha dimensione $n+1$.

Esercizio 9.16. Siano $p_0(x), p_1(x), \ldots, p_n(x) \in \mathbb{K}[x]_{\leq n}$ polinomi non nulli con $p_i(x)$ di grado i per ogni $i = 0, \ldots, n$. Dimostrare che sono linearmente indipendenti.

Esercizio 9.17. Dimostrare che la successione $1, x, x(x-1), x(x-1)(x-2)$ è una base di $\mathbb{K}[x]_{\leq 3}$ e che l'applicazione

$$f\colon \mathbb{K}[x]_{\leq 3} \to \mathbb{K}^4, \qquad f(p(x)) = (p(0), p(1), p(2), p(3))$$

è iniettiva.

Esercizio 9.18. Siano $a_1, a_2, \ldots, a_n, a_{n+1} \in \mathbb{K}$ numeri distinti. Dimostrare che gli $n+1$ polinomi

$$p_0(x) = 1, \quad p_1(x) = x - a_1, \quad p_2(x) = (x-a_1)(x-a_2), \ldots$$
$$p_n(x) = (x-a_1)(x-a_2)\cdots(x-a_n)$$

sono una base di $\mathbb{K}[x]_{\leq n}$ e che l'applicazione

$$f\colon \mathbb{K}[x]_{\leq n} \to \mathbb{K}^{n+1}, \qquad f(p(x)) = (p(a_1), p(a_2), \ldots, p(a_n), p(a_{n+1}))$$

è iniettiva.

Esercizio 9.19. Utlizzare l'esercizio precedente per dimostrare che ogni polinomio di grado n possiede al più n radici distinte in $\mathbb{K}$.

Esercizio 9.20. Siano $a_0, a_1, \ldots, a_n \in \mathbb{K}$ numeri distinti. Provare che gli $n+1$ vettori di $\mathbb{K}^{n+1}$

$$v_0 = (1, 1, \ldots, 1),\ v_1 = (a_0, a_1, \ldots, a_n),\ v_2 = (a_0^2, a_1^2, \ldots, a_n^2), \ldots$$
$$\ldots, v_n = (a_0^n, a_1^n, \ldots, a_n^n)$$

sono linearmente indipendenti.

Esercizio 9.21. Sia $q(x)$ un polinomio non nullo di grado d, con $d \leq n$. Dimostrare che gli $n+1$ polinomi

$$p_0(x) = 1, \quad p_1(x) = x, \quad \ldots, \quad p_{d-1}(x) = x^{d-1},$$
$$p_d(x) = q(x), \quad p_{d+1}(x) = xq(x), \quad \ldots, \quad p_n(x) = x^{n-r}q(x)$$

sono una base di $\mathbb{K}[x]_{\leq n}$.

Esercizio 9.22. Siano $p(x)$ e $q(x)$ due polinomi di gradi n, d rispettivamente, con $d \leq n$ e $q(x) \neq 0$. Scrivere $p(x)$ come combinazione lineare della base definita nell'esercizio precedente e dedurre che si può scrivere

$$p(x) = h(x)q(x) + r(x)$$

con $h(x)$ di grado $\leq n-d$ e $r(x)$ di grado $< d$. Mostrare inoltre che h e r sono unici.

10. I numeri algebrici

Definizione 10.1. Un **numero algebrico** è un numero x, reale o complesso, che è radice di un polinomio non nullo a coefficienti interi.

Più precisamente, un numero $x \in \mathbb{C}$ è algebrico se e solo se esistono un intero positivo n ed $n+1$ numeri interi $a_0, a_1, \ldots, a_n$ tali che

$$a_n \neq 0, \qquad a_0 + a_1x + \cdots + a_nx^n = 0.$$

Ogni numero razionale $x = p/q$ è algebrico poiché è radice del polinomio $qx - p$. Il numero $\sqrt{2}$ è algebrico poiché è radice del polinomio $x^2 - 2$. L'unità immaginaria i è un numero algebrico poiché è radice del polinomio $x^2 + 1$.

Un numero che non è algebrico viene detto **trascendente**. È possibile dimostrare che esistono numeri reali trascendenti: valgono ad esempio i seguenti teoremi.

Teorema 10.2. *Il numero di Nepero e è trascendente.*

Teorema 10.3. *Il numero π è trascendente.*

Si può inoltre dimostrare che i numeri trascendenti sono "di più" dei numeri algebrici, nel senso indicato dal seguente teorema.

Teorema 10.4. *Siano $A \subset \mathbb{R}$ l'insieme dei numeri algebrici reali e $T \subset \mathbb{R}$ l'insieme dei numeri trascendenti reali (per definizione $\mathbb{R} = A \cup T$).*
*Allora esistono applicazioni iniettive $A \to T$, ma **non esiste** alcuna applicazione surgettiva $A \to T$.*

Le dimostrazioni dei Teoremi 10.2, 10.3 e 10.4 richiedono tecniche troppo avanzate per il corso di Algebra Lineare. Lo studente interessato potrà chiedere la dimostrazione della trascendenza di e al docente di Algebra 1 o Analisi 1 (I anno, II semestre) e la dimostrazione dei Teoremi 10.3 e 10.4 al docente del corso di Algebra 2 (II anno, II semestre). Se il docente si rifiuta potrete studiarvele da soli sul libro di G.H. Hardy e E.M. Wright *An introduction to the theory of numbers.*

In queste note utilizzeremo la teoria degli spazi vettoriali per dimostrare in maniera semplice ed elegante che i numeri algebrici formano un campo di numeri, ossia dimostreremo il

Teorema 10.5. *Siano $z, w \in \mathbb{C}$ due numeri algebrici. Allora $-z, z+w, zw$ sono algebrici e, se $z \neq 0$, allora z^{-1} è algebrico.*

Esercizio 10.6. Vero o falso? La somma di due numeri trascendenti è trascendente.

Esercizio 10.7. Vero o falso? L'inverso di un numero trascendente è trascendente.

Esercizio 10.8. Vero o falso? Il coniugato di un numero trascendente è trascendente.

Esercizio 10.9. È possibile dimostrare in maniera del tutto elementare che se $z \neq 0$ è algebrico, allora anche $-z$ e z^{-1} sono algebrici. Sapete dirmi come?

Dimostrazione del Teorema 10.5. Salvo avviso contrario, considereremo il campo dei numeri complessi $\mathbb{C}$ come uno spazio vettoriale su $\mathbb{Q}$.

Lemma 10.10. *Sia $U \subset \mathbb{C}$ un sottospazio vettoriale di dimensione finita su $\mathbb{Q}$. Se $1 \in U$ e $uv \in U$ per ogni $u, v \in U$, allora U è un campo ed ogni elemento di U è un numero algebrico.*

Dimostrazione. Per dimostrare che U è un campo basta dimostrare che che se $u \in U$, $u \neq 0$, allora $u^{-1} \in U$. Sia $e_1, \ldots, e_n \in U$ una base di U come spazio vettoriale su $\mathbb{Q}$; allora gli n vettori di U

$$ue_1, ue_2, ue_3, \ldots, ue_n$$

sono linearmente indipedenti e quindi una base. Infatti se fosse

$$a_1ue_1 + a_2ue_2 + a_3ue_3 + \cdots + a_nue_n = 0$$

si avrebbe

$$u(a_1e_1 + a_2e_2 + a_3e_3 + \cdots + a_ne_n) = 0.$$

Utilizzando l'ipotesi che $u \neq 0$

$$a_1e_1 + a_2e_2 + a_3e_3 + \cdots + a_ne_n = 0$$

e per la lineare indipendenza di $e_1, \ldots, e_n$ ne segue $a_0 = \cdots = a_{n-1} = 0$.
Dunque $ue_1, ue_2, ue_3, \ldots, ue_n$ generano U; in particolare esistono n numeri razionali $b_1, \ldots, b_n$ tali che

$$1 = b_1ue_1 + b_2ue_2 + \cdots + b_nue_n = u(b_1e_1 + b_2e_2 + \cdots + b_ne_n).$$

Dimostriamo adesso che ogni $z \in U$ è un numero algebrico. Se U ha dimensione n su $\mathbb{Q}$, allora gli $n+1$ vettori

$$1, z, z^2, \ldots, z^n$$

sono linearmente dipendenti. Esistono quindi $n+1$ numeri razionali $a_0, \ldots, a_n$ non tutti nulli a tali che

$$a_0 + a_1 z + a_2 z^2 + \cdots + a_n z^n = 0.$$

Moltiplicando per un denominatore comune non è restrittivo supporre $a_i \in \mathbb{Z}$ per ogni i e quindi z è radice di un polinomio non nullo a coefficienti interi di grado $\leq n$. □

Definiamo il **grado** di un numero algebrico $z \in \mathbb{C}$ come in più piccolo intero positivo n tale che z è radice di un polinomio di grado n a coefficienti interi. Ad esempio un numero algebrico è razionale se e solo se ha grado 1; i numeri algebrici i e $\sqrt{2}$ hanno grado 2.

Esercizio 10.11. Sia $z \in \mathbb{C}$ un numero algebrico di grado $n > 0$. Dimostrare che i numeri

$$1, z, z^2, \ldots, z^{n-1}$$

sono linearmente indipendenti su $\mathbb{Q}$.

Definizione 10.12. Sia $z \in \mathbb{C}$ un numero algebrico di grado n. Denotiamo con $\mathbb{Q}[z] \subset \mathbb{C}$ il sottospazio vettoriale

$$\mathbb{Q}[z] = L(1, z, \ldots, z^{n-1}) = \{a_0 + a_1 z + a_2 z^2 + \cdots + a_{n-1} z^{n-1} \mid a_0, \ldots, a_{n-1} \in \mathbb{Q}\}.$$

Se $w \in \mathbb{C}$ è un altro numero algebrico, di grado m, indichiamo $\mathbb{Q}[z, w] \subset \mathbb{C}$ il sottospazio vettoriale

$$\mathbb{Q}[z, w] = L(1, z, w, \ldots, z^i w^j, \ldots), \qquad 0 \leq i < n,\ 0 \leq j < m.$$

Notiamo che $\mathbb{Q}[z]$ e $\mathbb{Q}[z, w]$ sono finitamente generati e quindi di dimensione finita $\mathbb{Q}$.

Lemma 10.13. *Siano z, w numeri algebrici di gradi n, m rispettivamente, allora $\mathbb{Q}[z, w]$ è un campo.*

Dimostrazione. Sappiamo che $\mathbb{Q}[z, w]$ è un sottospazio vettoriale di $\mathbb{C}$ che contiene $\mathbb{Q}$ e di dimensione finita. Basta quindi dimostrare che se $u, v \in \mathbb{Q}[z, w]$ allora $uv \in \mathbb{Q}[z, w]$.
Dimostriamo come primo passo che $z^i w^j \in \mathbb{Q}[z, w]$ per ogni $i, j \geq 0$. Se $i < n$ e $j < m$ ciò è vero per definizione. Per induzione su $i + j$ basta dimostraee che se $i \geq n$ o $j \geq m$ possiamo scrivere $z^i w^j$ come combinazione lineare di monomi $z^a w^b$, con $a + b < i + j$. Supponiamo per fissare le idee che $i - n \geq j - m$; in caso contrario basterà ripetere il ragionamento con w al posto di z.
Siccome z ha grado n vale una relazione del tipo

$$b_0 + b_1 z + \cdots + b_n z^n = 0, \qquad b_n \neq 0,$$

e quindi per ogni $i \geq n$ ed ogni j vale

$$z^i w^j = z^n z^{i-n} w^j = \left(-\frac{b_0}{b_n} - \frac{b_1}{b_n} z - \cdots - \frac{b_{n-1}}{b_n} z^{n-1}\right) z^{i-n} w^j.$$

Se $u, v \in \mathbb{Q}[z]$, allora u, v sono entrambi combinazioni lineari a coefficienti razionali di $z^i w^j$ e quindi il prodotto u, v è una combinazione lineare di $z^i w^j$; per quanto visto $z^i w^j \in \mathbb{Q}[z, w]$ per ogni $i, j \geq 0$ e dunque uv è combinazione lineare di vettori del sottospazio $\mathbb{Q}[z, w]$. $\square$

La dimostrazione del Teorema 10.5 è del tutto chiara. Per i due lemmi precedenti, se z, w sono algebrici il sottospazio vettoriale $\mathbb{Q}[z, w]$ ha dimensione finita su $\mathbb{Q}$, è un campo di numeri ed ogni elemento di $\mathbb{Q}[z, w]$ è algebrico. In particolare sono algebrici i numeri

$$-z, z^{-1}, z + w, wz \in \mathbb{Q}[z, w].$$

Esercizio 10.14 ($*$). Possiamo generalizzare la definizione di $\mathbb{Q}[z, w]$ ad una successione finita di $z_1, \dots, z_n$ di numeri algebrici, ponendo $\mathbb{Q}[z_1, \dots, z_n]$ uguale al sottospazio vettoriale generato da tutti i monomi

$$z_1^{i_1} \cdots z_n^{i_n}, \qquad 0 \leq i_j < \text{grado di } z_j.$$

Si assuma che $z_i^2 \in \mathbb{Q}$ per ogni i e che $\mathbb{Q}[z_1, \dots, z_n]$ abbia dimensione 2^n su $\mathbb{Q}$. Dimostrare che se $u \in \mathbb{Q}[z_1, \dots, z_n]$ e $u^2 \in \mathbb{Q}$, allora u è un multiplo razionale di un monomio $z_1^{i_1} \cdots z_n^{i_n}$.

Nota: il risultato del precedente esercizio può risultare utile per dimostrare che le radici quadrate dei numeri primi sono linearmente indipendenti su $\mathbb{Q}$.

Esercizio 10.15 ($*$). Siano $\mathbb{K} \subset L \subset \mathbb{C}$ due sottocampi, con $\mathbb{K}$ di dimensione finita come spazio vettoriale su $\mathbb{Q}$ e L di dimensione finita come spazio vettoriale su $\mathbb{K}$. Dimostrare che L ha dimensione finita come spazio vettoriale su $\mathbb{Q}$ e vale la formula

$$\dim_{\mathbb{K}} L = \frac{\dim_{\mathbb{Q}} L}{\dim_{\mathbb{Q}} \mathbb{K}}.$$

Dedurre che ogni somma di radici quadrate di numeri razionali è un numero algebrico di grado uguale ad una potenza di 2.

11. Tutoraggio del 6 novembre 2006

Esercizio 11.1. Vero o falso? Se A è una matrice quadrata e $traccia(A) = 0$, allora $traccia(A^2) = 0$.

Esercizio 11.2. Si consideri l'applicazione lineare

$$F \colon M_{2,2}(\mathbb{K}) \to M_{2,2}(\mathbb{K})$$

data da

$$F(A) = \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix} A + A \begin{pmatrix} 0 & -1 \\ 2 & -1 \end{pmatrix}$$

e se ne calcoli il rango.

Esercizio 11.3. Vero o falso? Esiste una matrice 4×4 in cui la somma dei coefficienti di ogni singola riga è uguale a 2 e la somma dei coefficienti di ogni singola colonna è uguale a 1.

Esercizio 11.4. Nello spazio vettoriale $M_{4,4}(\mathbb{R})$ delle matrici 4×4 a coefficienti reali si consideri il sottoinsieme U delle matrici tali che la somma dei coefficienti di ogni singola riga e di ogni singola colonna è uguale a 0. Dimostrare che U è un sottospazio vettoriale e se ne calcoli la dimensione.

Esercizio 11.5. Provare che se $A \in M_{n,n}(\mathbb{K})$ è antisimmetrica, allora A^2 è simmetrica. Trovare due matrici antisimmetriche A, B tali che

$$A - A^2 = \begin{pmatrix} 4 & 2 \\ -2 & 4 \end{pmatrix}, \qquad B - B^2 = \begin{pmatrix} 2 & 2 & 0 \\ 0 & 2 & 2 \\ -2 & 0 & 2 \end{pmatrix}$$

Dimostrare poi che non esiste alcuna matrice antisimmetrica C tale che $C - C^2 = I$.
(Sugg.: per semplificare i conti, può essere utile ricordare che ogni matrice quadrata si scrive in modo unico come somma di una matrice simmetrica e di una antisimmetrica.)

Esercizio 11.6. Una matrice $M \in M_{n,n}(\mathbb{R})$ è detta *Markoviana* se ogni suo coefficiente è maggiore od uguale a 0 e se la somma dei coefficienti di ogni colonna è uguale a 1. Dimostrare che il prodotto di due matrici Markoviane è ancora una matrice Markoviana. Mostrare inoltre che, se $n > 1$, allora le matrici Markoviane sono contenute in un sottospazio vettoriale proprio di $M_{n,n}(\mathbb{R})$.

Esercizio 11.7. Sia A una matrice $m \times k$ e B una matrice $k \times m$. Si supponga che $k < m$. Si dimostri che la matrice AB non è invertibile.

Esercizio 11.8. Dimostrare che ogni matrice $A \in M_{m,n}(\mathbb{K})$, di rango k, può scriversi nella forma $A = BC$ dove B è una matrice $m \times k$ e C è una matrice $k \times n$.

Esercizio 11.9. Sia V lo spazio vettoriale dei polinomi a coefficienti reali di grado $\leq 2n$. Siano $c_1, \ldots, c_n$ numeri reali tali che $c_i^2 \neq c_j^2$ per $i \neq j$. Dimostrare che se $p(c_i) = p(-c_i)$ per $i = 1, \ldots, n$ allora $p(x) = p(-x)$, per ogni $x \in \mathbb{R}$.

Esercizio 11.10. Sia V uno spazio vettoriale di dimensione finita. Siano F e G due applicazioni lineari di V in V. Si dimostri che

$$rg(GF) = rg(F) - \dim\left(F(V) \cap Ker(G)\right)$$
$$\dim Ker(GF) = \dim Ker(F) + \dim\left(F(V) \cap Ker(G)\right).$$

Esercizio 11.11. Sia V uno spazio vettoriale di dimensione finita. Siano F e G due applicazioni lineari di V in V. Si assuma che

$$V = Im(F) \oplus Im(G) = Ker(F) \oplus Ker(G).$$

Si dimostri che $rg(G + F) = rg(G) + rg(F)$.

Esercizio 11.12. Sia $\mathbb{K} = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Mostrare che ogni elemento $\alpha \in \mathbb{K}$ può scriversi in modo unico come

$$\alpha = (a + b\sqrt{2}) + \sqrt{3}(c + d\sqrt{2}), \quad a, b, c, d \in \mathbb{Q}$$

Sia $\tau : \mathbb{K} \to \mathbb{K}$ definita da

$$\tau(\alpha) = (a + b\sqrt{2}) - \sqrt{3}(c + d\sqrt{2}).$$

a) Dimostrare che τ è $\mathbb{Q}$-lineare.
b) Dimostrare che $\tau(\alpha\beta) = \tau(\alpha)\tau(\beta)$.
c) Dimostrare che se $\sqrt{5} \in \mathbb{K}$, allora $\tau(\sqrt{5}) = \pm\sqrt{5}$. Trarne un assurdo.

12. Esonero del 13 novembre 2006

Esercizio 12.1. Per quali valori di $t \in \mathbb{R}$ i tre vettori

$$v_1 = \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix}, \quad v_2 = \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix}, \quad v_3 = \begin{pmatrix} 2 \\ 2 \\ t \end{pmatrix} \in \mathbb{R}^3$$

sono linearmente dipendenti?

Soluzione 1. I vettori v_1, v_2 e v_3 sono dipendenti se e solo se esistono tre numeri reali a, b, c non tutti nulli, tali che $av_1 + bv_2 + cv_3$ è il vettore nullo in $\mathbb{R}^3$; quindi, se e solo se esistono $(a, b, c) \neq (0, 0, 0)$ tali che

$$\begin{cases} a + 3b + 2c = 0 \\ 2a + 2b + 2c = 0 \\ a + b + tc = 0 \end{cases}$$

Questo sistema è equivalente al sistema

$$\begin{cases} a = b \\ c = -2a \\ (1 - t)c = 0 \end{cases}$$

che ha soluzioni non banali se e solo se $t = 1$.

Quindi v_1, v_2, v_3 sono linearmente dipendenti se e solo se $t = 1$.

Esercizio 12.2. Calcolare il prodotto di matrici

$$\begin{pmatrix} 1 & 2 & 3 \\ -2 & 0 & 5 \\ -3 & -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -2 & 1 \\ 0 & 2 \end{pmatrix}$$

e determinarne il rango.

Soluzione 2.

$$\begin{pmatrix} 1 & 2 & 3 \\ -2 & 0 & 5 \\ -3 & -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -2 & 1 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} -3 & 8 \\ -2 & 10 \\ -1 & -1 \end{pmatrix}.$$

Il rango di questa matrice è il numero di colonne indipendenti. Le due colonne

$$\begin{pmatrix} -3 \\ -2 \\ -1 \end{pmatrix} \quad \begin{pmatrix} 8 \\ 10 \\ -1 \end{pmatrix}$$

sono vettori indipendenti, poiché non sono proporzionali. Quindi il rango della matrice è 2.

Esercizio 12.3. Sia $V \subseteq M_{2,2}(\mathbb{R})$ il sottospazio vettoriale formato dalle matrici A tali che

$$A \begin{pmatrix} 1 & -1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 1 & 2 \end{pmatrix} A.$$

Determinare una base di V.

Soluzione 3. Sia

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2,2}(\mathbb{R}).$$

La condizione affinché A appartenga a V è quindi

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

cioè

$$\begin{pmatrix} a+b & -a+2b \\ c+d & -c+2d \end{pmatrix} = \begin{pmatrix} a-c & b-d \\ a+2c & b+2d \end{pmatrix}.$$

Le condizioni sui coefficienti di A sono quindi date da questo sistema

$$\begin{cases} a+b = a-c \\ -a+2b = b-d \\ c+d = a+2c \\ -c+2d = b+2d \end{cases}$$

che è equivalente a

$$\begin{cases} b+c = 0 \\ a-b-d = 0 \end{cases}$$

Quindi

$$V = \left\{ \begin{pmatrix} b+d & b \\ -b & d \end{pmatrix} \ b,d \in \mathbb{R} \right\} = \left\{ d \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} \ b,d \in \mathbb{R} \right\}$$

In altre parole, V è il sottospazio di $M_{2,2}(\mathbb{R})$ generato dalle matrici:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$$

Queste matrici sono indipendenti in $M_{2,2}(\mathbb{R})$ (perché non sono proporzionali), quindi sono una base per V.

Esercizio 12.4. Si consideri l'applicazione lineare

$$F\colon \mathbb{R}^4 \to \mathbb{R}^3$$

definita in coordinate da

$$F(x,y,z,w) = (x-y-w, y-z, z-x+w).$$

Descrivere la matrice A tale che $F = L_A$, determinare una base del nucleo di F ed una base dell'immagine di F.

Soluzione 4. La matrice A associata ad F, cioè tale che

$$F(x,y,z,w) = A \begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix},$$

è

$$A = \begin{pmatrix} 1 & -1 & 0 & -1 \\ 0 & 1 & -1 & 0 \\ -1 & 0 & 1 & 1 \end{pmatrix}.$$

Il nucleo di F è descritto dall equazioni

$$\begin{cases} x-y-w = 0 \\ y-z = 0 \\ z-x+w = 0 \end{cases}$$

Quindi ha equazioni parametriche

$$\begin{cases} x = \alpha \\ y = \beta \\ z = \beta \\ w = \beta - \alpha \end{cases} \quad \alpha, \beta \in \mathbb{R}.$$

Una base è dunque data, per esempio, dai vettori $\{(1, 0, 0, -1), (0, 1, 1, 1)\}$.

Poiché il nucleo, come abbiamo appena verificato, ha dimensione 2, per il teorema delle dimensioni il rango di F è $\dim(\mathbb{R}^4) - 2 = 2$. Dunque l'immagine $F(\mathbb{R}^4)$ ha dimensione 2. Inoltre, l'immagine è generata dai vettori colonna di A. Quindi, per trovare una base, è sufficiente trovare due vettori colonna di A indipendenti. Prendo, ad esempio, il primo e il secondo:

$$\{(1, 0, -1), (-1, 1, 0)\}$$

è una base per l'immagine.

Esercizio 12.5. Sia V lo spazio vettoriale dei polinomi di grado ≤ 3 a coefficienti reali e sia $F: V \to V$ l'applicazione lineare

$$F(p(x)) = p(x + 2).$$

Descrivere la matrice associata a tale trasformazione nella base $1, x, x^2, x^3$.

Soluzione 5. La matrice associata ad F nella base data, ha come vettori colonna i vettori delle coordinate delle immagini dei vettori della base. Devo dunque scrivere le coordinate di $F(1)$, $F(x)$, $F(x^2)$, $F(x^3)$ rispetto alla base $1, x, x^2, x^3$.

$F(1) = 1$ ha coordinate $(1, 0, 0, 0)$;

$F(x) = 2 + x$ ha coordinate $(2, 1, 0, 0)$;

$F(x^2) = (x + 2)^2 = 4 + 4x + x^2$ ha coordinate $(4, 4, 1, 0)$;

$F(x^3) = (x + 2)^3 = 8 + 12x + 6x^2 + x^3$ ha coordinate $(8, 12, 6, 1)$.

