

**Appunti provvisori del secondo semestre
del corso di Matematica Discreta**

Pietro Di Martino e Giovanni Gaiffi, 28 maggio 2015

Indice

Capitolo 1. Spazi vettoriali e applicazioni lineari	5
1. Introduzione	5
2. Definizione di spazio vettoriale e primi esempi	5
3. Sottospazi vettoriali	12
4. Intersezione e somma di sottospazi vettoriali	19
5. Base di uno spazio vettoriale	21
6. Applicazioni lineari	31
7. Matrici e vettori in colonna per rappresentare applicazioni lineari e elementi di uno spazio vettoriale	35
8. Esercizi di fine capitolo	44
Capitolo 2. Il rango delle applicazioni lineari e la riduzione a scalini delle matrici	49
1. Le operazioni elementari sulle colonne	49
2. La riduzione a scalini per colonne applicata allo studio delle basi	55
3. Il teorema della dimensione del nucleo e dell'immagine di una applicazione lineare	61
4. La riduzione a scalini per colonne vista come moltiplicazione per matrici invertibili	62
5. La riduzione a scalini per righe	66
6. Ancora sulla riduzione a scala di una matrice e lo studio delle applicazioni lineari	70
7. Altri esercizi	74
Capitolo 3. Sistemi lineari	83
1. Risolvere un sistema usando le operazioni elementari di riga	83
2. Altri esercizi	89
3. Come funziona Google	101
Capitolo 4. La formula di Grassmann	107
1. La formula di Grassmann per le intersezioni e le somme di sottospazi.	107
2. Un metodo per calcolare l'intersezione di due sottospazi vettoriali	109
3. Somma diretta di sottospazi	112
4. Altri esercizi	114
Capitolo 5. Applicazioni lineari e matrici invertibili	115

1. Endomorfismi lineari invertibili	115
2. Il metodo per trovare l'inversa (se esiste) di una matrice quadrata	117
3. Cambiamento di base nel caso degli endomorfismi lineari	119
4. Altri esercizi	122
Capitolo 6. Informazioni sul determinante	125
1. Definizione del determinante di una matrice quadrata	125
2. Il determinante e il calcolo del rango di una matrice	127
3. Il teorema di Binet	128
4. Proprietà del determinante rispetto alle mosse di riga e di colonna	129
5. Altri esercizi	130
Capitolo 7. Diagonalizzazione di endomorfismi lineari	133
1. Autovalori e autovettori di un endomorfismo lineare	133
2. Il polinomio caratteristico di un endomorfismo	136
3. Una strategia per scoprire se un endomorfismo è diagonalizzabile	138
4. Il criterio della molteplicità algebrica e della molteplicità geometrica	142
5. Esempi	145
6. Altri esercizi	149
Capitolo 8. Alcune osservazioni sulla fattorizzazione dei polinomi	155
1. Polinomi irriducibili e teorema di fattorizzazione unica	155
2. Fattorizzazione in $\mathbb{C}[x]$, $\mathbb{R}[x]$, $\mathbb{Q}[x]$	159
3. Esercizi	170
Capitolo 9. Prodotti scalari e spazi euclidei	177
1. Prodotto scalare	177
2. Ortogonalità	178
3. La disuguaglianza di Cauchy-Schwarz	182
4. Sottospazi ortogonali	183
5. Esercizi	184
Indice analitico	187
Bibliografia	189

CAPITOLO 1

Spazi vettoriali e applicazioni lineari

1. Introduzione

In questo capitolo introduciamo la struttura che caratterizza il corso di Algebra Lineare: la struttura di spazio vettoriale. Sarà data la definizione di spazio vettoriale, alcuni esempi (tra quelli su cui lavoreremo di più), e verranno studiate le proprietà di questi spazi.

È possibile (probabile) che alcuni abbiano già incontrato il termine vettore in fisica, che abbiano operato con tali vettori del piano (\mathbb{R}^2) o dello spazio (\mathbb{R}^3) senza probabilmente soffermarsi sulla struttura di spazio vettoriale (su \mathbb{R}) del piano e dello spazio.

Lo studio degli spazi vettoriali ha notevoli applicazioni. Ad esempio fornisce strumenti potenti per l'analisi della risolubilità e, in caso di esistenza di soluzioni, per la risoluzione dei sistemi lineari.

Per citare una applicazione molto utilizzata della risoluzione di sistemi lineari, osserveremo come l'algoritmo page rank di google sia basato proprio sulla soluzione di un enorme sistema lineare.

2. Definizione di spazio vettoriale e primi esempi

Come detto, in questo e nei prossimi capitoli concentreremo l'attenzione sulla struttura matematica di spazio vettoriale V su un campo \mathbb{K} .

DEFINIZIONE 1.1. Un insieme V si dice **uno spazio vettoriale sul campo** \mathbb{K} se sono definite due funzioni a valori in V :

- Una funzione da $V \times V$ in V , che chiameremo **addizione vettoriale**), che ad ogni coppia di elementi u, v di V associa un elemento di V che indicheremo con $u+v$ (e che chiameremo **somma vettoriale** di u e v).
- Una funzione tra un elemento di \mathbb{K} ed un elemento di V , che chiameremo **moltiplicazione scalare**), che ad ogni coppia di elementi λ di \mathbb{K} e v di V associa un elemento di V che indicheremo con $\lambda \cdot v$ (e che chiameremo **prodotto scalare** di λ con v). Spesso, quando non ci saranno ambiguità nella scrittura, ometteremo il simbolo \cdot , e indicheremo il risultato del prodotto scalare di λ e v , con λv .

E se tali funzioni rispettano le seguenti proprietà:

(1) **Proprietà associativa dell'addizione:** $\forall u, v, w \in V$ vale $(u + v) + w = u + (v + w)$

(2) **Proprietà commutativa dell'addizione:** $\forall v, w \in V$ vale $v + w = w + v$

(3) **Esistenza dell'elemento neutro per l'addizione:** esiste $O \in V$ tale che $\forall v \in V$ vale $v + O = v$

(4) **Esistenza dell'opposto per l'addizione:** $\forall v \in V$ esiste un elemento w in V tale che $v + w = O$

(5) **Proprietà distributive della moltiplicazione per scalare:** $\forall \lambda, \mu \in \mathbb{K}, \forall v, w \in V$ vale:

$$\begin{cases} \lambda(v + w) = \lambda v + \lambda w \\ (\lambda + \mu)v = \lambda v + \mu v \end{cases}$$

(6) **Proprietà associativa della moltiplicazione per scalare:** $\forall \lambda, \mu \in \mathbb{K}, \forall v \in V$ vale $(\lambda\mu)v = \lambda(\mu v)$

(7) **Proprietà di esistenza dell'invariante moltiplicativo:** $\forall v \in V$ vale $1 \cdot v = v$ (dove con 1 abbiamo indicato l'elemento neutro della moltiplicazione del campo \mathbb{K}).

Se V è uno spazio vettoriale su un campo \mathbb{K} , chiameremo **vettori** gli elementi di V e **scalari** gli elementi del campo \mathbb{K} .

OSSERVAZIONE 1.2. È importante sottolineare come la definizione di spazio vettoriale coinvolga due insiemi: V (i cui elementi saranno chiamati **vettori**) e il campo \mathbb{K} su cui V è spazio vettoriale. Infatti, per avere uno spazio vettoriale V , è richiesto tra le altre cose, che sia definita una addizione tra gli elementi di V , ma anche una moltiplicazione tra un elemento di \mathbb{K} ed un elemento di V (in particolare, mostreremo esempi in cui, dato un fissato insieme V , è possibile definire una operazione di questo tipo, con le proprietà volute, rispetto ad un campo \mathbb{K} , ma non rispetto ad un campo \mathbb{F} diverso da \mathbb{K}). Per questo, non ha senso parlare di spazio vettoriale V , senza indicare il campo \mathbb{K} su cui V è spazio vettoriale.

OSSERVAZIONE 1.3. Le prime quattro proprietà, relative alla addizione (e che osserviamo non coinvolgono in nessun modo il campo \mathbb{K}), si possono sintetizzare dicendo che V è un *gruppo commutativo* rispetto alla somma.

OSSERVAZIONE 1.4. È importante sottolineare come nella definizione di spazio vettoriale si richieda che le funzioni addizione vettoriale e moltiplicazione scalare siano a valori in V , nella definizione di spazio vettoriale, ovvero si richiede che:

- Per ogni coppia di v, w in V la somma vettoriale $v + w$ sia un elemento di V . Si dice che V è **chiuso per l'addizione vettoriale**.
- Per ogni k in \mathbb{K} e per ogni v in V il prodotto scalare $k \cdot v$ sia un elemento di V . Si dice che V è **chiuso per la moltiplicazione scalare**.

Vediamo adesso alcuni primi esempi di spazio vettoriale:

ESEMPIO 1.5. L'esempio più banale segue dall'osservazione che ogni campo \mathbb{K} è uno spazio vettoriale su \mathbb{K} stesso, con le operazioni di addizione vettoriale e moltiplicazione per scalare che sono definite identiche alle operazioni di addizione e moltiplicazione del campo. In particolare dunque \mathbb{R} è uno spazio vettoriale su \mathbb{R} , così come \mathbb{Q} è uno spazio vettoriale su \mathbb{Q} .

È facile osservare come ogni campo \mathbb{K} sia uno spazio vettoriale su qualsiasi sottocampo \mathbb{F} di \mathbb{K} stesso, con le operazioni definite come sopra. Ad esempio \mathbb{R} è uno spazio vettoriale su \mathbb{Q} .

Osserviamo come il viceversa non sia vero, in particolare \mathbb{Q} non è uno spazio vettoriale su \mathbb{R} con le operazioni di addizione e moltiplicazione usuali. Il punto è che moltiplicando quello che dovrebbe essere un vettore (ovvero un elemento di \mathbb{Q}) per uno scalare (ovvero un generico elemento di \mathbb{R}) non sempre si ottiene un elemento di \mathbb{Q} , mentre, nella definizione di spazio vettoriale, si richiede che l'insieme sia chiuso per moltiplicazione scalare. Ad esempio:

$$\underbrace{\sqrt{2}}_{\in \mathbb{R}} \cdot \underbrace{2}_{\in \mathbb{Q}} = \underbrace{2\sqrt{2}}_{\notin \mathbb{Q}}$$

OSSERVAZIONE 1.6. È importante non fare confusione tra le operazioni di addizione e moltiplicazione che definiranno lo spazio vettoriale V su \mathbb{K} , e le operazioni di addizione e moltiplicazione che rendono un campo \mathbb{K} : quest'ultime sono funzioni da $\mathbb{K} \times \mathbb{K}$ in \mathbb{K} e non agiscono sugli elementi di V (a meno che, vedi Esempio 1.5, V non coincida proprio con \mathbb{K}).

OSSERVAZIONE 1.7. La moltiplicazione per scalare, viene anche detta **prodotto esterno**, proprio per rimarcare il fatto che, a differenza della somma vettoriale che è una operazione tra elementi di V , la moltiplicazione scalare mette in gioco anche il campo \mathbb{K} su cui V è spazio vettoriale, in quanto è tra un elemento di V ed un elemento di \mathbb{K} .

ESERCIZIO 1.8. Dimostrare che $\mathbb{R}^2 = \{(a, b) | a, b \in \mathbb{R}\}$, l'insieme delle coppie di numeri naturali (che possiamo vedere geometricamente come il piano) è uno spazio vettoriale su \mathbb{R} con le operazioni di somma vettoriale e

prodotto scalare definite, come ci aspettiamo, come segue:

$$(a, b) +_{\mathbb{R}^2} (c, d) \underbrace{=}_{def} (a + c, b + d)$$

$$\lambda \cdot_{\mathbb{R}^2} (a, b) \underbrace{=}_{def} (\lambda \cdot a, \lambda \cdot b)$$

ESERCIZIO 1.9. Dimostrare che l'insieme C dei punti del piano su una circonferenza di raggio r :

$$C = \{(a, b) \in \mathbb{R}^2 \mid a^2 + b^2 = r^2\}$$

non è uno spazio vettoriale su \mathbb{R} .

ESERCIZIO 1.10. Dimostrare che l'anello dei polinomi $\mathbb{K}[x]$ è uno spazio vettoriale su \mathbb{K} con la somma tra polinomi e il prodotto tra polinomi e costanti di \mathbb{K} definiti nel modo usuale.

ESERCIZIO 1.11. Dimostrare, generalizzando il risultato dell'Esercizio 1.8 che, dato un campo \mathbb{K} , l'insieme \mathbb{K}^n delle n -uple ordinate (a_1, a_2, \dots, a_n) di elementi di \mathbb{K} , che molto spesso rappresenteremo in colonna

$$\begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ \dots \\ \dots \\ a_{n-1} \\ a_n \end{pmatrix}$$

anziché in riga, è uno spazio vettoriale su \mathbb{K} con le operazioni di somma vettoriale definite come segue:

(1) La somma fra vettori di \mathbb{K}^n è definita da:

$$\begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ \dots \\ \dots \\ a_{n-1} \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ \dots \\ \dots \\ b_{n-1} \\ b_n \end{pmatrix} = \begin{pmatrix} a_1 + b_1 \\ a_2 + b_2 \\ a_3 + b_3 \\ \dots \\ \dots \\ a_{n-1} + b_{n-1} \\ a_n + b_n \end{pmatrix}$$

(2) Il prodotto tra un vettore di \mathbb{K}^n e uno scalare di \mathbb{K} è definito da:

$$\lambda \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ \dots \\ \dots \\ a_{n-1} \\ a_n \end{pmatrix} = \begin{pmatrix} \lambda a_1 \\ \lambda a_2 \\ \lambda a_3 \\ \dots \\ \dots \\ \lambda a_{n-1} \\ \lambda a_n \end{pmatrix}$$

Nel nostro corso l'esempio di spazio vettoriale che studieremo di più è quello di \mathbb{R}^n come spazio vettoriale su \mathbb{R} con le operazioni definite come sopra. Vedremo più avanti come gli spazi vettoriali non si limitino a \mathbb{R}^n (o più in generale \mathbb{K}^n), ma che, introducendo il concetto di base di uno spazio vettoriale e coordinate, potremo usare \mathbb{R}^n (\mathbb{K}^n) per trattare tutti gli spazi vettoriali (di dimensione finita) su \mathbb{R} (su \mathbb{K}).

ESERCIZIO 1.12. \mathbb{R}^n è anche uno spazio vettoriale su \mathbb{Q} ?

Fatti alcuni primi esempi di spazi vettoriali, siamo interessati a cominciare a scoprire qualche proprietà degli spazi vettoriali. In particolare cominciamo dalle proprietà dell'elemento neutro e dell'opposto dell'addizione vettoriale.

La proprietà 3, della Definizione 1.1 di spazio vettoriale, ci dice che esiste un elemento O di V che è elemento neutro per l'addizione vettoriale. Una prima curiosità può essere quella di capire se tale elemento neutro sia unico qualsiasi sia lo spazio vettoriale. La risposta è affermativa, come esplicitato dalla seguente proposizione:

PROPOSIZIONE 1.13. *Se V è uno spazio vettoriale su \mathbb{K} , l'elemento neutro O della somma vettoriale è unico.*

DIMOSTRAZIONE. Siano O e O' due elementi di V che sono elementi neutri dell'addizione vettoriale. Vogliamo mostrare che in realtà deve essere $O = O'$. Considerando la addizione tra O e O' , possiamo scrivere:

$$O \quad \underbrace{=} \quad O + O' \quad \underbrace{=} \quad O'$$

$O' \text{ è el.neutro addizione} \qquad O \text{ è el.neutro addizione}$

□

Dalla Proposizione 1.13 seguono altre proprietà interessanti:

COROLLARIO 1.14 (Unicità dell'opposto). *Sia V uno spazio vettoriale su \mathbb{K} . Per ogni v in V , sappiamo dalla proprietà 4 della Definizione 1.1 di spazio vettoriale, che esiste un opposto w di v , ovvero w è tale che $v + w = w + v = 0$. Ebbene ogni elemento ha uno¹ e un solo opposto.*

DIMOSTRAZIONE. Come già scritto, sappiamo che, se V è uno spazio vettoriale su \mathbb{K} , ogni v di V ha almeno un opposto per l'addizione. Vogliamo dimostrare che tale opposto è unico. Supponiamo dunque che esistano due elementi w e z opposti di v , e dimostriamo che necessariamente deve essere $w = z$. Consideriamo il vettore di V $w + v + z$: tale vettore, data la proprietà associativa dell'addizione vettoriale si può ottenere o addizionando il vettore $w + v$ al vettore z , oppure addizionando il vettore w al vettore $v + z$. Ovvero:

$$(w + v) + z = w + (v + z)$$

¹E questo appunto è quello che chiede la proprietà 4 della Definizione 1.1.

Abbiamo che:

$$\begin{array}{ccccc}
 (w + v) + z & \underbrace{=} & O + z & \underbrace{=} & z \\
 & w \text{ è opposto di } v & & \text{prop.3 Def.1.1} & \\
 w + (v + z) & \underbrace{=} & w + O & \underbrace{=} & w \\
 & z \text{ è opposto di } v & & \text{prop.3 Def.1.1} &
 \end{array}$$

Dunque $z = w$. □

COROLLARIO 1.15 (Legge di cancellazione). *Siano v, w, z tre vettori di uno spazio vettoriale V su \mathbb{K} , allora:*

$$v + z = w + z \Leftrightarrow v = w$$

DIMOSTRAZIONE. \Leftarrow) Se $v = w$ allora, per definizione di funzione, la funziona addizione vettoriale $+$ restituisce lo stesso valore se in input ha la stessa coppia di elementi $(v, z) = (w, z)$.

\Rightarrow) Se $v + w = v + z$ allora, per quanto appena osservato, addizionando l'opposto t di v (che a questo sappiamo essere unico) con $v + w$ e con $v + z$, si ottiene lo stesso vettore di V , ovvero:

$$t + (v + w) = t + (v + z)$$

Utilizzando la proprietà associativa della addizione vettoriale si ha:

$$\underbrace{(t + v)}_{=O} + w = \underbrace{(t + v)}_{=O} + z$$

Ovvero, essendo O l'elemento neutro per l'addizione:

$$w = z$$

□

È importante sottolineare la differenza tra l'elemento neutro della somma vettoriale, che abbiamo indicato con O , e l'elemento neutro della somma di \mathbb{K} , usualmente indicato con 0 : in particolare O è un vettore, appartiene a V , mentre 0 è uno scalare di \mathbb{K} . Osserviamo, ad esempio, come nel caso dello spazio vettoriale \mathbb{R}^2 su \mathbb{R} (trattato nell'Esercizio 1.8), il vettore O elemento neutro della addizione vettoriale sia l'elemento $(0, 0)$ di \mathbb{R}^2 , mentre l'elemento neutro di \mathbb{R} è lo 0 .

La seguente proposizione fornisce una relazione tra i due elementi O di V e 0 di \mathbb{K} , relazione legata al comportamento di 0 nel prodotto scalare:

PROPOSIZIONE 1.16. *Dato V spazio vettoriale su un campo \mathbb{K} vale la seguente legge, nota come **legge di annullamento del prodotto scalare**:*

$$\forall v \in V \quad 0 \cdot v = O$$

DIMOSTRAZIONE. Dato $v \in V$:

$$(0 + 0) \cdot v = \begin{array}{c} \overbrace{}^{0 \text{ è el.neutro addizione in } \mathbb{K}} \\ \nearrow \\ \searrow \\ \underbrace{} \\ \text{prop.distr.} \end{array} \begin{array}{l} 0 \cdot v \\ 0 \cdot v + 0 \cdot v \end{array}$$

Dall'uguaglianza tra i due vettori $0 \cdot v$ e $0 \cdot v + 0 \cdot v$, segue, addizionando ai due vettori il vettore w opposto di $0 \cdot v$, che:

$$0 \cdot v + w = (0 \cdot v + 0 \cdot v) + w$$

E inoltre $0 \cdot v + w = O$ per definizione di opposto, e:

$$(0 \cdot v + 0 \cdot v) + w \underset{\text{prop.ass.add.}}{=} 0 \cdot v + \underbrace{(0 \cdot v + w)}_{=O} = 0 \cdot v + O \underset{\text{def.el.neutro } O}{=} 0 \cdot v$$

Dunque $0 \cdot v = O$. □

ESERCIZIO 1.17. Dato V spazio vettoriale su un campo \mathbb{K} , e dato $v \neq O$ in V , dimostrare che, dato $a \in \mathbb{K}$, $a \cdot v = O$, se e solo se $a = 0$ (Suggerimento: se $a = 0$, è la tesi della Proposizione 1.16, se $a \cdot v = O$ osserviamo che se a fosse diverso da 0 sarebbe invertibile in \mathbb{K} ...).

Nella Proposizione 1.16 abbiamo utilizzato l'articolo determinato "lo" per l'opposto w di $0 \cdot v$, ma anche in questo caso la proprietà 4 nella Definizione 1.1, ci dice solo che esiste un opposto: siamo sicuri che l'opposto per l'addizione di un vettore sia unico? La risposta è sì (indicheremo l'opposto di v con $-v$).

ESERCIZIO 1.18. Dimostrare che dato uno spazio vettoriale V sul campo \mathbb{K} , ogni v di V , ha uno (questo lo sappiamo per la proprietà 4 appena citata) e un solo opposto per l'addizione vettoriale.

La seguente proposizione caratterizza l'opposto di un vettore v :

PROPOSIZIONE 1.19. *Dato V spazio vettoriale su un campo \mathbb{K} , il prodotto scalare di un qualsiasi vettore v per lo scalare -1 è l'opposto di v , ovvero, con le notazioni appena introdotte:*

$$-1 \cdot v = -v$$

DIMOSTRAZIONE. Basta osservare che:

$$O \underset{\text{Proposizione 1.16}}{=} 0 \cdot v = (-1+1) \cdot v \underset{\text{prop.dist.}}{=} -1 \cdot v + 1 \cdot v \underset{\text{invariante moltiplicativo}}{=} -1 \cdot v + v$$

Ovvero $-1 \cdot v$ è l'opposto per l'addizione di v , cioè $-1 \cdot v = -v$. □

3. Sottospazi vettoriali

Dato uno spazio vettoriale V sul campo \mathbb{K} viene abbastanza naturale definire un sottospazio vettoriale di V come segue:

DEFINIZIONE 1.20. Un **sottospazio vettoriale** W di V è un sottoinsieme $W \subseteq V$ che, con la restrizione agli elementi di W della addizione vettoriale $+$ e della moltiplicazione scalare \cdot definiti su V , è uno spazio vettoriale su \mathbb{K} .

OSSERVAZIONE 1.21. Dato uno spazio vettoriale V su un campo \mathbb{K} , esistono sempre dei sottospazi vettoriali di V . È infatti facile provare che V stesso, e l'insieme $\{O\}$, rientrano nella definizione di sottospazi vettoriali di V , qualunque sia V .

L'Osservazione 1.21 ci fornisce la motivazione per introdurre il termine di sottospazio vettoriale proprio di uno spazio vettoriale V :

DEFINIZIONE 1.22. Chiameremo **sottospazio proprio** (o non banale) di V un qualsiasi sottospazio vettoriale di V che sia diverso da V e dal sottospazio $\{O\}$.

Prima di dare esempi di sottospazi vettoriali propri di un dato spazio vettoriale V su \mathbb{K} , cerchiamo di capire come fare a verificare se un sottoinsieme W di V è anche un sottospazio di V . L'idea è che, alcune delle proprietà necessarie per essere uno spazio vettoriale (vedi Definizione 1.1), continuano a valere *a maggior ragione* in un insieme contenuto in V , e dunque non ci sia bisogno di provarle nuovamente. D'altra parte, è importante osservare come nella definizione di spazio vettoriale, le funzioni $+$ e \cdot definite su $V \times V$ e su $\mathbb{K} \times V$ abbiano come immagine V : dobbiamo dunque verificare che, ristrette agli elementi di W , l'immagine sia in W , ovvero che W sia chiuso per l'addizione vettoriale e per la moltiplicazione scalare.

La seguente proposizione afferma proprio che, in realtà, per provare che un sottoinsieme W di V sia sottospazio, basta verificare che W contenga l'elemento neutro della addizione vettoriale, e che sia chiuso per somma vettoriale e prodotto scalare:

PROPOSIZIONE 1.23. *Dato V spazio vettoriale su \mathbb{K} e W sottoinsieme di V , W è sottospazio vettoriale di V (rispetto alle operazioni $+$ e \cdot che rendono V uno spazio vettoriale su \mathbb{K}) se e solo se:*

- (1) *Il vettore O appartiene a W .*
- (2) *Per ogni $u, v \in W$ vale $u + v \in W$, ovvero W è chiuso rispetto all'addizione vettoriale $+$ di V .*
- (3) *Per ogni $k \in \mathbb{K}$ e per ogni $u \in W$ vale $k \cdot u \in W$, ovvero W è chiuso per la moltiplicazione scalare \cdot di V .*

DIMOSTRAZIONE. Una implicazione è ovvia: se W è un sottospazio vettoriale di V , per Definizione 1.22, deve essere un sottoinsieme di V che

verifica tutte le proprietà di spazio vettoriale su \mathbb{K} . Dunque in particolare deve verificare anche le tre proprietà elencate nella proposizione.

Viceversa verifichiamo che se valgono le tre proprietà esplicitate nella proposizione (esistenza dell'elemento neutro della somma e chiusura per somma vettoriale e moltiplicazione per scalare) allora W è sottospazio. Dobbiamo provare che valgono tutte le altre proprietà che definiscono uno spazio vettoriale.

Le proprietà associativa e commutativa dell'addizione, distributiva e associativa della moltiplicazione per scalare, valendo per tutti gli elementi di V , valgono anche per tutti gli elementi di W , che è un sottoinsieme di V .

Anche l'esistenza dell'invariante moltiplicativo 1 è garantita: infatti questo elemento appartiene al campo \mathbb{K} , ed è tale che $1 \cdot v = v$ per ogni v di V . Come prima, essendo W un sottoinsieme di V , ogni elemento w di W è anche elemento di V , e dunque $1 \cdot w = w$.

Rimane dunque, come verifica vera e propria, di provare l'esistenza in W , per ogni elemento w di W , dell'opposto per l'addizione. Ora sappiamo che in V tale opposto esiste: si tratta di provare che è un elemento che sta nel sottoinsieme W . Il punto è che, grazie all'Esercizio 1.18, sappiamo che l'opposto di w è il risultato del prodotto scalare tra -1 e w : ma essendo W , per ipotesi, chiuso per prodotto scalare, $-1 \cdot w$ è un elemento di W . \square

OSSERVAZIONE 1.24. Una variante alle tre condizioni della Proposizione 1.23 sostituisce al posto della condizione 1, che il vettore O appartenga a W , la condizione *1bis* che W sia diverso dal vuoto, cioè contenga almeno un elemento.

Ovviamente la condizione 1 implica la *1bis*: se $O \in W$, allora W ha almeno l'elemento O e dunque non è vuoto. Viceversa, è facile mostrare che, tenendo ferme le altre due condizioni, dalla condizione *1bis* segue la condizione 1. Sia infatti w un elemento di W (esiste perché W , per ipotesi, è diverso dal vuoto), allora dalla condizione 3 (W è chiuso per prodotto con scalari) e dalla Proposizione 1.16 (per ogni vettore v , $0 \cdot v = O$) si ha che $0 \cdot w = O \in W$.

A questo punto, cominciamo a vedere esempi di sottospazi vettoriali degli spazi vettoriali che abbiamo introdotto nel paragrafo precedente. Partiamo dal piano \mathbb{R}^2 come spazio vettoriale su \mathbb{R} con le operazioni di addizione vettoriale e moltiplicazione scalare introdotte nell'Esercizio 1.8: quali sono i suoi sottospazi vettoriali propri?

Partiamo da qualcosa che sicuramente non è sottospazio vettoriale di \mathbb{R}^2 . La Figura 1 mostra un esempio di un sottoinsieme di \mathbb{R}^2 che sicuramente non è un sottospazio vettoriale: la curva disegnata con tratto continuo non è un sottospazio vettoriale di \mathbb{R}^2 . Infatti, facendo l'addizione vettoriale dei vettori V_1 e V_2 appartenenti alla curva in questione, otteniamo il vettore $V_1 + V_2$ (chi ha familiarità con la somma vettoriale tra vettori del piano, magari per studi di fisica, riconoscerà nel disegno tratteggiato, la nota *regola del parallelogramma* che non appartiene alla curva stessa. Dunque il

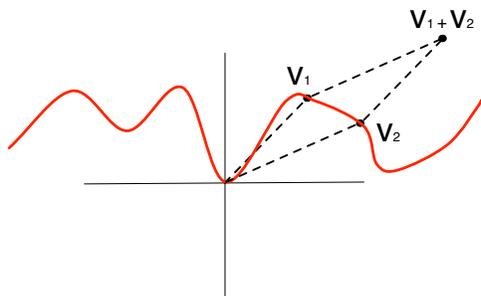


FIGURA 1. I due vettori V_1 e V_2 appartengono alla curva disegnata con tratto continuo, ma la loro somma $V_1 + V_2$ non appartiene alla curva: dunque la curva non è un sottospazio vettoriale di \mathbb{R}^2 .

sottoinsieme di \mathbb{R}^2 dei punti appartenenti alla curva disegnata con tratto continuo, non è un sottospazio di \mathbb{R}^2 perché non è chiusa per l'addizione vettoriale di \mathbb{R}^2 (la somma di due elementi dell'insieme è un elemento che non appartiene all'insieme).