Quindi la matrice associata ad F è

$$\begin{pmatrix} 1 & 2 & 4 & 8 \\ 0 & 1 & 4 & 12 \\ 0 & 0 & 1 & 6 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Esercizio 12.6. Dimostrare che ogni matrice 4×4 di rango 3 si può scrivere come somma di tre matrici 4×4 di rango 1.

Soluzione 6. Sia A una matrice 4×4 di rango 3. Chiamiamo A^i l'i-esimo vettore colonna di A. Poiché il rango è il numero di vettori colonna linearmente indipendenti, ci sarà un vettore colonna di A che è combinazione lineare degli altri 3. Supponiamo, per fissare le idee, che sia il primo vettore colonna A^1. Allora, esistono $\alpha, \beta, \gamma \in \mathbb{R}$ tali che $A^1 = \alpha A^2 + \beta A^3 + \gamma A^4$. Inoltre, siccome il rango di A è 3, i vettori A^2, A^3, A^4 sono indipendenti in $\mathbb{R}^4$; quindi, in particolare non sono il vettore nullo.

Consideriamo le matrici 4×4

$$B = \left(\alpha A^2, A^2, O, O\right), \; C = \left(\beta A^3, O, A^3, O\right), \; D = \left(\gamma A^4, O, O, A^4\right),$$

dove O denota il vettore colonna nullo $\in \mathbb{R}^4$. Allora,

$$A = \left(\alpha A^2 + \beta A^3 + \gamma A^4, A^2, A^3, A^4\right) = B + C + D.$$

Siccome A^2, A^3 e A^4 non sono il vettore nullo, $\operatorname{rank} B = \operatorname{rank} C = \operatorname{rank} D = 1$.

13. Permutazioni ed incroci

Per ogni intero positivo n, indichiamo con Σ_n l'insieme delle **permutazioni** su n elementi, ossia l'insisme di tutte le applicazioni *bigettive*

$$\sigma\colon \{1, \dots, n\} \to \{1, \dots, n\}.$$

Un modo conveniente di rappresentare una permutazione su n elementi è mediante una matrice $2 \times n$ in cui la prima riga contiene i numeri da 1 a n e la seconda riga le rispettive immagini, ossia

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

Le **trasposizioni** sono permutazioni che scambiano di posizione due elementi e lasciano invariati i rimanenti. Ad esempio, la permutazione

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

è una trasposizione. Per ogni $i < n$, denotiamo con $\tau_i \in \Sigma_n$ la trasposizione che scambia i con $i+1$:

$$\tau_i(i) = i+1, \qquad \tau_i(i+1) = i, \qquad \tau_i(a) = a \quad \forall\, a \neq i, i+1.$$

Diremo che un sottoinsieme $A \subset \{1, \dots, n\}$ di **due** elementi è un **incrocio** della permutazione σ se la restrizione di σ ad A è decrescente; in altri termini, un sottoinsieme

$$A = \{i, j\}, \quad \text{con} \quad i < j,$$

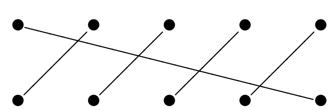
è un incrocio di σ se $\sigma(i) > \sigma(j)$. Indichiamo con $\delta(\sigma)$ il numero di incroci di σ. Ad esempio, l'identità ha zero incroci, le trasposizioni τ_i hanno un solo incrocio, mentre la permutazione

$$\sigma(i) = n + 1 - i$$

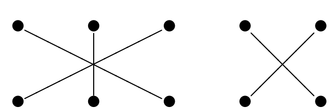
ha $n(n-1)/2$ incroci. In un certo senso, il numero di incroci è una misura della complessità della permutazione.

Osservazione 13.1. Una maniera di contare il numero di incroci di σ è la seguente. Per ogni $i = 1, \dots, n$ si disegna nel piano il segmento che unisce il punto di coordinate $(i, 0)$ con il punto di coordinate $(\sigma(i), 1)$ e poi si conta il numero di punti di intersezione dei vari segmenti. Bisogna però fare attenzione al fatto che, se per un punto passano h segmenti, con $h > 2$, allora ci troviamo di fronte ad una intersezione multipla ed a tale punto corrispondono $h(h-1)/2$ incroci. Ad esempio, le due permutazioni

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$$



$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$$



hanno entrambe 4 incroci.

Definizione 13.2. La **segnatura** $\varepsilon(\sigma) = \pm 1$ di una permutazione σ è definita dalla formula

$$\varepsilon(\sigma) = (-1)^{\delta(\sigma)}.$$

Esempio 13.3. Siano $i < j$ e sia σ la trasposizione che scambia i e j. Un sottoinsieme

$$A = \{a, b\}, \quad \text{con} \quad a < b,$$

è un incrocio se e solo se $a = i$ e $b \leq j$, oppure se $a \geq i$ e $b = j$; quindi $\delta(\sigma) = 2(j - i) - 1$.
Ne consegue che ogni trasposizione ha segnatura uguale a -1.

Esercizio 13.4. Siano $r < n$ e $\sigma \in \Sigma_n$ la permutazione

$$\sigma(i) = \begin{cases} i + r & \text{se } i \leq n - r \\ i - (n - r) & \text{se } i > n - r \end{cases}$$

Calcolare la segnatura di σ.

Le permutazioni, in quanto applicazioni di un insieme in sé, possono essere composte tra loro. Se $\sigma, \eta \in \Sigma_n$ definiamo il prodotto $\sigma\eta \in \Sigma_n$ come

$$\sigma\eta(i) = \sigma(\eta(i)), \qquad i = 1, \ldots, n.$$

Ad esempio

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

Notiamo che il prodotto di ogni trasposizione con sé stessa è uguale all'identità; in particolare $\tau_i\tau_i =$ identità per ogni i.

Teorema 13.5. *Date due permutazioni $\sigma, \eta \in \Sigma_n$, indichiamo con a il numero di sottoinsiemi $A \subseteq \{1, \ldots, n\}$ di due elementi che soddisfano le due condizioni:*

(1) *A è un incrocio di η.*
(2) *$\eta(A)$ è un incrocio di σ.*

Allora vale la formula

$$\delta(\sigma\eta) = \delta(\sigma) + \delta(\eta) - 2a$$

Dimostrazione. Per ogni insieme finito X indichiamo con $|X|$ la sua cardinalità, ossia il numero di elementi che contiene. Indichiamo con $\mathcal{P}$ la collezione di tutti i sottoinsiemi di $\{1, \ldots, n\}$ di cardinalità 2.
Notiamo che $A \in \mathcal{P}$ è un incrocio di $\sigma\eta$ se e soltanto se vale una delle seguenti due condizioni:

(1) A è un incrocio di η e $\eta(A)$ non è un incrocio di σ.
(2) A non è un incrocio di η e $\eta(A)$ è un incrocio di σ.

Indichiamo adesso con

$$\mathcal{C} = \{A \in \mathcal{P} \ : \ A \text{ è incrocio di } \eta\}.$$

$$\mathcal{D} = \{A \in \mathcal{P} \ : \ \eta(A) \text{ è incrocio di } \sigma\}.$$

Chiaramente $|\mathcal{C}| = \delta(\eta)$ e, siccome $\eta \colon \mathcal{P} \to \mathcal{P}$ è bigettiva, vale anche $|\mathcal{D}| = \delta(\sigma)$. Per definizione a è il numero di elementi di $\mathcal{C} \cap \mathcal{D}$. Denotiamo con c il numero di elementi di $\mathcal{C}$ che non appartengono a $\mathcal{D}$ e con d il numero di elementi di $\mathcal{D}$ che

non appartengono a $\mathcal{C}$.
Abbiamo visto che valgono le uguaglianze

$$a + c = \delta(\eta), \qquad a + d = \delta(\sigma), \qquad c + d = \delta(\sigma\eta).$$

Da tali uguaglianze segue che

$$\delta(\sigma\eta) = \delta(\sigma) + \delta(\eta) - 2a.$$

□

COROLLARIO 13.6. *La segnatura del prodotto è uguale al prodotto delle segnature, cioè, per ogni $\sigma, \eta \in \Sigma_n$ vale*

$$\varepsilon(\sigma\eta) = \varepsilon(\sigma)\varepsilon(\eta).$$

In particolare $\varepsilon(\sigma) = \varepsilon(\sigma^{-1})$.

DIMOSTRAZIONE. La prima uguaglianza segue immediatamente dal Teorema 13.5. Per la seconda basta osservare che

$$\varepsilon(\sigma)\varepsilon(\sigma^{-1}) = \varepsilon(\sigma\sigma^{-1}) = \varepsilon(\text{identità}) = 1.$$

□

COROLLARIO 13.7. *Se una permutazione σ è uguale al prodotto di k trasposizioni, allora $\varepsilon(\sigma) = (-1)^k$.*

DIMOSTRAZIONE. Ogni trasposizione ha segnatura -1. □

COROLLARIO 13.8. *Ogni permutazione σ si può scrivere come prodotto di $\delta(\sigma)$ trasposizioni τ_i.*

DIMOSTRAZIONE. Induzione su $\delta(\sigma)$. Se σ non ha incroci, allora σ è l'identità. Se invece σ è diversa dall'identità, allora l'applicazione bigettiva

$$\sigma\colon \{1, \dots, n\} \to \{1, \dots, n\}$$

non può essere crescente e dunque esiste almeno un indice $h < n$ tale che $\sigma(h) > \sigma(h + 1)$. Dimostriamo adesso che

$$\delta(\sigma\tau_h) = \delta(\sigma) - 1.$$

Infatti la trasposizione τ_h ha un unico incrocio $\{h, h+1\}$ che, per come abbiamo scelto h, è anche un incrocio di σ. Quindi per il Teorema 13.5

$$\delta(\sigma\tau_h) = \delta(\sigma) + \delta(\tau_h) - 2 = \delta(\sigma) - 1.$$

Per l'ipotesi induttiva la permutazione $\sigma\tau_h$ è prodotto di $\delta(\sigma) - 1$ trasposizioni τ_i e quindi

$$\sigma = \sigma(\tau_h\tau_h) = (\sigma\tau_h)\tau_h$$

è prodotto di $\delta(\sigma)$ trasposizioni τ_i. □

Supponiamo adesso di avere un insieme finito X e di considerare una permutazione di X, ossia un'applicazione bigettiva $f\colon X \to X$. In questo caso non possiamo definire il numero di incroci (per fare ciò bisognerebbe che X fosse ordinato) ma possiamo ugualmente definire la segnatura nel modo seguente:

Supponiamo che X abbia esattamente n elementi e scegliamo un'applicazione bigettiva

$$h\colon \{1, \dots, n\} \to X.$$

Allora l'applicazione

$$h^{-1}fh\colon \{1,\ldots,n\} \to \{1,\ldots,n\}$$

è bigettiva e possiamo definire

$$\varepsilon(f) = \varepsilon(h^{-1}fh).$$

Bisogna dimostrare che si tratta di una **buona definizione**, ossia che $\varepsilon(f)$ non dipende dalla scelta di h. Se prendiamo un'altra applicazione bigettiva

$$k\colon \{1,\ldots,n\} \to X,$$

allora $\sigma = k^{-1}h$ è una permutazione di $\{1,\ldots,n\}$ con inversa $\sigma^{-1} = h^{-1}k$ e quindi

$$\varepsilon(h^{-1}fh) = \varepsilon(\sigma^{-1}k^{-1}fk\sigma) = \varepsilon(\sigma^{-1})\varepsilon(k^{-1}fk)\varepsilon(\sigma) = \varepsilon(k^{-1}fk).$$

14. Permutazioni e cicli

Una *permutazione su n elementi* è una applicazione biunivoca

$$\sigma : \{1,2,3,4,\ldots,n-1,n\} \longrightarrow \{1,2,3,4,\ldots,n-1,n\}$$

L'insieme delle permutazioni su n elementi si denota con il simbolo $\mathfrak{S}_n$. Ovviamente $\mathfrak{S}_n$ è un insieme finito. La sua cardinalità è:

$$|\mathfrak{S}_n| = n!\,.$$

Le permutazioni, in quanto applicazioni si possono comporre. Date due permutazioni σ e τ si denota con il simbolo $\sigma\tau$ la permutazione τ composta con la permutazione σ. Ogni permutazione σ, in quanto applicazione biunivoca, ammette un'inversa σ^{-1}. Spesso, per denotare una permutazione, si usa il simbolo

$$\begin{pmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \ldots & \sigma(n-1) & \sigma(n) \end{pmatrix}$$

Per esempio, una permutazione σ su 10 elementi è la seguente

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 4 & 5 & 6 & 9 & 2 & 8 & 7 & 1 & 10 \end{pmatrix}$$

Si ha cioè $\sigma(1) = 3, \sigma(2) = 4, \sigma(3) = 5$ e così via. Si dice anche che la permutazione σ porta 1 in 3, 2 in 4, 3 in 5, e così via. A volte si tralascia di scrivere gli elementi lasciati fissi da una permutazione. In questo caso la (1) si scrive:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 5 & 6 & 9 & 2 & 8 & 7 & 1 \end{pmatrix}$$

Una permutazione del tipo

$$\sigma = \begin{pmatrix} a & b \\ b & a \end{pmatrix}$$

si dice una *trasposizione.* Insomma una trasposizione è una permutazione che lascia fissi tutti i numeri $1,\ldots,n$, tranne a e b che invece si scambiano tra loro. È utile impratichirsi con le notazioni. Per esempio, consideriamo le due trasposizioni $\sigma, \tau \in \mathfrak{S}_3$ definite da

$$\sigma = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, \qquad \tau = \begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix}.$$

Calcoliamo la composizione $\sigma\tau$. Secondo la nostra notazione abbiamo:

$$\sigma\tau(1) = \sigma(1) = 2\,, \sigma\tau(2) = \sigma(3) = 3\,, \sigma\tau(3) = \sigma(2) = 1$$

Dunque:

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

È istruttivo osservare che $\sigma\tau \neq \tau\sigma$. In effetti:

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Naturalmente esistono casi in cui due permutazioni commutano. Per esempio, questo avviene quando i due insiemi di numeri coinvolti nelle due permutazioni sono disgiunti. Per esempio, se $\sigma, \tau \in \mathfrak{S}_7$ sono definite da:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}, \qquad \tau = \begin{pmatrix} 6 & 7 \\ 7 & 6 \end{pmatrix}.$$

si ha $\sigma\tau = \tau\sigma$.

Lemma 14.1. *Ogni permutazione in $\mathfrak{S}_n$ può esprimere come prodotto di trasposizioni.*

Dimostrazione. Procediamo per induzione su n. Il caso $n = 1$ è banale. Assumiamo di aver dimostrato il teorema per $\mathfrak{S}_{n-1}$. Sia $\sigma \in \mathfrak{S}_n$. Si supponga che $\sigma(h) = n$. Sia τ la traspsizione definita da

$$\tau = \begin{pmatrix} n & h \\ h & n \end{pmatrix}.$$

Allora $\sigma\tau(n) = n$. Quindi si può considerare $\sigma\tau$ come una permutazione in $\mathfrak{S}_{n-1}$, dove la decomposizione in prodotto di trasposizioni è vera per induzione. □

Esempio 14.2.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 5 & 6 & 7 & 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 4 & 7 \\ 7 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & \\ 4 & 5 & 6 & 2 & 1 & 3 & \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & \\ 4 & 5 & 6 & 2 & 1 & 3 & \end{pmatrix}\begin{pmatrix} 3 & 6 \\ 6 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 4 & 5 & \\ 4 & 5 & 2 & 1 & \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 4 & 5 & \\ 4 & 5 & 2 & 1 & \end{pmatrix}\begin{pmatrix} 2 & 5 \\ 5 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 4 \\ 4 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 4 \\ 4 & 1 \end{pmatrix}$$

Dunque

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 5 & 6 & 7 & 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 4 \\ 4 & 1 \end{pmatrix}\begin{pmatrix} 2 & 5 \\ 5 & 2 \end{pmatrix}\begin{pmatrix} 3 & 6 \\ 6 & 3 \end{pmatrix}\begin{pmatrix} 4 & 7 \\ 7 & 4 \end{pmatrix}$$

Una *permutazione ciclica,* o più semplicemente un *ciclo*, è una permutazione del tipo

$$\begin{pmatrix} k_1 & k_2 & k_3 & \dots & k_{s-1} & k_s \\ k_2 & k_3 & k_4 & \dots & k_s & k_1 \end{pmatrix}$$

Per esempio di ciclo è il seguente:

$$\begin{pmatrix} 4 & 5 & 6 & 10 & 9 \\ 5 & 6 & 10 & 9 & 4 \end{pmatrix}$$

Due cicli

$$\begin{pmatrix} k_1 & k_2 & k_3 & \dots & k_{s-1} & k_s \\ k_2 & k_3 & k_4 & \dots & k_s & k_1 \end{pmatrix}, \begin{pmatrix} h_1 & h_2 & h_3 & \dots & h_{t-1} & h_t \\ h_2 & h_3 & k_h & \dots & k_{teo} & h_1 \end{pmatrix}$$

si dicono *disgiunti* se

$$\{k_1, k_2, k_3, \dots, k_{s-1}, k_s\} \cap \{h_1, h_2, h_3, \dots, h_{t-1}, h_t\} = \emptyset$$

TEOREMA 14.3. *Ogni permutazione si può esprimere in modo unico come un prodotto di cicli disgiunti.*

Prima di dimostrare il teorema decomponiamo la (1) in prodotto di cicli disgiunti. È molto semplice. Incominciamo da 1 e "seguiamolo". Si ha che 1 va in 3, 3 va in 5, 5 va in 9, 9 va in 1 e abbiamo chiuso il primo ciclo. Ora torniamo indietro e vediamo il primo numero che non sta nella lista precedente. È il numero 2. Seguiamolo: 2 va in 4, 4 va in 6, 6 va in 2, e abbiamo chiuso il secondo ciclo. Il primo numero tra quelli non presi ancora in considerazione è 8. Seguiamolo (per poco) perché 8 va in 7 e 7 va in 8 e anche questo ciclo è chiuso. L'ultimo ciclo è quello banale: 10 va in 10. Dunque abbiamo

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 4 & 5 & 6 & 9 & 2 & 8 & 7 & 1 & 10 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 5 & 9 \\ 3 & 5 & 9 & 1 \end{pmatrix} \begin{pmatrix} 2 & 4 & 6 \\ 4 & 6 & 2 \end{pmatrix} \begin{pmatrix} 7 & 8 \\ 8 & 7 \end{pmatrix} \begin{pmatrix} 10 \\ 10 \end{pmatrix}$$

La dimostrazione del Teorema 14.3 è modellata su questo esempio.
Premettiamo alcuni risultati.

LEMMA 14.4. *Sia $\sigma \in \mathfrak{S}_n$ e $h \in \{1, \dots, n\}$. Allora esiste un intero positivo s tale che $\sigma^s(h) = h$.*

DIMOSTRAZIONE. I numeri $\sigma^i(h)$ non possono essere tutti distinti per $i = 1, 2, 3, 4, 5, \dots$, semplicemente per il fatto che ogni $\sigma^i(h) \in \{1, \dots, n\}$. Dunque esistono due indici diversi, i e j, con $i > j$, tali che $\sigma^i(h) = \sigma^j(h)$. Ma allora, se $s = i - j$, si ha $\sigma^s(h) = h$. □

Per ogni h esisterà un *minimo numero intero*, positivo, ν_h tale che $\sigma^{\nu_h}(h) = h$.

COROLLARIO 14.5. *Sia $\sigma \in \mathfrak{S}_n$. Allora esiste un intero positivo k tale che $\sigma^k = id$.*

DIMOSTRAZIONE. Basta prendere $k = \nu_1 \cdots \nu_n$. □

Naturalmente esiste un *minimo numero intero*, positivo, d tale che $\sigma^d = 1$.

COROLLARIO 14.6. *L'insieme $\{\sigma^i(h)\}_{i\in\mathbb{Z}}$ coincide con l'insieme $\{h, \sigma(h), \dots, \sigma^{\nu_h-1}(h)\}$*

Dimostrazione. Poiché $\sigma^d = 1$, si ha $\sigma^{-1} = \sigma^{d-1}$. Sia m un intero positivo, allora $\sigma^{-m} = \sigma^{m(d-1)}$. Dunque dobbiamo solo far vedere che, se $N \geq 0$, allora

$$\sigma^N(h) \in \{h, \sigma(h), \dots, \sigma^{\nu_h - 1}(h)\}\,.$$

Si scriva $N = l\nu_h + r$, con $0 \leq r \leq \nu_h - 1$. Allora $\sigma^N(h) = \sigma^r(\sigma^{l\nu_h}(h)) = \sigma^r(h)$. □

L'insieme

$$\{h, \sigma(h), \dots, \sigma^{\nu_h - 1}(h)\}$$

si chiama *l'orbita di h secondo σ.*

Corollario 14.7. *Per ogni intero s l'orbita di h coincide con quella di $\sigma^s(h)$.*

Dimostrazione. Si ha $\{\sigma^i(h)\}_{i\in\mathbb{Z}} = \{\sigma^{s+i}(h)\}_{i\in\mathbb{Z}}$ e l'asserto segue dal Corollario precedente. □

Corollario 14.8. *Due orbite di σ o coincidono o sono disgiunte.*

Dimostrazione. Siano $h, k \in \{1, \dots, n\}$. Dire che l'orbita di h e di k non sono disgiunte vuol dire che $\sigma^s(h) = \sigma^t(k)$, per un qualche s e un qualche t. La conclusione segue dal Corollario 14.7. □

Dal momento che ogni $h \in \{1, \dots, n\}$ sta nella propria orbita, si ha che

Corollario 14.9. *L'insieme $\{1, \dots, n\}$ è unione disgiunta delle orbite di σ*

Dimostrazione. Dimostrazione del Teorema 14.3 Siano

$$\begin{aligned}
&\{h_1, \sigma(h_1), \dots, \sigma^{\nu_{h_1}-1}(h_1)\}\\
&\{h_2, \sigma(h_2), \dots, \sigma^{\nu_{h_2}-1}(h_2)\}\\
&\dots\\
&\{h_s, \sigma(h_s), \dots, \sigma^{\nu_{h_s}-1}(h_s)\}
\end{aligned}$$

le orbite di σ. Allora σ è la composizione dei cicli disgiunti

$$\begin{aligned}
&\begin{pmatrix} h_1 & \sigma(h_1) & \dots & \sigma^{\nu_{h_1}-1}(h_1) \\ \sigma(h_1) & \sigma^2(h_1) & \dots & h_1 \end{pmatrix}\\
&\begin{pmatrix} h_2 & \sigma(h_2) & \dots & \sigma^{\nu_{h_2}-1}(h) \\ \sigma(h_2) & \sigma^2(h_2) & \dots & h_2 \end{pmatrix}\\
&\dots\\
&\begin{pmatrix} h_s & \sigma(h_s) & \dots & \sigma^{\nu_{h_s}-1}(h_s) \\ \sigma(h_s) & \sigma^2(h_s) & \dots & h_s \end{pmatrix}
\end{aligned}$$

□

Definizione 14.10. Sia $\sigma \in \mathfrak{S}_n$. Sia s il numero dei cicli di σ. Si defisce il segno $\epsilon(\sigma)$ di σ ponendo $\epsilon(\sigma) = (-1)^{n-s}$.

Chiaramente se τ è una trasposizione si ha $\epsilon(\tau) = -1$

Teorema 14.11. *Sia $\sigma \in \mathfrak{S}_n$ e sia τ è una trasposizione, allora $\epsilon(\sigma\tau) = -\epsilon(\sigma)$.*

Dimostrazione. Dimostreremo che se i cicli di σ sono in numero di s, allora quelli di $\sigma\tau$ sono in numero di $s-1$ oppure di $s+1$. Questo ovviamente basta. Possiamo supporre che τ è la trasposizione che scambia 1 e 2. Ci sono due casi da considerare. (Si guardi prima l'esempio di sotto). Il primo caso è quello in cui 1 e 2 appartengono alla stessa orbita. Scriviamo quest'orbita

$$\{1,\ \sigma(1),\ \dots,\ \sigma^{t-1}(1),\ \sigma^t(1)=2,\ \sigma^{t+1}(1),\ \dots,\ \sigma^{\nu_1-1}(1)\}$$

Dal momento che $\sigma\tau(h)=\sigma(h)$ per $h\neq 1$ e $h\neq 2$, le orbite di $\sigma\tau$ che non contengono 1 e 2 coincidono con quelle di σ che non contengono 1 e 2. Invece la $\sigma\tau$-orbita di 1 si spezza in due orbite:

$$\{1,\ \sigma\tau(1)=\sigma(2)=\sigma^{t+1}(1),\ \dots,\ \sigma^{\nu_1-1}(1)\}\,,\qquad \{\sigma\tau(2)=\sigma(1),\ \dots,\sigma^{t-1}(1)\}\,.$$

Il secondo caso è quello in cui 1 e 2 appartengono a orbite diverse:

$$\{k,\sigma(k),\sigma^2(k),\dots,\sigma^s(k)=1,\dots,\sigma^{\nu_k-1}(k)\}\,,$$
$$\{h,\sigma(h),\sigma^2(h),\dots,\sigma^t(h)=2,\dots,\sigma^{\nu_h-1}(h)\}$$

Come prima, le orbite di $\sigma\tau$ che non contengono 1 e 2 coincidono con quelle di σ che non contengono 1 e 2. Mentre le due orbite di σ che contengono 1 e 2 si fondono, in $\sigma\tau$, in un'unica orbita:

$$\{k,\sigma(k),\sigma^2(k),\dots,(\sigma)^s(k)=1,(\sigma\tau)(1)=\sigma(2),\dots,\sigma^{\nu_l-1}(h)\,,$$
$$h,\sigma(h),\sigma^2(h),\dots,\sigma^t(h)=2,\sigma\tau(2)=\sigma(1),\dots,\sigma^{\nu_k-1}(k)\}\,.$$

□

Esempio 14.12.