Certo, il fatto di non essere sottospazio vettoriale, nell'esempio proposto, potrebbe dipendere dalla irregolarità della figura. Ci chiediamo dunque se più regolari, ad esempio una circonferenza C di centro l'origine del piano e raggio $r > 0$, sia sottospazio vettoriale di \mathbb{R}^2 . Dalla proprietà 1 della Proposizione 1.23, segue immediatamente che la risposta è no, una circonferenza del genere infatti non contiene l'elemento neutro dell'addizione O (che sappiamo essere il punto $(0, 0)$). Ma anche considerando l'insieme A unione della circonferenza C con O , si può dimostrare che A non è sottospazio vettoriale di \mathbb{R}^2 :

ESERCIZIO 1.25. Dimostrare che una circonferenza nel piano C (qualunque sia il raggio $r > 0$ e qualunque sia il centro) a cui si unisca anche O , non è mai un sottospazio vettoriale.

Siamo stati *sfortunati* con le circonferenze, proviamo con le rette. Come nel caso precedente, se non consideriamo rette passanti per l'origine O , dobbiamo comunque aggiungere O per poter sperare che siano sottospazi vettoriali di \mathbb{R}^2 . Ma anche in questo caso, l'aggiunta di O non basta, come si può vedere dalla Figura 2.

E se prendiamo le rette passanti per l'origine? Una retta r passante per l'origine del piano è caratterizzata dal numero reale k che identifica la *pendenza* della retta stessa (la retta avrà l'equazione $y = k \cdot x$). L'insieme r dei punti appartenenti alla retta è dunque il seguente:

$$r = \{(x, kx) | x \in \mathbb{R}\}$$

Ora osserviamo che $(0, 0) \in r$ e che per ogni coppia $(x_1, kx_1), (x_2, kx_2)$ di punti di r e per ogni $h \in \mathbb{R}$ si ha:

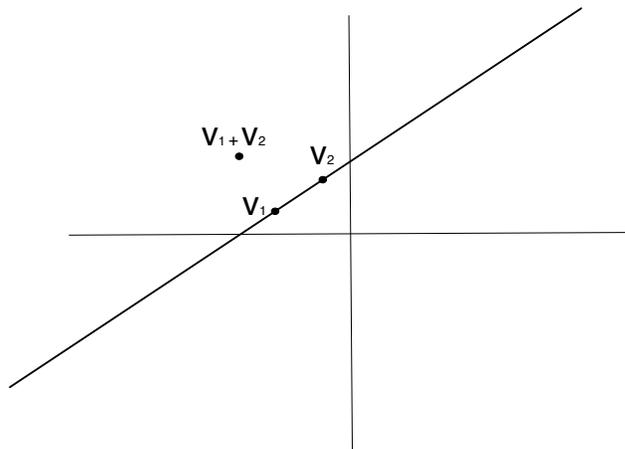


FIGURA 2. La somma di due vettori che giacciono su una retta non passante per l'origine non appartiene alla retta.

- $(x_1, kx_1) + (x_2, kx_2) = (x_1 + x_2, kx_1 + kx_2) = (x_1 + x_2, k(x_1 + x_2))$
Ovvero r è chiuso per addizione vettoriale.
- $h(x_1, kx_1) = (hx_1, hkx_1) = (hx_1, k(hx_1))$ Ovvero r è chiuso per moltiplicazione scalare.

Abbiamo dunque mostrato la seguente proposizione:

PROPOSIZIONE 1.26. *Le rette passanti per l'origine sono sottospazi vettoriali propri di \mathbb{R}^2 .*

Ma in realtà possiamo fare di più e dimostrare che le rette passanti per l'origine sono gli unici sottospazi vettoriali propri di \mathbb{R}^2 , e dunque caratterizzare completamente² i sottospazi vettoriali di \mathbb{R}^2 :

PROPOSIZIONE 1.27. *Le rette passanti per l'origine O sono tutti e soli i sottospazi vettoriali propri di \mathbb{R}^2 .*

DIMOSTRAZIONE. Che le rette passanti per l'origine siano sottospazi vettoriali propri di \mathbb{R}^2 lo abbiamo appena provato, dobbiamo provare che sono gli unici: ovvero che se V è un sottospazio proprio di \mathbb{R}^2 , allora V è una retta passante per l'origine. Indichiamo in grassetto i vettori del piano per non confonderli con gli scalari. Osserviamo che se V è sottospazio proprio, per definizione di sottospazio proprio, deve contenere un vettore \mathbf{v} diverso da \mathbf{O} . Ora, la chiusura di V per prodotto scalare ci dice che, per ogni numero reale h , tutti gli elementi $h \cdot \mathbf{v}$, ovvero la retta r che unisce \mathbf{O} con \mathbf{v} , sta in V . Per ora abbiamo dunque mostrato che un sottospazio proprio di \mathbb{R}^2 contiene un vettore non nullo (cioè un punto del piano diverso da O) e deve contenere tutta la retta passante dall'origine e da quel punto. Mostriamo

²È evidente che se si considera questo risultato, l'Esercizio 1.25 diventa una immediata conseguenza.

ora che se esistesse \mathbf{w} in V non appartenente alla retta r , allora V sarebbe tutto \mathbb{R}^2 (e dunque non sarebbe un sottospazio proprio di \mathbb{R}^2).

Se esistesse \mathbf{w} in $V \setminus r$, allora (per lo stesso ragionamento seguito per \mathbf{v}) in V sarebbe contenuta tutta la retta s passante per \mathbf{O} e \mathbf{w} . Ora V deve essere chiuso anche per somma vettoriale, e dunque, per concludere, ci basterebbe mostrare che scegliendo opportunamente due elementi, rispettivamente sulla retta s e sulla retta r , e addizionandoli si può ottenere come vettore somma qualsiasi elemento di \mathbb{R}^2 (ovvero dato un qualsiasi \mathbf{z} vettore di \mathbb{R}^2 , si possono scegliere opportunamente un vettore \mathbf{u} su s e un vettore \mathbf{f} su r in modo tale che $\mathbf{z} = \mathbf{u} + \mathbf{f}$). Lasciamo, per ora, questo punto al lettore (e alla sua intuizione geometrica): forniremo in seguito ulteriori strumenti per dimostrarlo. \square

Abbiamo trattato il caso \mathbb{R}^2 , concentriamoci adesso sull'anello dei polinomi a coefficienti in \mathbb{K} , che abbiamo visto essere uno spazio vettoriale su \mathbb{K} .

ESERCIZIO 1.28. Dimostrare che l'insieme $\mathbb{K}^{\leq n}[x]$, i cui elementi sono il polinomio 0 e i polinomi a coefficienti in \mathbb{K} di grado minore o uguale ad n , è un sottospazio vettoriale di $\mathbb{K}[x]$ qualsiasi sia $n \in \mathbb{N}$.³

Svolgimento. Qualsiasi sia n , abbiamo per definizione di $\mathbb{K}^{\leq n}[x]$ che il polinomio nullo appartiene a $\mathbb{K}^{\leq n}[x]$. Dalla Proposizione 1.23 segue che rimane da verificare che $\mathbb{K}^{\leq n}[x]$ sia chiuso per addizione e per moltiplicazione per scalare. La chiusura rispetto a queste due operazioni segue dalle proprietà della funzione grado di un polinomio (che indichiamo con \deg), in particolare dalle seguenti:

(1) Per ogni coppia di polinomi non nulli $p(x), q(x) \in \mathbb{K}[x]$, si ha:

$$\deg(p(x) + q(x)) \leq \max(\deg(p(x)), \deg(q(x)))$$

(2) Per ogni polinomio $p(x) \in \mathbb{K}[x]$ e per ogni $\lambda \neq 0 \in \mathbb{K}$ si ha che:

$$\deg(\lambda \cdot p(x)) = \deg(p(x))$$

Dunque dati $p(x), q(x) \in \mathbb{K}^{\leq n}[x]$ si ha che:

$$\deg(p(x) + q(x)) \leq \max(\underbrace{\deg(p(x))}_{\leq n}, \underbrace{\deg(q(x))}_{\leq n}) \leq n$$

Ovvero $\mathbb{K}^{\leq n}[x]$ è chiuso per addizione vettoriale.

Per quanto riguarda la moltiplicazione per scalare, se λ è uno scalare abbiamo due possibilità:

- Se $\lambda = 0$, allora per la Proposizione 1.16, applicata allo spazio vettoriale $\mathbb{K}[x]$, di cui $p(x)$ fa parte, si ha che $\lambda \cdot p(x) = 0$ e 0 è un elemento di $\mathbb{K}^{\leq n}[x]$.

³Si deve aggiungere il polinomio 0 perché per tale polinomio spesso non si definisce il grado (talvolta si mette grado uguale a $-\infty$) dunque non rientra fra i polinomi di grado minore o uguale a n .

- Se $\lambda \neq 0$, allora abbiamo appena ricordato che il grado di $\lambda \cdot p(x)$ è uguale al grado di $p(x)$, e dunque è minore di n . Questo equivale a dire che $\lambda \cdot p(x) \in \mathbb{K}^{\leq n}[x]$.

Abbiamo dunque dimostrato che l'insieme $\mathbb{K}^{\leq n}[x]$, dei polinomi a coefficienti in \mathbb{K} di grado minore o uguale di un fissato n , è un sottospazio vettoriale di $\mathbb{K}[x]$. Studiamo adesso qualche altro sottoinsieme dell'anello dei polinomi a coefficienti in \mathbb{K} , per esempio quelli tali che tutti gli elementi (polinomi) che vi appartengono, hanno come radice un determinato scalare di \mathbb{K} .

ESEMPIO 1.29. Consideriamo il sottoinsieme L di $\mathbb{K}[x]$ che contiene tutti e soli i polinomi che hanno 1 come radice, ovvero:

$$L = \{p(x) \in \mathbb{K}[x] \mid p(1) = 0\}$$

Verifichiamo che L è un sottospazio vettoriale di $\mathbb{K}[x]$. Ricordiamo che $a \in \mathbb{K}$ si dice radice del polinomio $p(x) \in \mathbb{K}[x]$ se la valutazione del polinomio $p(x)$ in a è 0. La valutazione del polinomio $p(x)$ nell'elemento a di \mathbb{K} , è il valore di \mathbb{K} che si ottiene sostituendo alla variabile x il valore di a : indicheremo con $p(a)$ tale valutazione. Ad esempio, la valutazione in 2 del polinomio $p(x) = 3x^4 + 2x + 1$, indicata con $p(2)$, è 53, infatti:

$$p(2) = 3 \cdot 2^4 + 2 \cdot 2 + 1 = 3 \cdot 16 + 4 + 1 = 53$$

Nel caso dei polinomi costanti, ovvero che non dipendono da x la valutazione del polinomio $p(x)$ in qualsiasi elemento a di \mathbb{K} è sempre il valore costante del polinomio. Ad esempio se $p(x) = 5$, allora la valutazione di $p(x)$, per qualsiasi elemento di \mathbb{K} è 5.

- (1) Il polinomio 0, che è il vettore O di $\mathbb{K}[x]$, appartiene a L , infatti ha 1 come radice (addirittura ogni elemento di \mathbb{K} è una radice di 0).
- (2) Se $p(x), q(x) \in L$ allora $(p + q)(x)$ appartiene a L , infatti:

$$(p + q)(1) \underbrace{=}_{\text{definizione di somma tra polinomi}} p(1) + q(1) \underbrace{=}_{p(x) \in L, q(x) \in L} 0 + 0 = 0$$

- (3) Se $p(x) \in L$ e $k \in \mathbb{K}$ allora $kp(x) \in L$, infatti:

$$(k \cdot p)(1) = k \cdot p(1) \underbrace{=}_{p(x) \in L} k \cdot 0 = 0$$

OSSERVAZIONE 1.30. Dal teorema di Ruffini sappiamo che, dato un polinomio (in una variabile a coefficienti in un campo \mathbb{K}) $p(x)$, avere una radice a in \mathbb{K} equivale ad essere divisibile per il polinomio $x - a$. Dunque il sottoinsieme L dell'Esempio 1.29, si può riscrivere anche come segue:

$$L = \{p(x) \in \mathbb{K}[x] \mid p(1) = 0\} = \{p(x) \in \mathbb{K}[x] \mid x - 1 \mid p(x)\}$$

Seguendo il procedimento descritto nell'Esempio 1.29, mostrare la seguente generalizzazione.

PROPOSIZIONE 1.31. Dato un campo \mathbb{K} ed un elemento a di \mathbb{K} , l'insieme L così definito:

$$L = \{p(x) \in \mathbb{K}[x] \mid p(a) = 0\} = \{p(x) \in \mathbb{K}[x] \mid x - a \mid p(x)\}$$

è un sottospazio vettoriale di $\mathbb{K}[x]$.

Chiudiamo il paragrafo con un esercizio di riconoscimento di sottospazi vettoriali di $\mathbb{R}^{\leq n}[x]$: si raccomanda di provare a svolgerlo, prima di vedere la risoluzione proposta.

ESERCIZIO 1.32. Dire quali dei seguenti sottoinsiemi di $\mathbb{R}^{\leq n}[x]$ sono sottospazi vettoriali di $\mathbb{R}^{\leq n}[x]$:

- (1) $V_1 = \{p(x) \in \mathbb{R}^{\leq n}[x] \mid p(2) = 0\}$
- (2) $V_2 = \{p(x) \in \mathbb{R}^{\leq n}[x] \mid p(1) = 1\}$
- (3) $V_3 = \{p(x) \in \mathbb{R}^{\leq n}[x] \mid p(x) = \sum_{i=0}^n a_i x^i, \quad a_i \in \mathbb{Z}\}$
- (4) $V_4 = \{p(x) \in \mathbb{R}^{\leq n}[x] \mid p(1) = -p(2)\}$
- (5) $V_5 = \{p(x) \in \mathbb{R}^{\leq n}[x] \mid \sum_{i=0}^{\lfloor n/2 \rfloor} a_{2i} x^{2i}\}$ Dove con $\lfloor n/2 \rfloor$ indichiamo la parte intera di $n/2$.

Svolgimento. Analizziamo punto per punto le richieste dell'esercizio

- (1) V_1 è il sottoinsieme di $\mathbb{R}^{\leq n}[x]$ dei polinomi che valutati in 2 si annullano, dunque che hanno 2 come radice.

Che V_1 sia un sottospazio vettoriale di $\mathbb{R}^{\leq n}[x]$ segue dal fatto che, dalla Proposizione 1.31, V_1 è uno spazio vettoriale (essendo un sottospazio vettoriale di $\mathbb{K}[x]$), inoltre è, per definizione, contenuto in $\mathbb{R}^{\leq n}[x]$ (i suoi elementi sono polinomi in $\mathbb{R}^{\leq n}[x]$, che verificano una specifica proprietà): dunque è sottospazio di $\mathbb{R}^{\leq n}[x]$.

- (2) V_2 è il sottoinsieme di $\mathbb{R}^{\leq n}[x]$ dei polinomi che, valutati in 1, danno come valore 1.

V_2 è un insieme che non verifica nessuna delle tre proprietà che definiscono un sottospazio vettoriale, ma per dimostrare che non è un sottospazio vettoriale basta osservare che una di esse non vale, per esempio basta osservare che il polinomio 0 non appartiene a V_2 . Infatti il polinomio 0 valutato in qualsiasi elemento vale sempre 0 e non 1. È comunque un utile esercizio provare che V_2 non è chiuso né per addizione vettoriale, né per moltiplicazione per scalare.

- (3) V_3 è il sottoinsieme di $\mathbb{R}^{\leq n}[x]$ dei polinomi che hanno coefficienti interi.

Il polinomio 0 appartiene a V_3 e la somma di due polinomi a coefficienti interi è un polinomio a coefficienti interi: quindi V_3 è chiuso per l'addizione. *Sfortunatamente* però V_3 non è chiuso per la moltiplicazione per scalare; infatti sia $p(x) \in V_3$ non zero, se scegliamo un qualsiasi numero reale a che non sia intero e nemmeno razionale (per essere sicuri che non ci siano semplificazioni), per esempio $\sqrt{2}$, allora $a \cdot p(x)$ è un polinomio non a coefficienti interi. Quindi V_3 non è sottospazio vettoriale di $\mathbb{R}^{\leq n}[x]$.

(4) V_4 è il sottoinsieme di $\mathbb{R}^{\leq n}[x]$ dei polinomi che, valutati in 1, danno come valore l'opposto della valutazione del polinomio in 2.

Si osserva subito che 0 appartiene a V_4 . Siano $p(x)$ e $g(x)$ polinomi di V_4 allora valutiamo la loro addizione e la moltiplicazione per uno scalare $r \in \mathbb{R}$ e verifichiamo se continua a valere la proprietà che definisce V_4 :

$$(p+g)(1) \stackrel{\text{def.somma.pol.}}{=} p(1)+g(1) \stackrel{\text{def.somma.pol.}}{=} -p(2)-g(2) \stackrel{\text{def.somma.pol.}}{=} -(p+g)(2)$$

$$\underbrace{p(x) \in V_4}_{g(x) \in V_4}$$

$$(r \cdot p)(1) = r \cdot p(1) \stackrel{\text{def.somma.pol.}}{=} r \cdot (-p(2)) = -(r \cdot p)(2)$$

$$\underbrace{p(x) \in V_4}$$

Quindi V_4 è un sottospazio vettoriale di $\mathbb{R}^{\leq n}[x]$.

(5) V_5 è il sottoinsieme di $\mathbb{R}^{\leq n}[x]$ dei polinomi che hanno coefficienti diversi da zero solo per i termini di grado pari.

Il polinomio 0 appartiene a V_5 . Ora osserviamo che la somma tra due polinomi è definita facendo le somme tra monomi dello stesso grado, quindi se sommiamo due polinomi con solo monomi di grado pari otteniamo un polinomio formato solo da monomi di grado pari. Dalle proprietà del grado (ed in particolare dal fatto che la moltiplicazione per scalare, o annulla il polinomio se lo scalare è lo 0, oppure lascia inalterato il grado), segue che V_5 è chiuso anche per moltiplicazione per scalare e quindi è un sottospazio vettoriale di $\mathbb{R}^{\leq n}[x]$.

ESERCIZIO 1.33. Dimostrare che, se V è uno spazio vettoriale su \mathbb{K} , diverso dallo spazio $\{O\}$, e \mathbb{K} è infinito, allora anche V ha infiniti vettori.

4. Intersezione e somma di sottospazi vettoriali

In questo paragrafo mostreremo come, a partire da due sottospazi vettoriali U e W di uno spazio vettoriale V , si possano costruire altri due importanti sottospazi vettoriali: l'intersezione $U \cap W$ e la *somma* $U + W$.

Cominciamo con l'osservare che l'intersezione è un sottospazio vettoriale:

PROPOSIZIONE 1.34. *Sia V uno spazio vettoriale su un campo \mathbb{K} , U e W due sottospazi vettoriali di V , allora $U \cap W$ è un sottospazio vettoriale di V .*

DIMOSTRAZIONE. Dobbiamo mostrare che $U \cap W$ verifica le proprietà della Definizione 1.20:

(1) Essendo U e W due sottospazi vettoriali di V , $O \in U$ e $O \in W$, e dunque $O \in U \cap W$.

(2) Siano $v_1, v_2 \in U \cap W$ allora:

$$\left\{ \begin{array}{l} \underbrace{v_1 + v_2 \in U}_{U \text{ è sottospazio}} \\ \underbrace{v_1 + v_2 \in W}_{W \text{ è sottospazio}} \end{array} \right. \Rightarrow v_1 + v_2 \in U \cap W$$

(3) Sia $v \in U \cap W$ allora per ogni $\lambda \in \mathbb{K}$ si ha:

$$\left\{ \begin{array}{l} \underbrace{\lambda \cdot v \in U}_{U \text{ è sottospazio}} \\ \underbrace{\lambda \cdot v \in W}_{W \text{ è sottospazio}} \end{array} \right. \Rightarrow \lambda \cdot v \in U \cap W$$

□

Osserviamo ora che, se H è un sottoinsieme di V contenuto sia in U che in W , allora H è contenuto in $U \cap W$. Questa semplice osservazione, unita alla proposizione 1.34, ci permette di concludere che:

PROPOSIZIONE 1.35. *Dati U e W sottospazi vettoriali di uno spazio vettoriale V su un campo \mathbb{K} , $U \cap W$ è il più grande sottospazio vettoriale di V contenuto sia in U che in W .*

A questo punto andiamo alla caccia del più piccolo sottospazio contenente i sottospazi U e W di uno spazio vettoriale V . Qui verrebbe naturale considerare l'unione insiemistica: se infatti $U \cup W$ fosse sempre un sottospazio di V , sarebbe sicuramente il più piccolo sottospazio contenente sia U che W (provarlo per esercizio).

Ma in generale non è vero che $U \cup W$ è un sottospazio vettoriale di V .

ESERCIZIO 1.36. Provare che se $V = \mathbb{R}^2$ e U e W sono due rette distinte passanti per O , allora $U \cup W$ non è un sottospazio di V .

Suggerimento. Basta mostrare che, presi $u \in U$ e $w \in W$, entrambi diversi dall'origine, $v + w$ non appartiene mai alla unione $U \cup W$.

L'esempio delle rette nel piano ci suggerisce che, il più piccolo sottospazio vettoriale di V che contiene sia U sia W , deve necessariamente (per essere chiuso per la somma) contenere tutti gli elementi della forma $u + w$ dove $u \in U$ e $w \in W$. Introduciamo dunque una definizione:

DEFINIZIONE 1.37. Dati due sottospazi vettoriali U e W di uno spazio vettoriale V su \mathbb{K} , chiamiamo **somma** di U e W l'insieme

$$U + W = \{u + w \mid u \in U, w \in W\}$$

Mostreremo ora come, se U e W sono spazi vettoriali, l'insieme somma $U + W$ è un sottospazio vettoriale di V :

PROPOSIZIONE 1.38. *Dati due sottospazi vettoriali U e W di uno spazio vettoriale V su \mathbb{K} , l'insieme $U + W$ è un sottospazio vettoriale di V (ed è dunque il più piccolo sottospazio contenente sia U che W).*

DIMOSTRAZIONE. L'elemento O appartiene sia ad U che a W , e dunque anche ad $U + W$, infatti possiamo scriverlo come somma nel modo che segue:

$$O = \underbrace{O}_{\in U} + \underbrace{O}_{\in W}$$

Ora dati $a \in \mathbb{K}$ e $x, y \in U + W$, per definizione di $U + W$ esistono u_1, u_2 in U e w_1, w_2 in W tali che: $x = u_1 + w_1$ e $y = u_2 + w_2$. Sfruttando la chiusura per addizione vettoriale e per moltiplicazione scalare di U e W (che sono sottospazi di V) si ha:

$$\begin{aligned} x + y &= (u_1 + w_1) + (u_2 + w_2) = \underbrace{(u_1 + u_2)}_{\in U} + \underbrace{(w_1 + w_2)}_{\in W} \in U + W \\ ax &= a(u_1 + w_1) = \underbrace{au_1}_{\in U} + \underbrace{aw_1}_{\in W} \in U + W \end{aligned}$$

□

5. Base di uno spazio vettoriale

Sia V uno spazio vettoriale su un campo \mathbb{K} e supponiamo che gli n vettori v_1, v_2, \dots, v_n stiano in V . Allora ripercorrendo in parte il ragionamento seguito nella sezione precedente, quando abbiamo introdotto lo spazio vettoriale somma di due spazi vettoriali, necessariamente (per la proprietà di V di essere chiuso per addizione vettoriale e moltiplicazione per scalare) in V ci staranno anche tutti i multipli scalari dei vari v_i , e le loro somme. Ovvero, se v_1, v_2, \dots, v_n sono n vettori di V , allora per qualsiasi scelta di n elementi k_1, k_2, \dots, k_n (non necessariamente distinti) di \mathbb{K} il vettore:

$$v = k_1v_1 + \dots + k_nv_n = \sum_{i=1}^n k_iv_i$$

appartiene a V .

DEFINIZIONE 1.39. Dato un insieme di vettori $\{v_1, v_2, \dots, v_k\}$ di V , spazio vettoriale sul campo \mathbb{K} , il vettore:

$$v = k_1v_1 + \dots + k_nv_n$$

con $\{k_1, k_2, \dots, k_n\}$ scalari di \mathbb{K} , si dice una **combinazione lineare** dei vettori v_1, v_2, \dots, v_k . I k_i sono detti **coefficienti** della combinazione lineare.

ESEMPIO 1.40. Consideriamo lo spazio vettoriale \mathbb{R}^3 su \mathbb{R} con le operazioni di addizione vettoriale e moltiplicazione per scalare introdotti⁴ nell'esercizio 1.11, e i due vettori seguenti:

$$v_1 = \begin{pmatrix} 3 \\ -1 \\ 3 \end{pmatrix} \quad v_2 = \begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix}$$

⁴D'ora in avanti, tutte le volte che tratteremo gli spazi vettoriali \mathbb{K}^n su \mathbb{K} ometteremo di fare questa precisazione, dunque - salvo esplicita dichiarazione - si supporrà che le operazioni su \mathbb{K}^n siano quelle definite nell'Esercizio 1.11.

Allora il vettore v_3 seguente:

$$v_3 = \begin{pmatrix} 5 \\ -1 \\ 7 \end{pmatrix} = 1 \cdot \begin{pmatrix} 3 \\ -1 \\ 3 \end{pmatrix} + 2 \cdot \begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix}$$

è una combinazione lineare dei vettori v_1, v_2 con coefficienti 1 e 2.

DEFINIZIONE 1.41. Dati uno spazio vettoriale V su \mathbb{K} ed un insieme $A = \{v_1, v_2, \dots, v_t\}$ di vettori di V , l'insieme di tutte le combinazioni lineari a coefficienti in \mathbb{K} di $\{v_1, v_2, \dots, v_t\}$ si chiama **Span** dell'insieme A , e si indica con il simbolo $Span(A)$ o con il simbolo $\langle v_1, v_2, \dots, v_t \rangle$.

PROPOSIZIONE 1.42. *Dato uno spazio vettoriale V sul campo \mathbb{K} , per ogni $t > 0$ e per ogni scelta di vettori $\{v_1, v_2, \dots, v_t\}$ di V si ha che $Span(v_1, v_2, \dots, v_t)$ è un sottospazio vettoriale.*

ESERCIZIO 1.43. Dimostrare la Proposizione 1.42.

OSSERVAZIONE 1.44. Dati uno spazio vettoriale V su un campo \mathbb{K} , e un sottoinsieme A di V , composto da n (con $t > 0$) vettori v_1, \dots, v_t , abbiamo già osservato che un qualsiasi sottospazio di V che contenga A deve contenere $Span(A)$. La Proposizione 1.42 ci dice che $Span(A)$ è un sottospazio di V . Dunque abbiamo un'altra caratterizzazione di $Span(A)$: è il più piccolo sottospazio vettoriale di V che contenga A . In conseguenza di questa osservazione, si dice anche che $Span(A)$ è il **sottospazio generato** dai vettori v_1, \dots, v_t .

OSSERVAZIONE 1.45. Non è detto che lo Span di n vettori, con $n > 0$, sia un sottospazio vettoriale **proprio** di V : può accadere che $V = Span(v_1, \dots, v_n)$. Inoltre lo Span del solo vettore O è il sottospazio $V = \{O\}$.

ESERCIZIO 1.46. Dimostrare, scegliendo opportunamente un sottoinsieme finito A di vettori di \mathbb{R}^3 , tale che $Span(A) = \mathbb{R}^3$, quanto enunciato nell'Osservazione 1.45, ovvero che esistono $Span$ di insiemi finiti di vettori di uno spazio vettoriale V , che non sono sottospazi vettoriali propri di V , in quanto sono uguali a V stesso.

DEFINIZIONE 1.47. Un insieme di vettori $\{v_1, v_2, \dots, v_k\}$ di V per cui

$$V = Span(v_1, \dots, v_t)$$

si dice **un insieme di generatori** di V . In tal caso si dice anche che i vettori v_1, v_2, \dots, v_k **generano** V .

L'esistenza di un sistema finito di generatori per uno spazio vettoriale V su un campo \mathbb{K} è un fatto, come si può intuire, molto importante: si riduce infatti la descrizione di uno spazio vettoriale (che, se \mathbb{K} ha cardinalità infinita, sappiamo dall'Esercizio 1.33, avere infiniti vettori), alla lista di un numero finito di vettori (i generatori), dalle cui combinazioni lineari si possono ottenere tutti i vettori di V .

Dato un sistema di generatori $\{v_1, \dots, v_t\}$ di V sappiamo dunque che ogni v in V si può scrivere, con una opportuna scelta dei coefficienti k_1, \dots, k_t , come:

$$(5.1) \quad v = \sum_{i=1}^t k_i v_i$$

Ci chiediamo se, fissato l'insieme dei generatori, tali coefficienti caratterizzano un vettore (questo ci permetterebbe di descrivere ogni vettore come una t -upla di elementi di \mathbb{K}), ovvero se la scrittura nell'Equazione 5.1 è, in generale, unica (il che ci direbbe che, fissato il sistema di generatori, ogni vettore v di V è univocamente identificato e dunque determinato, dall'unica scelta di coefficienti per cui vale l'uguaglianza espressa in 5.1). In generale la risposta a questa domanda è no, come possiamo vedere dal seguente esempio:

ESEMPIO 1.48. Consideriamo i 4 vettori di \mathbb{R}^3 seguenti:

$$\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 2 \\ 4 \end{pmatrix}$$

e lo Span dei 4 vettori. Il vettore di \mathbb{R}^3 seguente:

$$\begin{pmatrix} 2 \\ 2 \\ 5 \end{pmatrix}$$

appartiene allo Span dei 4 vettori, infatti:

$$\begin{pmatrix} 2 \\ 2 \\ 5 \end{pmatrix} = 1 \cdot \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + 1 \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} + 1 \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} + 0 \cdot \begin{pmatrix} 2 \\ 2 \\ 4 \end{pmatrix}$$

Ma tale combinazione lineare non è unica, ad esempio un'altra combinazione lineare dei 4 vettori che restituisce il vettore cercato è la seguente:

$$\begin{pmatrix} 2 \\ 2 \\ 5 \end{pmatrix} = 0 \cdot \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + 0 \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} + 1 \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} + 1 \cdot \begin{pmatrix} 2 \\ 2 \\ 4 \end{pmatrix}$$

ESERCIZIO 1.49. Dimostrare che i 4 vettori dell'esempio precedente generano \mathbb{R}^3 , quindi che ogni vettore di \mathbb{R}^3 può essere scritto come combinazione lineare di questi 4 vettori.

Abbiamo dunque che, in generale, la scrittura di un vettore che appartiene allo Span di n vettori non è unica. Ci chiediamo allora quale ulteriore condizione bisogna imporre sugli n vettori di cui consideriamo lo Span, per poter essere sicuri che ogni elemento dello spazio venga espresso in maniera unica come combinazione lineare. Il concetto chiave è quello di *indipendenza lineare*:

DEFINIZIONE 1.50. Dato uno spazio vettoriale V su \mathbb{K} , si dice che un insieme finito (non vuoto) di vettori $\{v_1, v_2, \dots, v_r\}$ è un **insieme di vettori linearmente indipendenti** su \mathbb{K} se l'unico modo di scrivere il vettore O come combinazione lineare di questi vettori (a coefficienti in \mathbb{K}) è con tutti i coefficienti nulli, ossia se

$$a_1v_1 + a_2v_2 + \dots + a_rv_r = O \iff a_1 = a_2 = \dots = a_r = 0$$

Talvolta si dice anche, più brevemente, che i vettori v_1, v_2, \dots, v_r sono **linearmente indipendenti**.

Se invece i vettori v_1, v_2, \dots, v_r non sono linearmente indipendenti, si dice che sono **linearmente dipendenti** su \mathbb{K} (o che l'insieme $\{v_1, v_2, \dots, v_r\}$ è un **insieme di vettori linearmente dipendenti**).

Il concetto di lineare indipendenza di un insieme di vettori $A = \{v_1, \dots, v_n\}$ in particolare equivale al fatto che nessuno dei vettori v_i si possa scrivere come combinazione lineare dell'insieme ottenuto da A togliendo il vettore v_i , ovvero che nessun v_i appartenga allo *Span* dell'insieme di vettori formato dai vettori di A tranne v_i :

PROPOSIZIONE 1.51. *Un insieme $A = \{v_1, \dots, v_n\}$ di vettori di uno spazio vettoriale V su \mathbb{K} è un insieme di vettori linearmente indipendenti se e solo se nessun v_i appartenente ad A si può scrivere come combinazione lineare dell'insieme $B = A \setminus \{v_i\}$ (ovvero v_i non appartiene a $\text{Span}(B)$).*

DIMOSTRAZIONE. \Rightarrow) Sia A un insieme di vettori linearmente indipendenti e supponiamo per assurdo che esista un v_i che si scriva come combinazione lineare dei vettori di A diversi da lui. Possiamo senza perdere di generalità supporre che tale vettore sia quello che abbiamo indicato con v_1 , e dunque stiamo supponendo che $v_1 \in \text{Span}(v_2, \dots, v_n)$, ovvero che esistono $n - 1$ scalari a_2, \dots, a_n di \mathbb{K} tali che:

$$\underbrace{\sum_{i=2}^n a_i \cdot v_i}_{a_2 \cdot v_2 + \dots + a_n \cdot v_n} = v_1$$

Ma da questa, aggiungendo ad entrambi i membri dell'uguaglianza l'opposto di v_1 , seguirebbe che:

$$a_2 \cdot v_2 + \dots + a_n \cdot v_n - v_1 = O$$

Ovvero avremmo trovato una combinazione lineare non nulla (perché il coefficiente di v_1 è uguale a -1 (vedi Proposizione 1.19) dei vettori di A , contro l'ipotesi che A sia un insieme di vettori linearmente indipendenti.

\Leftarrow) Siano i vettori di A tali che nessuno di loro si può scrivere come combinazione lineare degli altri vettori di A . Supponiamo per assurdo che A sia un insieme di vettori linearmente dipendenti. Allora devono esistere

n scalari a_i , non tutti nulli, tali che:

$$\underbrace{\sum_{i=1}^n a_i \cdot v_i}_{a_1 \cdot v_1 + \dots + a_n \cdot v_n} = O$$

Non essendo, per ipotesi, i coefficienti tutti nulli, almeno uno dei coefficienti deve essere diverso da zero. Eventualmente riordinando l'ordine dei vettori (dovrebbe essere abbastanza ovvio che la dipendenza lineare di un insieme di vettori non dipende dall'ordine in cui si elencano) possiamo supporre che sia a_1 diverso da 0, e scrivere:

$$\sum_{i=2}^n -a_i \cdot v_i = a_1 \cdot v_1$$

Ed essendo $a_1 \in \mathbb{K}$ diverso da 0, esiste l'inverso a_1^{-1} di a_1 in \mathbb{K} . Moltiplicando per questo inverso otteniamo:

$$\sum_{i=2}^n \frac{-a_i}{a_1} \cdot v_i = v_1$$

Ottenendo, contro l'ipotesi iniziale, che v_1 è combinazione lineare di v_2, \dots, v_n . □

OSSERVAZIONE 1.52. La caratteristica di essere un insieme di vettori linearmente dipendenti, come ben espresso dalla definizione, è, per l'appunto, una caratteristica che riguarda l'intero insieme dei vettori. Ad esempio, può accadere (ma non in generale) che se da un insieme di n vettori linearmente dipendenti ne togliamo uno, l'insieme residuo, costituito da $n - 1$ vettori, risulta un insieme di vettori linearmente indipendenti. Daremo un esempio fra poco: il lettore provi intanto a pensare ad un esempio nello spazio vettoriale \mathbb{R}^2 .

ESERCIZIO 1.53. Dimostrare che un insieme composto da un unico vettore v , diverso dal vettore nullo, è sempre un insieme di vettori linearmente indipendenti (Suggerimento: vedi Esercizio 1.17).

ESERCIZIO 1.54. Sia V uno spazio vettoriale su \mathbb{K} . Dimostrare che se $A = \{v_1, \dots, v_n\}$ è un sottoinsieme di V di vettori linearmente indipendenti, allora qualsiasi sottoinsieme non vuoto di A è un insieme di vettori linearmente indipendenti.

ESERCIZIO 1.55. Considerati i vettori dell'Esempio 1.48:

$$\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 2 \\ 4 \end{pmatrix}$$

Dimostrare che:

- (1) l'insieme contenente questi vettori è un insieme di vettori linearmente dipendenti, mostrando esplicitamente una combinazione lineare di questi vettori che sia uguale a 0, ma non abbia tutti i coefficienti nulli,
- (2) gli insiemi costituiti rispettivamente dai primi tre vettori, e dagli ultimi tre, sono entrambi linearmente indipendenti,
- (3) in riferimento a quanto detto nell'Osservazione 1.52, mostrare che se invece si considera l'insieme costituito dal primo, secondo e quarto vettore, tale insieme continua ad essere un insieme di vettori linearmente dipendenti.

Abbiamo definito cosa è un insieme di generatori di uno spazio vettoriale, e cosa significa insieme di vettori linearmente indipendenti. Consideriamo gli insiemi di vettori che verificano entrambe queste due proprietà:

DEFINIZIONE 1.56. Sia V uno spazio vettoriale su \mathbb{K} , un insieme di vettori $\{v_1, v_2, \dots, v_n\}$ di V , che genera lo spazio V e che è un insieme di vettori linearmente indipendenti si dice una **base** (finita) di V .

OSSERVAZIONE 1.57. Nella Definizione 1.56 è specificato *finita*. Non sempre uno spazio vettoriale ammette un numero finito di generatori, e di conseguenza nemmeno una base finita. Un caso che abbiamo incontrato di spazio vettoriale che non ammette una base finita è lo spazio vettoriale $\mathbb{K}[x]$ dei polinomi a coefficienti in \mathbb{K} . Basta osservare che i termini di grado n di un polinomio, si ottengono solo inserendo nell'insieme dei generatori un polinomio che contenga $a_n x^n$ con a_n diverso da 0 (perché?). A questo punto sorge spontanea la domanda: ma tale spazio vettoriale ammetterà una base infinita oppure non ha una base? Per rispondere però dovremmo ampliare la definizione di combinazione lineare (e poi di indipendenza lineare) a insiemi infiniti⁵. Ma in questo corso considereremo quasi esclusivamente spazi vettoriali che ammettono una base finita, e ad ogni modo, cercheremo solo basi di spazi vettoriali che ne hanno una finita.

Fissata la definizione di base finita⁶ di uno spazio vettoriale, siamo interessati a rispondere alle seguenti due domande:

- (1) se fissiamo una base di uno spazio vettoriale, siamo sicuri che ogni vettore dello spazio si scrive in maniera unica come combinazione lineare degli elementi della base?
- (2) Se uno spazio vettoriale V ammette un insieme finito di generatori, si può dedurre che V ha una base finita?

⁵Questo si fa chiedendo che le combinazioni lineari che appaiono nelle formule siano comunque composte da un numero finito di addendi, ovvero che tranne un numero finito di coefficienti, tutti gli altri siano uguali a 0. Dopodiché non è difficile verificare che l'insieme delle potenze di x con esponente $n \in \mathbb{N}$ è una base di $\mathbb{K}[x]$.

⁶D'ora innanzi non ricorderemo più questo aspetto, sottintendendo che tutti i risultati che proveremo si riferiranno al caso finito.

Cominciamo analizzando il primo aspetto. Fissiamo dunque uno spazio vettoriale V (sul campo \mathbb{K}) e supponiamo che ammetta una base finita $\{v_1, v_2, \dots, v_n\}$. Dimostriamo che effettivamente la definizione di base permette di avere un'unica rappresentazione di ogni vettore di V come combinazione lineare dei vettori della base:

PROPOSIZIONE 1.58. *Ogni vettore $v \in V$ si scrive in modo unico come combinazione lineare degli elementi della base.*

DIMOSTRAZIONE. Il vettore v si può scrivere come combinazione lineare degli elementi della base perché, per definizione, gli elementi della base generano V . L'unicità di una tale combinazione lineare è conseguenza della lineare indipendenza degli elementi della base. Infatti, supponiamo che si possa scrivere:

$$v = a_1v_1 + a_2v_2 + \dots + a_nv_n = b_1v_1 + b_2v_2 + \dots + b_nv_n$$

dove gli a_i e i b_j sono elementi del campo \mathbb{K} . Allora:

$$v - v = O = (a_1 - b_1)v_1 + (a_2 - b_2)v_2 + \dots + (a_n - b_n)v_n$$

Ma sappiamo che i vettori v_1, v_2, \dots, v_n sono linearmente indipendenti. Dunque la combinazione lineare che abbiamo scritto sopra, e che ha come risultato O , deve avere tutti i coefficienti nulli.

Questo implica che $a_i - b_i = 0$ per ogni i , ovvero che $a_i = b_i$ per ogni i . Abbiamo dunque provato che esiste un solo modo di scrivere v come combinazione lineare degli elementi della base data. \square

OSSERVAZIONE 1.59. Una precisazione importante sul significato di **in modo unico**: si intende che per ottenere lo specifico vettore v , i coefficienti di ciascun vettore della base sono fissati, ma ovviamente (vale la proprietà commutativa) possiamo cambiare l'ordine degli addendi della combinazione lineare. Ad esempio se $\{v_1, v_2\}$ è una base dello spazio vettoriale V e $v = 3v_1 + 7v_2$, possiamo scrivere anche $v = 7v_2 + 3v_1$. Quello che rimane fisso (ed è quello che ci dice la Proposizione 1.58) è la corrispondenza vettore-coefficiente: ovvero devo scegliere 3 per il vettore v_1 e 7 per il vettore v_2 .

Se fissiamo una volta per tutte l'ordine degli elementi della base, ed è quello che solitamente si fa, allora fissiamo definitivamente la sequenza dei coefficienti.

Visti i risultati provati, dovrebbe cominciare ad essere chiara l'importanza di essere in grado di determinare, se possibile, la base di uno spazio vettoriale. Un primo risultato molto significativo da questo punto di vista, è riassunto nel prossimo teorema, che risponde alla seconda questione sulle basi che avevamo sollevato, ovvero se il fatto che uno spazio vettoriale V abbia un insieme finito di generatori, garantisce o no che V abbia una base finita. Il teorema è importante non solo dal punto di vista teorico (si riassume dicendo che si può sempre **estrarre** una base da un insieme finito di generatori), ma anche *pratico*. Infatti dalla dimostrazione del teorema segue

una caratterizzazione della base che sarà utile per ricavare, appunto concretamente, una base, una volta conosciuto un insieme finito di generatori dello spazio vettoriale.

TEOREMA 1.60. *Sia V uno spazio vettoriale (sul campo \mathbb{K}) diverso da $\{O\}$ e generato dall'insieme finito di vettori non nulli $\{w_1, w_2, \dots, w_s\}$. Allora è possibile estrarre da $\{w_1, w_2, \dots, w_s\}$ un sottoinsieme $\{w_{i_1}, w_{i_2}, \dots, w_{i_n}\}$ (con $n \leq s$) che è una base di V .*

DIMOSTRAZIONE. Consideriamo l'insieme:

$$\mathcal{M} = \{A \subseteq \{w_1, w_2, \dots, w_s\} \mid A \text{ è un insieme di vettori lin. ind.}\}$$

e notiamo che \mathcal{M} non è vuoto, in quanto contiene certamente i sottoinsiemi di $\{w_1, w_2, \dots, w_s\}$ di cardinalità 1, tipo $\{w_1\}$ o $\{w_2\}$ (vedi Esercizio 1.53). Fra tutti gli elementi di \mathcal{M} consideriamone uno di cardinalità massima: $W = \{w_{i_1}, w_{i_2}, \dots, w_{i_n}\}$ (sicuramente è $n \geq 1$ ossia tale insieme non è vuoto). Questo W è proprio il nostro candidato ad essere una base di V .

Osserviamo per prima cosa che W , per come lo abbiamo costruito (vedi Esercizio 1.54), è un insieme di vettori linearmente indipendenti: resta da dimostrare che genera V .

Per questo bisogna mostrare che con combinazioni lineari dei vettori di W possiamo ottenere uno qualunque dei vettori $\{w_1, w_2, \dots, w_s\}$ che sappiamo, per ipotesi, generare V ⁷.

Se $\{w_{i_1}, w_{i_2}, \dots, w_{i_n}\} = \{w_1, w_2, \dots, w_s\}$ abbiamo già finito: i vettori di partenza costituiscono di già un insieme di vettori linearmente indipendenti, e dunque sono una base finita di V .

Se invece

$$\{w_{i_1}, w_{i_2}, \dots, w_{i_n}\} \subsetneq \{w_1, w_2, \dots, w_s\}$$

allora prendiamo un vettore, diciamo w_r , che non appartiene a $\{w_{i_1}, w_{i_2}, \dots, w_{i_n}\}$. Dobbiamo dimostrare che w_r si può scrivere come combinazione lineare dei vettori $\{w_{i_1}, w_{i_2}, \dots, w_{i_n}\}$.

Se consideriamo l'insieme $\{w_r, w_{i_1}, w_{i_2}, \dots, w_{i_n}\}$ notiamo che certamente questo non è un insieme di vettori linearmente indipendenti, altrimenti apparterebbe a \mathcal{M} e non sarebbe più vero che $\{w_{i_1}, w_{i_2}, \dots, w_{i_n}\}$ ha cardinalità massima fra gli elementi di \mathcal{M} .

Dunque esiste una combinazione lineare:

$$a_r w_r + a_{i_1} w_{i_1} + a_{i_2} w_{i_2} + \dots + a_{i_n} w_{i_n} = 0$$

che è non banale, ossia i coefficienti non sono tutti zero. In particolare risulta che non può essere $a_r = 0$, altrimenti resterebbe una combinazione lineare non banale:

$$a_{i_1} w_{i_1} + a_{i_2} w_{i_2} + \dots + a_{i_n} w_{i_n} = 0$$

che contraddirebbe la lineare indipendenza di $\{w_{i_1}, w_{i_2}, \dots, w_{i_n}\}$.

⁷Verificare di aver capito bene questo passaggio! In pratica stiamo dicendo che se lo *Span* di un insieme di vettori di uno spazio vettoriale V , contiene un insieme di generatori di V , allora quello *Span* è uguale a V .

Visto dunque che $a_r \neq 0$, si può dividere tutto per a_r ottenendo:

$$w_r = -\frac{a_{i_1}}{a_r}w_{i_1} - \frac{a_{i_2}}{a_r}w_{i_2} - \dots - \frac{a_{i_n}}{a_r}w_{i_n}$$

che è la combinazione lineare cercata. □

OSSERVAZIONE 1.61. Dalla dimostrazione del Teorema 1.60 segue la seguente caratterizzazione, a cui abbiamo già accennato: ogni sottoinsieme massimale di vettori linearmente indipendenti dell'insieme dei generatori di V è una base di V ; questo ci suggerisce che la base di uno spazio vettoriale non è unica. Osserviamo infatti che se uno spazio vettoriale V ammette una base finita v_1, \dots, v_n allora anche $\lambda \cdot v_1, v_2, \dots, v_n$ è una base di V , diversa dalla precedente, qualsiasi sia $\lambda \in \mathbb{K} \setminus \{0\}$.

L'Osservazione 1.61 sottolinea il fatto che uno spazio vettoriale che ammette una base ne ammette anche altre (se il campo \mathbb{K} è infinito, ne ammette infinite altre). Può dunque sorgere il dubbio che il numero di elementi di una base di uno spazio vettoriale V dipenda dalla base scelta e non da V . Il seguente teorema (che dimostreremo nel Paragrafo 2 del Capitolo 2), risponde a questo legittimo dubbio:

TEOREMA 1.62. *Sia V uno spazio vettoriale sul campo \mathbb{K} che ammette una base finita. Allora tutte le basi di V hanno la stessa cardinalità.*

Possiamo dunque dare la seguente definizione:

DEFINIZIONE 1.63. Sia V uno spazio vettoriale con basi di cardinalità $n \geq 1$. Tale cardinalità n è detta la **dimensione** di V . Diremo inoltre che lo spazio vettoriale $\{O\}$ ha dimensione 0.

ESERCIZIO 1.64. Dimostrare che $\mathbb{K}^{\leq n}[x]$ (che sappiamo dall'Esercizio 1.28 essere un sottospazio vettoriale di $\mathbb{K}[x]$) ha dimensione $n + 1$. (Suggerimento: mostrare che $\{1, x, x^2, \dots, x^n\}$ è una base).

ESERCIZIO 1.65. Consideriamo il seguente sottoinsieme di $\mathbb{Q}[x]$:

$$W = \{p(x) \in \mathbb{Q}[x] \mid \deg(p(x)) \leq 3 \text{ e } p(x) \text{ è divisibile per } (x - 4)\}$$

- (1) Dimostrare che W è sottospazio vettoriale di $\mathbb{Q}[x]$.
- (2) Trovare la dimensione di W .

Svolgimento. Per dimostrare che W è un sottospazio di $\mathbb{Q}[x]$ basta osservare che W è l'intersezione di due sottospazi di $\mathbb{Q}[x]$, ovvero U , l'insieme dei polinomi di grado minore o uguale a 3, e V , l'insieme dei polinomi divisibili per $x - 4$ (o equivalentemente che si annullano in 4).

Per trovare la dimensione del sottospazio W , ne determineremo una base. Osserviamo che un polinomio $p(x)$ di W è per definizione del tipo:

$$\underbrace{(x - 4)}_{\text{divisibile per } x-4} \cdot \underbrace{(ax^2 + bx + c)}_{\text{di grado } \leq 3} \quad a, b, c \in \mathbb{Q}$$

Ovvero:

$$p(x) = ax^2(x - 4) + bx(x - 4) + c(x - 4)$$

Quindi $\{(x-4), x(x-4), x^2(x-4)\}$ è un insieme di generatori di W .

Lasciamo al lettore il compito di verificare che questi tre vettori sono anche linearmente indipendenti (come del resto tutti gli insiemi di polinomi composti da polinomi che a due a due hanno grado diverso). Quindi $\{(x-4), x(x-4), x^2(x-4)\}$ è una base di W , che dunque abbiamo scoperto avere dimensione 3.

ESERCIZIO 1.66. Dati due sottospazi vettoriali U e W di uno spazio vettoriale V su \mathbb{K} :

- (1) dimostrare che la dimensione del sottospazio intersezione $U \cap W$ è minore o uguale del minimo tra la dimensione di U e quella di W ,
- (2) discutere quando la dimensione dell'intersezione è esattamente uguale al minimo tra la dimensione di U e quella di W .

ESERCIZIO 1.67. Sia W il sottospazio di \mathbb{R}^3 generato dai vettori: $(1, -1, 0)$ e $(b-1, b+1, -b)$ (con $b \in \mathbb{R}$) e U il sottoinsieme di \mathbb{R}^3 definito da:

$$U = \{(x, y, z) \in \mathbb{R}^3 \mid x + y + 2z = 0\}$$

- (1) Dimostrare che U è sottospazio di \mathbb{R}^3 .
- (2) Calcolare la dimensione di U e, al variare di $b \in \mathbb{R}$, la dimensione di W .
- (3) Calcolare, al variare di $b \in \mathbb{R}$, la dimensione di $U \cap W$.

Svolgimento. Il vettore $(0, 0, 0)$ appartiene ad U infatti: $0 + 0 + 2 \cdot 0 = 0$. Siano (x_1, y_1, z_1) e (x_2, y_2, z_2) due vettori di U e consideriamo:

$$(x_1, y_1, z_1) + (x_2, y_2, z_2) = (x_1 + x_2, y_1 + y_2, z_1 + z_2)$$

e

$$\lambda \cdot (x_1, y_1, z_1) = (\lambda x_1, \lambda y_1, \lambda z_1)$$

al variare di λ in \mathbb{R} . Dobbiamo mostrare che questi due elementi appartengono ancora ad U , ma la verifica è del tutto banale infatti:

$$(x_1 + x_2) + (y_1 + y_2) + 2(z_1 + z_2) = \underbrace{x_1 + y_1 + 2z_1}_{=0} + \underbrace{x_2 + y_2 + 2z_2}_{=0} = 0$$

e

$$\lambda x_1 + \lambda y_1 + 2\lambda z_1 = \lambda \underbrace{(x_1 + y_1 + 2z_1)}_{=0} = 0$$

Per determinare la dimensione di U cerchiamo di identificarne una base. Il sottospazio U è determinato dalla condizione $x + y + 2z$ che ha due gradi di libertà, ovvero se assegnamo un valore s alla variabile z , e un valore t alla variabile y abbiamo che il valore di x è univocamente determinato ed è uguale a $-t - 2s$, si ha cioè:

$$\begin{cases} y = s \\ z = t \\ x = -t - 2s \end{cases}$$

e quindi ogni vettore (x, y, z) di U è del tipo:

$$(-t - 2s, t, s) = (-1, 1, 0) \cdot t + (-2, 0, 1) \cdot s$$

cioè $\{(-1, 1, 0), (-2, 0, 1)\}$ è un insieme di generatori di U (quindi la dimensione di U è minore o uguale a 2). È facile mostrare che i due vettori sono anche linearmente indipendenti (esercizio!) e quindi $\{(-1, 1, 0), (-2, 0, 1)\}$ è una base di U e la dimensione di U è 2.

Per quanto riguarda la dimensione di W bisogna capire, al variare di $b \in \mathbb{R}$, se i due vettori $(1, -1, 0)$ e $(b-1, b+1, -b)$ siano linearmente indipendenti (e quindi costituiscano una base di W di cardinalità 2) oppure linearmente dipendenti (e quindi $\dim(W) = 1$ e una sua base è composta da uno dei due vettori):

$$h \cdot (1, -1, 0) + l \cdot (b-1, b+1, -b) = (0, 0, 0)$$

Otteniamo il sistema:

$$\begin{cases} h + l \cdot (b-1) = 0 \\ -h + l \cdot (b+1) = 0 \\ -bl = 0 \end{cases}$$

Se $b \neq 0$ allora l deve essere uguale a zero e di conseguenza anche $h = 0$. Quindi se $b \neq 0$ i due vettori $(1, -1, 0)$ e $(b-1, b+1, -b)$ sono linearmente indipendenti. Se $b = 0$ allora il sistema diventa:

$$\begin{cases} h - l = 0 \\ -h + l = 0 \\ 0 = 0 \end{cases}$$

Che è risolto per ogni scelta di $h = l$ e quindi $(1, -1, 0)$ e $(b-1, b+1, -b)$ sono linearmente dipendenti e W ha dimensione uno.

Infine, per calcolare la dimensione di $U \cap W$, osserviamo che i generatori di W stanno in U infatti:

$$1 - 1 + 2 \cdot 0 = 0 \quad \text{e} \quad (b-1) + (b+1) + 2 \cdot (-b) = 2b - 2b = 0$$

Quindi $W \subseteq U$ e $W \cap U = W$. Perciò abbiamo già trovato la dimensione di $W \cap U$ nel punto precedente.

6. Applicazioni lineari

Abbiamo introdotto la struttura di spazio vettoriale e il concetto di sottospazio vettoriale; è naturale chiedersi quali funzioni “rispettano” queste strutture, ovvero quali funzioni mandano sottospazi in sottospazi.⁸

Mostriamo con un esempio che, in generale, la proprietà di mandare sottospazi in sottospazi non è garantita da una funzione:

⁸Ovvero se f è una funzione da uno spazio vettoriale V ad uno spazio vettoriale W , vorremmo che per ogni sottospazio U di V , l'immagine $f(U)$ di U tramite f , fosse un sottospazio di W .

ESEMPIO 1.68. Consideriamo la funzione $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ definita da

$$f\left(\begin{pmatrix} x \\ y \end{pmatrix}\right) = \begin{pmatrix} x \\ x^2 \end{pmatrix}$$

La funzione f manda i punti $\begin{pmatrix} x \\ x \end{pmatrix}$, con la prima e seconda coordinata uguali, ovvero i punti della retta di equazione $x = y$, nella parabola di equazione $y = x^2$. Ma, come sappiamo dalla Proposizione 1.27, la retta $y = x$, passando dall'origine, è un sottospazio di \mathbb{R}^2 , mentre la parabola non lo è (è facile mostrarlo direttamente, e comunque sappiamo dalla Proposizione 1.27 che i sottospazi propri di \mathbb{R}^2 sono le rette passanti per l'origine).

Dobbiamo dunque considerare funzioni (applicazioni) con proprietà *particolari*:

DEFINIZIONE 1.69. Siano V e W spazi vettoriali di dimensione finita sul campo \mathbb{K} . Una applicazione L da V a W è detta **lineare** se soddisfa le seguenti due proprietà:

$$(6.1) \quad \forall v_1, v_2 \in V \quad L(v_1 + v_2) = L(v_1) + L(v_2)$$

$$(6.2) \quad \forall \lambda \in \mathbb{K} \quad \forall v \in V \quad L(\lambda v) = \lambda L(v)$$

OSSERVAZIONE 1.70. Il soddisfare le due proprietà 6.1 e 6.2 della Definizione 1.69 da parte di una applicazione L , è equivalente a soddisfare la seguente proprietà:

$$(6.3) \quad \forall v_1, v_2 \in V, \forall a, b \in \mathbb{K} \quad L(av_1 + bv_2) = aL(v_1) + bL(v_2)$$

ESERCIZIO 1.71. Dimostrare l'equivalenza tra il soddisfare le proprietà 6.1 e 6.2 e la proprietà 6.3 (ovvero provare che una applicazione L che soddisfa le due proprietà 6.1 e 6.2 necessariamente verifica anche la proprietà 6.3, e viceversa se L verifica la proprietà 6.3 allora necessariamente verifica anche le proprietà 6.1 e 6.2).

Data una applicazione lineare da uno spazio vettoriale V ad uno spazio vettoriale W (entrambi sul campo \mathbb{K}), ha proprietà molto importanti l'insieme degli elementi (vettori) di V che hanno come immagine lo O di W . Per questo diamo un nome a questo insieme:

DEFINIZIONE 1.72. Siano V e W spazi vettoriali sul campo \mathbb{K} e consideriamo una applicazione lineare L da V a W . Chiameremo **nucleo** di L , e lo indicheremo⁹ con $Ker L$, il seguente sottoinsieme di V :

$$Ker L = \{v \in V \mid L(v) = O\}$$

Cominciamo a delineare le prime proprietà del nucleo e dell'immagine di una applicazione lineare.

⁹La parola inglese per nucleo è kernel.

PROPOSIZIONE 1.73. *Siano V e W spazi vettoriali sul campo \mathbb{K} e L una applicazione lineare da V a W .*

- (1) *$\text{Ker } L$ è un sottospazio vettoriale di V .*
- (2) *$\text{Imm } L$ è un sottospazio vettoriale di W .*
- (3) *L è iniettiva¹⁰ se e solo se $\text{Ker } L = \{O\}$.*

DIMOSTRAZIONE. Lasciamo le prime due verifiche al lettore e discutiamo la terza proprietà che caratterizza le applicazioni lineari iniettive.

Supponiamo che L sia iniettiva e dimostriamo che $\text{Ker } L = O$. Facciamo vedere che l'unico elemento di V che viene mandato nello O di W ¹¹ è O .