I^o **caso:**

$$\sigma=\begin{pmatrix}1&2&3&4&5&6&7&8&9&10\\2&7&5&6&10&9&8&1&4&3\end{pmatrix}\,,\qquad \tau=\begin{pmatrix}1&2\\2&1\end{pmatrix}$$

Cicli di σ:

$$\begin{pmatrix}1&2&7&8\\2&7&8&1\end{pmatrix}\,,\quad\begin{pmatrix}3&5&10\\5&10&3\end{pmatrix}\,,\quad\begin{pmatrix}4&6&9\\6&9&4\end{pmatrix}$$

Dunque 1 e 2 appartengono a una stessa orbita di σ.
Cicli di $\sigma\tau$:

$$\begin{pmatrix}1&7&8\\7&8&1\end{pmatrix}\,,\quad\begin{pmatrix}1&2\\2&1\end{pmatrix}\,,\quad\begin{pmatrix}3&5&10\\5&10&3\end{pmatrix}\,,\quad\begin{pmatrix}4&6&9\\6&9&4\end{pmatrix}$$

Dunque, in questo caso, nel passare da σ a $\sigma\tau$, la prima orbita si spezza in due orbite e le altre rimangono inalterate.

II^o **caso:**

$$\sigma=\begin{pmatrix}1&2&3&4&5&6&7&8&9&10\\2&7&5&6&10&9&8&1&4&3\end{pmatrix}\,,\qquad \tau=\begin{pmatrix}1&3\\3&1\end{pmatrix}$$

Dunque 1 e 3 appartengono a due orbite distinte di σ.

Cicli di $\sigma\tau$:

$$\begin{pmatrix}1&5&3&2&7&8\\5&10&2&7&8&1\end{pmatrix}\,,\quad\begin{pmatrix}4&6&9\\6&9&4\end{pmatrix}$$

Dunque, in questo caso, nel passare da σ a $\sigma\tau$, le prime due orbite si fondono in una sola orbita e le altre (l'altra) rimangono inalterate.

Dal teorema precedente segue immediatamente il seguente corollario.

Corollario 14.13. *Sia σ una permutazione. Si esprima σ come prodotto di k trasposizioni. Allora $\epsilon(\sigma) = (-1)^k$.*

Il Corollario precedente implica il seguente:

Corollario 14.14. *Sian $\sigma, \tau \in \mathfrak{S}_n$. Allora $\epsilon(\sigma\tau) = \epsilon(\sigma)\epsilon(\tau)$.*

15. La matrice di Vandermonde

Sia $A = (a_{ij})$ una matrice quadrata di ordine n a coefficienti in un campo $\mathbb{K}$. Il determinante di A è dato dalla formula

$$\det(A) = \sum_{\sigma\in\Sigma_n} \varepsilon(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)},$$

dove Σ_n è l'insieme delle permutazioni di $\{1, \ldots, n\}$ e $\varepsilon(\sigma)$ è la segnatura di σ.
Valgono le seguenti proprietà:
1) Sviluppo di Laplace.
Se A_{ij} indica il minore $(n-1)\times(n-1)$ ottenuto togliendo ad A la i-esima riga e la j-esima colonna, allora per ogni $h = 1, \ldots, n$ valgono le formule

$$\det(A) = \sum_{j=1}^{n} a_{hj}(-1)^{h+j}\det(A_{hj}) = \sum_{i=1}^{n}(-1)^{i+h}\det(A_{ih})a_{ih},$$

2) Moltiplicando una riga od una colonna di A per un elemento $a \in \mathbb{K}$, anche $\det(A)$ viene moltiplicato per a.
3) Il determinante $\det(A)$ non cambia se ad una colonna viene aggiunto un multiplo di un'altra colonna. Lo stesso per le righe.
4) Se la matrice A possiede due colonne uguali, allora $\det(A) = 0$.
5) Vale il teorema di Binet: $\det(AB) = \det(A)\det(B)$.

Come esempio di applicazione delle precedenti regole, calcoliamo il determinante della matrice di Vandermonde; più precisamente proviamo che

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_0 & x_1 & \cdots & x_n \\ \vdots & \vdots & \ddots & \vdots \\ x_0^{n-1} & x_1^{n-1} & \cdots & x_n^{n-1} \\ x_0^n & x_1^n & \cdots & x_n^n \end{vmatrix} = \prod_{i>j}(x_i - x_j)$$

Ragioniamo per induzione su n, considerando il polinomio

$$p(t) = \prod_{j=0}^{n-1}(t - x_j) = t^n + \sum_{i=0}^{n-1} a_i t^i.$$

Sommando all'ultima riga della matrice di Vandermonde la combinazione lineare a coefficienti a_i delle rimanenti righe si ottiene

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_0 & x_1 & \cdots & x_n \\ \vdots & \vdots & \ddots & \vdots \\ x_0^{n-1} & x_1^{n-1} & \cdots & x_n^{n-1} \\ x_0^n & x_1^n & \cdots & x_n^n \end{vmatrix} = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_0 & x_1 & \cdots & x_n \\ \vdots & \vdots & \ddots & \vdots \\ x_0^{n-1} & x_1^{n-1} & \cdots & x_n^{n-1} \\ p(x_0) & p(x_1) & \dots & p(x_n) \end{vmatrix}$$

Dato che $p(x_i) = 0$ per ogni $i < n$ e $p(x_n) = \prod_{n>j}(x_n - x_j)$ si ha

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_0 & x_1 & \cdots & x_n \\ \vdots & \vdots & \ddots & \vdots \\ x_0^{n-1} & x_1^{n-1} & \cdots & x_n^{n-1} \\ x_0^n & x_1^n & \cdots & x_n^n \end{vmatrix} = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_0 & x_1 & \cdots & x_n \\ \vdots & \vdots & \ddots & \vdots \\ x_0^{n-1} & x_1^{n-1} & \cdots & x_n^{n-1} \\ 0 & 0 & \cdots & p(x_n) \end{vmatrix} =$$

$$= p(x_n) \begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_0 & x_1 & \cdots & x_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ x_0^{n-1} & x_1^{n-1} & \cdots & x_{n-1}^{n-1} \end{vmatrix} = \prod_{n>j}(x_n - x_j) \prod_{n>i>j}(x_i - x_j).$$

Possiamo quindi affermare che la matrice di Vandermonde

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ x_0 & x_1 & \cdots & x_n \\ \vdots & \vdots & \ddots & \vdots \\ x_0^{n-1} & x_1^{n-1} & \cdots & x_n^{n-1} \\ x_0^n & x_1^n & \cdots & x_n^n \end{pmatrix} \tag{2}$$

è **invertibile se e soltanto se** $x_i \neq x_j$ **per ogni** $i \neq j$. Vediamo adesso alcune applicazioni di questo fatto.

TEOREMA 15.1. *Siano $v_0, \dots, v_n$ vettori di uno spazio vettoriale V su di un campo $\mathbb{K}$. Supponiamo che la relazione*

$$v_0 + tv_1 + \cdots + t^n v_n = 0$$

sia soddisfatta per almeno $n + 1$ valori distinti di $t \in \mathbb{K}$. Allora $v_0 = v_1 = \cdots = v_n = 0$.

DIMOSTRAZIONE. Tra i valori di t che soddisfano la precedente relazione scegliamone $n + 1$ distinti $t_0, t_1, \dots, t_n$. Otteniamo quindi $n + 1$ relazioni che possono essere scritte come un'uguaglianza tra due righe di vettori

$$(v_0, v_1, \dots, v_n)V = (0, 0, \dots, 0),$$

dove

$$V = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ t_0 & t_1 & \cdots & t_n \\ \vdots & \vdots & \ddots & \vdots \\ t_0^{n-1} & t_1^{n-1} & \cdots & t_n^{n-1} \\ t_0^n & t_1^n & \cdots & t_n^n \end{pmatrix}$$

Abbiamo dimostrato che la matrice di Vandermonde V è invertibile e, moltiplicando a destra per V^{-1}, la precedente uguaglianza si ottiene

$$(0,0,\dots,0) = (0,0,\dots,0)V^{-1} = (v_0, v_1, \dots, v_n)VV^{-1} = (v_0, v_1, \dots, v_n).$$

□

Corollario 15.2. *Ogni polinomio non nullo di grado n a coefficienti in un campo $\mathbb{K}$ possiede al più n radici.*

Dimostrazione. Bisogna dimostrare che se, dati $a_0, \dots, a_n \in \mathbb{K}$ esistono almeno $n+1$ valori di t tali che

$$a_0 + ta_1 + \dots + t^n a_n = 0,$$

allora $a_0 = a_1 = \dots = a_n = 0$. Basta applicare il teorema precedente al caso $V = \mathbb{K}$. □

Corollario 15.3. *Siano $A_0, \dots, A_k, B_0, \dots, B_k$ matrici $n \times n$ e si assuma che*

$$A_0 + tA_1 + \dots + t^k A_k = B_0 + tB_1 + \dots + t^k B_k$$

per infiniti valori di $t \in \mathbb{K}$. Allora per ogni matrice C, di tipo $n \times n$, vale

$$A_0 + CA_1 + \dots + C^k A_k = B_0 + CB_1 + \dots + C^k B_k.$$

Dimostrazione. Possiamo scrivere

$$(A_0 - B_0) + t(A_1 - B_1) + \dots + t^k(A_k - B_k) = 0$$

e quindi per il Teorema 15.1, applicato allo spazio vettoriale delle matrici, si ha $A_i - B_i = 0$ per ogni indice i. In particolare $C^i A_i = C^i B_i$ per ogni matrice C di tipo $n \times n$. □

Esercizio 15.4. Dimostrare che il rango della matrice di Vandermonde (2) è uguale al massimo numero di elementi distinti dell'insieme $\{x_0, x_1, \dots, x_n\}$.

Esercizio 15.5. Calcolare il determinante

$$\begin{vmatrix} x_1 & \cdots & x_n \\ \vdots & \ddots & \vdots \\ x_1^{n-1} & \cdots & x_n^{n-1} \\ x_1^n & \cdots & x_n^n \end{vmatrix}$$

16. La matrice aggiunta

Se A è una matrice $n \times n$, denotiamo con $\tilde{A} = (\tilde{a}_{ij})$ la sua **matrice aggiunta**, ossia la matrice di coefficienti

$$\tilde{a}_{ij} = (-1)^{i+j} \det(A_{ji}).$$

(Notare lo scambio di indici di riga e colonna.) Se $n = 1$ si pone per convenzione $\tilde{A} = (1)$.

Ad esempio, la matrice aggiunta di

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

è

$$\tilde{A} = \begin{pmatrix} 4 & -2 \\ -3 & 2 \end{pmatrix}$$

Proposizione 16.1. *Per ogni matrice quadrata A vale*

$$A\tilde{A} = \tilde{A}A = \det(A)I.$$

In particolare, se $\det(A) \neq 0$*, allora* $A^{-1} = \dfrac{\tilde{A}}{\det(A)}$.

Dimostrazione. Indichiamo $(c_{ij}) = A\tilde{A}$; bisogna dimostrare che $c_{ii} = \det(A)$ per ogni i e che $c_{ij} = 0$ per ogni $i \neq j$. Fissiamo due indici i, j e indichiamo con $B = (b_{hk})$ la matrice i cui coefficienti sono definiti come

$$b_{hk} = a_{hk} \quad \text{se} \quad h \neq j; \qquad\qquad b_{jk} = a_{ik}.$$

Notiamo che se $i = j$ allora $A = B$, mentre se $i \neq j$, allora la matrice B ha due righe uguali e quindi $\det(B) = 0$.
Inoltre

$$c_{ij} = \sum_{k=1}^{n} a_{ik}\tilde{a}_{kj} = \sum_{k=1}^{n} a_{ik}(-1)^{j+k}\det(A_{jk}),$$

e, poiché $a_{ik} = b_{jk}$ e $A_{jk} = B_{jk}$ ne segue che

$$c_{ij} = \sum_{k=1}^{n} a_{ik}(-1)^{j+k}\det(A_{jk}) = \sum_{k=1}^{n} b_{jk}(-1)^{j+k}\det(B_{jk}) = \det(B),$$

dove l'ultima uguaglianza segue dallo sviluppo di Laplace del determinante di B rispetto alla i-esima riga.
Abbiamo quindi dimostrato che $A\tilde{A} = \det(A)I$; la dimostrazione dell'uguaglianza $\tilde{A}A = \det(A)I$ è del tutto simile (basta scambiare gli indici di riga con quelli di colonna) ed è lasciata per esercizio al lettore. □

Esercizio 16.2. Calcolare le inverse delle seguenti matrici

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & -1 \\ 0 & -1 & 1 \\ 1 & 1 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

Esercizio 16.3. Sia A una matrice $n \times n$, con $n \geq 2$. Dimostrare che

$$\det(\tilde{A}) = \det(A)^{n-1}.$$

17. Il teorema di Cayley-Hamilton

Siano A, B due matrici $n \times n$ a coefficienti in un campo $\mathbb{K}$. Se indichiamo con t una indeterminata, allora ogni coefficiente di $A - tB$ è un polinomio di grado minore od uguale ad 1 in t a coefficienti in $\mathbb{K}$ e di conseguenza il determinante $\det(A - tB)$ è un polinomio di grado minore od uguale a n.

Definizione 17.1. Il polinomio

$$p_A(t) = \det(A - tI)$$

viene detto polinomio caratteristico della matrice A.

Ad esempio il polinomio caratteristico della matrice

$$A = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$$

è uguale a

$$p_A(t) = \det(A - tI) = \begin{vmatrix} 1-t & 2 \\ 1 & 1-t \end{vmatrix} = (1-t)^2 - 2 = t^2 - 2t - 1.$$

TEOREMA 17.2 (Cayley-Hamilton). *Siano A una matrice $n \times n$ a coefficienti in un campo $\mathbb{K}$ e $p_A(t) \in \mathbb{K}[t]$ il suo polinomio caratteristico.*
Se $p_A(t) = a_0 + a_1 t + \cdots + a_n t^n$, allora

$$a_0 I + a_1 A + \cdots + a_n A^n = 0.$$

DIMOSTRAZIONE. Consideriamo la matrice aggiunta di $A - tI$; ogni coefficiente di $\widetilde{A - tI}$ è un polinomio di grado $\leq n-1$ in t e quindi si può scrivere

$$\widetilde{A - tI} = B_0 + tB_1 + \cdots + t^{n-1} B_{n-1},$$

dove ogni B_i è una matrice $n \times n$ a coefficienti in $\mathbb{K}$. Segue dalla Proposizione 16.1 che per ogni $t \in \mathbb{K}$ vale

$$p_A(t) I = (A - tI)(\widetilde{A - tI}) = (A - tI)(B_0 + tB_1 + \cdots + t^{n-1} B_{n-1}).$$

Sviluppando il prodotto, tale uguaglianza diventa

$$\begin{aligned} & a_0 I + a_1 t I + \cdots + a_n t^n I = \\ &= AB_0 + t(AB_1 - B_0) + t^2(AB_2 - B_1) + \cdots + t^{n-1}(AB_{n-1} - B_{n-2}) + t^n(-B_{n-1}) \end{aligned}$$

che, per il Corollario 15.3 applicato scegliendo $C = A$, implica

$$\begin{aligned} & a_0 I + a_1 A + \cdots + a_n A^n = \\ &\qquad = AB_0 + A(AB_1 - B_0) + A^2(AB_2 - B_1) + \cdots + A^n(-B_{n-1}) \\ &\qquad\qquad = (A - A)B_0 + (A^2 - A^2)B_1 + \cdots + (A^n - A^n)B_{n-1} = 0. \end{aligned}$$

□

ESERCIZIO 17.3. Calcolare il polinomio caratteristico delle matrici dell'Esercizio 16.2.

ESERCIZIO 17.4. Una matrice quadrata A si dice **nilpotente** se $A^m = 0$ per qualche $m > 0$. Sia A di tipo $n \times n$; dimostrare che se $p_A(t) = (-t)^n$, allora A è nilpotente.

ESERCIZIO 17.5 ($*$). Sia A di tipo $n \times n$; dimostrare che se A è nilpotente, allora $p_A(t) = (-t)^n$. (Sugg.: dimostrare preliminarmente che per ogni numero complesso $z \neq 0$ vale $\det(A - zI) \neq 0$.)

18. Tutoraggio del 27 novembre 2006

Esercizio 18.1. Calcolare l'inversa della matrice

$$\begin{pmatrix} 1 & 0 & 2 \\ 2 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

Esercizio 18.2. Dimostrare che il determinante di una matrice antisimmetrica di ordine 351 si annulla.

Esercizio 18.3. Sia A una matrice quadrata di ordine 2. Trovare una formula per il calcolo del determinante in funzione delle tracce di A ed A^2.

Esercizio 18.4. Vero o falso? Ogni matrice 2×4 nella quale i determinanti dei minori 2×2 formati da due colonne adiacenti si annullano ha rango minore di 2.

Esercizio 18.5. Sia A una matrice 10×10 Calcolare, in funzione di $\det(A)$, il determinante della seguente matrice 20×20

$$\begin{pmatrix} 6A & 5A \\ A & 2A \end{pmatrix}$$

Esercizio 18.6. Calcolare il determinante della matrice $n \times n$, con $n \geq 3$,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ n+1 & n+2 & n+3 & n+4 & \dots & 2n \\ 2n+1 & 2n+2 & 2n+3 & 2n+4 & \dots & 3n \\ \dots & & & & & \\ (n-1)n+1 & (n-1)n+2 & (n-1)n+3 & (n-1)n+4 & \dots & n^2 \end{pmatrix}$$

Esercizio 18.7. Siano $v_0, v_1, \dots, v_n$ vettori di uno spazio vettoriale sul campo $\mathbb{K}$. Dimostrare che se

$$v_0 + tv_1 + t^2 v_2 + \cdots + t^n v_n = 0$$

per infiniti valori di $t \in \mathbb{K}$ allora $v_0 = v_1 = \cdots = v_n = 0$. (Sugg.: Vandermonde).

Esercizio 18.8. Dimostrare, senza fare il conto esplicito, che il determinante della matrice

$$\begin{pmatrix} 4 & 2 & 2 & 2 & 8 & 6 & 6 \\ 1 & -1 & -1 & 3 & 0 & 2 & 4 \\ 2 & 1 & -1 & 3 & 5 & 7 & -1 \\ 2 & 1 & 6 & 0 & 3 & -8 & 3 \\ 2 & 1 & 1 & 0 & -2 & 7 & 3 \\ 2 & 1 & 1 & 0 & 0 & 7 & 3 \\ 2 & 1 & 1 & 0 & 2 & 7 & 3 \end{pmatrix}$$

è uguale a 0.

Esercizio 18.9. Indichiamo con d_k, $k \geq 1$, il determinante della matrice $k \times k$

$$\begin{pmatrix} 6 & 1 & 0 & 0 & 0 & \dots & 0 \\ 1 & 6 & 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 6 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & 6 & 1 & \dots & \\ & & & \dots & & & \\ 0 & 0 & 0 & 0 & 0 & \dots & 6 \end{pmatrix}$$

($d_1 = 6$, $d_2 = 35$ eccetera). Dimostrare che per ogni $k \geq 3$ vale $d_k = 6d_{k-1} - d_{k-2}$. Siano x, y le radici del polinomio $t^2 - 6t + 1$. Dimostrare che per ogni $k \geq 3$ vale

$$x^k = 6x^{k-1} - x^{k-2}, \qquad y^k = 6y^{k-1} - y^{k-2}.$$

Determinare due numeri reali a, b tali che

$$d_k = ax^k + by^k$$

per ogni $k \geq 1$.

19. Dualità

Considereremo, in questa nota, spazi vettoriali di dimensione finita su di un campo $\mathbb{K}$.

Sia V un $\mathbb{K}$-spazio vettoriale. Lo *spazio duale di* V è lo spazio

$$V^* = \mathcal{L}(V, \mathbb{K}).$$

Dunque i vettori dello spazio duale sono applicazioni lineari di V in $\mathbb{K}$:

$$\varphi \in V^*, \qquad \text{vuol dire} \qquad \varphi : V \to \mathbb{K} \qquad \text{(lineare)}.$$

Gli elementi di V^* si chiamano anche *forme lineari su* V. Naturalmente, date due forme lineari $\varphi, \psi \in V^*$, dire che $\varphi = \psi$, vuol dire che $\varphi(v) = \psi(v)$ per ogni $v \in V$:

$$\boxed{\varphi, \psi \in V^*, \ \varphi = \psi \iff \varphi(v) = \psi(v), \ \forall v \in V} \tag{3}$$

Sia ora

$$F : V \longrightarrow W,$$

una applicazione lineare. Definiamo *l'applicazione lineare duale di* F

$$F^* : W^* \longrightarrow V^*,$$
$$\psi \mapsto F^*(\psi)$$

nel modo seguente. Dato $\psi \in W^*$, definiamo $F^*(\psi) \in V^*$ ponendo:

$$F^*(\psi)(v) = \psi(F(v)), \qquad \forall v \in V.$$

Dunque $F^*(\psi) : V \to \mathbb{K}$ non è altro che l'applicazione lineare composta:

$$F^*(\psi) = \psi \circ F : V \xrightarrow{F} W \xrightarrow{\psi} \mathbb{K}$$

È immediato verificare che $F^* : W^* \to V^*$ è lineare e cioè che

$$F^*(\psi + \psi') = F^*(\psi) + F^*(\psi'), \quad F^*(a\psi) = aF^*(\psi), \forall \psi, \psi' \in W^*, \quad a \in \mathbb{K}.$$

Infatti, per ogni $v \in V$

$$F^*(\psi + \psi')(v) = (\psi + \psi')F(v) = \psi f(v) + \psi' F(v) = F^*(\psi)(v) + F^*(\psi')(v),$$

e

$$F^*(a\psi)(v) = (a\psi)(F(v)) = a(\psi F(v)) = aF^*(\psi)(v).$$

È molto importante notare che la definizione di F^* è *intrinseca*, non dipende cioè dalla scelta di basi in V e W. Si considerino applicazioni lineari

$$V \xrightarrow{F} W \xrightarrow{G} U$$

e si consideri anche l'identità $1_V : V \to V$. Valgono le seguenti proprietà:

$$(4) \qquad (GF)^* = F^*G^* : U^* \longrightarrow V^* ; \qquad (1_V)^* = 1_{V^*} : V^* \longrightarrow V^* .$$

Anche in questo caso le dimostrazioni sono immmediate. Dobbiamo far vedere che

$$(GF)^*(\psi) = F^*G^*(\psi) , \quad \forall \psi \in U^* ; \qquad (1_V)^*(\varphi) = \varphi , \quad \forall \varphi \in V^* .$$

Questo vuol dire che dobbiamo mostrare che

$$\begin{aligned} (GF)^*(\psi)(u) &= F^*G^*(\psi)(u) , \quad \forall \psi \in U^* , \quad \forall u \in U ; \\ (1_V)^*(\varphi)(v) &= \varphi(v) , \quad \forall \varphi \in V^* \quad \forall v \in V ; \end{aligned}$$

In effetti si ha:

$$\begin{aligned} (GF)^*(\psi)(u) &= \psi GF(u) = (G^*(\psi))(F(u)) = (F^*G^*\psi)(u) , \\ (1_V)^*(\varphi)(v) &= \varphi 1_V(v) = \varphi(v) . \end{aligned}$$

Consideriamo ora le basi. Supponiamo che $\mathbf{e} = (e_1, \dots, e_n)$ sia una base di V. Consideriamo le n applicazioni lineari:

$$\varphi_i : V \longrightarrow \mathbb{K} , \qquad i = 1, \dots, n ,$$

definite da

$$\varphi_i(e_i) = 1 , \qquad \varphi_i(e_j) = 0 , \quad \text{se} \qquad i \neq j .$$

L'applicazione lineare φ_i non è altro che l'applicazione *"coordinata i-esima"*. Dato $v \in V$, se si scrive v nella base $\mathbf{e}$ si ha:

$$\boxed{v = x_1e_1 + x_2e_2 + \cdots + x_ne_n \qquad \Rightarrow \qquad \varphi_i(v) = x_i}$$

Ricordiamo che le applicazioni lineari φ_i, per $i = 1, \dots, n$, formano una base di V^*. Infatti, dato un qualsiasi elemento $\psi \in V^*$ e un *qualsiasi vettore*

$$v = x_1e_1 + x_2e_2 + \cdots + x_ne_n \in V ,$$

si ha:

$$\begin{aligned} \psi(v) &= x_1\psi(e_1) + x_2\psi(e_2) + \cdots + x_n\psi(e_n) \\ &= \psi(e_1)\varphi_1(v) + \psi(e_2)\varphi_2(v) + \cdots + \psi(e_n)\varphi_n(v) , \end{aligned}$$

il che vuol dire che:

$$\psi = \psi(e_1)\varphi_1 + \psi(e_2)\varphi_2 + \cdots + \psi(e_n)\varphi_n .$$

Dunque le applicazioni lineari φ_i, $i = 1, \dots, n$ generano V^*. Sono anche linearmente indipendenti perché, se

$$c_1\varphi_1 + c_2\varphi_2 + \cdots + c_n\varphi_n = 0 ,$$

allora, per ogni $i = 1, \dots, n$, si ha:

$$c_1\varphi_1(e_i) + c_2\varphi_2(e_i) + \cdots + c_n\varphi_n(e_i) = c_i = 0 .$$

La base $\boldsymbol{\varphi} = (\varphi_1, \dots, \varphi_n)$ prende il nome di *base duale della base* $\mathbf{e}$.