Primo passo: lo O di V ha come immagine lo O di W . Infatti:

$$(6.4) \quad L(O) \underbrace{=}_{\text{def. } O} L(O + O) \underbrace{=}_{L \text{ lineare}} L(O) + L(O)$$

Essendo W uno spazio vettoriale, esiste l'opposto w di $L(O)$, ed aggiungendo w ad entrambi i membri dell'equazione 6.4, si ottiene proprio $L(O) = O$ (dove il primo O è l'elemento neutro in V , e il secondo, l'elemento neutro in W).

A questo punto, essendo L iniettiva, non ci possono essere altri elementi di V , diversi da O , che hanno la stessa immagine. Dunque $\text{Ker } L = \{O\}$.

Ci resta da provare il viceversa, ovvero che se $\text{Ker } L = \{O\}$ allora L è iniettiva. Consideriamo dunque due vettori v, u che hanno la stessa immagine tramite L , e mostriamo che deve essere necessariamente $u = v$. Da $L(u) = L(v)$ sommando da entrambe le parti l'opposto $-L(v)$ di $L(v)$ si ottiene:

$$L(u) - L(v) = O$$

E per linearità di L possiamo scrivere

$$L(u - v) = O$$

Per ipotesi (il $\text{Ker } L$ contiene solo lo O), l'elemento $u - v$ deve essere O , ovvero $u - v = O$, cioè $u = v$. □

Vogliamo adesso mostrare che una qualsiasi applicazione lineare L tra due spazi vettoriali V e W su \mathbb{K} , è completamente caratterizzata una volta che si conoscano i valori di L su una base di V . Questa proprietà delle applicazioni lineari è molto importante anche dal punto di vista algoritmico, perché ci dice che possiamo calcolare qualsiasi immagine tramite L di vettori di V ,

¹⁰Ricordiamo che una applicazione f tra due insiemi A e T è detta iniettiva se per ogni a, b di A , $f(a) = f(b)$ implica $a = b$. La stessa proprietà si può enunciare dicendo che per ogni a, b in A , se $a \neq b$ allora $f(a) \neq f(b)$ (ovvero l'iniettività significa che non ci sono elementi diversi di A che hanno la stessa immagine tramite f).

¹¹Dovremmo indicare diversamente lo O di V e lo O di W , ad esempio usando O_V e O_W , in quanto in generale non saranno lo stesso elemento. Per non appesantire, quando non ci sia confusione sul fatto che stiamo parlando di un elemento di V o di W , useremo sempre la notazione O .

conoscendo in partenza un numero finito di valori (le immagini tramite L dei vettori di una base di V).

Consideriamo dunque due spazi vettoriali V, W di dimensione finita (rispettivamente n e m) sullo stesso campo \mathbb{K} , e una applicazione lineare:

$$L : V \rightarrow W$$

Scegliamo in V una base $\{e_1, \dots, e_n\}$.

Quello che vogliamo è mostrare che, per ogni v di V , riusciamo a scrivere $L(v)$ in termini dei valori $L(e_1), \dots, L(e_n)$. Questo è abbastanza immediato, infatti dato $v \in V$, sappiamo che v si può scrivere in modo unico come combinazione lineare degli elementi della base scelta, ovvero che esistono n scalari b_i tali che:

$$v = b_1 e_1 + \dots + b_n e_n = \sum_{i=1}^n b_i e_i$$

Per la linearità di L si ha che:

$$(6.5) \quad L(v) = b_1 L(e_1) + \dots + b_n L(e_n) = \sum_{i=1}^n b_i L(e_i)$$

Abbiamo dunque mostrato la seguente proposizione:

PROPOSIZIONE 1.74. *Se L è una applicazione lineare tra due spazi vettoriali V e W su \mathbb{K} , allora per conoscere qual è l'immagine di un qualsiasi elemento $v \in V$ tramite L , basta conoscere le immagini tramite L degli elementi di una base scelta di V e le coordinate (b_1, \dots, b_n) di v rispetto alla stessa base.*

A questo punto possiamo caratterizzare lo spazio vettoriale $Imm L$ con L applicazione lineare.

PROPOSIZIONE 1.75. *Se L è una applicazione lineare tra due spazi vettoriali V e W su \mathbb{K} , ed $\{e_1, \dots, e_n\}$ è una base di V , allora:*

$$Imm L = Span(L(e_1), \dots, L(e_n))$$

ESERCIZIO 1.76 (Importante!). Dimostrare la proposizione 1.75.

ESERCIZIO 1.77. Dimostrare che dati due spazi vettoriali V e W , e fissata una base $\{e_1, \dots, e_n\}$ di V , e n elementi w_1, \dots, w_n di W , esiste una e una sola applicazione lineare L da V in W tale che, per ogni i , $L(e_i) = w_i$.

ESERCIZIO 1.78. Siano v_1, \dots, v_n n vettori linearmente indipendenti di uno spazio vettoriale V su \mathbb{K} . Sia L una applicazione lineare iniettiva da V in uno spazio vettoriale W su \mathbb{K} . Allora $L(v_1), \dots, L(v_n)$ sono n vettori linearmente indipendenti di W .

Svolgimento. Supponiamo esista una combinazione lineare degli $L(v_i)$ nulla, ovvero che esistano n elementi di \mathbb{K} a_1, \dots, a_n tali che:

$$(6.6) \quad \sum_{i=1}^n a_i \cdot L(v_i) = O_W$$

Per linearità di L , l'equazione 6.6 si può anche scrivere come segue:

$$(6.7) \quad L\left(\sum_{i=0}^n a_i \cdot v_i\right) = O_W$$

Ma per ipotesi L è iniettiva, e dunque l'equazione 6.7 implica che:

$$\sum_{i=0}^n a_i \cdot v_i = O_V$$

Ora essendo i v_i linearmente indipendenti, da questo segue che gli a_i sono tutti nulli. Dunque abbiamo dimostrato che l'unica combinazione lineare degli $L(v_i)$ nulla, è quella con tutti i coefficienti nulli.

7. Matrici e vettori in colonna per rappresentare applicazioni lineari e elementi di uno spazio vettoriale

Spesso in matematica, il modo di rappresentare gli oggetti può essere molto importante. Nel caso delle applicazioni lineari, è molto utile la rappresentazione tramite oggetti noti come *matrici*.

DEFINIZIONE 1.79. Dati due interi positivi m, n , una **matrice** $m \times n$ a coefficienti in \mathbb{K} è una griglia composta da m righe e n colonne in cui in ogni posizione c'è un elemento di \mathbb{K} (tali elementi vengono chiamati coefficienti della matrice):

$$(7.1) \quad A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & a_{m3} & \dots & a_{mn} \end{pmatrix}$$

Anche fissare con chiarezza la scelta degli indici dei coefficienti della matrice è importante: come si può notare, l'elemento che si trova nella riga i -esima dall'alto e nella colonna j -esima da sinistra viene indicato con a_{ij} . Spesso per indicare la matrice A in 1.1 useremo la notazione sintetica $A = (a_{ij})$ e talvolta, per ricordare quali sono le dimensioni della matrice, scriveremo:

$$A = (a_{ij}) \quad \begin{array}{l} i = 1, 2, \dots, m \\ j = 1, 2, \dots, n \end{array}$$

DEFINIZIONE 1.80. Dati due interi positivi m, n , chiamiamo $Mat_{m \times n}(\mathbb{K})$ l'insieme di tutte le matrici $m \times n$ a coefficienti in \mathbb{K} .

DEFINIZIONE 1.81. Sull'insieme $Mat_{m \times n}(\mathbb{K})$ possiamo in maniera *naturale* definire la addizione e la moltiplicazione per scalare. Date due matrici $A = (a_{ij})$ e $B = (b_{ij})$ in $Mat_{m \times n}(\mathbb{K})$ e dato uno scalare k in \mathbb{K} , definiamo:

- la matrice somma $A+B = C = (c_{ij})$, il cui generico coefficiente nella i -esima riga e j -esima colonna è ottenuto sommando i coefficienti nella stessa posizione (cioè alla i -esima riga e j -esima colonna) di A e di B . Ovvero per ogni $i \leq m$ e per ogni $j \leq n$ $c_{ij} = a_{ij} + b_{ij}$.

Vediamo un esempio di somma tra matrici in $Mat_{2 \times 3}(\mathbb{R})$:

$$\begin{pmatrix} 1 & 2 & 4 \\ 0 & 6 & 3 \end{pmatrix} + \begin{pmatrix} 2 & 2 & 2 \\ 5 & 6 & -8 \end{pmatrix} = \begin{pmatrix} 3 & 4 & 6 \\ 5 & 12 & -5 \end{pmatrix}$$

- la matrice moltiplicazione per scalare $k \cdot A = D = (d_{ij})$, il cui generico coefficiente nella i -esima riga e j -esima colonna è ottenuto moltiplicando lo scalare k per il coefficiente di A nella i -esima riga e j -esima colonna. Ovvero per ogni $i \leq m$ e per ogni $j \leq n$ $d_{ij} = k \cdot a_{ij}$.

Vediamo un esempio di moltiplicazione per scalare di una matrice in $Mat_{2 \times 3}(\mathbb{R})$:

$$3 \begin{pmatrix} 1 & 2 & 4 \\ 0 & 6 & 3 \end{pmatrix} = \begin{pmatrix} 3 & 6 & 12 \\ 0 & 18 & 9 \end{pmatrix}$$

ESERCIZIO 1.82. Dimostrare che, con le operazioni di addizione e moltiplicazione per scalare introdotte nella Definizione 1.81, $Mat_{m \times n}(\mathbb{K})$ è uno spazio vettoriale su \mathbb{K} .

ESERCIZIO 1.83. Dimostrare che la dimensione dello spazio vettoriale $Mat_{m \times n}(\mathbb{K})$ su \mathbb{K} è $m \times n$.

Oltre alle operazioni introdotte nella Definizione 1.81, si può introdurre un'altra operazione tra matrici: il cosiddetto *prodotto righe per colonne*. Per definire tale prodotto è importante anche l'ordine in cui si considerano le due matrici, in quanto sarà definito solo quando il numero di colonne di A è uguale al numero di righe di B . Cioè il prodotto righe per colonne tra una matrice A di $Mat_{m \times n}(\mathbb{K})$ e una matrice B di $Mat_{n \times k}(\mathbb{K})$ è definito solo se $n = h$.

DEFINIZIONE 1.84. Data una matrice $A = (a_{ij})$ di $Mat_{m \times n}(\mathbb{K})$ e una matrice $B = (b_{st})$ di $Mat_{n \times k}(\mathbb{K})$, il **prodotto riga per colonna** AB , è la matrice $C = (c_{rh})$ di $Mat_{m \times k}(\mathbb{K})$, i cui coefficienti, per ogni r, h , sono definiti come segue:

$$c_{rh} = a_{r1}b_{1h} + a_{r2}b_{2h} + a_{r3}b_{3h} + \cdots + a_{rn}b_{nh}$$

Ovvero per ottenere l'elemento c_{rh} dobbiamo moltiplicare progressivamente (ovvero il primo con il primo, il secondo con il secondo, e così via) gli elementi della r -esima riga di A , con gli elementi della h -esima colonna di B (da qui il nome prodotto riga per colonna) e sommare i risultati ottenuti.

ESEMPIO 1.85. Consideriamo la matrice A di $Mat_{2 \times 3}(\mathbb{R})$:

$$A = \begin{pmatrix} 1 & 2 & 4 \\ 0 & 6 & 3 \end{pmatrix}$$

e la matrice B di $Mat_{3 \times 3}(\mathbb{R})$:

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

La definizione ci dice che possiamo definire $C = AB$ e che C è la matrice di $Mat_{2 \times 3}(\mathbb{R})$ i cui coefficienti sono ottenuti come segue:

$$c_{11} = \underbrace{1 \cdot 2}_{a_{11} \cdot b_{11}} + \underbrace{2 \cdot 5}_{a_{12} \cdot b_{21}} + \underbrace{4 \cdot 0}_{a_{13} \cdot b_{31}} = 12$$

$$c_{12} = \underbrace{1 \cdot 2}_{a_{11} \cdot b_{12}} + \underbrace{2 \cdot 6}_{a_{12} \cdot b_{22}} + \underbrace{4 \cdot 1}_{a_{13} \cdot b_{32}} = 18$$

$$c_{13} = \underbrace{1 \cdot 2}_{a_{11} \cdot b_{13}} + \underbrace{2 \cdot (-8)}_{a_{12} \cdot b_{23}} + \underbrace{4 \cdot 0}_{a_{13} \cdot b_{33}} = -14$$

$$c_{21} = \underbrace{0 \cdot 2}_{a_{21} \cdot b_{11}} + \underbrace{6 \cdot 5}_{a_{22} \cdot b_{21}} + \underbrace{3 \cdot 0}_{a_{23} \cdot b_{31}} = 30$$

$$c_{22} = \underbrace{0 \cdot 2}_{a_{21} \cdot b_{12}} + \underbrace{6 \cdot 6}_{a_{22} \cdot b_{22}} + \underbrace{3 \cdot 1}_{a_{23} \cdot b_{32}} = 39$$

$$c_{23} = \underbrace{0 \cdot 2}_{a_{21} \cdot b_{13}} + \underbrace{6 \cdot (-8)}_{a_{22} \cdot b_{23}} + \underbrace{3 \cdot 0}_{a_{23} \cdot b_{33}} = -48$$

E dunque si ha:

$$AB = C = \begin{pmatrix} 12 & 18 & -14 \\ 30 & 39 & -48 \end{pmatrix}$$

OSSERVAZIONE 1.86. In particolare il prodotto definito in 1.84 rappresenta una nuova operazione sull'insieme $Mat_{n \times n}(\mathbb{K})$. Si può verificare che, con la somma introdotta in precedenza e col prodotto righe per colonne l'insieme $Mat_{n \times n}(\mathbb{K})$ è un anello (non commutativo!).

ESERCIZIO 1.87. Mostrare, trovando un opportuno esempio, che date due matrici $n \times n$ A, B , in generale non vale la proprietà commutativa del prodotto riga per colonna (si trovano esempi anche con $n = 2$). E dunque che $Mat_{n \times n}(\mathbb{K})$ è un esempio di anello non commutativo.

Quello di cui vogliamo discutere ora, dopo aver introdotto questo nuovo oggetto matematico, è come poterlo utilizzare per descrivere una applicazione lineare con una notazione *conveniente*.

Sia dunque L una applicazione lineare, tra due spazi vettoriali V, W di dimensione finita (rispettivamente n e m) sullo stesso campo \mathbb{K} . Scegliamo in V una base $\mathcal{B}_V = \{e_1, \dots, e_n\}$ e in W una base $\mathcal{B}_W = \{\epsilon_1, \epsilon_2, \dots, \epsilon_m\}$.

Dalla Proposizione 1.74, sappiamo che per caratterizzare L , basta sapere l'immagine di L sui vettori di una base di V . Consideriamo dunque i vettori

di W $L(e_1), \dots, L(e_n)$. Essendo vettori di W , sappiamo che ognuno di essi può essere scritto come combinazione lineare dei vettori di \mathcal{B}_W . Ovvero, per ogni i , esistono (unici) m scalari a_{ji} (con j che varia da 1 a m) tali che:

$$L(e_i) = \sum_{j=1}^m a_{ji} \epsilon_j = a_{1i} \epsilon_1 + a_{2i} \epsilon_2 + \dots + a_{mi} \epsilon_m$$

Possiamo esprimere il vettore $L(e_i)$ in colonna come segue¹²:

$$(7.2) \quad L(e_i) = \begin{pmatrix} a_{1i} \\ a_{2i} \\ a_{3i} \\ \dots \\ \dots \\ a_{mi} \end{pmatrix}.$$

Consideriamo ora un generico $v \in V$. Scriviamo v come combinazione lineare dei vettori di \mathcal{B}_V . Esistono n scalari b_i tali che:

$$v = b_1 e_1 + \dots + b_n e_n = \sum_{i=1}^n b_i e_i$$

Usando la notazione in colonna appena introdotta per descrivere i vettori, e fissata la base \mathcal{B}_V , possiamo scrivere:

$$v = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ \dots \\ \dots \\ b_n \end{pmatrix}$$

Sappiamo già (vedi Equazione 6.5), che

$$L(v) = b_1 L(e_1) + \dots + b_n L(e_n) = \sum_{i=1}^n b_i L(e_i)$$

Sostituendo quello che sappiamo da 7.2, si ha:

$$L(v) = \sum_{i=1}^n b_i L(e_i) = \sum_{i=1}^n b_i \left(\sum_{j=1}^m a_{ji} \epsilon_j \right)$$

ovvero:

$$L(v) = b_1 (a_{11} \epsilon_1 + a_{21} \epsilon_2 + \dots + a_{m1} \epsilon_m) + \dots + b_n (a_{1n} \epsilon_1 + a_{2n} \epsilon_2 + \dots + a_{mn} \epsilon_m)$$

¹²Da qui in poi, useremo spesso, per uno spazio vettoriale di cui sia stata fissata una base, questa notazione per i vettori. Notazione che, dato un vettore v , lo descrive scrivendo ordinatamente in colonna i coefficienti di v rispetto alla base fissata.

Usando la notazione in colonna appena introdotta, l'uguaglianza può essere scritta nella seguente forma:

$$L(v) = b_1 \begin{pmatrix} a_{11} \\ a_{21} \\ a_{31} \\ \dots \\ \dots \\ a_{m1} \end{pmatrix} + \dots + b_n \begin{pmatrix} a_{1n} \\ a_{2n} \\ a_{3n} \\ \dots \\ \dots \\ a_{mn} \end{pmatrix}$$

ovvero

$$(7.3) \quad L(v) = \begin{pmatrix} b_1 a_{11} + b_2 a_{12} + \dots + b_n a_{1n} \\ b_1 a_{21} + b_2 a_{22} + \dots + b_n a_{2n} \\ b_1 a_{31} + b_2 a_{32} + \dots + b_n a_{3n} \\ \dots \\ \dots \\ b_1 a_{m1} + b_2 a_{m2} + \dots + b_n a_{mn} \end{pmatrix}$$

Una semplice verifica ci permette di osservare che con le notazioni introdotte, e con la definizione di prodotto riga per colonna tra matrici (in questo caso la matrice dei coefficienti di v è una matrice $n \times 1$), l'equazione 7.3 si può scrivere:

$$(7.4) \quad L(v) = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & a_{m3} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ \dots \\ \dots \\ b_n \end{pmatrix}$$

Abbiamo dunque trovato che, fissate una base $\mathcal{B}_V = \{e_1, \dots, e_n\}$ di V , ed una base \mathcal{B}_W di W , la matrice seguente:

$$[L]_{\substack{\mathcal{B}_V \\ \mathcal{B}_W}} = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & a_{m3} & \dots & a_{mn} \end{pmatrix}$$

che ha come elementi della sua i -esima colonna, i coefficienti di $L(e_i)$ rispetto alla base \mathcal{B}_W di W fissata, caratterizza l'applicazione lineare L .

Tale matrice infatti, permette di calcolare, per ogni v di V , i coefficienti del vettore $L(v)$ di W , rispetto alla base \mathcal{B}_W , in maniera algoritmica e semplice. Abbiamo dunque mostrato che:

PROPOSIZIONE 1.88. *Ad ogni applicazione lineare L da uno spazio vettoriale V di dimensione n ad uno spazio vettoriale W di dimensione m ,*

una volta fissate una base \mathcal{B}_V di V e una base \mathcal{B}_W di W , è possibile associare una e una sola matrice $[L]_{\mathcal{B}_W}^{\mathcal{B}_V}$ di $\text{Mat}_{m \times n}(\mathbb{K})$ tale, per ogni vettore

$v \in V$, le cui coordinate rispetto alla base \mathcal{B}_V sono espresse dal vettore co-

lonna $\begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ \dots \\ \dots \\ b_n \end{pmatrix}$, il vettore colonna che rappresenta $L(v)$ rispetto alla base

\mathcal{B}_W è:

$$[L]_{\mathcal{B}_W}^{\mathcal{B}_V} \cdot \begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ \dots \\ \dots \\ b_n \end{pmatrix}$$

Tale matrice si dice **matrice associata** all'applicazione lineare L nelle basi \mathcal{B}_V di V e \mathcal{B}_W di W

PROPOSIZIONE 1.89. *Dati due spazi vettoriali V e W di dimensione rispettivamente n e m su \mathbb{K} , e fissate una base $\mathcal{B}_V = \{e_1, \dots, e_n\}$ di V e una base $\mathcal{B}_W = \{\epsilon_1, \epsilon_2, \dots, \epsilon_m\}$ di W , l'applicazione ϕ dall'insieme delle applicazioni lineari tra V e W alle matrici di $\text{Mat}_{m \times n}(\mathbb{K})$, che associa a L la matrice $[L]_{\mathcal{B}_W}^{\mathcal{B}_V}$, è bigettiva.*

\mathcal{B}_W

DIMOSTRAZIONE. Siano S e T due applicazioni lineari da V in W tali che $\phi(S) = \phi(T)$, ovvero che le matrici associate a S e T rispetto alle basi \mathcal{B}_V e \mathcal{B}_W siano uguali. Per come sono definite le matrici associate, questo significa che S e T coincidono su \mathcal{B}_V . Dall'Esercizio 1.77 segue che $S = T$, ovvero che ϕ è iniettiva.

Vogliamo mostrare ora che ϕ è surgettiva, ovvero che per ogni matrice $M \in \text{Mat}_{m \times n}(\mathbb{K})$ esiste una applicazione lineare L da V in W tale che $\phi(L) = M$. Ma questo è facile, infatti sia:

$$M = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & a_{m3} & \dots & a_{mn} \end{pmatrix}$$

Allora basta considerare l'applicazione lineare L , definita da:

$$L(e_i) = \sum_{j=1}^m a_{ji} \epsilon_j$$

□

Da ora in poi, per semplificare la notazione, ometteremo il riferimento alle basi tutte le volte che potremo farlo senza creare ambiguità, e indicheremo con $[L]$ la matrice associata ad L . Notiamo - e lo mostreremo nel prossimo esempio - che la matrice $[L]$ associata all'applicazione L , non dipende solo da L stessa, ma anche dalle basi scelte per V e W .

Vediamo un esempio di determinazione della matrice di una applicazione lineare rispetto a basi diverse.

ESEMPIO 1.90. Consideriamo gli spazi vettoriali \mathbb{R}^4 e \mathbb{R}^3 con le loro basi standard, rispettivamente

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, e_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, e_4 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

e

$$\epsilon_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \epsilon_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \epsilon_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

Consideriamo l'applicazione lineare

$$L : \mathbb{R}^4 \rightarrow \mathbb{R}^3$$

così definita¹³:

$$L(e_1) = 2\epsilon_1 + \sqrt{3}\epsilon_2$$

$$L(e_2) = 3\epsilon_1 + \epsilon_2 + \epsilon_3$$

$$L(e_3) = \epsilon_1 + 7\epsilon_2 + 8\epsilon_3$$

$$L(e_4) = 2\epsilon_2 + 4\epsilon_3$$

A questa applicazione corrisponde la seguente matrice relativamente alle basi standard:

$$[L]_{\substack{e_1, e_2, e_3, e_4 \\ \epsilon_1, \epsilon_2, \epsilon_3}} = \begin{pmatrix} 2 & 3 & 1 & 0 \\ \sqrt{3} & 1 & 7 & 2 \\ 0 & 1 & 8 & 4 \end{pmatrix}$$

Consideriamo ora una base diversa di \mathbb{R}^4 (verificare che si tratta davvero di una base !):

$$v_1 = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, v_2 = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}, v_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}, v_4 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

¹³Sappiamo, dall'Esercizio 1.77, che, per determinare l'immagine di una applicazione lineare da V a W , e dunque per definirla, basta definire l'immagine degli elementi di una base di V .

e una base diversa anche di \mathbb{R}^3 (anche qui verificare !):

$$w_1 = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, w_2 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, w_3 = \begin{pmatrix} 0 \\ 0 \\ 2 \end{pmatrix}$$

Proviamo a scrivere la matrice

$$[L] \begin{matrix} v_1, v_2, v_3, v_4 \\ w_1, w_2, w_3 \end{matrix}$$

che rappresenta la stessa applicazione lineare L ma rispetto a due basi diverse da quelle standard (osserveremo, come già anticipato, che troveremo una matrice diversa da $[L] \begin{matrix} e_1, e_2, e_3, e_4 \\ e_1, e_2, e_3 \end{matrix}$).

Procediamo esattamente come nel caso precedente (in cui i conti però erano immediati): nella prima colonna della matrice che stiamo per costruire, dovremo mettere il vettore $L(v_1)$ scritto in termini della base $\{w_1, w_2, w_3\}$. Calcoliamolo, facendo in un primo tempo riferimento alle basi standard (d'altra parte la nostra L la abbiamo definita tramite le basi standard, dunque non possiamo far altro che ripartire da quella definizione).

$$L(v_1) = L \left(\begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} \right) = L \left(\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \right) + L \left(\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \right) = \begin{pmatrix} 5 \\ \sqrt{3} + 1 \\ 1 \end{pmatrix}$$

Fin qui, questo vettore è scritto ancora in termini della base standard di \mathbb{R}^3 . Ora dobbiamo esprimerlo in termini della base $\{w_1, w_2, w_3\}$, ovvero dobbiamo trovare a, b, c scalari tali che:

$$\begin{pmatrix} 5 \\ \sqrt{3} + 1 \\ 1 \end{pmatrix} = a \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} + b \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} + c \begin{pmatrix} 0 \\ 0 \\ 2 \end{pmatrix}$$

Impareremo tra breve a risolvere questi sistemi in maniera algoritmica, per ora accontentiamoci di verificare che risulta

$$\begin{pmatrix} 5 \\ \sqrt{3} + 1 \\ 1 \end{pmatrix} = (4 - \sqrt{3}) \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} + (\sqrt{3} + 1) \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} - 2 \begin{pmatrix} 0 \\ 0 \\ 2 \end{pmatrix}$$

e dunque

$$L(v_1) = (4 - \sqrt{3})w_1 + (\sqrt{3} + 1)w_2 - 2w_3$$

Allora il vettore da inserire come prima colonna della matrice

$$[L] \begin{matrix} v_1, v_2, v_3, v_4 \\ w_1, w_2, w_3 \end{matrix}$$

è

$$\begin{pmatrix} 4 - \sqrt{3} \\ \sqrt{3} + 1 \\ -2 \end{pmatrix}$$

Procedendo allo stesso modo per le altre colonne si ottiene (verificare!):

$$[L] \begin{matrix} v_1, v_2, v_3, v_4 \\ w_1, w_2, w_3 \end{matrix} = \begin{pmatrix} 4 - \sqrt{3} & -4 & -8 & -2 \\ \sqrt{3} + 1 & 8 & 9 & 2 \\ -2 & \frac{5}{2} & \frac{11}{2} & 2 \end{pmatrix}$$

OSSERVAZIONE 1.91. Dati due spazi vettoriali V, W , esiste una sola applicazione lineare da V a W la cui matrice associata è indipendente dalle basi scelte. Si tratta della *applicazione nulla* $\mathcal{O} : V \rightarrow W$ che manda ogni $v \in V$ in $0 \in W$. Qualunque siano le basi scelte, la matrice associata a tale applicazione avrà tutti i coefficienti uguali a 0.

ESEMPIO 1.92. Consideriamo l'applicazione lineare L definita nell'Esempio 1.90. Abbiamo già trovato la matrice $[L]$ rispetto alle basi canoniche di \mathbb{R}^4 e \mathbb{R}^3 :

$$[L] \begin{matrix} e_1, e_2, e_3, e_4 \\ \epsilon_1, \epsilon_2, \epsilon_3 \end{matrix} = \begin{pmatrix} 2 & 3 & 1 & 0 \\ \sqrt{3} & 1 & 7 & 2 \\ 0 & 1 & 8 & 4 \end{pmatrix}$$

Supponiamo di voler calcolare l'immagine del vettore v di \mathbb{R}^4 seguente:

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

Per quello che abbiamo appena osservato, si ha che i coefficienti di $L(v)$ nella base canonica di \mathbb{R}^3 , sono dati dal prodotto riga per colonna seguente:

$$L(v) = [L] \begin{matrix} e_1, e_2, e_3, e_4 \\ \epsilon_1, \epsilon_2, \epsilon_3 \end{matrix} \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix} = \begin{pmatrix} 11 \\ \sqrt{3} + 31 \\ 42 \end{pmatrix}$$

OSSERVAZIONE 1.93. Consideriamo l'applicazione *identità* $I : V \rightarrow V$, che lascia fisso ogni elemento di v : $I(v) = v \quad \forall v \in V$, e fissiamo la base \mathcal{B} di V . Si verifica che la matrice $[I] = (a_{ij})$ associata ad I rispetto a \mathcal{B} sia in arrivo che in partenza (ovvero $[I]_{\mathcal{B}} = (a_{ij})$), è la matrice quadrata

di formato $n \times n$ che ha tutti i coefficienti uguali a 0 eccetto quelli sulla diagonale, che sono invece uguali a 1: $a_{ij} = 0$ se $i \neq j$ e $a_{ii} = 1$ per ogni $i = 1, 2, \dots, n$.

Tale matrice è l'elemento neutro rispetto alla moltiplicazione riga per colonna in $Mat_{n \times n}(K)$ (verificare per esercizio).

Nel seguito useremo il simbolo I per indicare sia la applicazione lineare I sia la matrice identità, anche senza specificare di che formato sia (2×2 , 3×3 , $n \times n \dots$), visto che il contesto renderà sempre chiaro il significato.

8. Esercizi di fine capitolo

ESERCIZIO 1.94. Si consideri la funzione $L : \mathbb{R}^3 \rightarrow \mathbb{R}^2$ definita sulle coordinate rispetto alle basi standard di \mathbb{R}^3 e \mathbb{R}^2 da:

$$L \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x - 2y - z \\ x + y + z \end{pmatrix}$$

- (1) Verificare che L è lineare.
- (2) Scrivere la matrice associata ad L rispetto alle basi standard di \mathbb{R}^3 e \mathbb{R}^2 .
- (3) Determinare una base di $\text{Ker } L$ e $\text{Imm } L$.

Svolgimento. Cominciamo, provando che effettivamente L è un'applicazione lineare¹⁴, ovvero:

- $\forall v, w \in \mathbb{R}^3$ si ha che $L(v + w) = L(v) + L(w)$. Controlliamo che sussista questa uguaglianza; siano (x_1, y_1, z_1) e (x_2, y_2, z_2) le coordinate di v e w rispettivamente allora: $(v + w) = (x_1 + x_2, y_1 + y_2, z_1 + z_2)$ quindi:

$$L(v + w) = L \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 \\ z_1 + z_2 \end{pmatrix} = \begin{pmatrix} (x_1 + x_2) - 2(y_1 + y_2) - (z_1 + z_2) \\ (x_1 + x_2) + (y_1 + y_2) + (z_1 + z_2) \end{pmatrix}$$

Mentre:

$$L(v) + L(w) = \begin{pmatrix} x_1 - 2y_1 - z_1 \\ x_1 + y_1 + z_1 \end{pmatrix} + \begin{pmatrix} x_2 - 2y_2 - z_2 \\ x_2 + y_2 + z_2 \end{pmatrix} = \begin{pmatrix} (x_1 + x_2) - 2(y_1 + y_2) - (z_1 + z_2) \\ (x_1 + x_2) + (y_1 + y_2) + (z_1 + z_2) \end{pmatrix}$$

- $\forall v \in V$ e $\forall k \in \mathbb{K}$ si ha che $L(k \cdot v) = k \cdot L(v)$. Anche in questo caso proviamo questa uguaglianza:

$$L(k \cdot v) = L \begin{pmatrix} k \cdot x \\ k \cdot y \\ k \cdot z \end{pmatrix} = \begin{pmatrix} k \cdot x - 2k \cdot y - k \cdot z \\ k \cdot x + k \cdot y + k \cdot z \end{pmatrix}$$

Mentre:

$$k \cdot L(v) = k \cdot \begin{pmatrix} x - 2y - z \\ x + y + z \end{pmatrix} = \begin{pmatrix} k \cdot x - 2k \cdot y - k \cdot z \\ k \cdot x + k \cdot y + k \cdot z \end{pmatrix}$$

¹⁴In effetti allo stesso modo in cui proviamo questo risultato, si può provare che sono applicazioni lineari da \mathbb{R}^n a \mathbb{R}^m tutte le applicazioni che agiscono sulle coordinate in maniera che il risultato sia una combinazione lineare delle stesse.

A questo punto, per scrivere la matrice associata a L rispetto alle basi standard:

$$\mathfrak{B}_{\mathbb{R}^2} = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$$

$$\mathfrak{B}_{\mathbb{R}^3} = \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\}$$

bisogna calcolare, le coordinate rispetto alla base $\mathfrak{B}_{\mathbb{R}^2}$, dell'immagine degli elementi di $\mathfrak{B}_{\mathbb{R}^3}$ tramite L :

$$L \left(\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \right) = \begin{pmatrix} 1 \\ 1 \end{pmatrix}; \quad L \left(\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right) = \begin{pmatrix} -2 \\ 1 \end{pmatrix}; \quad L \left(\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right) = \begin{pmatrix} -1 \\ 1 \end{pmatrix}$$

Perciò la matrice associata a L nelle basi $\mathfrak{B}_{\mathbb{R}^3}$ di \mathbb{R}^3 e $\mathfrak{B}_{\mathbb{R}^2}$ di \mathbb{R}^2 è la seguente:

$$[A]_{\substack{\mathfrak{B}_{\mathbb{R}^3} \\ \mathfrak{B}_{\mathbb{R}^2}}} = \begin{pmatrix} 1 & -2 & -1 \\ 1 & 1 & 1 \end{pmatrix}$$

Sappiamo (vedi Esercizio 1.76) che $Imm L$ è generata dai vettori

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

ma, in questo caso, sappiamo anche *immediatamente* che questi non sono una base (se fossero linearmente indipendenti, sarebbe facile mostrare, per esempio usando il Teorema 1.60, che \mathbb{R}^2 ha dimensione ≥ 3 , mentre sappiamo che la dimensione di \mathbb{R}^2 è 2). Lasciamo al lettore la verifica che, presi due qualunque vettori fra i tre scritti sopra, tali vettori costituiscono una base di $Imm L$.

Per trovare una base di $Ker L$, cerchiamo di capire come sono fatti i suoi elementi. Per definizione un vettore v sta in $Ker L$ se $L(v) = 0$. Questo

si traduce, se poniamo $v = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$, nella relazione:

$$\begin{pmatrix} 1 & -2 & -1 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

Ovvero abbiamo il sistema:

$$\begin{aligned} x - 2y - z &= 0 \\ x + y + z &= 0 \end{aligned}$$

Risolviamo il sistema e troviamo:

$$\begin{aligned} x &= 2 \cdot \left(-\frac{2}{3}z\right) + z = -\frac{1}{3}z \\ y &= -\frac{2}{3}z \end{aligned}$$

Osserviamo che ci sono infinite soluzioni, una per ogni scelta di $z \in \mathbb{R}$. I vettori che stanno in $\text{Ker } L$ sono dunque della forma:

$$\begin{pmatrix} -\frac{1}{3}z \\ -\frac{2}{3}z \\ z \end{pmatrix} = z \begin{pmatrix} -\frac{1}{3} \\ -\frac{2}{3} \\ 1 \end{pmatrix}$$

Quindi il vettore:

$$\begin{pmatrix} -\frac{1}{3} \\ -\frac{2}{3} \\ 1 \end{pmatrix}$$

genera $\text{Ker } L$ e costituisce anche una base. In particolare L non è iniettiva perché $\text{Ker } L$ non è composto dal solo vettore nullo.

ESERCIZIO 1.95. Dimostrare che l'insieme $S \subseteq \mathbb{R}^4$ delle soluzioni del seguente sistema lineare:

$$2x + y + t + 2z = 0$$

$$x + 3t + z = 0$$

$$x + y - 2t + z = 0$$

è un sottospazio vettoriale di \mathbb{R}^4 . Secondo voi questo risultato vale anche in generale per qualunque sistema di equazioni lineari?

ESERCIZIO 1.96. Sia $a \in \mathbb{R}$. Consideriamo in \mathbb{R}^4 il sottospazio V_a dato dalle soluzioni del seguente sistema lineare:

$$\begin{cases} x + 2y + z = 0 \\ ay + z + 3t = 0 \end{cases}$$

e il sottospazio W_a generato dai vettori

$$\begin{pmatrix} a+1 \\ 0 \\ 1 \\ a \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ -1 \\ 0 \end{pmatrix}.$$

Calcolare, per $a = 3$, $\dim V_a \cap W_a$ e $\dim (V_a + W_a)$.

Calcolare, al variare di $a \in \mathbb{R}$, $\dim V_a \cap W_a$ e $\dim (V_a + W_a)$.

ESERCIZIO 1.97. Sia $a \in \mathbb{R}$ e siano $f_a : \mathbb{R}^4 \rightarrow \mathbb{R}^3$, $g_a : \mathbb{R}^4 \rightarrow \mathbb{R}^3$ le funzioni date da

$$f_a(x, y, z, t) = (x + 2y + z, y + (a+1)z, t + 1)$$

$$g_a(x, y, z, t) = ((a+1)x + 2y + z, ay + (a+1)z, az + (a+1)t)$$

(1) Perché g_a è una applicazione lineare mentre f_a non lo è?

(2) Scrivere una base per $\text{Ker } g_a$, quando $a = 5$.

(3) Scrivere una base per $\text{Ker } g_a$, al variare di $a \in \mathbb{R}$.

ESERCIZIO 1.98. Sia $F : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ l'applicazione lineare definita, nella base standard di \mathbb{R}^2 , dalla matrice:

$$[F] = \begin{pmatrix} 2 & 1 \\ 4 & 2 \end{pmatrix}$$

Trovare $\text{Ker } F$ e $\text{Imm } F$.

ESERCIZIO 1.99. Sia $F : \mathbb{C}^3 \rightarrow \mathbb{C}^3$ l'applicazione lineare definita, nella base standard di \mathbb{C}^3 , dalla matrice:

$$[F] = \begin{pmatrix} -1 & 0 & -1 \\ 0 & 1 & i \\ 2-i & i & 1-i \end{pmatrix}$$

Trovare $\text{Ker } F$ e $\text{Imm } F$.

ESERCIZIO 1.100. Sia $F : \mathbb{C}^3 \rightarrow \mathbb{C}^3$ l'applicazione lineare definita, nella base standard di \mathbb{C}^3 , dalla matrice:

$$[F] = \begin{pmatrix} -1 & 0 & i \\ 2 & 1 & 2i \\ 2-i & 1 & 2i-1 \end{pmatrix}$$

Trovare $\text{Ker } F$ e $\text{Imm } F$.

ESERCIZIO 1.101. Consideriamo i seguenti sottoinsiemi V e W dello spazio vettoriale $\mathbb{R}^{\leq 3}[x]$:

$$V = \{p(x) \in \mathbb{R}_3[x] \mid p(-1) = 0\}$$

e

$$W = \{p(x) \in \mathbb{R}_3[x] \mid p'(1) = 0\}$$

(Nota: con $p'(x)$ indichiamo la derivata del polinomio $p(x)$.)

- (1) Dimostrare che V e W sono sottospazi vettoriali di $\mathbb{R}^{\leq 3}[x]$.
- (2) Determinare una base di V , W , $W + V$ e $W \cap V$.

ESERCIZIO 1.102. Consideriamo la matrice a coefficienti in \mathbb{R}

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

Sia V lo spazio vettoriale delle matrici 2×2 a coefficienti in \mathbb{R} . Quale è la sua dimensione?

Dire se l'applicazione $L : V \rightarrow V$ tale che per ogni matrice X vale

$$L(X) = XB - BX$$

è lineare. Se è lineare, calcolare la dimensione del nucleo e dell'immagine.

ESERCIZIO 1.103. Consideriamo i due seguenti sottoinsiemi di \mathbb{R}^3 :

$$A = \left\{ \left(\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} \right) \right\}$$

$$\mathcal{B} = \left\{ \begin{pmatrix} 3 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\}$$

- (1) Dimostrare che \mathcal{B} è una base di \mathbb{R}^3 e che i vettori di A sono linearmente indipendenti. Completare poi A ad una base \mathcal{C} di \mathbb{R}^3 .
- (2) Considerata l'applicazione lineare $L : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ definita da $L(x, y, z) = (x+y, z, z)$ trovare una base di $\text{Ker } L$ e $\text{Imm } L$ e scrivere la matrice $[M]_{\mathcal{B}}^{\mathcal{C}}$ associata alla base \mathcal{C} in partenza e alla base \mathcal{B} in arrivo.

ESERCIZIO 1.104. Siano

$$V_a = \left\langle \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} a \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right\rangle$$

e

$$W = \left\langle \begin{pmatrix} 2 \\ 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix} \right\rangle$$

due sottospazi di \mathbb{R}^4 .

- (1) Al variare di a in \mathbb{R} , trovare la dimensione di $V_a + W$ e di $V_a \cap W$;
- (2) Dire per quali valori dei parametri $a, b \in \mathbb{R}$ il vettore

$$\begin{pmatrix} 1 \\ 1 \\ b \\ 0 \end{pmatrix}$$

appartiene al sottospazio $V_a \cap W$.

ESERCIZIO 1.105. Consideriamo lo spazio vettoriale $\mathbb{R}[x]^{\leq 4}$. Sia

$$V = \{p(x) \in \mathbb{R}[x]^{\leq 4} \mid p(0) = p(1) = p(2)\}$$

- Si dimostri che V è un sottospazio vettoriale di $\mathbb{R}[x]^{\leq 4}$.
- Si calcoli la dimensione di V .

ESERCIZIO 1.106. Sia $\mathcal{T} : \text{Mat}_{n \times n}(\mathbb{K}) \rightarrow \mathbb{K}$ la funzione *traccia* definita da

$$\mathcal{T}((a_{ij})) = a_{11} + a_{22} + \cdots + a_{nn}.$$

- (1) Dimostrare che \mathcal{T} è una applicazione lineare (per la struttura di spazio vettoriale su $\text{Mat}_{n \times n}(\mathbb{K})$ vedi l'Esercizio 1.82).
- (2) Dimostrare che per ogni $A, B \in \text{Mat}_{n \times n}(\mathbb{K})$ vale $\mathcal{T}(AB) = \mathcal{T}(BA)$.

CAPITOLO 2

Il rango delle applicazioni lineari e la riduzione a scalini delle matrici

1. Le operazioni elementari sulle colonne

Consideriamo una generica matrice in $Mat_{m \times n}(\mathbb{K})$:

$$(1.1) \quad A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & a_{m3} & \dots & a_{mn} \end{pmatrix}$$

e i tre seguenti tipi di *mossa* sulle colonne, detti anche **operazioni elementari sulle colonne** di una matrice:

- (1) si somma alla colonna i la colonna j moltiplicata per uno scalare λ ;
- (2) si moltiplica la colonna s per uno scalare $k \neq 0$;
- (3) si permutano fra di loro due colonne, diciamo la i e la j .

Quello che vogliamo mostrare è che, attraverso l'utilizzo di queste 3 mosse, si può sempre trasformare una qualsiasi matrice $m \times n$ in una matrice a forma detta *a scalini (per colonne)*.

ESEMPIO 2.1. Prima di dare una definizione formale di cosa sia una

matrice a scalini per colonne, vediamo alcuni esempi, in quanto la visualizzazione rende piuttosto bene l'idea di cosa si intenda:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ \sqrt{3}+1 & 1 & 0 & 0 \\ -2 & \frac{5}{2} & 1 & 0 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 & 0 & 0 \\ \sqrt{3}+1 & 1 & 0 & 0 \\ -2 & 7 & 0 & 0 \\ \sqrt{3} & 4 & 1 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ -2 & 1 & 0 & 0 \\ -8 & 4 & 1 & 0 \\ -5 & 1 & 0 & 0 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ -2 & \frac{5}{2} & 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ -2 & 1 & 0 & 0 & 0 \\ -8 & 4 & 3 & 0 & 0 \\ -2 & 1 & 0 & 4 & 0 \\ 0 & 0 & 0 & 9 & 1 \end{pmatrix}$$

Per una vera definizione di matrice a scalini per colonne possiamo seguire questa strada: chiamiamo *profondità* di una colonna la posizione occupata, contata dal basso, dal suo più alto coefficiente diverso da zero. Alla colonna nulla (con tutte i coefficienti uguali a 0) assegnamo per convenzione profondità 0.

ESEMPIO 2.2. Consideriamo la seguente matrice:

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

Consideriamo la prima colonna della matrice A :

$$\begin{pmatrix} 0 \\ \sqrt{3} + 1 \\ -2 \end{pmatrix}$$

In questa colonna, il numero diverso da 0 che è più in alto è $\sqrt{3}+1$. Contando dal basso $\sqrt{3}+1$ è in seconda posizione, dunque la colonna ha profondità 2. Analogamente per la seconda colonna:

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

il numero diverso da 0 più in alto è $4 - \sqrt{3}$ che è in terza posizione contando dal basso, dunque la profondità della colonna è 3. E infine il numero diverso da 0 più in alto per la terza colonna è -2 , che è in prima posizione contando dal basso. Dunque la terza colonna ha profondità 1.

A questo punto possiamo dare la definizione di matrice a scalini per colonne.

DEFINIZIONE 2.3. Una matrice A in $Mat_{m \times n}(\mathbb{K})$, si dice **in forma a scalini per colonne** se rispetta le seguenti proprietà:

- leggendo la matrice da sinistra a destra, le colonne non nulle si incontrano tutte prima della colonne nulle;
- leggendo la matrice da sinistra a destra, le profondità delle sue colonne non nulle risultano strettamente decrescenti.

DEFINIZIONE 2.4. In una matrice in forma a scalini per colonna, i coefficienti diversi da zero più alti di posizione di ogni colonna non nulla si chiamano **pivot**.

ESEMPIO 2.5. Se consideriamo le matrici a scalini dell'Esempio 2.1, i pivot sono i coefficienti in neretto:

$$\begin{pmatrix} \mathbf{1} & 0 & 0 & 0 \\ \sqrt{3} + 1 & \mathbf{1} & 0 & 0 \\ -2 & \frac{5}{2} & \mathbf{1} & 0 \end{pmatrix} \quad \begin{pmatrix} \mathbf{1} & 0 & 0 & 0 \\ \sqrt{3} + 1 & \mathbf{1} & 0 & 0 \\ -2 & 7 & 0 & 0 \\ \sqrt{3} & 4 & \mathbf{1} & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ \mathbf{1} & 0 & 0 & 0 \\ -2 & \mathbf{1} & 0 & 0 \\ -8 & 4 & \mathbf{1} & 0 \\ -5 & 1 & 0 & 0 \end{pmatrix} \quad \begin{pmatrix} \mathbf{1} & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 \\ -2 & \frac{5}{2} & 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} \mathbf{1} & 0 & 0 & 0 & 0 \\ -2 & \mathbf{1} & 0 & 0 & 0 \\ -8 & 4 & \mathbf{3} & 0 & 0 \\ -2 & 1 & 0 & \mathbf{4} & 0 \\ 0 & 0 & 0 & 9 & \mathbf{1} \end{pmatrix}$$

TEOREMA 2.6. *Data una matrice A in $Mat_{m \times n}(\mathbb{K})$ è sempre possibile, usando (un numero finito di¹) operazioni elementari sulle colonne, ridurre la matrice in forma a scalini per colonne.*

DIMOSTRAZIONE. Procediamo per induzione sul numero di righe m .

Il caso base, $m = 1$, è immediato. Se la matrice è composta da una riga nulla è già una matrice $1 \times n$ in forma a scalini; se invece ha qualche coefficiente non 0, con la terza delle operazioni elementari sulle colonne (ovvero la permutazione di colonne), si può portare un coefficiente non zero all'inizio della riga, dopodiché, utilizzando più volte la prima operazione per colonna, si possono ridurre a zero tutti gli altri coefficienti.

Supponiamo ora che l'enunciato sia vero per tutte le matrici con $m - 1$ righe, e dimostriamolo per matrici con m righe. Sia A una matrice $m \times n$. Se una riga di A è nulla, possiamo considerare la matrice A' ottenuta da A togliendo tale riga. Per ipotesi induttiva, visto che A' ha $m - 1$ righe, sappiamo che possiamo, usando solo le operazioni elementari sulle colonne, ridurre

¹Questa precisazione è importante perché fa intuire come sia possibile costruire un algoritmo per ridurre una matrice in forma a scalini per colonne.

a scalini per colonne A' . Osserviamo a questo punto che la stessa sequenza di operazioni per colonne riduce a scalini anche A . Infatti, sommando tra loro due colonne (prima operazione elementare), o moltiplicando una colonna per uno scalare k diverso da 0 (seconda operazione elementare), o infine permutando due colonne (terza ed ultima operazione elementare ammessa sulle colonne), i valori su una riga composta da tutti 0, rimangono 0.

Se invece A non ha righe nulle, vuol dire che in A esiste una colonna di profondità m (prova a spiegare perché). Possiamo supporre che sia la prima colonna da sinistra (se non lo è possiamo sempre fare uno scambio di colonne), e dunque che $a_{1,1}$ sia diverso da zero. A questo punto, sottraendo tale colonna, moltiplicata per opportuni scalari, alle altre colonne, si giunge ad avere una matrice A' del tipo:

$$(1.2) \quad A' = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & a_{m3} & \dots & a_{mn} \end{pmatrix}$$

Prima di proseguire con la dimostrazione del teorema vediamo, con un esempio, come effettivamente sia possibile trasformare una matrice A con $a_{1,1}$ diverso da 0, in una matrice della forma 1.2.

Consideriamo la matrice:

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

E vediamo come è possibile trasformarla nella forma di A' , usando solo le operazioni elementari sulle colonne.

- Moltiplichiamo la prima colonna di A per $\frac{1}{3}$ (seconda operazione elementare). Scriveremo, come si può vedere qui sotto, $[1] = \frac{1}{3}[1]$ per indicare che sostituiamo alla prima colonna il risultato a destra dell'uguaglianza:

$$A = \begin{pmatrix} 3 & 2 & -1 \\ 0 & 1 & 2 \\ -1 & 0 & 0 \\ 1 & 4 & 2 \end{pmatrix} \xrightarrow{[1]=\frac{1}{3}[1]} A_1 = \begin{pmatrix} 1 & 2 & -1 \\ 0 & 1 & 2 \\ -\frac{1}{3} & 0 & 0 \\ \frac{1}{3} & 4 & 2 \end{pmatrix}$$

- Sommiamo alla seconda colonna della matrice A_1 ottenuta, -2 volte la prima colonna di A_1 (scriveremo $[2] = [2] - 2[1]$):

$$A_1 \xrightarrow{[2]=[2]-2[1]} A_2 = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 2 \\ -\frac{1}{3} & \frac{2}{3} & 0 \\ \frac{1}{3} & \frac{10}{3} & 2 \end{pmatrix}$$

- Sommiamo alla terza colonna della matrice A_2 ottenuta, la prima colonna di A_2 (scriveremo $[3] = [3] + [1]$):

$$A_2 \xrightarrow{[3]=[3]+[1]} A_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ -\frac{1}{3} & \frac{2}{3} & -\frac{1}{3} \\ \frac{1}{3} & \frac{10}{3} & \frac{7}{3} \end{pmatrix}$$

A questo punto possiamo tornare alla dimostrazione del nostro teorema.

Per ipotesi induttiva sappiamo che possiamo ridurre a scalini la sottomatrice di A' seguente:

$$\begin{pmatrix} 0 & 0 & \dots & 0 \\ a_{22} & a_{23} & \dots & a_{2n} \\ a_{32} & a_{33} & \dots & a_{3n} \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ a_{m2} & a_{m3} & \dots & a_{mn} \end{pmatrix}$$

che ha una riga (e una colonna) in meno di A . Si osserva subito che le stesse mosse, operate sulla matrice A' , la riducono a scalini. \square

OSSERVAZIONE 2.7. Quando si riduce una matrice A in $Mat_{m \times n}(\mathbb{K})$ in forma a scalini, la forma a scalini ottenuta non è unica, basta osservare che se B è in forma scalini, allora anche $k \cdot B$ è a scalini (con $k \in \mathbb{K}$).

OSSERVAZIONE 2.8. In quasi tutte le matrici dell'Esempio 2.1, in ogni colonna il coefficiente più alto diverso da zero è uguale a 1. Questa richiesta non rientra nella definizione di matrice a scalini per colonne. È vero o falso che quando si riduce una matrice A in $Mat_{m \times n}(\mathbb{K})$ in forma a scalini con questa ulteriore proprietà (ovvero che in ogni colonna il coefficiente più alto diverso da zero valga 1), la forma a scalini ottenuta è unica?

ESERCIZIO 2.9. Vista la dimostrazione del teorema, provare a scrivere un algoritmo che data in input una matrice A in $Mat_{m \times n}(\mathbb{K})$, restituisce una forma a scalini per colonne di A .

Nel seguito, ci interesserà anche una forma ancora più *particolare* di matrice a scalini per colonne:

DEFINIZIONE 2.10. Una matrice A in $Mat_{m \times n}(\mathbb{K})$, si dice **in forma a scalini per colonne ridotta** se:

- A è a scalini per colonne,
- Tutte le entrate nella stessa riga di un pivot, precedenti (leggendo la riga da sinistra a destra) al pivot, sono nulle.

ESEMPIO 2.11. Ecco le forme a scalini ridotte per alcune delle matrici dell'Esempio 2.1:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ \sqrt{3} + 1 & 1 & 0 & 0 \\ -2 & \frac{5}{2} & 1 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ \sqrt{3}+1 & 1 & 0 & 0 \\ -2 & 7 & 0 & 0 \\ \sqrt{3} & 4 & 1 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ -2-7-7\sqrt{3} & 7 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

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

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

PROPOSIZIONE 2.12. *Data una matrice A in forma a scalini per colonne, è sempre possibile, usando solo la prima delle operazioni elementari sulle colonne, portare A in forma a scalini per colonna ridotta.*

ESERCIZIO 2.13. Dimostrare la Proposizione 2.12.

COROLLARIO 2.14. *Ogni matrice A può essere trasformata, attraverso le operazioni elementari sulle colonne, in una matrice in forma a scalini per colonna ridotta.*

DIMOSTRAZIONE. Basta applicare il Teorema 2.6, per trasformare A in A' matrice in forma a scalini, e poi applicare la Proposizione 2.12 per trasformare A' in A'' in forma a scalini ridotta. \square

Prima di proseguire verso lo studio delle applicazioni lineari tramite la *manipolazione* delle matrici corrispondenti, soffermiamoci ad analizzare alcune proprietà di quelle che abbiamo chiamato *operazioni elementari sulle colonne*.

Data una matrice A $m \times n$, a coefficienti in un campo \mathbb{K} , le n colonne possono essere considerati n vettori di \mathbb{K}^m . Ad esempio se abbiamo la matrice:

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

possiamo considerare i 4 vettori di \mathbb{R}^5 seguenti:

$$v_1 = \begin{pmatrix} 1 \\ 0 \\ 3 \\ 4 \\ 7 \end{pmatrix}, v_2 = \begin{pmatrix} 0 \\ 1 \\ 2 \\ 3 \\ -1 \end{pmatrix}, v_3 = \begin{pmatrix} 3 \\ 2 \\ 1 \\ 0 \\ 0 \end{pmatrix}, v_4 = \begin{pmatrix} 1 \\ 0 \\ 3 \\ 1 \\ 0 \end{pmatrix}$$

Data una matrice A in $Mat_{m \times n}(\mathbb{K})$, indicate con v_1, \dots, v_n i vettori di \mathbb{K}^m formati dalle colonne di A , si può in particolare considerare il sottospazio di \mathbb{K}^m generato da v_1, \dots, v_n , ovvero $Span(v_1, \dots, v_n)$.

PROPOSIZIONE 2.15. *Operando attraverso le operazioni elementari sulle colonne di una matrice, lo Span dei vettori colonna rimane invariato. Ovvero se indichiamo con v_1, \dots, v_n i vettori colonna di una matrice A in $Mat_{m \times n}(\mathbb{K})$, per ogni matrice A' ottenuta da A attraverso le operazioni elementari sulle colonne, si ha, indicando con w_1, \dots, w_n i vettori colonna di A' , che:*

$$Span(v_1, \dots, v_n) = Span(w_1, \dots, w_n)$$

DIMOSTRAZIONE. Basta osservare che:

- $Span(v_1, \dots, v_i, \dots, v_n) = Span(v_1, \dots, v_i + k \cdot v_j, \dots, v_n)$. Infatti se un vettore v appartiene a $Span(v_1, \dots, v_i, \dots, v_n)$ allora può essere scritto come

$$v = \lambda_1 v_1 + \dots + \lambda_i v_i + \dots + \lambda_j v_j + \dots + \lambda_n v_n$$

Ma questo vettore può essere scritto anche come

$$v = \lambda_1 v_1 + \dots + \lambda_i (v_i + k \cdot v_j) + \dots + (\lambda_j - k \lambda_i) v_j + \dots + \lambda_n v_n$$

dunque appartiene anche a $Span(v_1, \dots, v_i + k \cdot v_j, \dots, v_n)$.

Viceversa, se un vettore w appartiene a $Span(v_1, \dots, v_i + k \cdot v_j, \dots, v_n)$ allora può essere scritto come

$$w = \mu_1 v_1 + \dots + \mu_i (v_i + k \cdot v_j) + \dots + \mu_j v_j + \dots + \mu_n v_n$$

Si nota che può essere allora scritto anche come

$$w = \mu_1 v_1 + \dots + \mu_i v_i + \dots + (\mu_j + k \mu_i) v_j + \dots + \mu_n v_n$$

dunque appartiene anche a $Span(v_1, \dots, v_i, \dots, v_n)$.

- Se $k \neq 0$, $Span(v_1, \dots, v_i, \dots, v_n) = Span(v_1, \dots, k \cdot v_i, \dots, v_n)$ (dimostrazione simile alla precedente, anzi ancora più immediata).
- $Span(v_1, \dots, v_i, \dots, v_j, \dots, v_n) = Span(v_1, \dots, v_j, \dots, v_i, \dots, v_n)$ (dimostrazione simile alla precedente, anzi ancora più immediata).

□

Un'altra osservazione importante, riguardo alle operazioni elementari sulle colonne, è che ogni singola operazione è *reversibile*. Ossia, una volta fatta, possiamo fare la sua inversa e tornare esattamente alla matrice di partenza.

2. La riduzione a scalini per colonne applicata allo studio delle basi

Possiamo utilizzare le osservazioni sul metodo di riduzione a scalini per colonne per dimostrare finalmente il Teorema 1.62.