È utile usare la seguente notazione. Data una riga $\mathbf{v} = (v_1, \dots, v_n)$ di vettori in V e una riga $\boldsymbol{\xi} = (\xi_1, \dots, \xi_n)$ di forme in V^*, si definisce la matrice

$${}^t\boldsymbol{\xi} \cdot \mathbf{v} \in M_{n,n}(\mathbb{K}) ,$$

ponendo

$$({}^t\boldsymbol{\xi} \cdot \mathbf{v})_{s,t} = \xi_t(v_s)\,.$$

Naturalmente, se $\mathbf{e}$ è una base di V e se $\boldsymbol{\varphi}$ è la base duale di V^*, si ha

$$(5) \qquad {}^t\boldsymbol{\varphi} \cdot \mathbf{e} = I\,,$$

dove $I \in M_{n,n}(\mathbb{K})$ è la matrice identità.

Proposizione 19.1. *Sia $F : V \to W$ una applicazione lineare. Si fissi una base $\mathbf{e}$ di V e una base $\mathbf{f}$ di W. Sia $\boldsymbol{\varphi}$ la base duale di $\mathbf{e}$ in V^* e $\boldsymbol{\psi}$ la base duale di $\mathbf{f}$ in W^*. Si consideri l'applicazione duale $F^* : W^* \to V^*$. Sia A la matrice di F nelle basi $\mathbf{e}$ e $\mathbf{f}$. Allora la matrice di F^*, nelle basi $\boldsymbol{\psi}$ e $\boldsymbol{\varphi}$, è la matrice trasposta ${}^tA$.*

Dimostrazione. Si ha:

$$(6) \qquad F(\mathbf{e}) = \mathbf{f}A.$$

Poniamo

$$(7) \qquad F^*(\boldsymbol{\psi}) = \boldsymbol{\varphi}B\,.$$

Da una parte, usando la (5), applicata alle basi $\mathbf{e}$ e $\boldsymbol{\varphi}$, si ha:

$${}^t(F^*(\boldsymbol{\psi})) \cdot \mathbf{e} = {}^t(\boldsymbol{\varphi}B) \cdot \mathbf{e} = {}^tB^t\boldsymbol{\varphi} \cdot \mathbf{e} = {}^tB\,.$$

Dall'altra, usando la (5), applicata alle basi $\mathbf{f}$ e $\boldsymbol{\psi}$, si ottiene,

$${}^t(F^*(\boldsymbol{\psi})) \cdot \mathbf{e} = {}^t\boldsymbol{\psi} \cdot F(\mathbf{e}) = {}^t\boldsymbol{\psi} \cdot \mathbf{f}A = A.$$

Dunque $B = {}^tA$. □

Possiamo riconoscere nella (6) e nella (7) un fatto che è già noto. Queste relazioni ci dicono che se A è la matrice della applicazione lineare F nelle basi $\mathbf{e}$ e $\mathbf{f}$, allora le coordinate $(y_1, \dots, y_m)$, nella base $\mathbf{f}$, dell' immagine, tramite F, del vettore di coordinate $(x_1, \dots, x_1)$, sono date da

$$(y_1, \dots, y_n) = (x_1, \dots, x_m)^tA$$

o, equivalentemente da

$$\begin{pmatrix} y_1 \\ y_2 \\ \cdot \\ \cdot \\ \cdot \\ y_m \end{pmatrix} = A \begin{pmatrix} x_1 \\ x_2 \\ \cdot \\ \cdot \\ \cdot \\ x_n \end{pmatrix}$$

Osserviamo inoltre che, in virtù della Proposizione appena dimostrata, la relazione (4) può essere vista come un riflesso della ben nota proprietà della trasposizione:

$${}^t(AB) = {}^tB^tA\,, \qquad {}^tI = I\,.$$

Infine, dal fatto che il rango per righe di una matrice è uguale al rango per colonne della matrice stessa, segue che:

Teorema 19.2. *Sia $F : V \to W$ una applicazione lineare. Sia $F^* : W^* \to V^*$ l'applicazione lineare duale. Allora*

$$rg(F) = rg(F^*)\,.$$

È interessante dare una dimostrazione di questo teorema che non dipenda dalla conoscenza del fatto che il rango per righe di una matrice sia uguale al suo rango per colonne. In questo modo riusciremo a dare una dimostrazione (più) concettuale di questa fondamentale proprietà delle matrici.

Sia $U \subset V$ un sottospazio vettoriale. Definiamo un sottospazio $Ann(U) \subset V^*$, detto *l'annullatore di* U, nel modo seguente:

$$Ann(U) = \{\varphi \in V^* \ : \ \varphi(u) = 0 \,,\, \forall\, u \in U\}.$$

Chiaramente $Ann(U)$ è un sottospazio vettoriale di V^*. Infatti si verifica subito che

$$\varphi, \psi \in V^*,\, c \in \mathbb{K} \qquad \Longrightarrow \qquad \varphi + \psi,\, c\varphi \in V^*.$$

PROPOSIZIONE 19.3. *Sia* $U \subset V$ *un sottospazio vettoriale. Allora*

$$\dim Ann(U) = \dim V - \dim U\,.$$

DIMOSTRAZIONE. Sia $d = \dim U$ e $n = \dim V$. Sia $(e_1, \dots, e_d)$ una base di U. La si completi a una base $\mathbf{e} = (e_1, \dots, e_d, e_{d+1}, \dots, e_n)$ di V. Sia $(\varphi_1, \dots, \varphi_n)$ la base duale di $\mathbf{e}$. Poiché $\varphi_s(e_t) = 0$, per $t = 1, \dots, d$ e $s = d+1, \dots, n$, si ha che φ_s si annulla su U per $s = d+1, \dots, n$. Dunque $\varphi_s \in Ann(U)$, per $s = d+1, \dots, n$. Dimostriamo che $(\varphi_{d+1}, \dots, \varphi_n)$ è una base di $Ann(U)$. Basta mostrare che $L(\varphi_{d+1}, \dots, \varphi_n) = Ann(U)$. Sia $\psi \in Ann(U)$. Scriviamo

$$\psi = c_1\varphi_1 + \cdots + c_n\varphi_n\,.$$

Poiché $e_i \in U$, per $i = 1, \dots, d$, si ha:

$$\psi(e_i) = c_i = 0\,, \qquad i = 1, \dots, d\,,$$

e dunque

$$\psi = c_{d+1}\varphi_1 + \cdots + c_n\varphi_n\,.$$

$\square$

COROLLARIO 19.4. *Sia* $U \subset V$ *un sottospazio vettoriale. Se* $Ann(U) = V^*$, *allora* $U = \{0\}$

DIMOSTRAZIONE. $\dim(U) = \dim(V) - \dim Ann(U) = 0$. $\square$

LEMMA 19.5. *Siano* $F : V \to W$ *una applicazione lineare e* $F^* : W^* \to V^*$ *l'applicazione lineare duale. Allora*

$$Ker(F^*) = Ann(Im(F))\,.$$

DIMOSTRAZIONE.

$$\psi \in Ann(Im(F)) \quad \Longleftrightarrow \quad \psi(F(u)) = 0\,, \quad \forall\, u \in V \quad \Longleftrightarrow$$
$$(F^*\psi)(u) = 0\,, \quad \forall\, u \in V \quad \Longleftrightarrow \quad (F^*\psi) = 0 \quad \Longleftrightarrow \psi \in Ker(F^*)$$

Possiamo ora dare una dimostrazione *intrinseca* del Teorema 19.2. Sia dunque F come nel Teorema. Usando il Lemma precedente e la Proposizione 19.3, si ottiene:

$$\begin{aligned} rg(F^*) &= \dim Im(F^*) = \dim W^* - \dim Ker(F^*) = \dim W^* - \dim Ann(Im(F)) \\ &= dim(W^*) - \dim W + \dim(Im(F)) = \dim(Im(F)) = rg(F) \end{aligned}$$

$\square$

Corollario 19.6. *Sia $A \in M_{n,m}(\mathbb{K})$ una matrice. Allora il rango per righe di A è uguale al rango per colonne di A.*

Dimostrazione. Siano $\mathbf{e}$ e $\mathbf{f}$ le basi standard di $\mathbb{K}^m$ e $\mathbb{K}^n$. Sia $\boldsymbol{\varphi}$ la base duale di $\mathbf{e}$ e $\boldsymbol{\psi}$ la base duale di $\mathbf{f}$. Allora, dalla Proposizione 19.1, segue che la matrice di $(L_A)^*$ nelle basi $\boldsymbol{\psi}$ e $\boldsymbol{\varphi}$ non è altro che ${}^tA$. Possiamo quindi scrivere che

$$(L_A)^* = L_{{}^tA}\,.$$

Dal teorema precedente segue che $rg(A) = rg({}^tA)$. $\square$

Un utile fatto che riguarda gli annullatori è il seguente:

Lemma 19.7. *Siano U e W sottospazi di V. Allora*

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

Dimostrazione. Si ha:

$$\begin{aligned} &\varphi \in Ann(U) \cap Ann(W) \quad \iff \quad \varphi(u) = \varphi(w) = 0\,, \forall\ u \in U\,,\ \forall\ w \in W \\ &\iff \quad \varphi(u + w) = 0\,, \forall\ u \in U\,,\ \forall\ w \in W \quad \iff \quad \varphi(v) = 0\,, \forall\ v \in U + W \\ &\iff \quad \varphi \in Ann(U + W)\,. \end{aligned}$$

$\square$

Terminiamo dimostrando che vi è un *isomorfismo canonico* tra V e il suo doppio duale V^{**}. Con questo intendiamo che la definizione di questo isomorfismo prescinde dalla scelta di basi in V e in V^{**}. L'isomorfismo canonico

$$\Phi : V \longrightarrow V^{**}$$

è definito nel modo seguente. Per ogni v in V, l'elemento $\Phi(v)$ in V^{**} è la forma lineare, su V^*,

$$\begin{aligned} \Phi(v) :\, &V^* \longrightarrow \mathbb{K} \\ &\psi \mapsto \Phi(v)(\psi) \end{aligned}$$

dove:

$$\Phi(v)(\psi) = \psi(v) \in \mathbb{K}\,.$$

Che, per ogni *fissato* $v \in V$, $\Phi(v)$ sia una forma lineare su V^* è evidente. Infatti, per ogni $\psi, \psi' \in V^*$ e $c \in \mathbb{K}$ si ha:

$$\begin{aligned} \Phi(v)(\psi + \psi') &= (\psi + \psi')(v) = \psi(v) + \psi'(v) = \Phi(v)(\psi) + \Phi(v)(\psi') \\ \Phi(v)(c\psi) &= (c\psi)(v) = c\psi(v) = c\Phi(v)(\psi)\,. \end{aligned}$$

Che Φ sia una applicazione lineare di V in V^{**} è anche evidente. Bisogna dimostrare che

$$\begin{aligned} \Phi(v + v') &= \Phi(v) + \Phi(v')\,, \\ \Phi(cv) &= c\Phi(v)\,. \end{aligned}$$

Dobbiamo quindi dimostrare che, per ogni $\psi \in V^*$, si ha:

$$\begin{aligned} \Phi(v + v')(\psi) &= (\Phi(v) + \Phi(v'))(\psi)\,, \\ \Phi(cv)(\psi) &= c\Phi(v)(\psi)\,. \end{aligned}$$

Per quello che riguarda la prima eguaglianza, si ha:

$$\Phi(v+v')(\psi) = \psi(v+v') = \psi(v)+\psi(v') = \Phi(v)(\psi)+\Phi(v')(\psi) = (\Phi(v)+\Phi(v'))(\psi)$$

Per la seconda:

$$\Phi(cv)(\psi) = \psi(cv) = c\psi(v) = c\Phi(v)(\psi)\,.$$

In conclusione $\Phi : V \to V^{**}$ è una applicazione lineare. Dal momento che V e V^{**} hanno la stessa dimensione, per dimostrare che Φ è un isomorfismo basta dimostrare che Φ è iniettiva. Supponiamo che

$$\Phi(v) = 0$$

Questo vuol dire che,

$$\Phi(v)(\psi) = 0\,, \qquad \forall\ \psi \in V^*\,.$$

Poiché $\Phi(v)(\psi) = \psi(v)$, si ha:

$$\psi(v) = 0\,, \qquad \forall\ \psi \in V^*\,.$$

Questo vuol dire che

$$Ann(v) = V^*\,.$$

Per il Corollario 19.4, ciò implica che $v = 0$ Q.E.D.

20. Tutoraggio del 4 dicembre 2006

Esercizio 20.1. Calcolare l'inversa della matrice

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

Esercizio 20.2. Vero o falso? Se B è una matrice quadrata tale che ${}^tB \cdot B = I$, allora $\det(B) = \pm 1$.

Esercizio 20.3. Vero o falso? Se A e B sono due matrici quadrate dello stesso ordine, allora $\det(AB - BA) = 0$.

Esercizio 20.4. Siano $p = (a, b)$ e $q = (c, d)$ due punti distinti del piano $\mathbb{R}^2$. Dimostrare che il luogo dei punti $(x, y) \in \mathbb{R}^2$ tali che

$$\begin{vmatrix} x & y & 1 \\ a & b & 1 \\ c & d & 1 \end{vmatrix} = 0$$

coincide con la retta affine passante per p e q.

Esercizio 20.5. Si consideri la base $\mathbf{v} = (v_1, v_2, v_3)$ di $\mathbb{R}^3$ data dai vettori

$$v_1 = \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix}, \quad v_2 = \begin{pmatrix} 2 \\ -1 \\ 0 \end{pmatrix}, \quad v_3 = \begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix}.$$

Detarminare la base duale.

Esercizio 20.6. Sia $f\colon M_{2,2}(\mathbb{K}) \to M_{2,2}(\mathbb{K})$ l'applicazione lineare

$$f(A) = 3A - {}^tA.$$

Calcolare il determinante di f.

Esercizio 20.7. Sia V lo spazio vettoriale dei polinomi di grado minore od uguale a 3 e sia $f\colon V \to V$ l'applicazione lineare

$$f(P)(x) = P(2-x).$$

(1) Calcolare il determinante di f.
(2) $(*)$ Trovare una base di V nella quale f si rappresenta con una matrice diagonale.

Esercizio 20.8. Dati due punti $p = (p_1, p_2)$, $q = (q_1, q_2)$ del piano $\mathbb{R}^2$ denotiamo con

$$A(p,q) = \begin{vmatrix} p_1 & q_1 \\ p_2 & q_2 \end{vmatrix}.$$

Dimostrare che:

(1) Se $r\colon \mathbb{R}^2 \to \mathbb{R}^2$ è una rotazione di centro 0, allora

$$A(r(p), r(q)) = A(p,q).$$

(2) Se $s\colon \mathbb{R}^2 \to \mathbb{R}^2$ è la simmetria rispetto ad una retta passante per l'origine, allora

$$A(r(p), r(q)) = -A(p,q).$$

(3) Il valore assoluto di $A(p,q)$ è uguale al doppio dell'area del triangolo di vertici $0, p, q$.

21. Tutoraggio dell'11 dicembre 2006

Esercizio 21.1. Sia $H \subset \mathbb{R}^3$ il piano di equazione $x + 2y - z = 0$. Determinare un funzionale lineare $f\colon \mathbb{R}^3 \to \mathbb{R}$ tale che $H = \ker(f)$ e $f(1,1,2) = 4$.

Esercizio 21.2. Vero o falso?

- Sia A una matrice quadrata, allora $rg(A) = rg(A^2)$.
- Siano A e B matrici invertibili, allora AB e BA sono coniugate.

Esercizio 21.3. Calcolare gli autovettori dell'applicazione lineare

$$f\colon \mathbb{R}^2 \to \mathbb{R}^2, \qquad f(x,y) = (x+y, x-2y).$$

Esercizio 21.4. Siano V e W spazi vettoriali. Siano U un sottospazio di W. Dimostrare che $\mathcal{L}(V,U)$ è un sottospazio di $\mathcal{L}(V,W)$. Sia U' un altro sottospazio di W, dimostrare che

$$\mathcal{L}(V, U \cap U') = \mathcal{L}(V,U) \cap \mathcal{L}(V,U')\,.$$

Esercizio 21.5. Sia $F : \mathbb{Q}(\sqrt{2}, \sqrt{3}) \longrightarrow \mathbb{Q}(\sqrt{2}, \sqrt{3})$ l'unico isomorfismo lineare tale che

$$\begin{aligned} &F(q) = q\,, \forall q \in \mathbb{Q}\,,\\ &F(\sqrt{2}) = -\sqrt{2}\,, \quad F(\sqrt{3}) = -\sqrt{3}\,,\\ &F(ab) = F(a)F(b)\,, \quad \forall a,\, b \in \mathbb{Q}(\sqrt{2}, \sqrt{3})\,. \end{aligned}$$

Calcolare $\det(F)$ e $tr(F)$.

Esercizio 21.6. Sia V lo spazio vettoriale dei polinomi di grado ≤ 3 a coefficienti in $\mathbb{R}$. Calcolare il determinante dell'applicazione lineare $F : V \longrightarrow V$ definita da
$$F(p(x)) = \frac{d^2p(x)}{d^2x} + 5\frac{dp(x)}{dx}\,.$$

Esercizio 21.7. Sia $A = (a_{ij})$ una matrice diagonale con $a_{ii} \neq a_{jj}$ per ogni $i \neq j$ e sia B una matrice tale che $AB = BA$. Dimostrare che esiste un polinomio $p(t)$ tale che $B = p(A)$. Cosa si può dire se sostituiamo A con una matrice ad essa coniugata?
(Sugg.: per un vecchio esercizio B deve essere diagonale. Vandermonde.)

Esercizio 21.8. Siano V spazio vettoriale di dimensione finita e $f_1, \ldots, f_n \in V^*$. Dimostrare che $f_1, \ldots, f_n$ sono linearmente indipendenti se e solo se l'applicazione
$$V \to \mathbb{K}^n, \qquad v \mapsto (f_1(v), \ldots, f_n(v))$$
è surgettiva.

Esercizio 21.9. Siano date due applicazioni lineari $F\colon V \to \mathbb{K}^n$, $G\colon V \to W$ tra spazi vettoriali di dimensione finita su $\mathbb{K}$. Dimostrare che le seguenti condizioni sono equivalenti:

(1) Esiste $H\colon W \to \mathbb{K}^n$ lineare tale che $HG = F$.
(2) $\ker G \subseteq \ker F$.
(3) $ImF^* \subseteq ImG^*$.

Esercizio 21.10. Siano n, m interi positivi fissati. Per ogni coppia di indici $i = 1, \ldots, n$, $j = 1, \ldots, m$ indichiamo con $E_{ij} \in M_{n,m}(\mathbb{K})$ la matrice con coefficiente 1 nella posizione i, j e coefficiente 0 altrove.

(1) Data $A = (a_{ij}) \in M_{m,n}(\mathbb{K})$, calcolare $tr(AE_{ij})$.
(2) Per ogni $A \in M_{m,n}(\mathbb{K})$ si consideri l'applicazione
$$\Phi_A\colon M_{n,m}(\mathbb{K}) \to \mathbb{K}, \qquad \Phi_A(B) = tr(AB).$$
Dimostrare che Φ_A è lineare.
(3) Dimostrare che l'applicazione
$$\Phi\colon M_{m,n}(\mathbb{K}) \to M_{n,m}(\mathbb{K})^*, \qquad A \mapsto \Phi_A,$$
è lineare ed iniettiva. Dedurre che Φ è un isomorfismo di spazi vettoriali.
(4) $(*)$ Dimostrare che per ogni coppia di spazi vettoriali di dimensione finita V, W esiste un isomorfismo naturale
$$\mathcal{L}(V, W)^* \simeq \mathcal{L}(W, V).$$

22. Polinomi in un endomorfismo

Sia V uno spazio vettoriale su $\mathbb{K}$. Si consideri una applicazione lineare
$$F : V \longrightarrow V\,.$$
Una tale applicazione si chiama anche un **endomorfismo** di V. Naturalmente ha senso considerare tutte le potenze di F:
$$F^k : V \longrightarrow V\,.$$

Si pone $F^0 = I$. Ha senso anche considerare le combinazioni lineari

$$a_0F^k + a_1F^{k-1} + a_2F^{k-2} + \cdots + a_{k-1}F + a_kI : V \longrightarrow V$$

Dunque, dato un qualsiasi polinomio $p(t) \in \mathbb{K}[t]$, ha senso considerare

$$p(F) : V \longrightarrow V\,.$$

Quindi, per ogni polinomio $p(t) \in \mathbb{K}[t]$, si ha

$$p(F) \in \mathcal{L}(V, V)\,.$$

Dal momento che

$$\dim \mathcal{L}(V, V) = (\dim V)^2\,,$$

non appena $k \geq (\dim V)^2$, i $k+1$ endomorfismi $I, F, F^2, \dots F^k$ sono linearmente dipendenti in $\mathcal{L}(V, V)$ e quindi esiste una relazione lineare non banale

$$a_0F^k + a_1F^{k-1} + a_2F^{k-2} + \cdots + a_{k-1}F + a_kI = 0\,, \qquad (a_0, \dots, a_k) \neq (0, \dots, 0)\,.$$

In altri temini esiste un polinomio $p(t) \in \mathbb{K}[t]$, $p(t) \neq 0$, tale che

$$p(F) = 0\,.$$

A meno di moltiplicare $p(t)$ per una costante diversa da 0, si può sempre assumere che un tale polinomio sia **monico**, e cioè che il coefficiente del suo termine di grado massimo sia uguale a 1:

$$p(t) = t^h + a_1t^{h-1} + \cdots + a_h$$

Tra tutti i polinomi monici (e quindi non nulli) che si annullano in F scegliamone uno di grado minimo. Un tale polinomio è unico perché se ce ne fossero due

$$p(t) = t^h + a_1t^{h-1} + \cdots + a_h\,, \qquad p'(t) = t^h + a'_1t^{h-1} + \cdots + a'_h\,,$$

posto

$$r(t) = p(t) - q(t) = ct^s + \dots, \qquad c \neq 0\,,$$

risulterebbe $s < h$ e il polinomio $r(t)/c$ sarebbe un polinomio monico di grado strettamente inferiore al grado di $p(t)$, che si annulla su F. Il che è assurdo a meno che non sia $p'(t) = p(t)$.
Denoteremo con $q_F(t)$ il polinomio monico di grado minimo che si annulla in F e lo chiameremo **polinomio minimo** di F. Osserviamo che, se $V \neq 0$, allora il polinomio minimo ha sempre grado maggiore di 0. Infatti l'unico polinomio monico di grado 0 è $p(t) = 1$ e quindi $p(F) = I \neq 0$.

Lemma 22.1. *Sia $p(t)$ un polinomio tale che $p(F) = 0$. Allora esiste un polinomio $f(t) \in \mathbb{K}[t]$ tale che $p(t) = q_F(t)f(t)$*

Dimostrazione. Per definizione, $\deg p(t) \geq \deg q_F(t)$. Quindi esistono polinomi $f(t)$ e $r(t)$ tali che $p(t) = f(t)q_F(t) + r(t)$ e $\deg r(t) < \deg q_A(t)$. Poiché

$$0 = p(F) = f(F)q_F(F) + r(F) = r(F)$$

si deve avere $r(t) = 0$, per la minimalità di $q_F(t)$. $\square$

23. Autovettori

Sia $F : V \to V$ una applicazione lineare. Un **autovettore** per F è un vettore *non nullo* $v \in V$ tale che

$$F(v) = \lambda v.$$

In questo caso si dice che λ è un **autovalore** di F.