TEOREMA 2.16. *Sia V uno spazio vettoriale sul campo \mathbb{K} che ammette una base finita. Allora tutte le basi di V hanno la stessa cardinalità.*

DIMOSTRAZIONE. Prendiamo due basi di V : $\{e_1, e_2, \dots, e_n\}$ e $\{v_1, v_2, \dots, v_r\}$. Dobbiamo dimostrare che $n = r$. Scegliamo per il momento di usare $\{e_1, e_2, \dots, e_n\}$ come base di V ; ogni vettore v_j potrà essere espresso in maniera unica come combinazione lineare dei vettori e_1, e_2, \dots, e_n e possiamo quindi pensarlo come un vettore colonna

$$v_j = \begin{pmatrix} a_{j1} \\ a_{j2} \\ \dots \\ a_{jn} \end{pmatrix}$$

Possiamo formare una matrice M ponendo uno accanto all'altro i vettori v_1, v_2, \dots, v_r : M sarà del tipo $n(\text{righe}) \times r(\text{colonne})$.

Sappiamo che possiamo ridurre a scalini la M con le mosse di colonna ottenendo una nuova matrice M' . Ma che tipo di scalini avrà M' ? Lo spazio generato dai vettori colonna di M' è uguale allo spazio generato dai vettori colonna di M , dunque a V , visto che i vettori colonna di M sono i v_j che sono una base di V per ipotesi. Allora i vettori colonna di M' non possono formare degli scalini *lunghi*, ovvero la differenza di profondità tra colonne adiacenti non può essere più di 1. Per esempio, se M' fosse:

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

si vedrebbe subito che il vettore

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

che ha tutti i coefficienti uguali a 0 eccetto un 1 in corrispondenza dello scalino lungo, non potrebbe venire generato dalle colonne di M' . Il fatto che in M' non ci siano scalini lunghi si può esprimere anche dicendo che la profondità dei vettori colonna deve scendere ad ogni passo di 1 da sinistra a destra, e con gli scalini si deve *toccare il fondo*. Questo è possibile solo se ci sono abbastanza colonne, ossia se $r \geq n$.

Possiamo ripetere tutto il discorso invertendo il ruolo delle basi $\{e_1, e_2, \dots, e_n\}$ e $\{v_1, v_2, \dots, v_r\}$: in tal modo otterremo che deve valere $n \geq r$. Dunque $n = r$ come volevamo dimostrare \square

COROLLARIO 2.17. *In uno spazio vettoriale V di dimensione n , dati n vettori linearmente indipendenti questi sono anche una base di V . Allo stesso modo, dati n vettori che generano V questi sono anche una base di V .*

DIMOSTRAZIONE. Fissiamo una base di V e_1, e_2, \dots, e_n e siano v_1, v_2, \dots, v_n vettori linearmente indipendenti.

Esprimiamo i vettori v_1, v_2, \dots, v_n in termini della base e_1, e_2, \dots, e_n e poniamoli in colonna uno accanto all'altro. Così facendo otteniamo una matrice M che è $n \times n$. La matrice M' in forma a scalini ridotta ottenuta a partire da M è la matrice identità: $M' = I$. Il perché si basa su osservazioni già fatte, ma ripetiamole per esercizio: se i vettori v_1, v_2, \dots, v_n sono linearmente indipendenti allora lo *Span* delle colonne di M ha dimensione n . Ma tale *Span* coincide con lo *Span* delle colonne di M' : le n colonne di M' devono dunque essere indipendenti. Questo può accadere solo se sono non nulle e di profondità diverse. L'unico modo è che $M' = I$. Riassumendo, lo *Span* delle colonne di M , ovvero $\text{Span}(v_1, v_2, \dots, v_n)$, è uguale allo *Span* delle colonne di $M' = I$, che è tutto V . Abbiamo dimostrato che i vettori v_1, v_2, \dots, v_n generano V , e dunque sono una base.

Per quel che riguarda l'altra parte dell'enunciato, ossia quella in cui si considerano dei vettori v_1, v_2, \dots, v_n che generano V , per dimostrare che sono linearmente indipendenti basta applicare il Teorema 1.60: se non fossero linearmente indipendenti sarebbe possibile estrarre un sottoinsieme di cardinalità minore di n che è una base, dunque lo spazio avrebbe due basi di cardinalità diversa, assurdo.

□

Considerazioni simili a quelle esposte fin qui ci permettono di descrivere un criterio concreto per decidere se, dato uno spazio vettoriale V di dimensione n ed una base e_1, e_2, \dots, e_n di V , e dati n vettori v_1, v_2, \dots, v_n di V , tali vettori costituiscono una base di V o no. Il criterio è il seguente: esprimiamo i vettori v_1, v_2, \dots, v_n trovandone i coefficienti rispetto alla base e_1, e_2, \dots, e_n e poniamoli in colonna uno accanto all'altro. Così facendo otteniamo una matrice M che è $n \times n$. Ora possiamo ridurre M in forma a scalini ridotta M' : se M' è l'identità allora $\{v_1, v_2, \dots, v_n\}$ è una base di V , altrimenti no. Proviamo a capire il perché di quest'ultima affermazione.

Nella dimostrazione del Teorema 2.16 abbiamo visto che se $\{v_1, v_2, \dots, v_n\}$ è una base allora la forma a scalini ridotta M' non ha scalini *lunghi*. Ma le matrici M e M' di cui stiamo parlando sono di forma $n \times n$, quindi M' è la matrice identità.

Viceversa, se M' è l'identità, le sue n colonne generano V . Questo implica che le n colonne di M generano V , ossia che v_1, v_2, \dots, v_n generano V . Per il Corollario 2.17 si conclude che v_1, v_2, \dots, v_n sono una base.

ESEMPIO 2.18. Facciamo ora un semplice esempio concreto di *riconoscimento* di una base. Consideriamo \mathbb{R}^4 con la sua base standard e poi i vettori

$$v_1 = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, v_2 = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}, v_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}, v_4 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Si noti che si tratta dei vettori utilizzati nell'Esempio 1.90 alla fine del Paragrafo 7 del Capitolo 1; il lettore avrà dunque già verificato che si tratta di una base. Ma ora possiamo farlo col nuovo metodo.

Scriviamo dunque la matrice

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

e cerchiamo di portarla in forma a scalini ridotta. Sottraendo la quarta colonna alla terza otteniamo

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

Sottraendo la terza colonna alla seconda otteniamo

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

e infine sottraendo la seconda colonna alla prima troviamo la matrice identità come volevamo:

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

Dunque $\{v_1, v_2, v_3, v_4\}$ è una base di \mathbb{R}^4 . In questo esempio i calcoli erano particolarmente semplici, ma è già possibile notare la “convenienza” di questo metodo.

Un'altra importante applicazione delle osservazioni sulla riduzione a scalini per colonne è data dal prossimo teorema, il quale - in un certo senso - è il *duale* del Teorema 1.60. In quel caso avevamo dimostrato che da un insieme A di generatori di uno spazio V si può sempre estrarre una base di V (ovvero trovare un sottoinsieme di A che è base di V). Ora dimostriamo che un insieme B di vettori linearmente indipendenti di V si può sempre completare ad una base di V (ovvero esiste un insieme C che contiene B e che è base di V). La dimostrazione del teorema, non solo garantisce teoricamente che questo completamento si può fare, ma descrive anche un algoritmo per trovare un completamento.

TEOREMA 2.19 (Teorema del Completamento). *Dato uno spazio vettoriale V di dimensione n , ogni sottoinsieme $B = \{v_1, \dots, v_k\} \subset V$ di vettori linearmente indipendenti di cardinalità k , con $1 \leq k \leq n$, può essere completato ad una base di V aggiungendo a B $n - k$ vettori di $V \setminus \text{Span}(B)$.*

DIMOSTRAZIONE. Per prima cosa si scrivono i vettori v_1, v_2, \dots, v_k come vettori colonna rispetto a una base data, e si considera la matrice M che ha questi vettori colonna come colonne. Poi si riduce M in forma a scalini per colonne. Tutte le volte che troviamo uno scalino lungo (diciamo di altezza $i \geq 2$, dove l'altezza è la differenza di profondità tra due colonne adiacenti che formano lo scalino lungo) possiamo facilmente trovare $i - 1$ vettori w_1, w_2, \dots, w_{i-1} tali che $\{v_1, v_2, \dots, v_k, w_1, w_2, \dots, w_{i-1}\}$ è ancora un insieme di vettori linearmente indipendenti. Supponiamo infatti che M abbia uno scalino di lunghezza i , ovvero in una certa colonna abbia il pivot alla riga t e nella colonna successiva alla riga $t + i$, e sia $i > 1$. Allora per j che varia tra 1 ed $i - 1$, basta scegliere come vettore w_j il vettore definito come segue: w_j ha tutti 0 tranne un 1 in corrispondenza della riga $t + j$ -esima. È facile osservare infatti che ogni w_j così costruito non appartiene allo $\text{Span}(v_1, \dots, v_k, w_1, \dots, w_{j-1})$. Dunque, per la Proposizione 1.51, ad ogni aggiunta di w_j , l'insieme $\{v_1, \dots, v_k, w_1, \dots, w_{j-1}, w_j\}$ rimane un insieme di vettori linearmente indipendenti di V .

Concludiamo la dimostrazione, e poi esemplificheremo quanto abbiamo spiegato qui in simboli.

Ripetendo questa *aggiunta* di vettori w_k per ogni scalino lungo che troviamo in M , troviamo alla fine n vettori linearmente indipendenti, dunque una base di V come richiesto. \square

ESEMPIO 2.20. Illustriamo il metodo descritto con un esempio. Supponiamo che $V = \mathbb{R}^7$ e siano dati i 4 vettori linearmente indipendenti che, scritti rispetto alla base standard di \mathbb{R}^7 , sono rappresentati come segue:

$$v_1 = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 2 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \quad v_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 2 \\ 1 \\ 0 \\ 3 \end{pmatrix}, \quad v_3 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \quad v_4 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 2 \end{pmatrix}$$

La matrice M in questo caso è:

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 2 & 2 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 3 & 1 & 2 \end{pmatrix}$$

e una sua riduzione a scalini per colonne è :

$$M' = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 1 & 0 & \mathbf{1} & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 1 \end{pmatrix}$$

Il primo scalino lungo ha altezza 3 (tra i due pivot della seconda e terza colonna, indicati in neretto, c'è infatti una differenza di profondità di 3). Come osservato nella dimostrazione del Teorema 2.19, i vettori

$$w_1 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad w_2 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

non appartengono al sottospazio generato dalle colonne di M' (che coincide col sottospazio generato da v_1, v_2, v_3, v_4), e si osserva immediatamente che $\{v_1, v_2, v_3, v_4, w_1, w_2\}$ è un insieme di vettori linearmente indipendenti di \mathbb{R}^7 .

Similmente, prendendo in considerazione il secondo scalino lungo (che ha altezza 2), notiamo che il vettore

$$w_3 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

non appartiene al sottospazio generato da $v_1, v_2, v_3, v_4, w_1, w_2$. A questo punto $\{v_1, v_2, v_3, v_4, w_1, w_2, w_3\}$ sono un insieme di vettori linearmente indipendenti di \mathbb{R}^7 , e si può concludere che formano una base di \mathbb{R}^7 , sia osservando che quando si scrive la matrice 7×7 M'' formata da tali vettori la sua forma a scalini ridotta è l'identità (abbiamo proprio aggiunto a M tre vettori che *accorciano* i suoi scalini lunghi...), sia avendo in mente che \mathbb{R}^7 ha dimensione 7, perciò ogni insieme di vettori linearmente indipendenti di cardinalità 7 è una sua base.

3. Il teorema della dimensione del nucleo e dell'immagine di una applicazione lineare

Il teorema del completamento, ha come importante corollario un risultato che stabilisce una relazione tra la dimensione del nucleo e quella dell'immagine di una applicazione lineare.

TEOREMA 2.21. *Considerata una applicazione lineare $L : V \rightarrow W$, dove V e W sono spazi vettoriali su un campo \mathbb{K} , vale*

$$\dim \text{Ker } L + \dim \text{Imm } L = \dim V$$

DIMOSTRAZIONE. Sia $n = \dim V$ e consideriamo il $\text{Ker } L$ che sappiamo essere un sottospazio di V .

Osserviamo che se $\text{Ker } L = V$ (ovvero ha dimensione n) o $\text{Ker } L = \{O\}$ (ovvero ha dimensione 0) è facile dimostrare la tesi del teorema. Infatti, nel primo caso L è l'applicazione nulla, e dunque $\text{Imm } L$, che contiene solo il vettore O , è il sottospazio di dimensione $\{0\}$ di W .

Nel secondo caso, dalla Proposizione 1.75 sappiamo che $(L(e_1), \dots, L(e_n))$ (dove con (e_1, \dots, e_n) abbiamo indicato una base di V) genera $\text{Imm } L$, e, visto che $\text{Ker } L = \{O\}$, ovvero L è iniettiva, dall'Esercizio 1.78, sappiamo che $(L(e_1), \dots, L(e_n))$ sono linearmente indipendenti. Dunque $(L(e_1), \dots, L(e_n))$ costituiscono una base di $\text{Imm } L$, che ha dimensione n .

Mettiamoci dunque nel caso in cui $\dim \text{Ker } L = k$, con $0 < k < n$, e sia $\{z_1, \dots, z_k\}$ una base di $\text{Ker } L$. Per il teorema del completamento possiamo trovare w_1, \dots, w_{n-k} tali che $\{z_1, \dots, z_k, w_1, \dots, w_{n-k}\}$ sia una base di V . Sappiamo che $\text{Imm } L$ è il sottospazio generato da

$$L(z_1), \dots, L(z_k), L(w_1), \dots, L(w_{n-k})$$

ma, essendo gli z_j nel nucleo di L , per ogni $j = 1, \dots, k$, $L(z_j) = O$ e allora

$$\text{Imm } L = \langle L(w_1), \dots, L(w_{n-k}) \rangle.$$

Abbiamo per ora dimostrato che $\dim \text{Imm } L \leq n - k$. Vorremmo far vedere, per concludere la dimostrazione del teorema, che $\dim \text{Imm } L = n - k$. Questo è vero se $L(w_1), \dots, L(w_{n-k})$ sono linearmente indipendenti.

Consideriamo dunque una combinazione lineare nulla degli $L(w_i)$:

$$a_1 L(w_1) + \dots + a_{n-k} L(w_{n-k}) = O$$

e facciamo vedere che i coefficienti di tale combinazione lineare devono essere tutti nulli.

Per linearità l'equazione sopra equivale a:

$$L(a_1 w_1 + \dots + a_{n-k} w_{n-k}) = O$$

ossia

$$a_1 w_1 + a_2 w_2 + \dots + a_{n-k} w_{n-k} \in \text{Ker } L$$

Ma allora possiamo esprimere $a_1 w_1 + \dots + a_{n-k} w_{n-k}$ come combinazione lineare di z_1, \dots, z_k visto che questi sono una base di $\text{Ker } L$:

$$a_1 w_1 + \dots + a_{n-k} w_{n-k} = b_1 z_1 + \dots + b_k z_k$$

dove i $b_j \in \mathbb{K}$, che diventa

$$a_1 w_1 + \cdots + a_{n-k} w_{n-k} - b_1 z_1 + \cdots - b_k z_k = O$$

Essendo $\{z_1, \dots, z_k, w_1, \dots, w_{n-k}\}$ una base di V , tutti i coefficienti nella equazione sopra devono essere uguali a 0. In particolare $a_1 = \cdots = a_{n-k} = 0$, come volevamo. \square

DEFINIZIONE 2.22. Una applicazione lineare bigettiva $L : V \rightarrow W$, tra due spazi vettoriali V e W sul campo \mathbb{K} , si dice un **isomorfismo lineare**.

Dal Teorema 2.21 segue che:

- Se $L : V \rightarrow W$ è una applicazione lineare iniettiva allora $\dim \text{Imm } L = \dim V$. Infatti sappiamo che $\text{Ker } L = \{O\}$, dunque $\dim \text{Ker } L = 0$, e quindi dal teorema si ha $\dim \text{Imm } L = \dim V$.
- Se $L : V \rightarrow W$ è un isomorfismo lineare allora $\dim V = \dim W$. Infatti se L è bigettiva, in particolare è iniettiva (dunque $\dim \text{Imm } L = \dim V$), e surgettiva (dunque $\text{Imm } L = W$ e quindi $\dim \text{Imm } L = \dim W$).
- Se $L : V \rightarrow W$ è una applicazione lineare iniettiva, allora L pensata come applicazione da V ad $\text{Imm } L$ è un isomorfismo lineare.

4. La riduzione a scalini per colonna vista come moltiplicazione per matrici invertibili

La riduzione a scalini per colonna risulta molto utile anche per lo studio delle applicazioni lineari, ed in particolare per la determinazione di dimensione e base dell'immagine di una applicazione lineare.

Dati due spazi vettoriali V e W sul campo \mathbb{K} di dimensione n e m rispettivamente, consideriamo una applicazione lineare:

$$L : V \rightarrow W$$

Fissiamo una base $\{e_1, e_2, \dots, e_n\}$ di V e una base $\{\epsilon_1, \epsilon_2, \dots, \epsilon_m\}$ di W . Indichiamo con $[L]$ la matrice, di forma $m \times n$, associata a L nelle basi scelte.

Per quanto abbiamo fin qui detto, possiamo, tramite un numero finito k di operazioni elementari sulle colonne di $[L]$, portarla in forma a scalini ridotta. Ma c'è di più. Ogni operazione elementare sulle colonne corrisponde a moltiplicare la matrice iniziale $[L] \in \text{Mat}_{m \times n}(\mathbb{K})$, a destra, per una matrice B $n \times n$ invertibile. Per esempio la mossa:

- si somma alla colonna i la colonna j moltiplicata per lo scalare λ ; corrisponde a moltiplicare la nostra matrice per la matrice quadrata $n \times n$ (chiamiamola $M_{ij\lambda}$) che ha tutti 1 sulla diagonale, e 0 in tutte le altre caselle eccetto che nella casella alla "riga j , colonna i ", dove troviamo λ .

ESERCIZIO 2.23. Dimostrare che moltiplicando $[L]$ in $\text{Mat}_{m \times n}(\mathbb{K})$ per la matrice $M_{ij\lambda}$ definita sopra, si ottiene proprio la matrice $[L]'$ uguale ad $[L]$ tranne che per la colonna i -esima, che in $[L]'$ è ottenuta sommando alla colonna i -esima di $[L]$, λ volte la colonna j -esima di $[L]$.

Verifichiamo che $M_{ij\lambda}$ è effettivamente invertibile nell'anello $Mat_{n \times n}(\mathbb{K})$ (vedi l'Osservazione 1.86) esibendo la sua inversa; ricordiamo che l'inversa $M_{ij\lambda}^{-1}$ deve soddisfare $M_{ij\lambda}M_{ij\lambda}^{-1} = M_{ij\lambda}^{-1}M_{ij\lambda} = I$. Senza perderci in calcoli, possiamo trovare $M_{ij\lambda}^{-1}$ in maniera più astuta, pensando che ci deve dare la mossa inversa di quella compiuta, ovvero

- si sottrae alla colonna i la colonna j moltiplicata per lo scalare λ , che corrisponde a sommare alla colonna i la colonna j moltiplicata per lo scalare $-\lambda$;

Dunque $M_{ij\lambda}^{-1}$ sarà fatta come $M_{ij\lambda}$, differendo solo per il coefficiente alla riga i e colonna j , in cui, al posto di λ , comparirà $-\lambda$, pertanto secondo la nostra notazione potremo indicarla con $M_{ij(-\lambda)}$.

ESERCIZIO 2.24. Provare che effettivamente

$$M_{ij\lambda} \cdot M_{ij(-\lambda)} = I = M_{ij(-\lambda)} \cdot M_{ij\lambda}$$

ESERCIZIO 2.25. Provare che anche per le mosse corrispondenti alle altre due operazioni elementari sulle colonne si trovano delle matrici invertibili che le realizzano.

Dunque, ridurre a scalini per colonne la matrice $[L]$ equivale a moltiplicare $[L]$ a destra per tante matrici invertibili $[M_1], [M_2], \dots, [M_k]$ ed avere che $[L][M_1][M_2] \cdots [M_k]$ è in forma a scalini ridotta.

Per semplificare la notazione, chiamiamo $[M]$ la matrice $n \times n$ ottenuta moltiplicando tra loro a destra le matrici $[M_i]$, ovvero:

$$[M] = [M_1] \cdot \dots \cdot [M_k]$$

$[M]$ è invertibile, visto che è il prodotto di matrici invertibili, e la sua inversa è

$$[M]^{-1} = [M_k]^{-1} \cdot \dots \cdot [M_1]^{-1}$$

Dalla Proposizione 1.88, sappiamo che ad $[M]$ è associata ad una applicazione lineare $M : V \rightarrow V$. Ci chiediamo: quale è la applicazione lineare associata a $[L][M]$? È proprio la

$$L \circ M : V \rightarrow W$$

dato che il prodotto fra matrici è stato definito in modo da rispettare la composizione fra applicazioni. Vale infatti il teorema, la cui dimostrazione lasciamo come esercizio (con suggerimento):

TEOREMA 2.26. *Siano V, W, U spazi vettoriali su \mathbb{K} , e fissiamo per ciascuno una base. Siano $T : V \rightarrow W$, $S : W \rightarrow U$ applicazioni lineari. Allora, rispetto alle basi fissate, vale:*

$$[S \circ T] = [S][T]$$

dove nel membro di destra stiamo considerando il prodotto righe per colonne fra matrici.

DIMOSTRAZIONE. Lasciata per esercizio (suggerimento: applicare le matrici $[S \circ T]$ e $[S][T]$ ai vettori colonna $\begin{pmatrix} 1 \\ 0 \\ \dots \\ 0 \end{pmatrix}$, $\begin{pmatrix} 0 \\ 1 \\ \dots \\ 0 \end{pmatrix}$ etc... e controllare che diano lo stesso risultato). \square

Torniamo all'applicazione L : sappiamo già che lo span delle colonne di $[L]$ coincide con lo span delle colonne della matrice ottenuta portando in forma a scalini $[L]$, ovvero che $Imm L$ coincide con l'immagine dell'applicazione lineare associata della matrice ottenuta portando in forma a scalini $[L]$ (tale applicazione lineare è $L \circ M$).

Riteniamo però istruttivo fornire una nuova dimostrazione di questo fatto.

PROPOSIZIONE 2.27. $Imm (L \circ M) = Imm L$, ossia, scritto con un'altra notazione, $(L \circ M)(V) = L(V)$.

Dimostriamo questa proposizione dimostrando più in generale che

PROPOSIZIONE 2.28. Sia

$$B : V \rightarrow V$$

una applicazione lineare invertibile. Allora vale $Imm L = Imm (L \circ B)$

DIMOSTRAZIONE. Dato che B è una funzione invertibile, è bigettiva, ossia $B(V) = V$. Dunque

$$Imm (L \circ B) = L(B(V)) = L(V)$$

\square

OSSERVAZIONE 2.29. Dopo quanto abbiamo dimostrato, abbiamo un algoritmo in 3 passi che, data una applicazione lineare tra due spazi vettoriali V e W , e fissata una base $\{e_1, e_2, \dots, e_n\}$ di V e una base $\{\epsilon_1, \epsilon_2, \dots, \epsilon_m\}$ di W , ci permette di determinare la dimensione ed una base di $Imm L$:

- (1) Scrivere la matrice $[L]$ associata ad L rispetto alle basi fissate,
- (2) ridurre $[L]$ in forma a scalini (che indichiamo con $[S]$) attraverso operazioni elementari su colonna,
- (3) Sapendo che $[L]$ e $[S]$ sono associate a due applicazioni lineari distinte, ma con la stessa immagine (ovvero $Imm L$), leggiamo le informazioni relative ad $Imm L$ attraverso la forma a scalini $[S]$ di $[L]$.

Ma come si leggono, tramite $[S]$, le informazioni cercate su $Imm L$? Ovvero come si applica il punto 3) sopra?

OSSERVAZIONE 2.30. Ricordiamo (vedi Esercizio 1.76) che $Imm L$ coincide con il sottospazio vettoriale generato dalle immagini degli elementi di una base dello spazio di partenza. Ossia, una volta fissate le basi, dai vettori colonna della matrice che rappresenta l'applicazione.

Tradotto nel nostro caso: $\text{Imm } L$ è il sottospazio vettoriale di W generato da $L(e_1), L(e_2), \dots, L(e_n)$, che sono i vettori corrispondenti alle colonne di $[L]$. Ma la proposizione garantisce che $\text{Imm } L = \text{Imm } (L \circ M)$, dunque $L(V)$ è anche generato dai vettori di W corrispondenti alle colonne di $[L][M]$. Ora, la matrice $[L][M]$ ha delle colonne *semplici* con cui lavorare, visto che è in forma a scalini ridotta. Si vede subito che le colonne non nulle di $[L][M]$ (dove sono presenti i pivot) formano un insieme di vettori linearmente indipendenti di \mathbb{K}^m , e dunque che i vettori di W corrispondenti a tali colonne, siccome appunto sono linearmente indipendenti e generano $\text{Imm } L$, sono una base di $\text{Imm } L$. In particolare $\dim \text{Imm } L$ è uguale al numero di scalini (pivot) della matrice ridotta a scala.

Ricordando il Teorema 2.16, e osservando che il numero di colonne non nulle in una matrice in forma a scalini corrisponde al numero di pivot, possiamo riassumere quanto abbiamo appena detto:

PROPOSIZIONE 2.31. *Data una matrice A , qualsiasi riduzione a scalini per colonne di A ottenuta attraverso le operazioni elementari su colonna, ha come invariante il numero n di pivot. In particolare, se vediamo A come la matrice associata ad una applicazione lineare L tra due spazi vettoriali V e W rispetto a due basi fissate di V e W , allora il numero n di pivot è la dimensione del sottospazio di W $\text{Imm } L$.*

A questo punto possiamo introdurre un concetto importante nello studio delle applicazioni lineari, quello di *rango* di una applicazione lineare.

DEFINIZIONE 2.32. Data una applicazione lineare $L : V \rightarrow W$, dove V e W sono due spazi vettoriali di dimensione finita sul campo \mathbb{K} , il **rango** di L è il numero $\dim \text{Imm } L$.

Le osservazioni fatte fin qui in particolare dimostrano il seguente:

TEOREMA 2.33. *Data una applicazione lineare L come sopra e fissate le basi, vale che il rango di L è uguale al numero di colonne non nulle che si trovano quando si trasforma $[L]$ in forma a scalini, ovvero al numero di pivot.*

OSSERVAZIONE 2.34. Se avessimo fissato altre basi avremmo avuto una matrice $[L]$ diversa, ma, trasformandola in forma a scalini, avremmo ancora ovviamente trovato lo stesso numero di colonne non nulle, giacché tale numero è $\dim \text{Imm } L$, ossia dipende dalla applicazione (è la dimensione della sua immagine) e non dalle basi scelte.

OSSERVAZIONE 2.35. Osserviamo che il rango di una applicazione lineare L è anche uguale al **massimo numero di colonne linearmente indipendenti** di $[L]$. Infatti sappiamo che $\text{Imm } L$ è il sottospazio vettoriale di W generato dai vettori colonna di $[L]$. Da questi vettori, come risulta dal Teorema 1.60, è possibile estrarre una base di $\text{Imm } L$ e, ricordando la dimostrazione di quel teorema, possiamo dire che $\dim \text{Imm } L$ è uguale al massimo numero di colonne linearmente indipendenti di $[L]$.

5. La riduzione a scalini per righe

Nei paragrafi precedenti di questo capitolo abbiamo studiato le operazioni elementari di colonna su una matrice. Possiamo ripetere molte delle cose dette operando sulle righe anziché sulle colonne.

Innanzitutto, data una matrice in $Mat_{m \times n}(\mathbb{K})$, è possibile definire le *mosse* sulle righe, dette anche **operazioni elementari sulle righe** di una matrice, in totale simmetria (ovvero sostituendo alla parola colonna, la parola riga) con quanto fatto per le colonne:

- (1) si somma alla riga i la riga j moltiplicata per uno scalare λ ;
- (2) si moltiplica la riga s per uno scalare $k \neq 0$;
- (3) si permutano fra di loro due righe, diciamo la i e la j .

Procedendo sempre in maniera simmetrica a quanto fatto nel caso delle colonne, si può definire la forma a scalini per righe di una matrice. Chiamiamo stavolta *profondità* di una riga la posizione occupata, contata da destra, dal suo coefficiente diverso da zero che sta più a sinistra sulla riga. Alla riga nulla (con tutte i coefficienti uguali a 0) assegnamo per convenzione profondità 0.

ESEMPIO 2.36. Ad esempio la riga:

$$(0, 0, 7, \sqrt{2}, 3, 0, 0, 9)$$

ha profondità 6, in quanto, il termine diverso da zero più a sinistra della riga è il 7, e se si comincia a contare da destra della riga, il 7 è alla posizione 6.

A questo punto possiamo dare la definizione di matrice a scalini per righe.

DEFINIZIONE 2.37. Una matrice A in $Mat_{m \times n}(\mathbb{K})$, si dice **in forma a scalini per righe** se rispetta le seguenti proprietà:

- leggendo la matrice dall'alto verso il basso, le righe non nulle si incontrano tutte prima della righe nulle;
- leggendo la matrice dall'alto verso il basso, le profondità delle sue righe non nulle risultano strettamente decrescenti.