Lemma 23.1. *Sia $F\colon V \to V$ un endomorfismo e sia $p(t) \in \mathbb{K}[t]$. Se $v \in V$ è un autovettore per F con autovalore λ, allora v è anche un autovettore per $p(F)$ con autovalore $p(\lambda)$.*

Dimostrazione. Se $F(v) = \lambda v$, allora

$$F^2(v) = F(F(v)) = F(\lambda v) = \lambda F(v) = \lambda^2 v.$$

Più in generale, si dimostra per induzione su k che $F^k(v) = \lambda^k v$: infatti

$$F^k(v) = F(F^{k-1}(v)) = F(\lambda^{k-1} v) = \lambda^{k-1} F(v) = \lambda^k v.$$

Quindi, se $p(t) = a_k t^k + \cdots + a_1 t + a_0$ si ha

$$p(F)(v) = a_k F^k(v) + \cdots + a_1 F(v) + a_0 v = (a_k \lambda^k + \cdots + a_1 \lambda + a_0)v = p(\lambda)v.$$

□

È utile dare una definizione equivalente di autovalore. Per ogni $\lambda \in \mathbb{K}$ definiamo

$$V_\lambda = \ker(F - \lambda I).$$

Notiamo che V_λ è un sottospazio vettoriale che dipende da λ e da F. Tuttavia, per semplicità notazionale, la dipendenza da F rimane sottointesa.
Siccome $v \in V_\lambda$ se e solo se $F(v) - \lambda v = 0$, si deduce immediatamente che λ è un autovettore se e solo se $V_\lambda \neq 0$.

Teorema 23.1. *Sia $F\colon V \to V$ un endomorfismo, sia $p(t) \in \mathbb{K}[t]$ e sia $\lambda \in \mathbb{K}$ un autovettore di F. Allora $p(F)(V_\lambda) \subseteq V_\lambda$ e vale una, ed una soltanto, delle seguenti due alternative:*

(1) *$p(\lambda) = 0$ e $p(F)(V_\lambda) = 0$.*
(2) *$p(\lambda) \neq 0$ e $p(F)\colon V_\lambda \to V_\lambda$ è iniettiva (e quindi un isomorfismo).*

Dimostrazione. Sia $v \in V_\lambda$, $v \neq 0$. Per il Lemma 23.1 si ha $p(F)(v) = p(\lambda)v \in V_\lambda$ e quindi $v \in \ker p(F)$ se e solo se $p(\lambda) = 0$. □

Corollario 23.2. *Sia $F\colon V \to V$ un endomorfismo e $p(t) \in \mathbb{K}[t]$ tale che $p(F) = 0$. Allora ogni autovalore di F è una radice di p.*

Dimostrazione. Sia λ è un autovalore. Siccome $p(F) = 0$, a maggior ragione $p(F)(V_\lambda) = 0$ e, per il Teorema 23.1, ne segue che $p(\lambda) = 0$. □

Corollario 23.3. *Gli autovalori di un endomorfismo F sono tutte e sole le radici in $\mathbb{K}$ del polinomio minimo $q_F(F)$.*

Dimostrazione. Che ogni autovalore è una radice segue dal corollario precedente. Viceversa, se $\lambda \in \mathbb{K}$ è una radice di $q_F(t)$, allora, per il teorema di Ruffini possiamo scrivere

$$q_F(t) = (t - \lambda)h(t),$$

con $\deg(h) = \deg(q_F) - 1$. Se λ non è un autovalore, allora l'applicazione lineare $F - \lambda I$ è iniettiva, quindi invertibile, e possiamo scrivere

$$h(F) = (F - \lambda I)^{-1} q_F(F) = 0,$$

in contraddizione con la minimalità del grado di q_F tra i polinomi che annullano F. $\square$

Esercizio 23.4. Sia $F\colon V \to V$ lineare e sia $\phi \in V^*$ un autovettore di F^*. Dimostrare che

$$F(\ker(\phi)) \subseteq \ker(\phi).$$

24. Il polinomio caratteristico

Definiamo ora il *polinomio caratteristico di F*. Il polinomio caratteristico di F è il polinomio $p_F(t)$ definito da:

$$p_F(t) = \det(tI - F)\,.$$

Che in effetti si tratti di un polinomio lo si vede nel modo che segue. Sia A la matrice di F in una base fissata. Si ha

$$p_F(t) = \det(tI - F) = \det(tI - A)\,.$$

dove nell'ultimo membro dell'eguaglianza, I denota la matrice identità. Chiaramente, se $n = \dim V$, si ha

$$p_A(t) = t^n + c_1 t^{n-1} + \cdots + c_0\,.$$

È immediato verificare che

$$c_1 = -tr(F)\,, \qquad c_0 = (-1)^n \det(F)\,.$$

Teorema 24.1. *Gli autovalori di F sono tutte e sole le radici di $p_F(t)$*

Dimostrazione. Si ha che λ è un autovalore di F se e solo se $(F - \lambda I)v = 0$ per un qualche vettore non nullo $v \in V$, ovvero se e solo se $\ker(F - \lambda I) \neq \{0\}$, ovvero se e solo se $\det(F - \lambda I) = 0$. Basta adesso osservare che

$$\det(F - \lambda I) = (-1)^n \det(\lambda I - F) = (-1)^n p_F(\lambda).$$

$\square$

Corollario 24.2. *(vero solo su $\mathbb{C}$) F ammette sempre un autovalore.*

Dimostrazione. Ogni polinomio non costante $p(t) \in \mathbb{C}[t]$ ammette una radice. Basta dunque prendere una radice di $p_F(t)$. $\square$

D'ora in poi assumiamo $\mathbb{K} = \mathbb{C}$. Scriviamo

$$p_F(t) = (t - \lambda_1)^{\nu_1} (t - \lambda_2)^{\nu_2} \cdots (t - \lambda_s)^{\nu_s}\,. \tag{8}$$

Si dice che ν_i è *la molteplicità algebrica di λ_i*.

Corollario 24.3. *(vero solo su $\mathbb{C}$) Ogni applicazione lineare $F : V \to V$ è triangolabile.*

Dire che una applicazione F è triangolabile vuol dire che si può trovare una base $v_1, \dots, v_n$ di V tale che:

$$F(v_i) \in L(v_1, \dots, v_i)\,, \quad \forall \quad i = 1, \dots, n\,.$$

Cosicché la matrice di F nella base $v_1, \dots, v_n$ è triangolare superiore.

Dimostrazione del Corollario 24.3. Procediamo per induzione sulla dimensione di V. Per il Corollario 24.2, esiste un autovettore v di F. Sia λ il corrispondente autovalore. Sia $U \subset V$ il sottospazio *proprio* definito da

$$U = Im(F - \lambda I)\,, \qquad \dim U < \dim V\,.$$

Si osservi che

$$F(U) \subset U\,.$$

Infatti se $u = (F - \lambda I)(w) \in U$, si ha:

$$F(u) = F(F - \lambda I)(w) = (F - \lambda I)F(w) \in Im(F - \lambda I) = U\,.$$

Dunque si può usare l'ipotesi induttiva alla restrizione $F_{|U}$ di F a U. Si può quindi trovare una base $u_1, \dots, u_m$ di U tale che

$$F_{|U}(u_i) = F(u_i) \in \mathcal{L}(u_1, \dots, u_i)\,, \quad \forall \quad i = 1, \dots, m\,.$$

Si completi ora la base $u_1, \dots, u_m$ di U a una base $u_1, \dots, u_m, v_1, \dots v_s$ di V. In questa base F è in forma triangolare. Infatti:

$$F(v_i) = F(v_i) - \lambda v_i + \lambda v_i = (F - \lambda)v_i + \lambda v_i \in U + \mathbb{C}v_i = L(u_1, \dots, u_m, v_i)\,.$$

□

Il seguente fondamentale teorema è vero per spazi vettoriali su campi arbitrari. Lo dimostreremo su $\mathbb{C}$ per poterci avvalere della triangolabilità delle matrici: ciò rende la dimostrazione più facile.

Teorema 24.4 (di Cayley Hamilton). *Sia $F : V \to V$ una applicazione lineare. Allora*

$$p_F(F) = 0\,.$$

Dimostrazione. Sia $v_1, \dots, v_n$ una base di V in cui l'applicazione lineare F abbia forma triangolare. Basta dimostrare che per ogni $i = 1, \dots, n$

$$p_F(F)v_i = 0\,.$$

Consideriamo l'espressione (8) di $p_F(t)$. Per definizione di base triangolare si ha

$$Fv_j = \lambda_j v_j + \sum_{s=1}^{j-1} c_s^{(j)} v_s\,. \tag{9}$$

Qui $\lambda_1, \dots, \lambda_n$ è la lista, con possibili ripetizioni, degli autovalori di F. Dimostriamo per induzione che

$$(F - \lambda_1 I) \cdots (F - \lambda_j I)v_j = 0\,.$$

Questo, ovviamente, implicherà che $p_F(F)v_i = 0$, per ogni $i = 1, \dots, n$. Il caso $j = 1$ non è che la (9) scritta per $j = 1$. Supponiamo dunque che

$$(F - \lambda_1 I) \cdots (F - \lambda_s I)v_s = 0 \quad s = 1, \dots, j - 1\,.$$

Usando l'ipotesi induttiva, si ha:

$$(F-\lambda_1 I)\cdots(F-\lambda_{j-1}I)(F-\lambda_j I)v_j = (F-\lambda_1 I)\cdots(F-\lambda_{j-1}I)\left(\sum_{s=1}^{j-1} c_s^{(j)} v_s\right) = 0\,.$$

□

Dal Lemma 22.1 e dal teorema di Cayley-Hamilton segue immediatamente il seguente:

COROLLARIO 24.5. *Sia $F : V \to V$ una applicazione lineare. Allora esiste un polinomio $f(t)$ tale che $p_F(t) = f(t)q_F(t)$.*

In particolare, con riferimento alla (8), si ha:

$$q_F(t) = (t-\lambda_1)^{\sigma_1}(t-\lambda_2)^{\sigma_1}\cdots(t-\lambda_s)^{\sigma_s}\,, \qquad \sigma_i \le \nu_i\,. \tag{10}$$

ESEMPIO 24.6. Si considerino le matrici

$$A = \begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix}, \qquad B = \begin{pmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \mu \end{pmatrix},$$

allora:

$$p_A(t) = (t-\lambda)^3\,, \qquad q_A(t) = (t-\lambda)^2\,,$$
$$p_B(t) = (t-\lambda)^2(t-\mu)\,, \qquad q_B(t) = (t-\lambda)(t-\mu)\,.$$

Una applicazione lineare $F : V \to V$ si dice *nilpotente* se $F^m = 0$, per qualche $m \ge 1$.

COROLLARIO 24.7. *Sia F una applicazione nilpotente. Allora*

$$F^{\dim V} = 0\,.$$

DIMOSTRAZIONE. Sia λ un autovalore di F. Si ha $F(v) = \lambda v$ per un vettore non nullo $v \in V$. Si ha $0 = F^m(v) = \lambda^m v$. Ne segue che $\lambda = 0$. In particolare:

$$p_F(t) = t^{\dim V}\,.$$

Per il teorema di Cayley-Hamilton si ha dunque $F^{\dim V} = 0$. □

Diamo di questo corollario una dimostrazione indipendente dal teorema di Cayley-Hamilton. Lo facciamo perché questa dimostrazione fa intervenire un lemma di per se stesso interessante.

LEMMA 24.8. *Sia $F : V \to V$ una applicazione lineare. Allora esiste $k \le \dim V$ tale che*

$$Ker(F^k) = Ker(F^{k+1}) = Ker(F^{k+2}) = \ldots$$
$$Im(F^k) = Im(F^{k+1}) = Im(F^{k+2}) = \ldots$$

DIMOSTRAZIONE. Si ha

$$Ker(F) \subseteq Ker(F^2) \subseteq Ker(F^3) \subseteq \cdots$$
$$Im(F) \supseteq Im(F^2) \supseteq Im(F^3) \supseteq \cdots$$

Sia $s = \dim KerF$. Se, nella catena dei nuclei, ad ogni passo si aumenta di dimensione, dopo al più $k = \dim V - s$ passi si arriva al punto in cui $\dim KerF^k = V$ e a quel punto la catena si stabilizza. Altrimenti, per un valore di $k \le \dim V$, deve accadere che $KerF^k = KerF^{k+1}$. Mostriamo che, allora, per ogni m, $KerF^{k+m} = KerF^{k+m+1}$. Infatti se $v \in KerF^{k+m+1}$, si ha

$$0 = F^{k+m+1}(v) = F^{k+1}F^m(v) = F^kF^m(v)$$

e quindi $v \in KerF^{k+m}$. Questo dimostra il Lemma per quello che riguarda i nuclei. Per quello che riguarda le immagini basta osservare che $\dim ImF^k = \dim V - \dim KerF^k$. □

Riimostriamo ora il Corollario 24.7 senza usare Cayley-Hamilton. Se $F^m = 0$, allora $KerF^m = V$ e dunque, per il Lemma, si ha $KerF^k = V$, per qualche $k \leq \dim V$. Questo vuol dire che $F^k = 0$, per qualche $k \leq \dim V$.

Un utile risultato è il seguente

PROPOSIZIONE 24.9. *Sia $F : V \to V$ una applicazione lineare. Sia $U \subset V$ un sottospazio di V tale che $F(U) \subseteq U$. Si consideri l'applicazione lineare $F_{|U} : U \to U$ ottenuta restringendo F al sottospazio U. Allora il polinomio caratteristico di $F_{|U}$ divide il polinomio caratteristico di F.*

$$p_F(t) = p_{F_{|U}}(t)f(t)\,.$$

DIMOSTRAZIONE. Sia $u_1, \dots, u_m$ una base di U e la si completi a una base $u_1, \dots, u_m, v_1, \dots, v_h$ di V. Poiché $F(U) \subseteq U$, la matrice di F in questa base è del tipo

$$A = \begin{pmatrix} B & C \\ 0 & D \end{pmatrix} \tag{11}$$

dove B è la matrice di $F_{|U}$ nella base $u_1, \dots, u_m$. Dunque:

$$p_F(t) = \det(tI - A) = \det(tI - B)\det(tI - D) = p_{F_{|U}}(t)\det(tI - D)\,.$$

□

ESERCIZIO 24.10. Dimostrare che nella matrice (11) si ha $C = 0$ se e solo se esiste un sottospazio $W \subset V$ tale che $U \cap W = \{0\}$, $U + W = V$ e $F(W) \subset W$.

25. Diagonalizzazione

Le considerazioni che seguono si svolgono nell'ambito dei numeri complessi. Sia $F : V \to V$ una applicazione lineare se ne consideri il polinomio caratteristico $p_F(t)$ e il polinomio minimo $q_F(t)$. Siano $\lambda_1, \dots, \lambda_s$ gli autovalori distinti di F. Con riferimento a (8) e (10), a ogni autovalore λ_i, $i = 1, \dots, s$, si associano due invarianti: la molteplicità algebrica di λ_i (e cioè la molteplicità ν_i di $t - \lambda_i$ in $p_F(t)$) e la molteplicità σ_i di $t - \lambda_i$ in $q_F(t)$. All'autovalore λ_i si associa un terzo invariante: *la molteplicita geometrica di* λ_i. Questa, per definizione, è la dimensione di $Ker(F - \lambda_i I)$. Si pone

$$V_{\lambda_i} = Ker(F - \lambda_i I)\,, \qquad \mu_i = \dim V_{\lambda_i}\,,$$

cosicché μ_i è la molteplicità geometrica di λ_i. Dimostriamo subito alcuni risultati riguardante i sottospazi V_{λ_i}.

Lemma 25.1. *Si consideri il sottospazio* $V_{\lambda_1}+\cdots+V_{\lambda_s}\subseteq V$*. Questo sottospazio in effetti si decompone in somma diretta:*

$$V_{\lambda_1}+\cdots+V_{\lambda_s}=V_{\lambda_1}\oplus\cdots\oplus V_{\lambda_s}\subseteq V$$

Dimostrazione. Bisogna dimostrare che ogni vettore $w\in V_{\lambda_1}+\cdots+V_{\lambda_s}$ si scrive in modo unico come somma di vettori in ciascun V_{λ_i}. Basta quindi verificare che se

$$w_1+\cdots+w_s=0\,,\qquad w_i\in V_{\lambda_i}\,,\quad i=1,\ldots,s\,,$$

allora $w_i=0$ per ogni $i=1,\ldots,s$. Questa asserzione è vera nel caso in cui $w_2=w_3=\cdots=w_s=0$. Procedendo per induzione, supponiamola vera per tutte le eguaglianze del tipo $w_1+\cdots+w_{j-1}=0$, dove j è un fissato indice minore o eguale a s. Sia data ora una eguaglianza del tipo

$$w_1+\cdots+w_j=0\,. \tag{12}$$

Si ha:

$$0=(F-\lambda_jI)(w_1+\cdots+w_j)=(\lambda_1-\lambda_j)w_1+\cdots+(\lambda_s-\lambda_{j-1})w_{j-1}\,.$$

Per induzione, si ha che $(\lambda_i-\lambda_j)w_i=0$, per ogni $i=1,\ldots,j-1$. Essendo $\lambda_i\neq\lambda_j$, per $i\neq j$, si ha che $w_i=0$, per ogni $i=1,\ldots,j-1$ e quindi, per la (12), anche $w_j=0$. □

Lemma 25.2. *Con le notazioni introdotte, si ha:*

$$\mu_i\le\nu_i\,,\qquad\forall\ i=1,\ldots,s.$$

Dimostrazione. Si consideri il sottospazio $V_{\lambda_i}\subseteq V$. Chiaramente $F(V_{\lambda_i})\subset V_{\lambda_i}$. Si può quindi applicare la Proposizione 24.9. Si ottiene

$$p_F(t)=p_{|V_{\lambda_i}}f(t)\,.$$

D'altro canto, il polinomio caratteristico della restrizione di F al sottospazio V_{λ_i} è uguale a $(t-\lambda_i)^{\dim V_{\lambda_i}}$ e cioè $(t-\lambda_i)^{\mu_i}$. Dunque $(t-\lambda_i)^{\mu_i}$ divide $p_F(t)$. Poiché

$$p_F(t)=(t-\lambda_1)^{\nu_1}(t-\lambda_2)^{\nu_2}\cdots(t-\lambda_s)^{\nu_s}$$

segue che $\mu_i\le\nu_i$. □

Diamo ora un primo criterio per la diagonalizzazione di una matrice.

Teorema 25.3. *Sia* $F:V\to V$ *una applicazione lineare. Sia*

$$p_F(t)=(t-\lambda_1)^{\nu_1}(t-\lambda_2)^{\nu_2}\cdots(t-\lambda_s)^{\nu_s}$$

Sia

$$\mu_i=\dim V_{\lambda_i}=\dim Ker(A-\lambda_iI)\,.$$

(Dunque, ν_i *è la molteplicità algebrica di* λ_i *e* μ_i *è la molteplicità geometrica di* λ_i*). Allora*

$$F\quad \text{è diagonalizzabile}\qquad\Longleftrightarrow\qquad \nu_i=\mu_i\,,\ \forall\ i=1,\ldots,s,$$

Dimostrazione. Evidentemente F è diagonalizzabile se e solo se

$$V=V_{\lambda_1}\oplus\cdots\oplus V_{\lambda_s}\,. \tag{13}$$

Per il Lemma 25.2, si ha $\dim V_{\lambda_i}=\mu_i\le\nu_i$, mentre, d'altra parte, $\nu_1+\cdots+\nu_s=\dim V$. Quindi la (13) vale se e solo se $\mu_i=\nu_i$, per $i=1,\ldots,s$. □

Vogliamo infine dare un criterio di diagonalizzazione in termini di polinomi minimi. Ci serve un lemma sui polinomi.

Lemma 25.4. *Siano $p_1(t), \dots, p_n(t)$ polinomi in $\mathbb{C}[t]$ privi di zeri comuni. Allora esistono polinomi $f_1(t), \dots, f_n(t)$ tali che*

$$f_1(t)p_1(t) + \cdots + f_n(t)p_n(t) = 1\,.$$

Dimostrazione. Si consideri il sottoinsieme $J \subset \mathbb{C}[t]$ definito da:

$$J = \{g(t) = h_1(t)p_1(t) + \cdots + h_n(t)p_n(t) \;:\; h_i(t) \in \mathbb{C}[t]\,, i = 1, \dots, n\}\,.$$

L'insieme J gode delle seguenti proprietà:
a) Se $h(t) \in J$, allora $-h(t) \in J$.
b) Se $h(t), k(t) \in J$, allora $h(t) + k(t) \in J$.
c) Se $h(t) \in J$ e $\alpha(t) \in \mathbb{C}[t]$ allora $\alpha(t)h(t) \in J$.
Sia ora $q(t) \in J \setminus \{0\}$ di grado minimo. Scriviamo

$$q(t) = f_1(t)p_1(t) + \cdots + f_n(t)p_n(t)\,.$$

Vogliamo dimostrare che $q(t)$ è un polinomio costante $q(t) = c \neq 0$. L'asserto seguirà dividendo i due membri della precedente eguaglianza per c. Supponiamo per assurdo che $q(t)$ non sia costante. Per ogni $i = 1, \dots, n$ si può scrivere

$$p_i(t) = q(t)f_i(t) + r_i(t)\,, \qquad \deg r_i(t) < \deg q(t)\,.$$

Poiché $p_i(t), q(t) \in J$, per le proprietà a), b) e c), si ha che $r(t) \in J$ contraddicendo la minimalità del grado di $q(t)$, a meno che non sia $r_i(t) = 0$. Ma allora $p_i(t) = q(t)f_i(t)$ e quindi un qualsiasi zero di $q(t)$, sarebbe uno zero comune ai $p_i(t)$, contro le ipotesi. □

Teorema 25.5. *Sia $F : V \to V$ una applicazione lineare.*

$$q_F(t) = (t - \lambda_1)^{\sigma_1}(t - \lambda_2)^{\sigma_2} \cdots (t - \lambda_s)^{\sigma_s}$$

il polinomio minimo di F. Allora:

$$F \quad \text{è diagonalizzabile} \quad \iff \quad \sigma_i = 1\,,\ \forall\ i = 1, \dots, s\,.$$

Dimostrazione. Supponiamo che F sia diagonalizzabile. Possiamo quindi assumere che, in una base opportuna, la matrice di F è una matrice diagonale. Scriveremo questa matrice diagonale nel modo seguente

$$\begin{pmatrix} \lambda_1 I_{\nu_1} & \dots & \dots & \dots \\ \dots & \lambda_2 I_{\nu_2} & \dots & \dots \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \lambda_s I_{\nu_s} \end{pmatrix}$$

dove, per $i = 1, \dots, s$ la matrice $\lambda_i I_{\nu_i}$ è la matrice diagonale $\nu_i \times \nu_i$ data da

$$\lambda_i I_{\nu_i} = \begin{pmatrix} \lambda_i & \dots & \dots & \dots \\ \dots & \lambda_i & \dots & \dots \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \lambda_i \end{pmatrix}\,.$$

Quindi

$$A - \lambda_1 I = \begin{pmatrix} 0 & \dots & \dots & \dots \\ \dots & (\lambda_2 - \lambda_1) I_{\nu_2} & \dots & \dots \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & (\lambda_s - \lambda_1) I_{\nu_s} \end{pmatrix}\,,$$

$$A - \lambda_2 I = \begin{pmatrix} (\lambda_1 - \lambda_2) I_{\nu_1} & \dots & \dots & \dots \\ \dots & 0 & \dots & \dots \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & (\lambda_s - \lambda_2) I_{\nu_s} \end{pmatrix} .$$

e così via. Ne segue che $(A - \lambda_1 I)(A - \lambda_2 I) \cdots (A - \lambda_s I) = 0$. Dunque, in virtù del Lemma 22.1, il polinomio minimo $q_A(t)$ divide $(t-\lambda_1)(t-\lambda_2)\cdots(t-\lambda_s)$. Da ciò e dal Corollario 23.3, si deduce che

$$q_A(t) = (t - \lambda_1)(t - \lambda_2) \cdots (t - \lambda_s) . \tag{14}$$

Viceversa supponiamo che $\sigma_i = 1$, per $i = 1, \dots, s$ e che dunque valga la (14). Dobbiamo dimostrare che

$$V = V_{\lambda_1} \oplus \cdots \oplus V_{\lambda_s} . \tag{15}$$

Definiamo

$$p_k(t) = \prod_{i : i \neq k}^{s} (t - \lambda_i)$$

Si osservi che

$$(t - \lambda_k) p_k(t) = q_F(t) . \tag{16}$$

In particolare si ha

$$(F - \lambda_k I) p_k(F) = q_F(F) = 0 . \tag{17}$$

I polinomi $p_1(t), \dots, p_s(t)$ non hanno zeri comuni. Quindi, per il Lemma 25.4, esistono polinomi $f_1(t), \dots, f_s(t)$ tali che

$$f_1(t) p_1(t) + \cdots + f_s(t) p_s(t) = 1 . \tag{18}$$

Per dimostrare la (15) consideriamo $v \in V$ e cerchiamo di scrivere v come somma di vettori appartenenti ai sottospazi V_{λ_i}. Per la (18), possiamo scrivere

$$v = f_1(F) p_1(F)(v) + \cdots + f_s(F) p_s(F)(v)$$

Basta quindi dimostrare che

$$f_k(F) p_k(F)(v) \in V_{\lambda_k} , \ k = 1, \dots, s ,$$

ma per questo basta far vedere che

$$F \left[f_k(F) p_k(F)(v) \right] = \lambda_k \left[f_k(F) p_k(F)(v) \right] ,$$

e cioè che

$$(F - \lambda_k I) \left[f_k(F) p_k(F)(v) \right] = 0 .$$

Usando l'osservazione (17), si ottiene

$$(F - \lambda_k I) f_k(F) p_k(F)(v) = f_k(F)(F - \lambda_k I) p_k(F)(v) = f_k(F)(0) = 0 .$$

$\square$

26. Polinomi in un endomorfismo (remix)

Definizione 26.1. Sia V uno spazio vettoriale su $\mathbb{K}$. Un **endomorfismo** di V è una qualsiasi applicazione lineare

$$F\colon V \longrightarrow V.$$

Ricordiamo che gli endomorfismi di V formano uno spazio vettoriale $\mathcal{L}(V,V)$ di dimensione $(\dim V)^2$. La composizione di due endomorfismi di V è ancora un endomorfismo di V. Se $F,G\colon V\to V$, chiameremo semplicemente *prodotto* il prodotto di composizione e scriveremo FG per indicare $F\circ G$, ossia $FG(v)=F(G(v))$ per ogni $v\in V$.