ESERCIZIO 2.38. Dire quale, tra le seguenti matrici, è in forma a scalini

per righe:

$$\begin{array}{l}
 \left(\begin{array}{cccc} 1 & 5 & 4 & 0 \\ 0 & 1 & \sqrt{7}+1 & 0 \\ 0 & 0 & 0 & 1 \end{array} \right) \\
 \left(\begin{array}{cccc} 1 & 3 & 0 & 9 \\ 0 & 1 & 3 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & \sqrt{3} \end{array} \right) \\
 \left(\begin{array}{cccc} 1 & 0 & 4 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 5 \end{array} \right) \\
 \left(\begin{array}{ccccc} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{array} \right)
 \end{array}
 \quad
 \begin{array}{l}
 \left(\begin{array}{cccc} 1 & 5 & 4 & 0 \\ 1 & 1 & \sqrt{7}+1 & 0 \\ 0 & 0 & 0 & 1 \end{array} \right) \\
 \left(\begin{array}{cccc} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array} \right) \\
 \left(\begin{array}{cccc} 0 & 1 & 0 & 7 \\ 0 & 0 & 1 & 5 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array} \right) \\
 \left(\begin{array}{ccccc} 1 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 5 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right)
 \end{array}$$

In totale simmetria con quanto dimostrato nel caso delle colonne è possibile dimostrare che:

TEOREMA 2.39. *Data una matrice A in $Mat_{m \times n}(\mathbb{K})$ è sempre possibile, usando (un numero finito di) operazioni elementari sulle righe, ridurre la matrice in forma a scalini per righe.*

In particolare, anche quando abbiamo una matrice in forma a scalini per riga, si possono definire i **pivot** della matrice, come i coefficienti più a sinistra delle righe non nulle.

Inoltre, anche nel caso delle righe, è possibile definire una forma a scalini *particolare*: la forma a **scalini per righe ridotta**. In questo caso, lasciamo come esercizio al lettore, di dare una definizione formale, presentando prima alcuni esempi di forma a scalini per righe ridotta.

ESEMPIO 2.40. Ecco alcune matrici in forma a scalini per righe ridotta:

$$\begin{array}{l}
 \left(\begin{array}{cccc} 1 & 0 & -1-5\sqrt{7} & 0 \\ 0 & 1 & \sqrt{7}+1 & 0 \\ 0 & 0 & 0 & 1 \end{array} \right) \\
 \left(\begin{array}{cccc} 1 & 0 & 0 & -20 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 5 \end{array} \right)
 \end{array}
 \quad
 \begin{array}{l}
 \left(\begin{array}{ccccc} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{array} \right) \\
 \left(\begin{array}{cccc} 0 & 1 & 0 & 7 \\ 0 & 0 & 1 & 5 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array} \right)
 \end{array}$$

COROLLARIO 2.41. *Ogni matrice A può essere trasformata, attraverso le operazioni elementari sulle righe, in una matrice in forma a scalini per righe ridotta.*

ESERCIZIO 2.42. Dimostrare il Corollario 2.41.

Proseguiamo lo studio delle analogie tra mosse per colonna e mosse per riga cercando di capire a cosa equivale una operazione elementare su riga in termini di operazioni tra matrici.

Ogni singola mossa (operazione elementare) sulle righe di una generica matrice A di $Mat_{m \times n}(\mathbb{K})$, equivale stavolta a moltiplicare A **a sinistra**, per una matrice $n \times n$ invertibile.² Per esempio la mossa:

- si somma alla riga i la riga j moltiplicata per uno scalare λ ;

corrisponde a moltiplicare la nostra matrice a sinistra per la matrice $n \times n$ che ha tutti 1 sulla diagonale, e 0 in tutte le altre caselle eccetto che nella casella identificata da “riga i , colonna j ”, dove troviamo λ .

Questa matrice, che indichiamo con $U_{ij\lambda}$, è la simmetrica rispetto alla diagonale della matrice $M_{ij\lambda}$ analoga usata nel caso delle mosse di colonna. È immediato verificare che è invertibile e $U_{ij\lambda}^{-1}$ è la simmetrica di $M_{ij\lambda}^{-1}$.

Consideriamo a questo punto una applicazione lineare:

$$L : V \rightarrow W$$

dove V e W sono due spazi vettoriali sul campo \mathbb{K} , di dimensione n e m rispettivamente.

Fissiamo come al solito una base in V e una in W e consideriamo la matrice $[L]$, associata a L .

Agire sulle righe di $[L]$ fino a ridurla in forma a scalini per righe ridotta equivale a dire che moltiplichiamo $[L]$ a sinistra per delle matrici invertibili $[U_1], [U_2], \dots, [U_s]$ fino a che $[U_s][U_{s-1}] \cdots [U_1][L]$ è in forma a scalini (per righe) ridotta.

Per semplificare la notazione, chiamiamo $[U] = [U_s][U_{s-1}] \cdots [U_1]$: sappiamo che $[U]$ è una matrice invertibile, visto che è il prodotto di matrici invertibili, e chiamiamo U l'applicazione lineare da W in W che, rispetto alla base fissata di W , ha per matrice $[U]$.

L'applicazione lineare associata a $[U][L]$ è proprio la

$$U \circ L : V \rightarrow W$$

come sappiamo per il Teorema 2.26.

Però in generale non è vero che $Imm L = Imm (U \circ L)$. In questo caso infatti, prima si applica L e poi una applicazione U bigettiva su W . Dunque l'immagine di $U \circ L$ sarà uguale all'immagine di U applicata a $Imm(L)$, che non è detto sia uguale ad $Imm(L)$. Vale però che la dimensione rimane invariata.

²Teniamo a mente questo cambiamento (da moltiplicazione a destra nel caso delle colonne, a moltiplicazione a sinistra nel caso delle righe, perché spiegherà alcune differenze che ci sono nelle risultato della riduzione per riga e per colonna.

TEOREMA 2.43. *Sia*

$$L : V \rightarrow W$$

una applicazione lineare fra due spazi vettoriali V e W sul campo \mathbb{K} . Sia

$$B : W \rightarrow W$$

una applicazione lineare invertibile. Allora vale $\text{Ker } L = \text{Ker } B \circ L$ e inoltre vale $\dim \text{Imm } L = \dim \text{Imm } (B \circ L)$, ossia L e $B \circ L$ hanno lo stesso rango.

DIMOSTRAZIONE. Dimostriamo per prima cosa che $\text{Ker } L = \text{Ker } B \circ L$. Verifichiamo innanzitutto che $\text{Ker } L \subseteq \text{Ker } B \circ L$.

Sia v un vettore di $\text{Ker } L$, allora $L(v) = O$. Ma $(B \circ L)(v) = B(L(v)) = B(O) = O$, per cui $v \in \text{Ker } B \circ L$.

Verifichiamo ora che $\text{Ker } B \circ L \subseteq \text{Ker } L$. Sia v' un vettore che appartiene a $\text{Ker } B \circ L$. Dobbiamo mostrare che $v' \in \text{Ker } L$, ossia che $L(v') = O$. Sappiamo che $(B \circ L)(v') = O$, ovvero che $B(L(v')) = O$. Ora, l'applicazione B è bigettiva, dunque iniettiva, e l'unico vettore che manda in O è O (vedi Proposizione 1.73), per cui deve valere $L(v') = O$.

A questo punto, possiamo applicare il Teorema 2.21 alle due applicazioni L e $B \circ L$. Otteniamo

$$\dim \text{Imm } L + \dim \text{Ker } L = \dim V$$

e

$$\dim \text{Imm } B \circ L + \dim \text{Ker } B \circ L = \dim V$$

Da queste due equazioni, sapendo che $\text{Ker } L = \text{Ker } B \circ L$, si ricava immediatamente che $\dim \text{Imm } L = \dim \text{Imm } (B \circ L)$. \square

Torniamo al nostro caso della applicazione lineare L tale che la sua matrice $[L]$ ha come forma a scalini per righe ridotta la matrice $[U][L]$. Come sappiamo, per calcolare il nucleo di L in concreto si risolve il sistema lineare

$$[L] \begin{pmatrix} x_1 \\ x_2 \\ \dots \\ \dots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \dots \\ 0 \end{pmatrix}$$

Una prima conseguenza del teorema appena dimostrato è che per calcolare il nucleo di L basterà risolvere il sistema lineare

$$[U][L] \begin{pmatrix} x_1 \\ x_2 \\ \dots \\ \dots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \dots \\ 0 \end{pmatrix}$$

in cui la matrice $[U][L]$ è molto più semplice perché è in forma a scalini ridotta per riga. Di questo aspetto ci occuperemo più estesamente nel prossimo capitolo, dedicato ai sistemi lineari.

Un'altra conseguenza del Teorema 2.43 è la seguente: siccome il rango di L e quello di $U \circ L$ sono uguali, allora il massimo numero di colonne linearmente indipendenti di $[L]$ deve essere uguale al massimo numero di colonne linearmente indipendenti della sua forma a scalini per righe $[U][L]$ (questo infatti è un modo di contare il rango, come sappiamo dalla Osservazione 2.35). Ma si vede subito che una matrice in forma a scalini per righe ha tante colonne linearmente indipendenti quanti sono i suoi scalini ossia quante sono le righe non nulle. Dunque abbiamo dimostrato:

TEOREMA 2.44. *Sia*

$$L : V \rightarrow W$$

una applicazione lineare tra gli spazi vettoriali V e W rispettivamente di dimensione n e m sul campo \mathbb{K} . Il rango di L (ovvero la dimensione della sua immagine) è uguale al numero di righe non nulle che si trovano quando si riduce una matrice associata $[L]$ in forma a scalini per righe.

Nel caso delle colonne avevamo osservato che il numero di colonne non zero della forma a scalini era uguale al massimo numero di colonne linearmente indipendenti della matrice iniziale: per ragioni puramente di simmetria lo stesso argomento vale anche per le righe (qui consideriamo le righe come dei vettori di uno spazio vettoriale, scritti per riga invece che per colonna come facciamo di solito). Completiamo allora il Teorema 2.44 come nel caso della riduzione per colonne:

TEOREMA 2.45. *Sia*

$$L : V \rightarrow W$$

una applicazione lineare tra gli spazi vettoriali V e W rispettivamente di dimensione n e m sul campo \mathbb{K} . Il rango di L (ovvero la dimensione della sua immagine) è uguale al numero di righe non nulle che si trovano quando si riduce una matrice associata $[L]$ in forma a scalini per righe. Tale numero è anche uguale al massimo numero di righe linearmente indipendenti della matrice $[L]$.

6. Ancora sulla riduzione a scala di una matrice e lo studio delle applicazioni lineari

Riassumendo e combinando tra loro i risultati degli ultimi due paragrafi si ha:

TEOREMA 2.46. *Data una applicazione lineare $L : V \rightarrow W$ tra due spazi vettoriali V e W sul campo \mathbb{K} , e data la matrice $[L]$ associata a L rispetto a due basi fissate di V e W :*

- (1) *Il massimo numero di righe linearmente indipendenti di $[L]$ è uguale al massimo numero di colonne linearmente indipendenti di $[L]$, ossia al rango di L .*

- (2) *Se si riduce la matrice $[L]$ in forma a scalini, sia che lo si faccia per righe, sia che lo si faccia per colonne, il numero di scalini che otterremo (ovvero il numero di pivot della matrice) sarà sempre uguale al rango di L .*

DEFINIZIONE 2.47. Data una matrice M , chiamiamo **rango della matrice** il massimo numero di colonne (o righe, abbiamo visto che è lo stesso) linearmente indipendenti di M .

OSSERVAZIONE 2.48. Con la definizione appena introdotta, e dal teorema 2.46, si ha che il rango di una applicazione lineare L coincide con quello di una sua matrice associata $[L]$ rispetto a due basi fissate. Dunque possiamo usare la parola rango senza fare troppa attenzione, applicandola sia alle matrici sia alle applicazioni.

Sappiamo inoltre che, se componiamo L a destra o a sinistra per una applicazione invertibile, il rango non cambia. Dunque, se moltiplichiamo $[L]$ a destra o a sinistra per matrici invertibili, anche il rango delle matrici non cambia.

Dall'Osservazione 2.48 segue un algoritmo piuttosto semplice per calcolare il rango (ovvero la dimensione dell'immagine) di una applicazione lineare L :

- (1) Scriviamo la matrice associata $[L]$ rispetto ad una qualunque coppia di basi.
- (2) Riduciamo $[L]$ a scalini usando sia mosse di riga sia mosse di colonna nell'ordine che ci torna più comodo.
- (3) Contiamo il numero di scalini (pivot) della matrice ridotta a scala.

Lo schema in Figura 1 riassume graficamente le relazioni tra le riduzioni a scala (per riga e per colonna) di una matrice $[L]$ associata ad una applicazione lineare L tra due spazi vettoriali V e W discusse fin qui.

Dunque, data L applicazione lineare tra due spazi vettoriali V e W sul campo \mathbb{K} , attraverso la riduzione a scala per colonne di una matrice associata a L , si può determinare una base di $\text{Imm } L$ considerando i vettori corrispondenti alle colonne non nulle della matrice così ottenuta. La base che troviamo con questo metodo ha il pregio di essere *a scalini*, e dunque si presta bene per alcuni scopi: ad esempio è quasi immediato, diremmo quasi *a colpo d'occhio*, stabilire se un certo vettore v appartiene ad $\text{Imm } L$, ovvero è combinazione lineare dei vettori di questa base oppure no.

Ma come abbiamo già accennato, e come vedremo anche nel prossimo capitolo, per determinare il $\text{Ker } L$, può essere comodo portare la matrice a scalini per righe: in questo caso dobbiamo necessariamente calcolare anche la forma a scalini per colonne per determinare una base di $\text{Imm } L$? La risposta a questa domanda è no, come spiegheremo tra poco: dalla forma a scalini per righe di una matrice associata ad L , si ricava una informazione che risulta utile per trovare una base di $\text{Imm } L$, che in generale però non sarà a scalini. Vediamo come partendo da un esempio.

$L : V \rightarrow W$ applicazione lineare

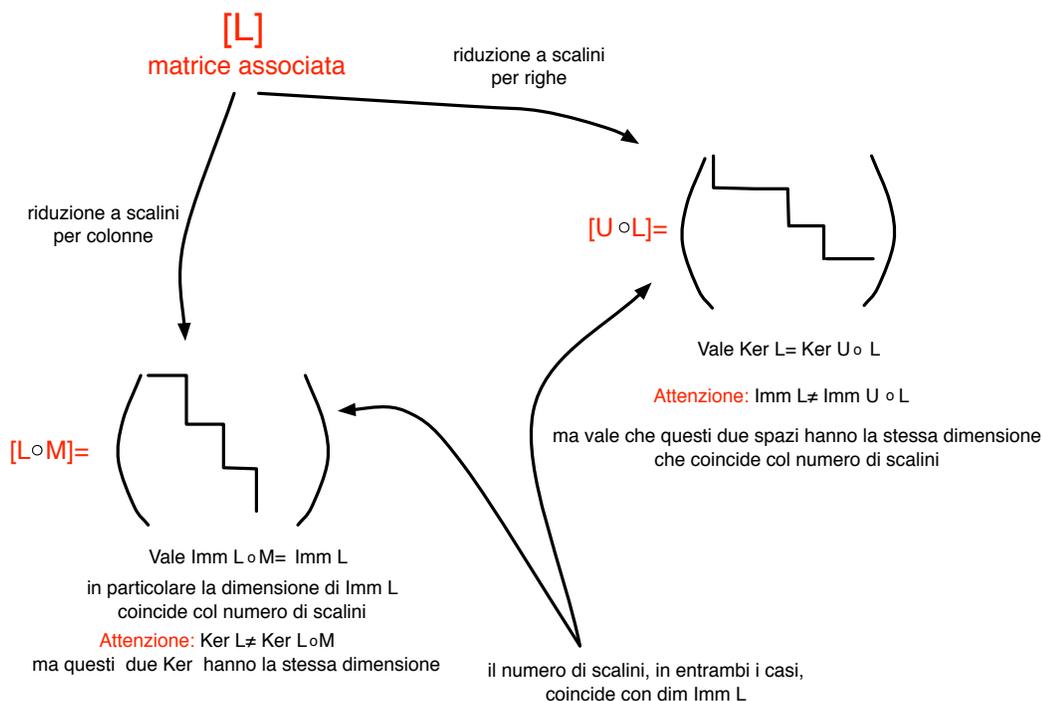


FIGURA 1. Schema riassuntivo sulla riduzione per righe e per colonne

Supponiamo che una applicazione lineare L , tra due spazi vettoriali V e W su \mathbb{K} , rispetto a certe basi fissate in V e W , sia rappresentata dalla matrice:

$$[L] = \begin{pmatrix} 1 & 2 & 5 & 7 & 18 \\ 4 & 8 & 14 & 20 & 54 \\ 2 & 4 & 7 & 10 & 28 \\ 3 & 6 & 9 & 13 & 36 \end{pmatrix}$$

Con operazioni di riga, si può portare $[L]$ nella forma a scalini per righe seguente (dove in neretto abbiamo indicato i pivot, e dunque la posizione degli scalini):

$$R = \begin{pmatrix} \mathbf{1} & 2 & 2 & 3 & 4 \\ 0 & 0 & \mathbf{3} & 4 & 6 \\ 0 & 0 & 0 & 0 & \mathbf{2} \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Osserviamo che gli scalini sono nella prima, nella terza e nella quinta colonna. Quello che vogliamo dimostrare è che da questo segue che la prima, la

terza e la quinta colonna **della matrice iniziale** $[L]$ (ATTENZIONE! Proprio della matrice iniziale $[L]$, non della sua forma ridotta a scalini per riga R) sono linearmente indipendenti, e quindi una base di $\text{Imm } L$ è data dai vettori corrispondenti alla prima (v_1), alla terza (v_2), e alla quinta colonna (v_3) di $[L]$:

$$\begin{pmatrix} 1 \\ 4 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 5 \\ 14 \\ 7 \\ 9 \end{pmatrix}, \begin{pmatrix} 18 \\ 54 \\ 28 \\ 36 \end{pmatrix}$$

Cerchiamo di capire come mai è proprio così. Supponiamo di estrarre dalla matrice iniziale la matrice più piccola in cui abbiamo tenuto solo la prima, la terza e la quinta colonna:

$$\begin{pmatrix} 1 & 5 & 18 \\ 4 & 14 & 54 \\ 2 & 7 & 28 \\ 3 & 9 & 36 \end{pmatrix}$$

Se su tale matrice facciamo le stesse identiche mosse di riga che avevamo fatto sulla $[L]$ per ottenere la sua forma a scalini per riga A , che matrice otterremo? Senza fare nessun conto, sappiamo già che otterremo la seguente matrice:

$$\begin{pmatrix} 1 & 2 & 4 \\ 0 & 3 & 6 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix}$$

Infatti durante le operazioni di riga ciascuna colonna si trasforma senza interagire con le altre colonne, dunque nel nostro caso le tre colonne si trasformano esattamente come si erano trasformate prima.

A questo punto però sappiamo che i tre vettori

$$\begin{pmatrix} 1 \\ 4 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 5 \\ 14 \\ 7 \\ 9 \end{pmatrix}, \begin{pmatrix} 18 \\ 54 \\ 28 \\ 36 \end{pmatrix}$$

sono linearmente indipendenti, perché la matrice che essi formano ha rango 3 (questo lo sappiamo perché abbiamo mostrato che le operazioni elementari per riga - o colonna - non modificano il rango della matrice). Ora il rango di L , ovvero $\dim \text{Imm } L$, è proprio 3 (la matrice ridotta a scalini per righe aveva appunto 3 scalini). Dunque tali vettori sono una base di $\text{Imm } L$.

Ricalcando questa dimostrazione, si può dimostrare in generale che:

PROPOSIZIONE 2.49. *Se A è una matrice $m \times n$ a valori su un campo \mathbb{K} , ed indichiamo con e_1, \dots, e_n le sue colonne, e B è una riduzione a scalini per righe di A , allora le colonne di A in corrispondenza alla posizione dei pivot di B formano una base dello Span delle colonne di A ($\text{Span}(e_1, \dots, e_n)$).*

OSSERVAZIONE 2.50. Si può anche considerare il caso 'simmetrico' a quello discusso: se abbiamo una matrice ridotta a scalini per colonna e vediamo che gli scalini sono, per esempio, nella seconda, nella terza e nella quarta riga, possiamo dedurre che la seconda, la terza e la quarta riga *della matrice iniziale* sono una base dello spazio generato dalle righe. A cosa potrebbe essere utile questa affermazione? Rifletteteci per esercizio, partendo dalla considerazione che il sistema dato dalle righe della matrice iniziale è equivalente al sistema in cui si considerano solo la seconda, la terza e la quarta riga...

OSSERVAZIONE 2.51. Quello che abbiamo dimostrato e riassunto nella Proposizione 2.49, permette di fornire un algoritmo per *estrarre* una base di uno spazio vettoriale, a partire da un insieme di generatori. Cosa che teoricamente sappiamo essere sempre possibile, a seguito del Teorema 1.60. Sia infatti V uno spazio vettoriale, di dimensione n e di cui conosciamo una base $\{e_1, \dots, e_n\}$. Consideriamo l vettori v_1, \dots, v_l di V , ed, in particolare, il sottospazio vettoriale di V $Span(v_1, \dots, v_l)$. Se vogliamo estrarre una base di $Span(v_1, \dots, v_l)$ da v_1, \dots, v_l (che sappiamo, per definizione, generare $Span(v_1, \dots, v_l)$), scriviamo le coordinate dei v_i rispetto alla base $\{e_1, \dots, e_n\}$ e le consideriamo (ogni n -upla di coordinate del singolo v_i) come colonne di una matrice M . A questo punto si porta M in forma a scalini per riga (chiamiamo la matrice a scalini per riga S), e, i vettori v_i con indice i in corrispondenza dei pivot di S formano una base di $Span(v_1, \dots, v_l)$, estratta dall'insieme di generatori $\{v_1, \dots, v_l\}$.

7. Altri esercizi

ESERCIZIO 2.52. Consideriamo l'applicazione lineare $L_a : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ dipendente dal parametro reale a e definita da:

$$L_a(x, y, z) = (ax + y + z, x + ay + z, -x + y + az)$$

- (1) Trovare per quali valori di a l'applicazione L_a non è surgettiva.
- (2) Fissato un valore \bar{a} di a per cui L_a non è surgettiva, determinare la dimensione di $Ker(L_{\bar{a}})$ e di $Imm(L_{\bar{a}})$, ed una base di quest'ultimo spazio vettoriale.

Svolgimento Scriviamo la matrice associata ad L_a rispetto alla base *canonica* e_1, e_2, e_3 di \mathbb{R}^3 (sia "in partenza", che come spazio "di arrivo").

Per scrivere la matrice $[L_a]$ associata ad L_a rispetto a questa base, bisogna calcolare le coordinate di $L_a(e_1)$, $L_a(e_2)$, $L_a(e_3)$ rispetto alla base e_1, e_2 ed e_3 :

$$\begin{cases} L_a(1, 0, 0) = (a, 1, -1) \\ L_a(0, 1, 0) = (1, a, 1) \\ L_a(0, 0, 1) = (1, 1, a) \end{cases}$$

Dunque:

$$[L_a] = \begin{pmatrix} a & 1 & 1 \\ 1 & a & 1 \\ -1 & 1 & a \end{pmatrix}$$

Riduciamo $[L_a]$ a scalini per righe, attraverso operazioni elementari di riga:

$$[L_a] \xrightarrow{(1) \odot (2)} A_1 = \begin{pmatrix} 1 & a & 1 \\ a & 1 & 1 \\ -1 & 1 & a \end{pmatrix} \xrightarrow[\substack{(2)=(2)-a(1) \\ (3)=(3)+(1)}]{} A_2 = \begin{pmatrix} 1 & a & 1 \\ 0 & 1-a^2 & 1-a \\ 0 & a+1 & a+1 \end{pmatrix}$$

Se $1-a^2$ è diverso da 0, ovvero se $a \neq \pm 1$, possiamo dividere la seconda riga per $1-a^2$ e avere uno scalino sulla seconda riga, in corrispondenza della seconda colonna. Dunque, prima di andare avanti, studiamo a parte i casi *sfortunati*, ovvero $a = 1$ e $a = -1$, per cui non si può procedere così.

- Se $a = 1$ la matrice A_2 è:

$$A_2 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 2 & 2 \end{pmatrix}$$

Dunque non è ancora a scalini per righe, ma basta fare la mossa di riga di scambiare la seconda con la terza riga per avere la forma a scalini cercata:

$$A_3 = \begin{pmatrix} \mathbf{1} & 1 & 1 \\ 0 & \mathbf{2} & 2 \\ 0 & 0 & 0 \end{pmatrix}$$

Si vede subito (si vedeva anche da A_2 a dire il vero...) che il rango di A_2 , che sappiamo essere uguale a rango di $[L_1]$, che è a sua volta uguale alla $\dim \text{Imm } L_1$, è 2 (tanto quanti sono i pivot, evidenziati in neretto nella matrice A_3). Dunque L_1 non è surgettiva (la dimensione di \mathbb{R}^3 è 3), e la dimensione del nucleo (dal Teorema 2.21) è 1.

- Se $a = -1$ la matrice A_2 è:

$$A_2 = \begin{pmatrix} \mathbf{1} & -1 & 1 \\ 0 & 0 & \mathbf{2} \\ 0 & 0 & 0 \end{pmatrix}$$

che è già in forma a scalini per righe. La lettura della matrice A_2 , ci dice che anche L_{-1} non è surgettiva, e anche in questo caso $\dim \text{Imm } L_{-1} = 2$ e $\dim \text{Ker } L_{-1} = 1$.

Occupiamoci dei casi diversi dai due precedenti (stiamo supponendo dunque che $a \neq \pm 1$):

$$A_2 \xrightarrow[\substack{(2)=\frac{(2)}{1-a^2}}]{} A_3 = \begin{pmatrix} 1 & a & 1 \\ 0 & 1 & \frac{1}{1+a} \\ 0 & 0 & (1-a)(a+2) \end{pmatrix}$$

In questo caso A_3 è in forma a scalini per righe, ma il numero di pivot dipende dal valore di $(1-a)(a+2)$. Se $(1-a)(a+2) = 0$ (ovvero se $a = 2$, perché siamo nel caso $a \neq \pm 1$) allora A_3 ha 2 pivot, e dunque L_2 non è surgettiva, altrimenti L_a ha tre pivot e dunque è surgettiva (e il nucleo ha, in questo caso, dimensione 0).

Concludendo il primo punto dell'esercizio, L_a è surgettiva per ogni valore di a diverso da $-1, 1, 2$. In questi 3 casi invece l'immagine ha dimensione 2 e il nucleo 1.

Per rispondere alla seconda domanda, fissiamo per esempio $a = 1$. Conosciamo già la riduzione a scalini per righe di L_1 che è:

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

Perciò una base di $Imm L_1$ è data dai vettori colonna della matrice $[L_1]$, associata ad L_1 rispetto alla base canonica, che si trovano in corrispondenza dei pivot (ovvero dalla prima e dalla seconda colonna). Scriviamo L_1 :

$$[L_1] = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ -1 & 1 & 1 \end{pmatrix}$$

E dunque una base di $Imm L_1$ è:

$$\left\{ \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \right\}$$

ESERCIZIO 2.53. Si consideri l'applicazione lineare $L : \mathbb{R}^5 \rightarrow \mathbb{R}^4$ che è data, nelle basi standard di \mathbb{R}^5 e \mathbb{R}^4 , dalla seguente matrice:

$$\begin{pmatrix} 1 & 3 & 4 & 0 & 0 \\ 6 & 9 & 11 & 8 & 3 \\ 5 & 6 & 7 & 8 & 3 \\ 1 & 0 & 0 & 2 & 0 \end{pmatrix}$$

e consideriamo poi i 4 vettori di \mathbb{R}^4 :

$$v_1 = \begin{pmatrix} 1 \\ 2 \\ 1 \\ 0 \end{pmatrix}, v_2 = \begin{pmatrix} 0 \\ 4 \\ 4 \\ 1 \end{pmatrix}, v_3 = \begin{pmatrix} 0 \\ 3 \\ 3 \\ 0 \end{pmatrix}, v_4 = \begin{pmatrix} 2 \\ 0 \\ 0 \\ 2 \end{pmatrix}$$

- Verificare che $\{v_1, v_2, v_3, v_4\}$ è una base di \mathbb{R}^4 .
- Scrivere la matrice associata all'applicazione L rispetto alla base standard di \mathbb{R}^5 e alla base $\{v_1, v_2, v_3, v_4\}$ di \mathbb{R}^4 .
- L'applicazione L è surgettiva?

ESERCIZIO 2.54. Siano V, W spazi vettoriali di dimensione finita sul campo \mathbb{K} e sia $L : V \rightarrow W$ una applicazione lineare di rango r . Dimostrare che

esistono una base di V e una base di W tali che la matrice $[L]$ associata a L rispetto a tali basi abbia la forma:

$$[L] = (a_{ij}) = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \dots \end{pmatrix}$$

in cui solo r coefficienti sono diversi da zero (e uguali a 1), ossia $a_{ij} = 0$ eccetto i coefficienti $a_{11} = a_{22} = \dots = a_{rr} = 1$.

ESERCIZIO 2.55. Sia A la matrice a coefficienti in \mathbb{Z} seguente:

$$A = \begin{pmatrix} 1 & 5 & -6 & 0 \\ 2 & -8 & -14 & 12 \\ -1 & 7 & 10 & 0 \end{pmatrix}$$

Per ogni p primo, denotiamo con A_p la matrice A pensata con i coefficienti in \mathbb{Z}_p . Determinare, al variare di p tra i primi, il rango della matrice A_p .