Naturalmente, sono endomorfismi tutte le potenze di F:

$$F^k : V \longrightarrow V\,.$$

Si pone per convenzione $F^0 = I$. Ha senso anche considerare le combinazioni lineari

$$a_0F^k + a_1F^{k-1} + a_2F^{k-2} + \cdots + a_{k-1}F + a_kI : V \longrightarrow V$$

Dunque, dato un qualsiasi polinomio

$$p(t)\in\mathbb{K}[t], \qquad p(t) = a_0 + a_1t + \cdots + a_nt^n,$$

ha senso considerare

$$p(F) : V \longrightarrow V, \qquad p(F) = a_0I + a_1F + \cdots + a_nF^n.$$

È importante osservare che l'applicazione

$$\mathbb{K}[t]\to\mathcal{L}(V,V), \qquad p(t)\mapsto p(F),$$

commuta con le operazioni di somma e prodotto. Cioè, per ogni coppia di polinomi $p,q\in\mathbb{K}[t]$ vale

$$(p+q)(F) = p(F)+q(F), \qquad pq(F) = p(F)q(F).$$

Dal momento che

$$\dim\mathcal{L}(V,V) = (\dim V)^2,$$

non appena $k\geq(\dim V)^2$, i $k+1$ endomorfismi $I,F,F^2,\dots F^k$ sono linearmente dipendenti in $\mathcal{L}(V,V)$ e quindi esiste una relazione lineare non banale

$$a_0F^k + a_1F^{k-1} + a_2F^{k-2} + \cdots + a_{k-1}F + a_kI = 0\,, \qquad (a_0,\dots,a_k)\neq(0,\dots,0)\,.$$

In altri temini esiste un polinomio $p(t)\in\mathbb{K}[t]$, $p(t)\neq 0$, tale che

$$p(F)=0\,.$$

A meno di moltiplicare $p(t)$ per una costante diversa da 0, si può sempre assumere che un tale polinomio sia **monico**, e cioè che il coefficiente del suo termine di grado massimo sia uguale a 1:

$$p(t) = t^h + a_1t^{h-1} + \cdots + a_.$$

Tra tutti i polinomi monici (e quindi non nulli) che si annullano in F scegliamone uno di grado minimo. Un tale polinomio è unico perché se ce ne fossero due

$$p(t) = t^h + a_1t^{h-1} + \cdots + a_h\,, \qquad p'(t) = t^h + a'_1t^{h-1} + \cdots + a'_h\,,$$

posto

$$r(t) = p(t) - q(t) = ct^s + \dots\,, \qquad c\neq 0\,,$$

risulterebbe $s < h$ e il polinomio $r(t)/c$ sarebbe un polinomio monico di grado strettamente inferiore al grado di $p(t)$, che si annulla su F. Il che è assurdo a meno che non sia $p'(t) = p(t)$.
Denoteremo con $q_F(t)$ il polinomio monico di grado minimo che si annulla in F e lo chiameremo **polinomio minimo** di F. Osserviamo che, se $V \neq 0$, allora il polinomio minimo ha sempre grado maggiore di 0. Infatti l'unico polinomio monico di grado 0 è $p(t) = 1$ e quindi $p(F) = I \neq 0$.

Lemma 26.2. *Sia $p(t)$ un polinomio tale che $p(F) = 0$. Allora il polinomio minimo $q_F(t)$ divide $p(t)$, cioè esiste un polinomio $f(t) \in \mathbb{K}[t]$ tale che $p(t) = q_F(t)f(t)$*

Dimostrazione. Sia $H \subset \mathbb{K}[t]$ l'insieme dei polinomi $p(t)$ che non sono divisibili per q_F e che annullano F:

$$H = \{p(t) \mid p(F) = 0,\ q_F(t)h(t) \neq p(t) \quad \forall\, h(t)\}.$$

Dobbiamo dimostrare che $H = \emptyset$. Osserviamo che il polinomio nullo è divisibile per q_F e quindi ogni $p \in H$ ha grado ≥ 0.
Supponiamo per assurdo $H \neq \emptyset$ e sia $r(t) \in H$ di grado minimo. Siccome $r(F) = 0$, si ha $\deg(r) \geq \deg(q_F)$, diciamo

$$r(t) = a_k t^k + \cdots + a_0, \qquad q_F(t) = t^h + \cdots + b_h, \quad k \geq h.$$

Il polinomio $s(t) = r(t) - a_k t^{k-h} q_F(t)$ ha grado minore di k e quindi non appartiene ad H. Siccome $s(F) = r(F) - a_k F^{k-h} q_F(F) = 0$ deve quindi esistere $h(t)$ tale che $s(t) = q_F(t)h(t)$ e quindi $r(t) = q_F(t)(h(t) + a_k t^{k-h})$, in contraddizione con la definizione di H. $\square$

Esercizio 26.3. Sia $a \in \mathbb{K}$. Calcolare il polinomio minimo di $F = aI$.

Esercizio 26.4. Sia F un endomorfismo tale che $F^2 = I$ e $F \neq \pm I$. Calcolare il polinomio minimo di F.

Esercizio 26.5. Siano $F, G\colon V \to V$ tali che $FG = GF$. Dimostrare che:
(1) Per ogni $h \geq 0$ vale $F^h G = G F^h$ (sugg.: induzione su h).
(2) Per ogni $h, k \geq 0$ vale $F^h G^k = G^k F^h$ (sugg.: induzione su k).
(3) Per ogni coppia di polinomi $p, q \in \mathbb{K}[t]$ vale $p(F)q(G) = q(G)p(F)$.

27. Autovettori (remix)

Sia $F : V \to V$ una applicazione lineare. Un **autovettore** per F è un vettore *non nullo* $v \in V$ tale che

$$F(v) = \lambda v.$$

per qualche $\lambda \in \mathbb{K}$. In questo caso si dice che λ è un **autovalore** di F.

Lemma 27.1. *Sia $F\colon V \to V$ un endomorfismo e $p(t) \in \mathbb{K}[t]$. Se $v \in V$ è un autovettore per F con autovalore λ, allora v è anche un autovettore per $p(F)$ con autovalore $p(\lambda)$.*

Dimostrazione. Se $F(v) = \lambda v$, allora

$$F^2(v) = F(F(v)) = F(\lambda v) = \lambda F(v) = \lambda^2 v.$$

Più in generale, si dimostra per induzione su k che $F^k(v) = \lambda^k v$: infatti

$$F^k(v) = F(F^{k-1}(v)) = F(\lambda^{k-1} v) = \lambda^{k-1} F(v) = \lambda^k v.$$

Quindi, se $p(t) = a_k t^k + \cdots + a_1 t + a_0$ si ha

$$p(F)(v) = a_k F^k(v) + \cdots + a_1 F(v) + a_0 v = (a_k \lambda^k + \cdots + a_1 \lambda + a_0) v = p(\lambda) v.$$

□

È utile dare una definizione equivalente di autovalore. Per ogni $\lambda \in \mathbb{K}$ definiamo

$$V_\lambda = \ker(F - \lambda I).$$

Notiamo che V_λ è un sottospazio vettoriale che dipende da λ e da F. Tuttavia, per semplicità notazionale, la dipendenza da F rimane sottointesa.
Siccome $v \in V_\lambda$ se e solo se $F(v) - \lambda v = 0$, si deduce immediatamente che λ è un autovalore per F se e solo se $V_\lambda \neq 0$.

Teorema 27.2. *Sia $F\colon V \to V$ un endomorfismo, $p(t) \in \mathbb{K}[t]$ e $\lambda \in \mathbb{K}$ un autovalore di F. Allora $p(F)(V_\lambda) \subseteq V_\lambda$ e vale una, ed una soltanto, delle seguenti due alternative:*

1. *$p(\lambda) = 0$ e $p(F)(V_\lambda) = 0$.*
2. *$p(\lambda) \neq 0$ e $p(F)\colon V_\lambda \to V_\lambda$ è iniettiva (e quindi un isomorfismo).*

Dimostrazione. Sia $v \in V_\lambda$, $v \neq 0$. Per il Lemma 27.1 si ha $p(F)(v) = p(\lambda) v \in V_\lambda$ e quindi $v \in \ker p(F)$ se e solo se $p(\lambda) = 0$. □

Corollario 27.3. *Sia $F\colon V \to V$ un endomorfismo e $p(t) \in \mathbb{K}[t]$ tale che $p(F) = 0$. Allora ogni autovalore di F è una radice di p.*

Dimostrazione. Sia λ è un autovalore. Siccome $p(F) = 0$, a maggior ragione $p(F)(V_\lambda) = 0$ e, per il Teorema 27.2, ne segue che $p(\lambda) = 0$. □

Corollario 27.4. *Gli autovalori di un endomorfismo F sono tutte e sole le radici in $\mathbb{K}$ del polinomio minimo $q_F(F)$.*

Dimostrazione. Che ogni autovalore è una radice segue dal corollario precedente. Viceversa, se $\lambda \in K$ è una radice di $q_F(t)$, allora, per il teorema di Ruffini possiamo scrivere

$$q_F(t) = (t - \lambda) h(t),$$

con $\deg(h) = \deg(q_F) - 1$. Se λ non è un autovalore, allora l'applicazione lineare $F - \lambda I$ è iniettiva, quindi invertibile, e possiamo scrivere

$$h(F) = (F - \lambda I)^{-1} q_F(F) = 0,$$

in contraddizione con la minimalità del grado di q_F tra i polinomi che annullano F. □

28. Il polinomio caratteristico (remix)

Definiamo ora il **polinomio caratteristico** di F. Il polinomio caratteristico di F è il polinomio $p_F(t)$ definito da:

$$p_F(t) = \det(F - tI)\,.$$

Che in effetti si tratti di un polinomio lo si vede nel modo che segue. Sia A la matrice di F in una base fissata. Allora, nella stessa base, $A - tI$ è la matrice di $F - tI$ per ogni $t \in \mathbb{K}$ e quindi

$$p_F(t) = p_A(t), \quad \text{dove} \quad p_A(t) = \det(A - tI).$$

Lemma 28.1. *Sia $A \in M_{n,n}(\mathbb{K})$. Allora*

$$p_A(t) = \det(A - tI) = (-1)^n t^n + c_1 t^{n-1} + \cdots + c_n$$

e valgono le uguaglianze

$$c_1 = (-1)^{n-1} tr(F)\,, \qquad c_n = \det(F)\,.$$

Dimostrazione. Segue immediatamente dalla definizione che $c_n = p_A(0) = \det(F - 0I) = \det(F)$. Denotando con a_{ij} e b_{ij} rispettivamente i coefficienti delle matrici A e $A - tI$, possiamo scrivere

$$\det(A - tI) = (a_{11} - t)\cdots(a_{nn} - t) + \sum_{\sigma \neq id} \varepsilon(\sigma) b_{1\sigma(1)} \cdots b_{n\sigma(n)},$$

dove la sommatoria è fatta su tutte le permutazioni σ di $\{1, \ldots, n\}$ diverse dall'identità.
Naturalmente, se $\sigma \neq id$, esistono almeno due indici i tali che $b_{i\sigma(i)}$ non contiene l'indeterminata t e quindi il prodotto $b_{1\sigma(1)} \cdots b_{n\sigma(n)}$ è un polinomio in t di grado minore od uguale a $n - 2$. Dunque i coefficienti di t^n e t^{n-1} in $p_A(t)$ coincidono con quelli di

$$(a_{11} - t)\cdots(a_{nn} - t) = (-1)^n t^n + (-1)^{n-1}(a_{11} + \cdots + a_{nn})t^{n-1} + \cdots\,.$$

□

Teorema 28.2. *Gli autovalori di F sono tutte e sole le radici di $p_F(t)$.*

Dimostrazione. Si ha che λ è un autovalore di F se e solo se $(F - \lambda I)v = 0$ per un qualche vettore non nullo $v \in V$, ovvero se e solo se $\ker(F - \lambda I) \neq \{0\}$, ovvero se e solo se $\det(F - \lambda I) = 0$. Basta adesso osservare che

$$\det(F - \lambda I) = p_F(\lambda).$$

□

Proposizione 28.3. *Sia $F : V \to V$ una applicazione lineare. Sia $U \subset V$ un sottospazio di V tale che $F(U) \subseteq U$. Si consideri l'applicazione lineare $F_{|U} : U \to U$ ottenuta restringendo F al sottospazio U. Allora il polinomio caratteristico di $F_{|U}$ divide il polinomio caratteristico di F:*

$$p_F(t) = p_{F_{|U}}(t) f(t)\,.$$

Dimostrazione. Sia $u_1, \ldots, u_m$ una base di U e la si completi a una base $u_1, \ldots, u_m, v_1, \ldots, v_h$ di V. Poiché $F(U) \subseteq U$, la matrice di F in questa base è del tipo

$$A = \begin{pmatrix} B & C \\ 0 & D \end{pmatrix}$$

dove B è la matrice di $F_{|U}$ nella base $u_1, \ldots, u_m$. Dunque

$$A - tI = \begin{pmatrix} B - tI & C \\ 0 & D - tI \end{pmatrix}$$

e quindi

$$p_F(t) = \det(A - tI) = \det(B - tI)\det(D - tI) = p_{F_{|U}}(t)\det(D - tI)\,.$$

□

Esempio 28.4. Dati n numeri $a_0, \ldots, a_{n-1} \in \mathbb{K}$, consideriamo la matrice (detta di Frobenius)

$$A = \begin{pmatrix} 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & \cdots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & a_{n-1} \end{pmatrix}$$

Il suo polinomio caratteristico si calcola facilmente con lo sviluppo di Laplace rispetto all'ultima colonna ed è uguale a

$$p_A(t) = (-1)^n \det(tI - A) = (-1)^n(t^n - a_{n-1}t^{n-1} - \cdots - a_1 t - a_0).$$

Ne deduciamo che ogni polinomio monico è, a meno del segno, uguale al polinomio caratteristico di una opportuna matrice.

Teorema 28.5 (Cayley Hamilton). *Sia $F : V \to V$ una applicazione lineare. Allora*

$$p_F(F) = 0\,.$$

Dimostrazione. Abbiamo già visto due dimostrazioni del teorema: una che utilizza lo sviluppo di Laplace e un'altra (su $\mathbb{K} = \mathbb{C}$) che utilizza l'esistenza di basi a ventaglio. Qui proponiamo una terza dimostrazione che utilizza gli stessi argomenti utilizzati nella dimostrazione della Proposizione 28.3.
Ragioniamo per induzione su $n = \dim V$; se $n = 0$ non c'è nulla da dimostrare. Supponiamo quindi $n > 0$ e consideriamo la famiglia di tutti i sottospazi $W \subset V$ tali che $U \neq V$ e $F(W) \subseteq W$. Da tale famiglia, che non è vuota poiché contiene il sottospazio $\{0\}$, scegliamo un sottospazio U della massima dimensione possibile: questa scelta implica in particolare che se W è un sottospazio tale che $U \subseteq W$ e $F(W) \subseteq W$, allora $W = U$ oppure $W = V$.
Denotiamo $r = n - \dim U$ e scegliamo una base $(u_{r+1}, u_{r+2}, \ldots, u_n)$ di U. Scegliamo poi un vettore $v \in V$ tale che $v \notin U$ e indichiamo con $d > 0$ il massimo intero tale che i vettori

$$v, F(v), \ldots, F^{d-1}(v), u_{r+1}, u_{r+2}, \ldots, u_n,$$

siano linearmente indipendenti. Questo significa che esistono, e sono unici, dei coefficienti $a_i, b_j \in \mathbb{K}$ tali che

$$F^d(v) = a_0 v + a_1 F(v) + \cdots + a_{d-1}F^{d-1}(v) + b_{r+1}u_{r+1} + \cdots + b_n u_n.$$

In particolare, se indichiamo con W il sottospazio vettoriale generato dai vettori $v, F(v), \ldots, F^{d-1}(v), u_{r+1}, u_{r+2}, \ldots, u_n$, si ha $F(W) \subseteq W$ e quindi, per quanto osservato precedentemente $W = V$ e $d = r$.

Nella base $v, F(v), \dots, F^{d-1}(v), u_{r+1}, u_{r+2}, \dots, u_n$, l'applicazione F si rappresenta con una matrice a blocchi

$$\begin{pmatrix} A & 0 \\ B & C \end{pmatrix}$$

dove C è la matrice che rappresenta la restrizione $F_{|U}$ nella base $u_{r+1}, u_{r+2}, \dots, u_n$ e

$$A = \begin{pmatrix} 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & \cdots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & a_{d-1} \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 0 & \cdots & 0 & b_{r+1} \\ 0 & 0 & \cdots & 0 & b_{r+2} \\ 0 & 0 & \cdots & 0 & b_{r+3} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & b_n \end{pmatrix}.$$

Per l'Esempio 28.4

$$p_A(t) = \pm(t^n - a_{n-1}t^{n-1} - \cdots - a_1 t - a_0)$$

e quindi

$$p_A(F)(v) = \pm(F^d(v) - a_0 v - a_1 F(v) - \cdots - a_{d-1}F^{d-1}(v)) \in U.$$

Siccome $F(U) \subseteq U$ si ha anche

$$p_A(F)(F^i(v)) = F^i(p_A(F)(v)) \in U$$

per ogni $i \geq 0$. Per ogni $i < d$ denotiamo $u_i = p_A(F)(F^i(v)) \in U$ Inoltre $p_F(t) = p_A(t)p_C(t)$; per l'ipotesi induttiva il teorema vale per la restrizione di F ad U e quindi $p_C(F)(u) = 0$ per ogni $u \in U$. Possiamo adesso dimostrare che i vettori della base $v, F(v), \dots, F^{d-1}(v), u_{r+1}, u_{r+2}, \dots, u_n$ appartengono al nucleo dell'applicazione lineare $p_F(F) = p_A(F)p_C(F)$. Infatti, per ogni $i > r$ vale

$$p_F(F)(u_i) = p_A(F)(p_C(F)u_i) = p_A(F)(0) = 0.$$

Per ogni $0 \leq i < d$ vale invece

$$p_F(F)(F^i v) = p_C(F)(p_A(F)(F^i v)) = p_C(F)(u_i) = 0.$$

□

Corollario 28.6. *Il polinomio minimo divide il polinomio caratteristico.*

Esercizio 28.7. Calcolare polinomio caratteristico, polinomio minimo, autovalori ed autovettori delle matrici (intese come endomorfismi di $\mathbb{C}^n$)

$$\begin{pmatrix} 4 & -5 \\ 2 & -3 \end{pmatrix}, \qquad \begin{pmatrix} 2 & 1 \\ -1 & 4 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 3 & 3 \\ -3 & -5 & -3 \\ 3 & 3 & 1 \end{pmatrix}.$$

Esercizio 28.8. Sia A una matrice reale $n \times n$. Calcolare la derivata in $t = 0$ della funzione $f(t) = \det(I + tA)$.

Esercizio 28.9. Sia $\dim V = n$ e $F \colon V \to V$ lineare di rango r. Dimostrare che t^{n-r} divide il polinomio caratteristico di F.

Esercizio 28.10. Indichiamo con $U_n \in M_{n,n}(\mathbb{K})$ la matrice che ha tutti i coefficienti uguali a 1. Calcolare i polinomi minimo e caratteristico di U_n (sugg.: calcolare U_n^2 ed utilizzare il risultato dell'Esercizio 28.9).

Esercizio 28.11. U_n come nell'esercizio precedente e $0_p \in M_{p,p}(\mathbb{K})$ la matrice nulla. Calcolare i polinomi minimo e caratteristico della matrice

$$\begin{pmatrix} U_n & 0 & U_n \\ 0 & 0_p & 0 \\ U_n & 0 & U_n \end{pmatrix} \in M_{2n+p,2n+p}(\mathbb{K}).$$

Esercizio 28.12. Sia $a \in \mathbb{K}$. Calcolare il determinante della matrice $n \times n$

$$A = (a_{ij}), \qquad a_{ij} = \begin{cases} 1 & \text{se } i \neq j, \\ a & \text{se } i = j. \end{cases}$$

29. La filtrazione dei nuclei

Lemma 29.1. *Sia $F\colon V \to V$ un endomorfismo lineare. Allora per ogni $h \geq 0$ vale*

$$\ker(F^h) \subseteq \ker(F^{h+1}), \qquad Im(F^{h+1}) \subseteq Im(F^h).$$

Inoltre si ha $\ker(F^h) = \ker(F^{h+1})$ *se e solo se* $Im(F^{h+1}) = Im(F^h)$.

Dimostrazione. Se $v \in \ker(F^h)$, allora $F^{h+1}(v) = F(F^h(v)) = F(0) = 0$ e quindi $v \in \ker(F^{h+1})$. Se $v \in Im(F^{h+1})$, allora esiste $u \in V$ tale che $v = F^{h+1}(u) = F^h(F(u))$ e quindi $v \in Im(F^h)$.
Poiché nucluo ed immagine sono sottospazi vettoriali di dimensione finita si ha

$$\ker(F^h) = \ker(F^{h+1}) \quad \text{se e solo se} \quad \dim\ker(F^h) = \dim\ker(F^{h+1}),$$

$$Im(F^{h+1}) = Im(F^h) \quad \text{se e solo se} \quad \dim Im(F^{h+1}) = \dim Im(F^h).$$

Infine per la formula delle dimensioni di nucleo ed immagine

$$\dim\ker(F^h) + \dim Im(F^h) = \dim\ker(F^{h+1}) + \dim Im(F^{h+1}).$$

□

Se V ha dimensione n, allora esiste un intero $h \leq n$ tale che $\dim\ker(F^h) = \dim\ker(F^{h+1})$.

Definizione 29.2. Data $F\colon V \to V$ siano

$$\sigma(F) = \min\{h \in \mathbb{Z} \mid h \geq 0,\ \ker(F^h) = \ker(F^{h+1})\},$$

$$Rad(F) = \ker(F^{\sigma(F)}).$$

Il sottospazio $Rad(F)$ viene detto **radicale** di F.

Si noti che $0 \leq \sigma(F) \leq n$ e $\sigma(F) = 0$ se e solo se F è invertibile.

Lemma 29.3. *Nelle notazioni precedenti, si ha* $\ker(F^h) = \ker(F^{h+1})$ *per ogni* $h \geq \sigma(F)$ *e* $v \in Rad(F)$ *se e solo se* $F^m(v) = 0$ *per qualche* $m \geq 1$.

Dimostrazione. Per provare entrambe le asserzioni è sufficicnte dimostrare per induzione su h che $\ker(F^{\sigma(F)+h}) \subseteq \ker(F^{\sigma(F)})$ per ogni $h > 0$: il caso $h = 1$ è vero per definizione di $\sigma(F)$. Sia dunque $v \in \ker(F^{\sigma(F)+h})$, allora $F(v) \in \ker(F^{\sigma(F)+h-1})$, per l'ipotesi induttiva $F(v) \in \ker(F^{\sigma(F)})$ e di conseguenza $v \in \ker(F^{\sigma(F)+1}) \subseteq \ker(F^{\sigma(F)})$. □

Una applicazione lineare $F : V \to V$ si dice **nilpotente** se $F^m = 0$, per qualche $m \geq 1$. Il più piccolo intero positivo s tale che $F^s = 0$ viene detto **indice di nilpotenza**. Osserviamo che F è nilpotente se e solo se $Rad(F) = V$.

Teorema 29.4. *Nelle notazioni precedenti, denotiamo con* $U = Rad(F) = \ker(F^{\sigma(F)})$ *e* $W = F^{\sigma(F)}(V)$*. Allora:*

(1) $F(U) \subseteq U$, $F(W) \subseteq W$.
(2) $F_{|W} \colon W \to W$ *è un isomorfismo.*
(3) $F_{|U} \colon U \to U$ *è nilpotente con indice di nilpotenza* $\sigma(F)$.
(4) $V = U \oplus W$.

Dimostrazione. Il primo punto è del tutto evidente. Per definizione di $\sigma(F)$ si ha $F(W) = F^{\sigma(F)+1}(V) = F^{\sigma(F)}(V) = W$. Ne segue che l'applicazione $F_{|W} \colon W \to W$ è surgettiva e quindi anche un isomorfismo. Per ogni $h \geq 0$ vale

$$\ker(F^h_{|U}) = \ker(F^h) \cap U, \qquad \ker(F^h_{|W}) = \ker(F^h) \cap W.$$

da cui segue che $\ker(F^h_{|U}) = U$ se e solo se $h \geq \sigma(F)$ e $U \cap W = \ker(F^\sigma_{|W}) = 0$. Dalla formula di Grassmann $\dim(U \oplus W) = n$ e quindi $V = U \oplus W$. □

Esercizio 29.5. Mostrare con un esempio che in generale $V \neq \ker(F) \oplus F(V)$.

30. Struttura delle applicazioni nilpotenti

Lemma 30.1. *Sia* $F \colon V \to V$ *un'applicazione nilpotente. Allora esiste una base* $(v_1, \dots, v_n)$ *di* V *in cui* F *si rappresenta con una matrice triangolare strettamente superiore (triangolare superiore con diagonale principale nulla).*

Dimostrazione. Sia $W = F(V)$ l'immagine di F; siccome $\dim W < \dim V$ e $F_{|W} \colon W \to W$ è ancora nilpotente, per induzione sulla dimensione possiamo trovare una base $v_1, \dots, v_r$ di W nella quale $F_{|W}$ si rappresenta con una matrice (a_{ij}) triagolare strettamente superiore: $a_{ij} = 0$ per ogni $i \geq j$.
Estendiamo $v_1, \dots, v_r$ ad una base $v_1, \dots, v_r, v_{r+1}, \dots, v_n$ di V. Per ogni j, $F(v_j) \in W$ e quindi $F(v_j)$ si scrive come combinazione lineare dei primi r vettori della base:

$$F(v_j) = \sum_{i=1}^r a_{ij} v_i \quad \text{per} \quad j \leq r; \qquad F(v_j) = \sum_{i=1}^r b_{ij} v_i \quad \text{per} \quad j > r.$$

La matrice che rappresenta F nella base $(v_1, \dots, v_n)$ è quindi una matrice a blocchi

$$\begin{pmatrix} (a_{ij}) & (b_{ij}) \\ 0 & 0 \end{pmatrix}, \qquad (b_{ij}) \in M_{r,n-r}(\mathbb{K}).$$

che è triangolare superiore con diagonale principale nulla. □

Proposizione 30.2. *Sia* $\dim V = n$ *e* $F \colon V \to V$ *nilpotente di indice* σ*. Allora vale:*

$$p_F(t) = \pm t^n, \qquad q_F(t) = t^\sigma, \qquad \sigma \dim(\ker(F)) \geq n.$$

Dimostrazione. In una opportuna base l'applicazione F si rappresenta con una matrice A triangolare superiore con diagonale principale nulla e quindi $\det(tI - A) = t^n$. Per il teorema di Cayley-Hamilton il polinomio minimo divide il polinomio caratteristico e quindi $q_F(t)$ deve necessariamente essere del tipo t^h con $1 \leq h \leq n$. Siccome $F^h = 0$ se e solo se $h \geq \sigma$ ne segue che $q_F(t) = t^\sigma$.
Per ogni intero $i \geq 0$ definiamo

$$A_i = \ker(F) \cap F^i(V), \qquad \alpha_i = \operatorname{rank}(F^i) - \operatorname{rank}(F^{i+1}).$$

Chiaramente $\alpha_h = 0$ per ogni $h \geq \sigma$ e

$$\alpha_0 + \alpha_1 + \cdots + \alpha_{\sigma-1} = \operatorname{rank}(F^0) = n.$$

Siccome l'applicazione

$$F\colon F^i(V) \to F^{i+1}(V)$$

è surgettiva ed ha come nucleo A_i, ne segue che $\alpha_i = \dim A_i$. Dato che

$$A_0 \supseteq A_1 \supseteq \cdots \supseteq A_{\sigma-1},$$

si ha $\alpha_0 \geq \alpha_1 \geq \cdots \geq \alpha_{\sigma-1}$ e quindi

$$n = \alpha_0 + \alpha_1 + \cdots + \alpha_{\sigma-1} \leq \sigma\alpha_0 = \sigma \dim(\ker(F)).$$

□

Esercizio 30.3. Sia $F\colon V \to V$ nilpotente. Dimostrare che $I - F$ è invertibile (sugg.: a cosa è uguale $(I - F)(I + F + F^2 + \cdots + F^n)$?).

Esercizio 30.4. Sia $F\colon V \to V$ nilpotente. Dimostrare che $I + F + F^2$ è invertibile.

Esercizio 30.5. Sia $F\colon V \to V$ nilpotente. Dimostrare che per ogni $a, b \in V$ esistono due vettori $x, y \in V$ tali che

$$Fx + x + y = a, \quad Fy + y - x = b.$$

Esercizio 30.6. Sia $\dim V = n$ e $F\colon V \to V$ nilpotente di indice σ. Sia $v \in V$ un vettore tale che $F^{\sigma-1}(v) \neq 0$. Dimostrare che il sottospazio

$$U = L(v, F(v), \ldots, F^{\sigma-1}(v))$$

è F-invariante (cioè $F(U) \subseteq U$) e di dimensione σ. Calcolare inoltre le dimensioni di $U \cap \ker F^i$ e $U \cap F^i(V)$ per ogni i.

Esercizio 30.7. Sia $\dim V = n$ e $F\colon V \to V$ nilpotente di indice σ. Dimostrare che $\sigma = n$ se e solo se esiste una base in cui F si rappresenta con la matrice

$$A = (a_{ij}), \qquad a_{ij} = \begin{cases} 1 & \text{se } \ i = j + 1, \\ 0 & \text{altrimenti.} \end{cases}$$

31. Molteplicità algebrica e geometrica di un autovalore

Sia $\lambda \in \mathbb{K}$ un autovalore di un endomorfismo $F : V \to V$. Abbiamo già osservato che λ è radice sia del polinomio minimo $q_F(t)$ che del polinomio caratteristico $p_F(t)$. Vogliamo associare a λ tre interi positivi che chiameremo *molteplicità algebrica, molteplicità geometrica e indice.*
La **molteplicità geometrica** μ di λ è per definizione la dimensione del nucleo di $F - \lambda I$:

$$\mu_\lambda = \dim \ker(F - \lambda I) = \dim V_\lambda.$$

Definiamo poi

$$\sigma_\lambda = \min\{h \in \mathbb{Z} \mid h \geq 0,\ \operatorname{rank}(F - \lambda I)^h = \operatorname{rank}(F - \lambda I)^{h+1}\},$$

$$\nu_\lambda = \dim Rad(F - \lambda I) = n - \operatorname{rank}(F - \lambda I)^h, \quad \forall\, h \geq \sigma_\lambda.$$

Chiameremo ν_λ **molteplicità algebrica** e σ_λ **indice** dell'autovalore λ. Poiché σ_λ coincide con l'indice di nilpotenza della restrizione di $F - \lambda I$ al proprio radicale, segue dalla Proposizione 30.2 che

$$\mu_\lambda \leq \nu_\lambda, \qquad \sigma_\lambda \leq \nu_\lambda, \qquad \nu_\lambda \leq \sigma_\lambda \mu_\lambda.$$

Segue immediatamente dalle definizioni che $\mu_\lambda = \nu_\lambda$ se e solo se $\sigma_\lambda = 1$. Segue invece dall'Esercizio 30.7 che se $\sigma_\lambda = \nu_\lambda$ allora $\mu_\lambda = 1$.

Teorema 31.1. *Nelle notazioni precedenti, l'indice e la molteplicità algebrica di λ sono uguali alle molteplicità di λ come radice dei polinomi minimo e caratteristico rispettivamente. In altri termini si ha*

$$q_F(t) = (t - \lambda)^{\sigma_\lambda} \hat{q}(t), \qquad \textit{con} \quad \hat{q}(\lambda) \neq 0,$$
$$p_F(t) = (t - \lambda)^{\nu_\lambda} \hat{p}(t), \qquad \textit{con} \quad \hat{p}(\lambda) \neq 0.$$

Dimostrazione. Per semplicità notazionale indichiamo $\nu = \nu_\lambda$, $\sigma = \sigma_\lambda$ e $\mu = \mu_\lambda$. A meno di sostituire $F - \lambda I$ con F non è restrittivo supporre $\lambda = 0$. Consideriamo la decomposizione in somma diretta $V = U \oplus W$ data dal Teorema 29.4: $U = \ker(F^\sigma)$, $W = F^\sigma(V)$.
La restrizione di F al sottospazio U è nilpotente di indice σ e quindi

$$p_{F_{|U}}(t) = t^\nu, \qquad q_{F_{|U}}(t) = t^\sigma.$$

La restrizione di F al sottospazio W è invertibile, quindi 0 non è un autovalore di $F_{|W}$ e

$$p_{F_{|W}}(0) \neq 0, \qquad q_{F_{|W}}(0) \neq 0.$$

Dato che $p_F(t) = p_{F_{|U}}(t) p_{F_{|W}}(t) = t^\nu p_{F_{|W}}(t)$ ne segue che $t = 0$ è una radice di molteplicità ν del polinomio caratteristico.
Il prodotto dei polinomi minimi delle restrizioni di F ai sottospazi U, W annula F e quindi

$$q_F(t) | q_{F_{|U}}(t) q_{F_{|W}}(t) = q_{F_{|W}}(t) t^\sigma.$$

D'altra parte, se prendiamo un vettore $v \in U = \ker F^\sigma$ tale che $F^{\sigma-1}(v) = u \neq 0$ si ha che u è un autovettore di F con autovalore 0 e quindi

$$q_{F_{|W}}(F) F^{\sigma-1}(v) = q_{F_{|W}}(F) u = q_{F_{|W}}(0) u \neq 0.$$

Dunque il polinomio minimo $q_F(t)$ non divide il prodotto $q_{F_{|W}}(t) t^{\sigma-1}$ e questo implica che $t = 0$ è una radice di molteplicità σ del polinomio minimo. $\square$

Esercizio 31.2. Calcolare i polinomi minimo e caratteristico delle seguenti matrici:

$$\begin{pmatrix} 2 & -2 & 1 \\ 1 & 1 & -1 \\ 1 & 2 & -2 \end{pmatrix}, \qquad \begin{pmatrix} 2 & 1 & -4 \\ 0 & 3 & 0 \\ 1 & 2 & -2 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 1 & 1 \\ 2 & 1 & 2 \\ 1 & 1 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 2 & 2 \\ 1 & 1 & 1 \\ 0 & -2 & -2 \end{pmatrix}.$$

32. Diagonalizzazione (remix)

Lemma 32.1. *Siano $\lambda_1, \dots, \lambda_s$ autovalori distinti di un endomorfismo F e si considerino i sottospazi $V_{\lambda_i} = \ker(F - \lambda_i I)$. Allora esiste una decomposizione in somma diretta:*

$$V_{\lambda_1} + \cdots + V_{\lambda_s} = V_{\lambda_1} \oplus \cdots \oplus V_{\lambda_s} \subseteq V.$$

Dimostrazione. Bisogna dimostrare che ogni vettore $w \in V_{\lambda_1} + \cdots + V_{\lambda_s}$ si scrive in modo unico come somma di vettori in ciascun V_{λ_i}. Basta quindi verificare che se

$$w_1 + \cdots + w_s = 0\,, \qquad w_i \in V_{\lambda_i}\,, \quad i = 1, \dots, s\,,$$

allora $w_i = 0$ per ogni $i = 1, \dots, s$. Applicando F otteniamo

$$0 = F(0) = \lambda_1 w_1 + \cdots + \lambda_s w_s.$$

Più in generae per ogni $h = 0, \dots, s-1$ vale

$$0 = F^h(0) = \lambda_1^h w_1 + \cdots + \lambda_s^h w_s.$$

Possiamo riscrivere tali eguaglianze in forma di prodotto riga per colonne

$$(w_1, \dots, w_s) \begin{pmatrix} 1 & \lambda_1 & \cdots & \lambda_1^{s-1} \\ 1 & \lambda_2 & \cdots & \lambda_2^{s-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \lambda_s & \cdots & \lambda_s^{s-1} \end{pmatrix} = (0, \dots, 0).$$

Siccome gli autovalori λ_i sono distinti, la matrice di Vandermonde è invertibile e quindi $(w_1, \dots, w_s) = (0, \dots, 0)$. □

Un endomorfismo F si dice **diagonalizzabile** se esiste una base rispetto alla quale F si rappresenta con una matrice diagonale. Equivalentemente $F\colon V \to V$ è diagonalizzabile se e solo se esiste una base di V fatta con autovettori per F.

Teorema 32.2. *Sia $\dim V = n$ e siano $\lambda_1, \dots, \lambda_s \in \mathbb{K}$ gli autovalori di un endomorfismo $F : V \to V$. Se indichiamo con μ_i la molteplicità geometrica di λ_i, allora F è diagonalizzabile se e soltanto se*

$$\mu_1 + \cdots + \mu_s = n.$$

Dimostrazione. Per il lemma precedente la somma dei sottospazi V_{λ_i} è diretta e quindi $V_{\lambda_1} \oplus \cdots \oplus V_{\lambda_s}$ ha dimensione $\mu_1 + \cdots + \mu_s$. Basta osservare che F è diagonalizzabile se e solo se

$$V = V_{\lambda_1} \oplus \cdots \oplus V_{\lambda_s}$$

□

Corollario 32.3. *Sia*

$$p_F(t) = \pm(t-\lambda_1)^{\nu_1}(t-\lambda_2)^{\nu_2}\cdots(t-\lambda_s)^{\nu_s}, \qquad \lambda_1,\ldots,\lambda_s \in \mathbb{K},\ \lambda_i \neq \lambda_j,$$

il polinomio caratteristico di un endomorfismo $F\colon V \to V$. *Allora* F *è diagonalizzabile se e solo se per ogni* i *vale* $\nu_i = \dim\ker(F-\lambda_i I)$.

Dimostrazione. Valgono sempre le diseguaglianze $\nu_i \geq \dim\ker(F-\lambda_i I)$ e l'uguaglianza $\nu_1+\cdots+\nu_s = \deg p_F = \dim V$. □

Corollario 32.4. *Sia*

$$p_F(t) = \pm(t-\lambda_1)^{\nu_1}(t-\lambda_2)^{\nu_2}\cdots(t-\lambda_s)^{\nu_s}, \qquad \lambda_1,\ldots,\lambda_s \in \mathbb{K},\ \lambda_i \neq \lambda_j,$$

il polinomio caratteristico di un endomorfismo $F\colon V \to V$. *Se* $\nu_i = 1$ *per ogni* i, *allora* F *è diagonalizzabile.*

Dimostrazione. Evidente. □

Corollario 32.5. *Sia*

$$q_F(t) = (t-\lambda_1)^{\sigma_1}(t-\lambda_2)^{\sigma_2}\cdots(t-\lambda_s)^{\sigma_s}, \qquad \lambda_1,\ldots,\lambda_s \in \mathbb{K},\ \lambda_i \neq \lambda_j,$$

il polinomio minimo di un endomorfismo $F\colon V \to V$. *Allora* F *è diagonalizzabile se e solo se per ogni* i *vale* $\sigma_i = 1$.

Dimostrazione. Per il Teorema 31.1, σ_i è uguale all'indice dell'autovalore λ_i. Sappiamo inoltre che l'indice di un autovalore è uguale a 1 se e solo se la molteplicità algebrica è uguale a quella geometrica. □

Esercizio 32.6. Tra le matrici dell'Esercizio 31.2, dire quali sono diagonalizzabili.

Esercizio 32.7. Sia F un endomorfismo tale che $F^2 = F$. Dimostrare che F è diagonalizzabile.

Esercizio 32.8. Sia F un endomorfismo tale che $F^2 = I$. Dimostrare che F è diagonalizzabile.

Esercizio 32.9. Mostrare che due matrici diagonalizzabili sono simili (coniugate) se e solo se hanno lo stesso polinomio caratteristico.

Esercizio 32.10. Trovare due matrici 4×4 nilpotenti dello stesso indice che non sono simili.

Esercizio 32.11. Sia I_n la matrice identità $n\times n$. Determinare i polinomi minimo e caratteristico della matrice

$$\begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix} \in M_{2n,2n}(\mathbb{K}).$$

Esercizio 32.12. Sia $A \in M_{n,n}(\mathbb{R})$ una matrice tale che $A^2+I=0$. Dimostrare che la traccia di A è uguale a 0 e che n è pari. (Sugg.: considerare A come una matrice a coefficienti complessi e determinare una relazione tra la traccia di A e le molteplicità geometriche degli autovalori.)

33. Variazioni su di un classico di algebra lineare

Questa sezione è divisa in varie sottosezioni, ognuna delle quali contiene una diversa dimostrazione del seguente celebre risultato:

Proposizione 33.1. *Sia V una spazio vettoriale su $\mathbb{C}$ di dimensione n e $F\colon V \to V$ un endomorfismo lineare. Allora F è nilpotente se e solo se* $\operatorname{trace}(F^k) = 0$ *per ogni $k = 1, \dots, n$.*

Prima dimostrazione: Vandermonde.

Ricordiamo che, dati un campo $\mathbb{K}$ e $x_1, \dots, x_n \in \mathbb{K}$ si ha

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_0 & x_1 & \cdots & x_n \\ \vdots & \vdots & \ddots & \vdots \\ x_0^{n-1} & x_1^{n-1} & \cdots & x_n^{n-1} \\ x_0^n & x_1^n & \cdots & x_n^n \end{vmatrix} = \prod_{i>j}(x_i - x_j)$$

e di conseguenza la matrice di Vandermonde

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ x_0 & x_1 & \cdots & x_n \\ \vdots & \vdots & \ddots & \vdots \\ x_0^{n-1} & x_1^{n-1} & \cdots & x_n^{n-1} \\ x_0^n & x_1^n & \cdots & x_n^n \end{pmatrix} \tag{19}$$

è **invertibile se e soltanto se** $x_i \neq x_j$ **per ogni** $i \neq j$.

Vediamo adesso alcune applicazioni di questo fatto.

Lemma 33.2. *Siano $x_1, \dots, x_n \in \mathbb{K}$ distinti e* diversi da 0. *Allora la matrice*

$$\begin{pmatrix} x_1 & \cdots & x_n \\ \vdots & \ddots & \vdots \\ x_1^{n-1} & \cdots & x_n^{n-1} \\ x_1^n & \cdots & x_n^n \end{pmatrix}$$

è invertibile.

Dimostrazione. Dividendo la prima colonna per x_1, la seconda per x_2 eccetera, si ottiene

$$\begin{vmatrix} x_1 & \cdots & x_n \\ \vdots & \ddots & \vdots \\ x_1^{n-1} & \cdots & x_n^{n-1} \\ x_1^n & \cdots & x_n^n \end{vmatrix} = x_1 \cdots x_n \cdot \begin{vmatrix} 1 & \cdots & 1 \\ x_1 & \cdots & x_n \\ \vdots & \ddots & \vdots \\ x_1^{n-1} & \cdots & x_n^{n-1} \end{vmatrix} \neq 0$$

□

Teorema 33.3. *Siano $x_1, \dots, x_n \in \mathbb{C}$ numeri complessi tali che*

$$x_1^k + x_2^k + \cdots + x_n^k = 0 \quad \textit{per ogni} \quad k = 1, \dots, n.$$

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

Dimostrazione. A meno di riordinare gli indici possiamo trovare un intero $0 \leq s \leq n$ tale che

$$x_i \neq 0 \quad \text{per} \quad i \leq s, \qquad x_{s+1} = x_{s+2} = \cdots = x_n = 0\,;$$

supponiamo $s > 0$ e mostriamo che tale ipotesi conduce ad una contraddizione. Siccome $s \leq n$, si ha

$$x_1^k + x_2^k + \cdots + x_s^k = 0 \quad \text{per ogni} \quad k = 1, \ldots, s.$$

Supponiamo che i numeri $x_1, \ldots, x_s$ assumano r valori distinti $y_1, \ldots, y_r$, con $1 \leq r \leq s$: allora, per ogni $k = 1, \ldots, r$ vale

$$0 = x_1^k + x_2^k + \cdots + x_s^k = a_1 y_1^k + \cdots + a_r y_r^k,$$

dove $a_i \in \mathbb{N}$ denota quanti sono gli x_j uguali a y_i. Possiamo riscrivere tali uguaglianze in forma di prodotto righe per colonne

$$\begin{pmatrix} y_1 & \cdots & y_r \\ \vdots & \ddots & \vdots \\ y_1^{r-1} & \cdots & y_r^{r-1} \\ y_1^r & \cdots & y_r^r \end{pmatrix} \begin{pmatrix} a_1 \\ \vdots \\ a_{r-1} \\ a_r \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}$$

e ci troviamo in contradizione con il lemma precedente. □

Dimostrazione della Proposizione 33.1. In una base opportuna l'applicazione F è rappresentata da una matrice triangolare superiore A; è immediato osservare che A è nilpotente se e solo se i coefficienti a_{ii} della diagonale principale sono tutti nulli e che

$$\text{trace}(F^k) = \text{trace}(A^k) = \sum_{i=1}^{n} a_{ii}^k.$$

□

Seconda dimostrazione: induzione sulla dimensione.

Lemma 33.4. *Sia $F\colon V \to V$ un endomorfismo e sia $U \subseteq$ un sottospazio vettoriale tale che $F(V) \subseteq U$. Allora $F(U) \subseteq U$ e vale*

$$\text{trace}(F) = \text{trace}(F_{|U}).$$

Dimostrazione. Sia $(v_1, \ldots, v_r)$ una base di U; estendiamola ad una base $(v_1, \ldots, v_n)$ di V. Sia A la matrice che rappresenta F in tale base, se $A = (a_{ij})$, $1 \leq i, j \leq n$, allora $\tilde{A} = (a_{ij})$, $1 \leq i, j \leq r$, rappresenta $F_{|U}$ nella base $(v_1, \ldots, v_r)$ e $a_{ij} = 0$ per ogni $i > r$. Ne segue che

$$\text{trace}(F) = \text{trace}(A) = \sum_{i=1}^{n} a_{ii} = \sum_{i=1}^{r} a_{ii} = \text{trace}(\tilde{A}) = \text{trace}(F_{|U}).$$

□

Lemma 33.5. *Sia V uno spazio vettoriale su $\mathbb{C}$ di dimensione $n > 0$ e $F\colon V \to V$ un endomorfismo lineare. Se $\text{trace}(F^k) = 0$ per ogni $k = 1, \ldots, n$, allora F non è invertibile.*

Dimostrazione. Per il teorema di Cayley-Hamilton esistono dei coefficienti $a_1, \dots, a_n \in \mathbb{C}$ tali che

$$p_F(F) = \det(F)I + \sum_{i=1}^{n} a_i F^i = 0.$$

Prendendo la traccia di tale equazione si ricava

$$\det(F)\operatorname{trace}(I) + \sum_{i=1}^{n} a_i \operatorname{trace}(F^i) = \det(F)n = 0.$$

□

Dimostrazione della Proposizione 33.1. Dimostriamo l'enunciato per induzione su n. Per $n = 1$ il risultato è ovvio. Supponiamo quindi $n > 1$ ed il risultato vero per ogni spazio di dimensione minore di n.
Se F è nilpotente, allora $U = F(V)$ è un sottospazio proprio e quindi, per l'ipotesi induttiva ed il lemma precedente

$$\operatorname{trace}(F^k) = \operatorname{trace}(F^k_{|U}) = 0$$

per ogni $k \leq \dim U$. D'altra parte per Cayley-Hamilton $F^{\dim U}(U) = 0$ e quindi $F^h = 0$ per ogni $h > \dim U$.
Supponiamo viceversa che $\operatorname{trace}(F^k) = 0$ per ogni $k = 1, \dots, n$; abbiamo visto che F non è invertibile e quindi $U = F(V)$ è un sottospazio proprio. Dunque

$$\operatorname{trace}(F^k) = \operatorname{trace}(F^k_{|U}) = 0$$

e per l'ipotesi induttiva $F_{|U}$ è nilpotente. Chiaramente se $F^h_{|U} = 0$ allora $F^{h+1} = 0$. □

Osservazione 33.6. Consideriamo n numeri complessi $x_1, \dots, x_n$ e, per ogni $k \geq 0$ denotiamo con $\psi_k = x_1^k + \cdots + x_n^k$ la somma delle potenze k-esime. Denotiamo inoltre con $\sigma_1, \dots, \sigma_n$ i coefficienti del polinomio monico che ha $x_1, \dots, x_n$ come radici:

$$\prod_{i=1}^{n}(t - x_i) = t^n + \sigma_1 t^{n-1} + \cdots + \sigma_n.$$

Si può dimostrare che ogni ψ_i si può esprimere con un polinomio a coefficienti *interi* (Esercizio 33.7) nelle variabili σ_i e, viceversa, che ogni σ_i si può esprimere con un polinomio a coefficienti *razionali* nelle variabili $\psi_1, \dots, \psi_n$.
Per il calcolo esplicito di tali polinomi, supponiamo che $x_1, \dots, x_n$ siano numeri reali. Allora, per $t \in \mathbb{R}$ in un intorno di 0, si ha lo sviluppo di Mac-Laurin

$$\log\left(\prod_{i=1}^{n}(1 - x_i t)\right) = \sum_{i=1}^{n} \log(1 - x_i t) = -\sum_{k\geq 1}\left(\sum_{i=1}^{n} \frac{x_i^k}{k}\right) t^k = -\sum_{k\geq 1} \frac{\psi_k}{k} t^k.$$

Ne segue che

$$1 + \sigma_1 t + \cdots + \sigma_n t^n = \prod_{i=1}^{n}(1 - x_i t)$$

$$= \exp(\log(\prod_{i=1}^{n}(1 - x_i t)) = \exp\left(-\sum_{k\geq 1} \frac{\psi_k}{k} t^k\right) = \sum_{n\geq 0} \frac{(-1)^n}{n!}\left(\sum_{k\geq 1} \frac{\psi_k}{k} t^k\right)^n.$$

Uguagliando i coefficienti delle potenze di t si trovano i polinomi cercati.

Esercizio 33.7. Nella stessa situazione dell'Osservazione 33.6, considerare la matrice (vedi Esempio 28.4)

$$A=\begin{pmatrix}0&0&\cdots&0&-\sigma_n\\1&0&\cdots&0&-\sigma_{n-1}\\0&1&\cdots&0&-\sigma_{n-2}\\\vdots&\vdots&\ddots&\vdots&\vdots\\0&0&\cdots&1&-\sigma_1\end{pmatrix}$$

Usare l'esistenza della forma triangolare per calcolare la traccia di A^k in funzione di $x_1,\ldots,x_n$. Si noti che trace(A^k) si può esprimere come un polinomio a coefficienti interi nelle variabili σ_i.

34. Esercizi gentilmente offerti da Lidia Stoppino

Esercizio 34.1. Sia V lo spazio vettoriale delle matrici reali 2×2. Trovare la dimensione e una base del sottospazio W generato da

$$A=\begin{pmatrix}1&2\\-1&3\end{pmatrix},\quad B=\begin{pmatrix}2&5\\1&-1\end{pmatrix},\quad C=\begin{pmatrix}5&15\\1&1\end{pmatrix},\quad D=\begin{pmatrix}3&4\\-2&5\end{pmatrix}.$$

Esercizio 34.2. Per quali valori del parametro reale h la seguente matrice ha rango rispettivamente 0, 1, 2 o 3?

$$\begin{pmatrix}1&0&1&0\\2&h&2&h\\1&1+h&1&2h\end{pmatrix}$$

Esercizio 34.3. Sia W il sottospazio vettoriale di $\mathbb{R}$ generato dai vettori

$$(1,1,1),\quad (2,0,1),\quad (0,2,1).$$

(1) Calcolare la dimensione e l'equazione cartesiana di W.
(2) Determinare una applicazione lineare $F\colon \mathbb{R}^3\to\mathbb{R}^3$ tale che $imF=W$.
(3) Determinare una applicazione lineare tale che
$$imF=W \qquad \text{e} \qquad kerF=L(1,0,1).$$
Una tale applicazione è unica?
(4) Mostrare che qualunque applicazione F come nel punto precedente ha $rgF^2=1$.
(5) È vero o falso che qualunque applicazione lineare F come nel punto (2) soddisfa che $rgF^2=1$?

Esercizio 34.4. Siano A e B due matrici quadrate dello stesso ordine simmetriche. Mostrare che AB è simmetrica se e solo se $AB=BA$.

Esercizio 34.5. Sia M_n la matrice reale di ordine n con tutti i coefficienti uguali a 1: calcolarne, per ogni $n\in\mathbb{N}$, autovalori e autovettori. Sono matrici diagonalizzabili?

Esercizio 34.6. Sia B una matrice nilpotente di ordine n. Mostrare che, se B ha rango $n-1$, allora il suo polinomio minimo $q_B(t)$ è uguale al polinomio caratteristico $p_B(t)=t^n$.

Esercizio 34.7. Sia A una matrice complessa quadrata.

- Mostrare che se A è diagonalizzabile, allora A^k è diagonalizzabile, per ogni k.
- Mostrare che se A è anche invertibile allora vale il viceversa.
- Il viceversa è vero in generale?

Esercizio 34.8. Sia A una matrice reale 3×3 la cui prima riga è $(1, 1, 1)$. Supponiamo che i vettori

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

siano autovettori per A.

(1) Qual è il rango di A?
(2) Mostrare che A è diagonalizzabile oppure nilpotente.
(3) Fare un esempio di una matrice siffatta diagonalizzabile, e di una nilpotente.
(4) Supponiamo che un autospazio abbia equazioni

$$y + x - 2z = y - x = 0.$$

Determinare i coefficienti di A.

Esercizio 34.9. Sia V lo spazio vettoriale delle matrici 2×2 reali. Siano

$$A = \begin{pmatrix} 3 & 0 \\ 0 & -1 \end{pmatrix}, \quad B_\alpha = \begin{pmatrix} -1 & \alpha \\ -1 & 1 \end{pmatrix}$$

con α parametro reale.
Si consideri l'applicazione $F_\alpha \colon V \to V$ definita così:

$$F_\alpha(M) = AM^tB, \qquad \text{per ogni } M \in V.$$

(1) Verificare che F_α è una applicazione lineare, e scriverne la matrice associata rispetto alla base standard di V.
(2) Per quali valori di α l'applicazione F_α è diagonalizzabile? Per quali valori F_α^2 è diagonalizzabile?
(3) Scrivere una base di V che diagonalizza F_α per $\alpha = -3$.

Esercizio 34.10. Sia A una matrice 2×2 reale.

(1) Mostrare che se $A^2 + I = 0$, allora A è coniugata a

$$B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

(2) Si supponga che $A^3 + A = 0$, e che A non sia coniugata a B. Determinare A.
(3) Si supponga che $A^4 + 2A^2 + I = 0$. Dire se A è simile a B oppure no.

35. Tutoraggio dell'8 gennaio 2007

Esercizio 35.1. Sia $F : \mathbb{R}^2 \to \mathbb{R}^2$ la riflessione di asse $\{y - 2x = 0\}$. Con una opportuna scelta di una base di $\mathbb{R}^2$, scrivere la matrice di F in forma diagonale.

Esercizio 35.2. Sia A una matrice 350×350 a coefficienti complessi. Si supponga che $A^3 = I$ e che $A \neq I$. Si dimostri che A è diagonalizzabile su $\mathbb{C}$ ma non su $\mathbb{R}$.

Esercizio 35.3. Si consideri la matrice

$$B = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & a \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Determinare i valori di a per cui A è nilpotente. Dimostrare che, se A non è nilpotente, allora è diagonalizzabile (su $\mathbb{C}$).

Esercizio 35.4. Sia V lo spazio vettoriale dei polinomi a coefficienti complesssi di grado minore o uguale a 3. Sia $F : V \to V$ l'applicazione lineare definita da

$$F(p(x)) = p(2x + 1)\,.$$

Trovare una base di V formata da autovettori di F e calcolarne i relativi autovalori. (Osservare che: $F(p(x)q(x)) = F(p(x))F(q(x))$)

Esercizio 35.5. Sia $F : \mathbb{K}^5 \to \mathbb{K}^5$ l'applicazione lineare definita da:

$$F(x, y, z, u, v) = (0, x, y, 0, u)\,.$$

Determinare i polinomi minimo e caratteristico di F.

Esercizio 35.6. Siano

$$B_1 = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad B_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad B_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}\,.$$

Sia M_3 lo spazio vettoriale delle matrici 3×3 a coefficienti in $\mathbb{K}$. Sia $D \subset M_3$ il sottospazio delle matrici diagonali. Sia $F : M_3 \to \mathbb{K}^3$ l'applicazione lineare definita da

$$F(A) = (\text{Traccia}(AB_1), \text{Traccia}(AB_2), \text{Traccia}(AB_3))\,.$$

Dimostrare che $M_3 = D \oplus \ker(F)$.

Esercizio 35.7. Sia $F : \mathbb{K}^3 \to \mathbb{K}^3$ l'applicazione lineare definita da:

$$F(x, y, z) = (y, z, 0)\,.$$

Dire, motivando la risposta, se esiste una applicazione lineare $G : \mathbb{K}^3 \to \mathbb{K}^3$ tale che $G^2 = F$?

Esercizio 35.8. Sia A una matrice invertibile $n \times n$ a coefficienti in $\mathbb{K}$. Dimostrare che

$$p_{A^{-1}}(t) = (-t)^n \frac{1}{\det A} \cdot p_A\left(\frac{1}{t}\right)$$

Esercizio 35.9. Sia Sia $F : \mathbb{R}^3 \to \mathbb{R}^3$ una applicazione lineare che lascia fissi i vettori (x, y, z) tali che $x+y+z = 0$ e, inoltre, tale che $F(1, 1, 1) = (-1, -1, -1)$. Una tale F è unica? Calcolare $\det(F)$ e $\text{Traccia}(F)$.

Esercizio 35.10. Sia A una matrice 4×4 a coefficienti in $\mathbb{K}$. Si supponga che $A^2 = I$.
1) Si dimostri che $A + I$ e $A - I$ non sono entrambe invertibili.
2) Si dimostri che $rg(A + I) + rg(A - I) = 4$.

36. Esonero del 17 gennaio 2007

Esercizio 36.1. Calcolare il determinante della matrice

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

Soluzione: $\det = -6$.

Esercizio 36.2. Calcolare l'inversa della matrice

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

Soluzione:

$$\begin{pmatrix} -1 & -1 & 1 \\ -2 & -1 & 2 \\ 2 & 1 & -1 \end{pmatrix}.$$

Esercizio 36.3. Calcolare i polinomi minimo e caratteristico della matrice

$$A = \begin{pmatrix} 0 & 2 & 1 \\ -1 & -3 & -1 \\ 1 & 2 & 0 \end{pmatrix}.$$

Soluzione: $q_A = (t + 1)^2$, $\det(tI - A) = (t + 1)^3$.

Esercizio 36.4. Dire, motivando la risposta, se la seguente matrice è diagonalizzabile e calcolarne gli autovalori.

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

Soluzione: La matrice ha quattro autovalori distinti $1, -1, 2, -2$ ed è quindi diagonalizzabile.

Esercizio 36.5. Sia $V \subset \mathbb{R}^4$ il sottospazio di equazione $x + y + z + t = 0$ e $w = (1, 0, 0, 0)$. Sia $F : \mathbb{R}^4 \to \mathbb{R}^4$ l'applicazione lineare tale che $f(v) = v$ per ogni $v \in V$ e $f(w) = (2, 1, -1, 0)$. Trovare una base di autovettori per F.

Soluzione: Sia (v_1, v_2, v_3) una base qualsiasi di V. Poiché $F(v_i) = v_i$, i vettori v_1, v_2, v_3 sono autovettori per F. Per completare (v_1, v_2, v_3) ad una base di autovettori è sufficiente trovare un autovettore v_4 per F non appartenente a V.
Poiché $w \notin V$, i vettori v_1, v_2, v_3, w generano $\mathbb{R}^4$ e quindi si può scrivere $v_4 = aw + v$, per qualche $a \in \mathbb{R}$ e $v \in V$. Se vogliamo che $v_4 \notin V$ bisogna imporre $a \neq 0$, mentre se vogliamo che v_4 sia un autovettore (con autovalore λ) bisogna risolvere l'equazione

$$f(v_4) = f(aw + v) = af(w) + v = \lambda v_4 = \lambda aw + \lambda v.$$

Siccome $h = f(w) - 2w \in V$, la precedente equazione diventa

$$2aw + ah + v = \lambda aw + \lambda v,$$

ossia

$$(2a - \lambda a)w = (\lambda - 1)v - ah.$$

Tale equazione ha come possibile soluzione $\lambda = 2$, $a = 1$ e $v = h$ e quindi il quarto autovettore è

$$v_4 = w + h = f(w) - w.$$

Esercizio 36.6. Sia V uno spazio vettoriale di dimensione finita e $F, G\colon V \to V$ due endomorfismi tali che:

(1) $FG = GF$.
(2) F è diagonalizzabile.
(3) G è nilpotente.

Dimostrare che esiste una base di autovettori di F rispetto alla quale la matrice di G è triangolare.

Soluzione: Indichiamo con $\lambda_1, \ldots, \lambda_s$ gli autovalori di F e con

$$V_i = \ker(F - \lambda_i I), \qquad i = 1, \ldots, s.$$

Siccome F è diagonalizzabile si ha

$$V = V_1 \oplus \cdots \oplus V_s.$$

Se $v \in V_i$, allora

$$(F - \lambda_i I)G(v) = FG(v) - \lambda_i G(v) = GF(v) - \lambda_i G(v) = G(F - \lambda_i I)(v) = G(0) = 0$$

e quindi $G(v) \in V_i$. In altri termini si ha $G\colon V_i \to V_i$ per ogni i. Siccome G è nilpotente, a maggior ragione è nilpotente la sua restrizione a V_i e quindi possiamo trovare una base $(v_1^i, \ldots, v_r^i)$ di V_i nella quale G si rappresenta con una matrice triangolare superiore.
Nella base di V ottenuta come unione delle basi dei sottospazi V_i costruite precedentemente, la matrice di F è diagonale e quella di G è triangolare superiore.

37. Appello del 24 gennaio 2007

Esercizio 37.1. Calcolare il prodotto di matrici

$$\begin{pmatrix} 2 & 1 & 3 \\ -2 & 1 & 5 \\ -3 & -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \\ 0 & 2 \end{pmatrix}$$

e se ne determini il rango.

Esercizio 37.2. Si consideri l'applicazione lineare

$$F\colon \mathbb{R}^4 \to \mathbb{R}^3$$

definita in coordinate da

$$F(x, y, z, w) = (x - y + 2w, 2y - 2z + 2w, 3x - 5y + 2z + 4w).$$

Descrivere la matrice A tale che $F = L_A$ e determinare una base del nucleo di F.

Esercizio 37.3. Sia $F\colon M_{2,2}(\mathbb{R}) \to M_{2,2}(\mathbb{R})$ l'applicazione lineare

$$F(A) = 2A - \text{traccia}(A) \begin{pmatrix} 1 & 2 \\ -1 & 1 \end{pmatrix}.$$

Calcolare il rango di F.

Esercizio 37.4. Si consideri la base $\mathbf{v} = (v_1, v_2, v_3)$ di $\mathbb{R}^3$ data dai vettori

$$v_1 = \begin{pmatrix} 2 \\ -1 \\ 1 \end{pmatrix}, \quad v_2 = \begin{pmatrix} -2 \\ 1 \\ 1 \end{pmatrix}, \quad v_3 = \begin{pmatrix} 1 \\ -1 \\ 2 \end{pmatrix}.$$

Determinarne la base duale.

Esercizio 37.5. Calcolare i polinomi minimo e caratteristico della matrice

$$A = \begin{pmatrix} 2 & 1 & 1 \\ 2 & 3 & 2 \\ 1 & 1 & 2 \end{pmatrix}$$

e discuterne la diagonalizzabilità sul campo dei numeri reali.

Esercizio 37.6. Sia $V \subset \mathbb{K}^4$ il sottospazio di equazione $x + y - z - t = 0$ e $w = (1, 0, 0, 0)$. Sia $F\colon \mathbb{K}^4 \to \mathbb{K}^4$ l'applicazione lineare tale che $f(v) = v$ per ogni $v \in V$ e $f(w) = (-2, 1, 0, 1)$.

(1) Calcolare il determinante di F.
(2) Dimostrare che, se $\mathbb{K} = \mathbb{R}$, allora non esiste alcuna applicazione lineare $G\colon \mathbb{R}^4 \to \mathbb{R}^4$ tale che $G^2 = F$.
(3) Cosa si può dire se $\mathbb{K} = \mathbb{C}$?

38. Appello del 6 febbraio 2007

Esercizio 38.1. Calcolare il prodotto di matrici

$$\begin{pmatrix} 2 & 1 & 3 \\ -2 & 1 & 5 \\ -3 & -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ -1 & 1 & 0 \\ 0 & 2 & 1 \end{pmatrix}$$

e se ne determini il rango.

Soluzione.

$$\begin{pmatrix} 1 & 7 & 5 \\ -3 & 11 & 3 \\ -2 & -1 & -3 \end{pmatrix}, \qquad \text{rango} = 3.$$

Esercizio 38.2. Si consideri l'applicazione lineare

$$F\colon \mathbb{R}^4 \to \mathbb{R}^3$$

definita in coordinate da

$$F(x, y, z, w) = (x - y + w, y - 2z + w, x - y + z).$$

Descrivere la matrice A tale che $F = L_A$ e determinare il rango di F.

Soluzione.

$$\begin{pmatrix} 1 & -1 & 0 & 1 \\ 0 & 1 & -2 & 1 \\ 1 & -1 & 1 & 0 \end{pmatrix}, \qquad \text{rango} = 3.$$

Esercizio 38.3. Calcolare i polinomi minimo e caratteristico della matrice

$$A = \begin{pmatrix} 4 & 2 & 4 \\ -2 & 0 & -4 \\ -2 & -2 & -2 \end{pmatrix},$$

e discuterne la diagonalizzabilità sul campo dei numeri reali.

Soluzione. Il polinomio caratteristico è $p_A(t) = (t-2)^2(t+2)$ e quindi gli autovalori sono $\lambda = 2$, con molteplicità algebrica 2 e $\lambda = -2$, con molteplicità algebrica 1. Siccome la molteplicità geometrica di un autovalore è sempre compresa tra 1 e la molteplicità algebrica, l'unico caso dubbio è per $\lambda = 2$. Siccome il rango di $A - 2I$ è unguale a 1, ne segue che le molteplicità geometriche sono uguali a quelle algebriche e la matrice è diagonalizzabile.
Il polinomio minimo di una matrice diagonalizzabile non ha fattori multipli e quindi $q_A = (t-2)(t+2)$.

Esercizio 38.4. Sia $F\colon M_{2,2}(\mathbb{R}) \to M_{2,2}(\mathbb{R})$ l'applicazione lineare

$$F(A) = 3A - A \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}.$$

Calcolare il rango di F.

Soluzione. Lo spazio vettoriale $M_{2,2}(\mathbb{R})$ ha dimensione 4 e quindi

$$rango(F) = 4 - \dim \ker(F).$$

Il nucleo è dato dalle matrici

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{tali che} \quad F(A) = \begin{pmatrix} 2a - 2b & 2b - 2a \\ 2c - 2d & 2d - 2c \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Quindi il nucleo è formato dalle matrici

$$\begin{pmatrix} a & a \\ c & c \end{pmatrix}$$

ed ha dimensione 2.

Esercizio 38.5. Si consideri l'applicazione lineare

$$F\colon \mathbb{R}^3 \to \mathbb{R}^3, \qquad F(x,y,z) = (x,-y,z).$$

Descrivere la matrice che rappresenta F nella base $\mathbf{v} = (v_1, v_2, v_3)$ di $\mathbb{R}^3$ data dai vettori

$$v_1 = \begin{pmatrix} 2 \\ -1 \\ 0 \end{pmatrix}, \quad v_2 = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}, \quad v_3 = \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}.$$

Soluzione. Bisogna rappresentare i vettori $F(v_i)$ nella base $\mathbf{v}$:

$$F(v_1) = F\begin{pmatrix} 2 \\ -1 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix} = 3v_1 - 4v_3.$$

$$F(v_2) = F\begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \\ 1 \end{pmatrix} = -2v_1 + v_2 + 4v_3.$$

$$F(v_3) = F\begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = 2v_1 - 3v_3.$$

La matrice è quindi

$$\begin{pmatrix} 3 & -2 & 2 \\ 0 & 1 & 0 \\ -4 & 4 & -3 \end{pmatrix}.$$

Esercizio 38.6. Siano $A, B \in M_{n,n}(\mathbb{R})$ due matrici nilpotenti tali che $AB = BA$. Dimostrare che:

(1) La matrice $A + tB$ è nilpotente per ogni $t \in \mathbb{R}$.
(2) $A^h B^k = 0$ per ogni coppia di interi non negativi h, k tali che $h + k \geq n$.

Soluzione. Siccome $AB = BA$ possiamo applicare il binomio di Newton

$$(A + tB)^s = A^s + stA^{s-1}B + \cdots + t^s B^s.$$

Dato che $A^n = B^n = 0$, ne segue che $(A + tB)^{2n-1}$ è combinazione lineare di matrici del tipo $A^h B^k$ con $h \geq n$ oppure $k \geq n$. Tali matrici sono nulle e quindi $(A + tB)^{2n-1} = 0$, ossia $A + tB$ è nilpotente.
In particolare

$$0 = (A + tB)^n = A^n + stA^{s-1}B + \cdots + t^n B^n.$$

per ogni t. Siccome i valori di t sono infiniti, segue dal Vandermonde che ogni coefficiente del polinonio $p(t) = (A + tB)^n$ è nullo (vedi la dimostrazione di Cayley-Hamilton a Pagina 44).

39. Appello del 26 giugno 2007

Esercizio 39.1. Calcolare il prodotto di matrici

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & -1 & 1 \\ 3 & 9 & 27 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 2 & 0 \\ 2 & -1 & 2 \end{pmatrix}$$

e determinarne il rango

Esercizio 39.2. Sia $F : \mathbb{R}^4 \to \mathbb{R}^3$ l'applicazione lineare definita da:

$$F(x, y, z, w) = (x - y, z - w, x + z - y + 2w)$$

a) Descrivere la matrice A tale che $F = L_A$
b) Determinare il rango di F^*.

Esercizio 39.3. Si consideri la matrice

$$A = \begin{pmatrix} -1 & 1 & -1 \\ 2 & 0 & -2 \\ 1 & 1 & -3 \end{pmatrix}$$

a) Calcolare il rango di $A + 2I$
b) Calcolare il polinomio caratteristico e il polinomio minimo di A
c) Determinare se A è diagonalizzabile.

Esercizio 39.4. Sia $B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Considerare l'applicazione lineare

$$F : M_{2,2}(\mathbb{R}) \to M_{2,2}(\mathbb{R})$$

definita da $F(A) = A - B^{-1}AB$. Calcolare il rango di F.

Esercizio 39.5. Sia $F : \mathbb{R}^3 \to \mathbb{R}^3$ l'applicazione lineare definita da:

$$F(x, y, z) = (x + y, y + z, x - z)\,.$$

Siano

$$v_1 = \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}, \quad v_2 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \quad v_3 = \begin{pmatrix} 0 \\ -1 \\ 0 \end{pmatrix}.$$

Scrivere la matrice di F nella base (v_1, v_2, v_3).

Esercizio 39.6. Sia A una matrice 3×3 a coefficienti complessi. Si supponga che $\operatorname{tr} A = \det A = 0$. Dimostrare che A è diagonalizzabile oppure nilpotente.

40. Appello del 27 settembre 2007

Esercizio 40.1. Calcolare il prodotto di matrici

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & -1 & 1 \\ 2 & 4 & 8 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 2 & 1 \\ 2 & -2 & 1 \end{pmatrix}$$

e determinarne il rango

Esercizio 40.2. Sia $F : \mathbb{R}^4 \to \mathbb{R}^4$ l'applicazione lineare definita da:

$$F(x, y, z, w) = (x - y + z, z - w, x + 2z - y - w, z + w)$$

a) Descrivere la matrice A tale che $F = L_A$
b) Determinare la dimensione di $\ker(F) \cap Im(F)$.

Esercizio 40.3. Si consideri la matrice

$$A = \begin{pmatrix} 4 & 1 & 0 \\ 2 & 5 & 0 \\ 1 & 1 & 3 \end{pmatrix}$$

a) Calcolare il rango di $A - 3I$.
b) Calcolare il polinomio caratteristico ed il polinomio minimo di A.
c) Determinare se A è diagonalizzabile.

Esercizio 40.4. Sia $B = \begin{pmatrix} 3 & 1 \\ -1 & 1 \end{pmatrix}$. Considerare l'applicazione lineare

$$F : M_{2,2}(\mathbb{R}) \to M_{2,2}(\mathbb{R})$$

definita da $F(A) = AB - 2A$. Calcolare il rango di F.

Esercizio 40.5. Siano $V \subset \mathbb{R}^4$ il sottospazio di equazione $x - y + z = 0$ e $p = (1, 0, 0, 0)$. Sia $F \colon \mathbb{R}^4 \to \mathbb{R}^4$ l'applicazione lineare tale che $f(v) = v$ per ogni $v \in V$ e $f(p) = (1, 2, 3, 4)$. Calcolare il determinante di F.

Esercizio 40.6. Sia $B \in M_{n,n}(\mathbb{R})$ e si consideri l'applicazione lineare

$$F : M_{n,n}(\mathbb{R}) \to M_{n,n}(\mathbb{R})$$

definita da $F(A) = BA + A$. Dimostrare che il rango di F è un multiplo di n.