Svolgimento. Il rango di una matrice non varia se si fanno operazioni di riga o di colonna. Con alcune operazioni di riga (*intere*, ossia in cui gli scalari che compaiono sono numeri interi) si ottiene

$$A \xrightarrow[\substack{[2]=2[1]-[2] \\ [3]=[1]+[3]}]{[3]=3[3]-2[3]} B = \begin{pmatrix} 1 & 5 & -6 & 0 \\ 0 & 18 & 2 & -12 \\ 0 & 12 & 4 & 0 \end{pmatrix} \xrightarrow{[3]=3[3]-2[3]} C = \begin{pmatrix} 1 & 5 & -6 & 0 \\ 0 & 18 & 2 & -12 \\ 0 & 0 & 8 & 24 \end{pmatrix}$$

Osserviamo che l'operazione di riga $[3] = 3[3] - 2[3]$ (che è in realtà la composizione di due operazioni elementari di riga, moltiplicare la terza riga per 3 e poi sostituirla con se stessa meno la seconda riga moltiplicata per 2) non può essere fatta in \mathbb{Z}_3 perché una delle due operazioni coinvolte è "sostituire la terza riga con se stessa moltiplicata per 3", che in \mathbb{Z}_3 non è una operazione ammessa (si può sostituire una riga con se stessa moltiplicata per λ ma λ deve essere diverso da 0). A parte il caso \mathbb{Z}_3 , le mosse che abbiamo fatto sono valide per tutti gli altri \mathbb{Z}_p . Dunque il rango di A_p sarà 3 per tutti i primi che non dividono 8 e 18, ovvero per tutti i primi diversi da 2 e da 3 (del resto il caso $p = 3$ doveva già essere studiato a parte). Ci rimane dunque da studiare questi due casi:

- Se $p = 2$, una riduzione a scalini di A_2 è data dalla seguente matrice (si ottiene riducendo modulo 2 la matrice C):

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

e dunque A_2 ha rango 1.

- Se $p = 3$, una riduzione a scalini di A_3 è la seguente matrice (si ottiene riducendo modulo 3 la matrice B , ovvero la matrice che avevamo prima di fare la mossa ‘proibita’ in \mathbb{Z}_3 , e poi facendo due ulteriori mosse di riga):

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

e dunque A_3 ha rango 2.

ESERCIZIO 2.56. Sia $f_h : (\mathbb{Z}_5)^3 \rightarrow (\mathbb{Z}_5)^3$, al variare di h in \mathbb{Z}_5 , l'applicazione lineare la cui matrice associata rispetto alle basi standard è la seguente:

$$[f_h] = \begin{pmatrix} 1 & h & 4 \\ 0 & 0 & 1 \\ 0 & h & 0 \end{pmatrix}$$

Sia V il sottospazio vettoriale di $(\mathbb{Z}_5)^3$ definito da $V = \{(x, y, z) \in (\mathbb{Z}_5)^3 \mid y - z = 0\}$. Studiare per quali valori di $h \in \mathbb{Z}_5$ si ha che $f_h(V) \subseteq V$.

Svolgimento. Troviamo una base di V . Gli elementi di V sono le terne di elementi di \mathbb{Z}_5 che risolvono il sistema lineare omogeneo $y - z = 0$. Perciò i vettori di V sono del tipo:

$$\begin{pmatrix} s \\ t \\ t \end{pmatrix}$$

Al variare di s e t in \mathbb{Z}_5 (in particolare li possiamo anche contare, sono 25). Dunque il generico vettore di V può essere scritto, al variare di s e t , come segue:

$$\begin{pmatrix} s \\ t \\ t \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} s + \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} t$$

Questo ci dice che i vettori:

$$v_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad v_2 = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$$

generano V , ed essendo anche linearmente indipendenti (perché?), sono una base di V (che dunque ha dimensione 2).

Cerchiamo ora una base di $f_h(V)$. Sappiamo che $f_h(V)$ è generata dall'immagine, tramite f_h , di una base di V , dunque calcoliamoci $f_h(v_1)$ e $f_h(v_2)$:

$$f_h(v_1) = \begin{pmatrix} 1 & h & 4 \\ 0 & 0 & 1 \\ 0 & h & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

$$f_h(v_2) = \begin{pmatrix} 1 & h & 4 \\ 0 & 0 & 1 \\ 0 & h & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} h+4 \\ 1 \\ h \end{pmatrix}$$

Osserviamo che $f_h(V) \subseteq V$ se e solo se $f_h(v_1)$ e $f_h(v_2)$ appartengono a V . Osserviamo subito che $f_h(v_1)$ appartiene a V (è uno dei due elementi della base di V trovata); cerchiamo di capire se $f_h(v_2)$ appartiene a $V = \text{Span}(v_1, v_2)$. Ovvero studiamo quando esistono $\alpha, \beta \in \mathbb{Z}_5$ tali che:

$$\begin{pmatrix} h+4 \\ 1 \\ h \end{pmatrix} = \alpha \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$$

Questo equivale a risolvere in \mathbb{Z}_5 il sistema lineare in α e β seguente:

$$\begin{pmatrix} \alpha \\ \beta \\ \beta \end{pmatrix} = \begin{pmatrix} h+4 \\ 1 \\ h \end{pmatrix}$$

Il sistema ammette soluzione se e solo se $h = 1$.

ESERCIZIO 2.57. Si consideri la trasformazione lineare $f : \mathbb{R}^3 \rightarrow \mathbb{R}^2$ definita da:

$$f(x, y, z) = (x - 2y - z, x + y + z)$$

Scrivere la matrice A di tale trasformazione rispetto alle basi canoniche di \mathbb{R}^3 e \mathbb{R}^2 e determinare una base dell'immagine e del nucleo di f .

Svolgimento. Per trovare la matrice A associata ad f rispetto alle basi canoniche di \mathbb{R}^3 e \mathbb{R}^2 è sufficiente calcolare i coefficienti, rispetto alla base canonica di \mathbb{R}^2 , dell'immagine degli elementi della base canonica di \mathbb{R}^3 . Tali coefficienti costituiscono le colonne ordinate della matrice cercata. Dunque la prima colonna di A è data dai coefficienti dell'immagine di $(1, 0, 0)$, la seconda colonna dai coefficienti dell'immagine di $(0, 1, 0)$ e la terza colonna dai coefficienti dell'immagine di $(0, 0, 1)$. Calcoliamoli:

$$f(1, 0, 0) = (1, 1) \quad f(0, 1, 0) = (-2, 1) \quad f(0, 0, 1) = (-1, 1)$$

Dunque la matrice A cercata è la seguente:

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

Per trovare una base dell'immagine di f (che è generata dalle colonne della matrice A) si osserva facilmente che la matrice ha rango 2 (perché?), dunque basta individuare due colonne linearmente indipendenti, per esempio le prime due. Dunque

$$\begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad \begin{pmatrix} -2 \\ 1 \end{pmatrix}$$

costituiscono una base di $\text{Im}(f)$.

Sappiamo per il Teorema 2.21 che $\text{Ker } f$ ha dimensione 1 in quanto:

$$\underbrace{\dim(\mathbb{R}^3)}_{=3} = \underbrace{\dim \text{Im}(f)}_{=2} + \dim \text{Ker } f$$

Per trovare una base di $\text{Ker } f$ con operazioni di riga trasformiamo A nella matrice a scalini per righe B :

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

I vettori $w = (x, y, z)$ di \mathbb{R}^3 appartenenti a $\text{Ker } f$, sono le soluzioni del sistema omogeneo $Aw = 0$, che è equivalente al sistema omogeneo $Bw = 0$, ovvero sono i vettori di \mathbb{R}^3 le cui coordinate risolvono il sistema:

$$\begin{cases} x - 2y - z = 0 \\ 3y + 2z = 0 \end{cases}$$

Il sistema ha una variabile libera z , e si ottiene che x e y devono essere:

$$x = -\frac{1}{3}z \quad y = -\frac{2}{3}z$$

Il generico vettore di $\text{Ker } f$ è dunque, al variare del valore t di z in \mathbb{R} , del tipo:

$$\begin{pmatrix} -\frac{1}{3}z \\ -\frac{2}{3}z \\ z \end{pmatrix} = \begin{pmatrix} -\frac{1}{3} \\ -\frac{2}{3} \\ 1 \end{pmatrix} z$$

E dunque il vettore:

$$\begin{pmatrix} -\frac{1}{3} \\ -\frac{2}{3} \\ 1 \end{pmatrix}$$

è una base di $\text{Ker } f$.

ESERCIZIO 2.58 (Attenzione, questo esercizio presenta una tecnica interessante). Consideriamo lo spazio vettoriale $\mathbb{R}_{\leq 3}[x]$ su \mathbb{R} dei polinomi a coefficienti reali, di grado minore o uguale a 3. Sia V il sottospazio di $\mathbb{R}_{\leq 3}[x]$, generato dai seguenti polinomi:

$$p_1(x) = x^3 - 2x + 3, \quad p_2(x) = x^3 + 1, \quad p_3(x) = x - 5, \quad p_4(x) = 2$$

Ovvero $V = \text{Span}(p_1(x), p_2(x), p_3(x), p_4(x))$.

- (1) Estrarre una base di V dall'insieme $\{p_1(x), p_2(x), p_3(x), p_4(x)\}$.
- (2) Completare la base di V ad una base di $\mathbb{R}_{\leq 3}[x]$.

Svolgimento: $\mathbb{R}_{\leq 3}[x]$ è uno spazio vettoriale su \mathbb{R} di dimensione 4, una cui base è $\{1, x, x^2, x^3\}$.

Facciamo vedere come *in un colpo solo* possiamo rispondere ad entrambe le domande dell'esercizio. Scriviamo le coordinate (le indichiamo in neretto)

dei vettori che generano V rispetto alla base di $\mathbb{R}_{\leq 3}[x]$ riportata sopra:

$$\begin{aligned} p_1(x) &= \mathbf{3} \cdot 1 + (-\mathbf{2}) \cdot x + \mathbf{0} \cdot x^2 + \mathbf{1} \cdot x^3 \\ p_2(x) &= \mathbf{1} \cdot 1 + \mathbf{0} \cdot x + \mathbf{0} \cdot x^2 + \mathbf{1} \cdot x^3 \\ p_3(x) &= -\mathbf{5} \cdot 1 + \mathbf{1} \cdot x + \mathbf{0} \cdot x^2 + \mathbf{0} \cdot x^3 \\ p_4(x) &= \mathbf{2} \cdot 1 + \mathbf{0} \cdot x + \mathbf{0} \cdot x^2 + \mathbf{0} \cdot x^3 \end{aligned}$$

A questo punto scriviamo la matrice A , 4×8 , che ha per colonne le coordinate dei vettori $(p_1(x), p_2(x), p_3(x), p_4(x), 1, x, x^2, x^3)$, rispettando questo ordine:

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

Portiamo A in forma a scalini per riga, innanzitutto scambiando l'ordine delle righe e portando la quarta riga come prima riga:

$$A_1 = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 3 & 1 & -5 & 2 & 1 & 0 & 0 & 0 \\ -2 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

$$A_1 \xrightarrow{[2]=[2]-3[1], [3]=[3]+2[1]} A_2 = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & -2 & -5 & 2 & 1 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

$$A_2 \xrightarrow{[3]=[3]+[2]} A_3 = \begin{pmatrix} \mathbf{1} & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & -\mathbf{2} & -5 & 2 & 1 & 0 & 0 & 0 \\ 0 & 0 & -\mathbf{4} & 2 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 \end{pmatrix}$$

A_3 è in forma a scalini per riga, ed ha i pivot (evidenziati in neretto) nella prima, seconda, terza e settima colonna. Questo ci dice che V ha dimensione 3, che una sua base è quella formata dai vettori $p_1(x) = x^3 - 2x + 3$, $p_2(x) = x^3 + 1$, $p_3(x) = x - 5$, e che questa base è completata ad una base di $\mathbb{R}_{\leq 3}[x]$ aggiungendo il vettore corrispondente ai coefficienti della settima colonna, ovvero x^2 .

È importante osservare come se avessimo applicato lo stesso algoritmo dopo aver dato un diverso ordine alla base di V , di $\mathbb{R}_{\leq 3}[x]$, o di entrambe, avremmo ottenuto un altro risultato. Del resto, sappiamo fin dal primo capitolo che la base di uno spazio vettoriale non è unica.

CAPITOLO 3

Sistemi lineari

1. Risolvere un sistema usando le operazioni elementari di riga

Illustreremo un metodo molto conveniente per risolvere sistemi lineari di equazioni.

Sappiamo già risolvere sistemi *omogenei*, ossia quelli in cui tutte le equazioni hanno la forma

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = 0$$

Sono i sistemi con cui abbiamo avuto a che fare quando abbiamo dovuto calcolare il nucleo di una applicazione lineare. Vogliamo mostrare che il metodo che abbiamo usato (ridurre la matrice associata a scalini per righe), si estende anche al caso di sistemi non omogenei. Questo metodo è noto anche col nome *metodo di eliminazione di Gauss*.

Cominciamo con un esempio. Consideriamo il sistema

$$\begin{cases} x + 2y + 2z + 2t = 1 \\ x + 5y + 6z - 2t = -5 \\ 8x - y - 2z - 2t = 0 \\ 2y + 6z + 8t = 3 \end{cases}$$

Per prima cosa, osserviamo che tutte le informazioni del sistema sono contenute nella seguente matrice di numeri (la *matrice completa associata al sistema*):

$$M = \begin{pmatrix} 1 & 2 & 2 & 2 & 1 \\ 1 & 5 & 6 & -2 & -5 \\ 8 & -1 & -2 & -2 & 0 \\ 0 & 2 & 6 & 8 & 3 \end{pmatrix}.$$

Ogni riga contiene i coefficienti di una delle equazioni (per esempio la terza equazione $8x - y - 2z - 2t = 0$ è ‘codificata’ dalla terza riga $(8 - 1 - 2 - 2 \ 0)$).

Sia $S \subset \mathbb{R}^4$ l’insieme delle soluzioni del sistema, ovvero il sottoinsieme

di \mathbb{R}^4 costituito dai vettori $\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}$ tali che, se poniamo $a = x, b = y, c = z, d = t$, tutte le equazioni del sistema diventano delle uguaglianze vere.

Si osserva subito che $\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}$ appartiene a S se e solo se il vettore

$$\begin{pmatrix} a \\ b \\ c \\ d \\ -1 \end{pmatrix} \in \mathbb{R}^5 \text{ soddisfa}$$

$$\begin{pmatrix} 1 & 2 & 2 & 2 & 1 \\ 1 & 5 & 6 & -2 & -5 \\ 8 & -1 & -2 & -2 & 0 \\ 0 & 2 & 6 & 8 & 3 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix},$$

cioè

$$M \begin{pmatrix} a \\ b \\ c \\ d \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Come sappiamo dal Paragrafo 5 del Capitolo 2, possiamo agire sulle righe di M con le mosse elementari di riga fino a ridurla a scalini per righe. Ci sono vari modi per farlo. Uno di essi ci porta alla seguente matrice M' :

$$M' = \begin{pmatrix} 1 & 2 & 2 & 2 & 1 \\ 0 & 1 & \frac{4}{3} & -\frac{4}{3} & -2 \\ 0 & 0 & 2 & -\frac{122}{7} & -18 \\ 0 & 0 & 0 & 2 & \frac{259}{139} \end{pmatrix}.$$

Sempre dal Paragrafo 5 del Capitolo 2 sappiamo anche che $M' = RM$ dove R è una matrice 4×4 invertibile.

Ora osserviamo che un vettore di \mathbb{R}^5 della forma $\begin{pmatrix} a \\ b \\ c \\ d \\ -1 \end{pmatrix}$ soddisfa

$$(1.1) \quad M \begin{pmatrix} a \\ b \\ c \\ d \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

se e solo se soddisfa

$$(1.2) \quad M' \begin{pmatrix} a \\ b \\ c \\ d \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Infatti se $\begin{pmatrix} a \\ b \\ c \\ d \\ -1 \end{pmatrix}$ soddisfa la (1.1) allora

$$M' \begin{pmatrix} a \\ b \\ c \\ d \\ -1 \end{pmatrix} = RM \begin{pmatrix} a \\ b \\ c \\ d \\ -1 \end{pmatrix} = R \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Viceversa, se $\begin{pmatrix} a \\ b \\ c \\ d \\ -1 \end{pmatrix}$ soddisfa la (1.2) allora vuol dire che

$$RM \begin{pmatrix} a \\ b \\ c \\ d \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

ma, poiché R è invertibile, possiamo moltiplicare entrambi i membri dell'uguaglianza per R^{-1} ottenendo

$$R^{-1}RM \begin{pmatrix} a \\ b \\ c \\ d \\ -1 \end{pmatrix} = R^{-1} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

ossia

$$M \begin{pmatrix} a \\ b \\ c \\ d \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

dunque $\begin{pmatrix} a \\ b \\ c \\ d \\ -1 \end{pmatrix}$ soddisfa la (1.1).

Abbiamo dimostrato che l'insieme $S \subseteq \mathbb{R}^4$ delle soluzioni del sistema associato alla matrice M coincide con l'insieme delle soluzioni del sistema associato alla matrice ridotta a scalini M' . Per trovare le soluzioni del sistema iniziale, dunque, possiamo studiare le soluzioni del sistema

$$\begin{cases} x + 2y + 2z + 2t = 1 \\ y + \frac{4}{3}z - \frac{4}{3}t = -2 \\ 2z - \frac{123}{7}t = -18 \\ 2t = \frac{259}{139} \end{cases}$$

Ciò è un grande vantaggio, perché questo sistema (come tutti i sistemi associati a matrici ridotte a scalini per righe) si risolve immediatamente: si ricava dall'ultima equazione $t = \frac{259}{278}$, poi si sostituisce questo valore di t nella penultima equazione e si ricava un valore per z e così via...troveremo la soluzione del sistema (sottolineiamo che, in questo caso, c'è una sola la soluzione).

Quanto abbiamo illustrato per questo esempio vale in generale per qualunque sistema di equazioni lineari, con dimostrazione analoga. Abbiamo dunque il seguente:

TEOREMA 3.1. *L'insieme delle soluzioni di un sistema di equazioni lineari associato alla matrice M (a coefficienti nel campo \mathbb{K}) coincide con l'insieme delle soluzioni del sistema associato alla matrice M' ottenuta riducendo M , attraverso operazioni di riga, in forma a scalini per righe (o a scalini per righe ridotta).*

Osserviamo innanzitutto che questo metodo può talvolta portare a sistemi finali rappresentati da matrici a scalini del tipo:

$$M' = \begin{pmatrix} 1 & 0 & 2 & 2 & 1 \\ 0 & 0 & 2 & 15 & -18 \\ 0 & 0 & 0 & 0 & 4 \end{pmatrix}.$$

Come si vede, c'è una riga che ha tutti i coefficienti uguali a 0 salvo l'ultimo: (0 0 0 0 4). Questo significa che il sistema non ammette soluzioni, poiché la corrispondente equazione $0x + 0y + 0z + 0t = 4$ non ha soluzioni. Dunque neppure il sistema iniziale, associato ad M , ammette soluzioni.

ESERCIZIO 3.2. Esprimere in generale il contenuto dell'osservazione qui sopra, ossia dimostrare che, dato un sistema con matrice associata M , e chiamata \overline{M} la sottomatrice di M ottenuta togliendo l'ultima colonna (chiamata talvolta la *matrice incompleta associata al sistema*), il sistema ammette soluzione se e solo se il rango di M è uguale al rango di \overline{M} .

Supponiamo ora che per un certo sistema l'insieme delle soluzioni S non sia vuoto: quali ulteriori caratteristiche possiede questo insieme?

Consideriamo un sistema lineare con m equazioni a coefficienti in \mathbb{K} e n incognite x_1, x_2, \dots, x_n , e sia M la matrice associata (tale matrice risulta di formato $m \times (n + 1)$). Innanzitutto è facile dimostrare che, se il sistema lineare è *omogeneo*, ossia se l'ultima colonna della matrice M ha i coefficienti tutti uguali a 0, l'insieme S delle soluzioni non è vuoto (contiene infatti il vettore O) ed è un sottospazio vettoriale di \mathbb{R}^n (vedi l'Esercizio 1.95; un modo conveniente per dimostrare che è un sottospazio è pensare all'insieme delle soluzioni come nucleo dell'applicazione lineare rappresentata dalla matrice \bar{M}). Invece, se il sistema non è omogeneo, si osserva che il vettore O non appartiene a S , dunque S non è un sottospazio vettoriale.

Studiamo prima il caso dei sistemi omogenei: come è possibile capire che dimensione ha il sottospazio S ?

Basta guardare la forma della matrice a scalini M' . Se possiede k scalini (ossia se il rango di M' , che del resto è uguale al rango di M , è uguale a k), allora S ha dimensione $n - k$. Infatti possiamo pensare ad S come al nucleo della applicazione lineare $\phi : \mathbb{K}^n \rightarrow \mathbb{K}^m$ che rispetto alle basi standard è rappresentata dalla matrice \bar{M}' , ossia dalla matrice M' meno l'ultima colonna. Ricordiamo (vedi Teorema 2.46) che il rango di ϕ , cioè la dimensione di $Imm \phi$, è uguale a k . Dunque, per il Teorema 2.21 sappiamo che $dim Ker \phi + dim Imm \phi = n$, ovvero $dim Ker \phi + k = n$ da cui, dato che $Ker \phi = S$, ricaviamo $dim S = n - k$.

OSSERVAZIONE 3.3. In concreto questo significa che, nel risolvere il sistema, ogni scalino lungo lascerà "libere" alcune variabili, come vediamo nel seguente esempio. Supponiamo che un certo sistema omogeneo a coefficienti in \mathbb{R} conduca alla matrice a scalini:

$$M' = \begin{pmatrix} 1 & 0 & 2 & 2 & 0 \\ 0 & 1 & \sqrt{3} & 12 & 0 \\ 0 & 0 & 0 & 6 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Allora il sistema finale associato è

$$\begin{cases} x + 2z + 2t = 0 \\ y + \sqrt{3}z + 12t = 0 \\ 6t = 0 \end{cases}$$

Risolvendolo, otteniamo dall'ultima equazione $t = 0$ e, sostituendo, $y = -\sqrt{3}z$ e $x = -2z$. La variabile z resta "libera" e l'insieme delle soluzioni è

il seguente sottospazio di \mathbb{R}^4 :

$$S = \left\{ \begin{pmatrix} -2z \\ -\sqrt{3}z \\ z \\ 0 \end{pmatrix} \mid z \in \mathbb{R} \right\} = \left\{ z \begin{pmatrix} -2 \\ -\sqrt{3} \\ 1 \\ 0 \end{pmatrix} \mid z \in \mathbb{R} \right\} = \left\langle \begin{pmatrix} -2 \\ -\sqrt{3} \\ 1 \\ 0 \end{pmatrix} \right\rangle$$

Cosa possiamo dire invece di S se il sistema non è omogeneo e ammette soluzioni? Sia M la matrice associata al sistema e sia M_o la matrice che si ricava da M ponendo uguali a 0 tutti i coefficienti dell'ultima colonna. Possiamo pensare M_o come la matrice associata al sistema omogeneo ottenuto dal sistema iniziale ponendo uguali a 0 tutti i membri di destra delle equazioni.

Chiamiamo S_o le soluzioni di questo sistema omogeneo e sia $v = \begin{pmatrix} a_1 \\ a_2 \\ \dots \\ a_n \end{pmatrix}$

un elemento di S .

TEOREMA 3.4. *Con le notazioni introdotte sopra, vale che*

$$S = v + S_o = \{v + w \mid w \in S_o\}$$

ossia le soluzioni del sistema iniziale si ottengono tutte sommando il vettore v alle soluzioni del sistema omogeneo.

DIMOSTRAZIONE. Sia $w = \begin{pmatrix} b_1 \\ b_2 \\ \dots \\ b_n \end{pmatrix} \in S_o$. Vogliamo mostrare che $v +$

$w \in S$. Sia $\gamma_1 x_1 + \gamma_2 x_2 + \dots + \gamma_n x_n = \delta$ una equazione del sistema. Allora b_1, b_2, \dots, b_n verificano

$$\gamma_1 b_1 + \gamma_2 b_2 + \dots + \gamma_n b_n = 0$$

mentre a_1, a_2, \dots, a_n verificano

$$\gamma_1 a_1 + \gamma_2 a_2 + \dots + \gamma_n a_n = \delta$$

Dunque

$$\begin{aligned} & \gamma_1(a_1 + b_1) + \gamma_2(a_2 + b_2) + \dots + \gamma_n(a_n + b_n) = \\ & = (\gamma_1 a_1 + \gamma_2 a_2 + \dots + \gamma_n a_n) + (\gamma_1 b_1 + \gamma_2 b_2 + \dots + \gamma_n b_n) = \delta + 0 = \delta \end{aligned}$$

Ripetendo questa osservazione per tutte le equazioni del sistema, si verifica dunque che $v + w \in S$.

Viceversa, sia $p = \begin{pmatrix} c_1 \\ c_2 \\ \dots \\ c_n \end{pmatrix} \in S$. Vogliamo dimostrare che $p \in v + S_o$.

Osserviamo che c_1, c_2, \dots, c_n verificano

$$\gamma_1 c_1 + \gamma_2 c_2 + \dots + \gamma_n c_n = \delta$$

Dunque

$$\begin{aligned} & \gamma_1(a_1 - c_1) + \gamma_2(a_2 - c_2) + \cdots + \gamma_n(a_n - c_n) = \\ & = (\gamma_1 a_1 + \gamma_2 a_2 + \cdots + \gamma_n a_n) - (\gamma_1 c_1 + \gamma_2 c_2 + \cdots + \gamma_n c_n) = \delta - \delta = 0 \end{aligned}$$

Ripetendo questa osservazione per tutte le equazioni del sistema dimostriamo che $v - p \in S_o$, dunque possiamo scrivere $p - v = w_o$ dove w_o è un certo elemento di S_o . Allora $p = v + w_o$ ossia $p \in v + S_o$. \square

COROLLARIO 3.5. *L'insieme S delle soluzioni di un sistema lineare non omogeneo, a coefficienti in \mathbb{K} , con m equazioni e n incognite, o è vuoto oppure è il traslato di un sottospazio vettoriale di \mathbb{K}^n , ossia è della forma $v + S_o$, dove S_o (l'insieme delle soluzioni del sistema omogeneo associato) è un sottospazio vettoriale di dimensione uguale a $n - (\text{rango di } M_o)$.*

OSSERVAZIONE 3.6. Invitiamo il lettore a considerare la “somiglianza” delle osservazioni su S qui sopra con quanto abbiamo visto nella prima parte del corso a riguardo dell'insieme delle soluzioni di una equazione diofantea lineare: anche in quel caso, se l'equazione diofantea non è omogenea, l'insieme delle soluzioni è dato da un “traslato” dell'insieme delle soluzioni della equazione omogenea associata.

Gli esercizi del prossimo paragrafo permetteranno di mettere in pratica il metodo di Gauss. Il lettore potrà inoltre trovare alla pagina web [**AlgGauss**] un ‘risolutore’ di sistemi lineari, basato sulla riduzione di Gauss, che mostra, a fini didattici, le mosse utilizzate.

2. Altri esercizi

ESERCIZIO 3.7. Discutere la risolubilità, ed eventualmente trovare tutte le soluzioni, del seguente sistema a coefficienti in \mathbb{Z}_5 :

$$(2.1) \quad \begin{cases} x_1 - x_2 + x_3 + x_4 = 1 \\ x_2 - x_4 = 0 \\ x_3 + x_4 = 1 \end{cases}$$

Svolgimento. La matrice completa associata al sistema 2.1 è:

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

che è già in forma a scalini per righe. Gli scalini sono 3, e il sistema è risolubile (il rango della matrice incompleta è 3 e dunque è uguale al rango della matrice completa). L'unica variabile libera è x_4 , quindi troveremo le soluzioni del sistema in funzione di x_4 e avremo 5 soluzioni distinte, una per ogni scelta possibile di x_4 in \mathbb{Z}_5 :

$$\begin{cases} x_1 = x_4 - (1 - x_4) - x_4 + 1 \\ x_2 = x_4 \\ x_3 = 1 - x_4 \end{cases} \longrightarrow \begin{cases} x_1 = x_4 \\ x_2 = x_4 \\ x_3 = 1 - x_4 \end{cases}$$

Le soluzioni del sistema sono dunque i vettori $(x_4, x_4, 1 - x_4, x_4)$ (appartendenti a $(\mathbb{Z}_5)^4$) per ogni scelta di x_4 in \mathbb{Z}_5 : abbiamo dunque cinque soluzioni.

ESERCIZIO 3.8. Discutere la risolubilità, ed eventualmente trovare tutte le soluzioni, del seguente sistema a coefficienti in \mathbb{Z}_7 :

$$(2.2) \quad \begin{cases} x_1 + x_2 - x_3 = 1 \\ x_1 + x_3 = 0 \\ x_1 + x_2 + 6x_3 = 0 \end{cases}$$

Svolgimento. La matrice completa associata al sistema 2.2 è:

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

Portiamola in forma a scalini con operazioni elementari di riga (ribadiamo che la scelta delle operazioni da effettuare non è univoca):

$$A \rightarrow A_1 = \begin{pmatrix} 1 & 1 & -1 & 1 \\ 0 & -1 & 2 & -1 \\ 1 & 1 & -1 & 0 \end{pmatrix} \rightarrow A_2 = \begin{pmatrix} 1 & 1 & -1 & 1 \\ 0 & -1 & 2 & -1 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

Il sistema associato alla matrice A_2 non ha soluzioni, come si vede osservando l'ultima riga, quindi il sistema (2.2) non ha soluzioni.

ESERCIZIO 3.9. Discutere la risolubilità, ed eventualmente trovare tutte le soluzioni, del seguente sistema a coefficienti in \mathbb{Q} :

$$(2.3) \quad \begin{cases} x_1 - 3x_2 + x_3 + 2x_4 = 0 \\ 2x_1 - 6x_2 + x_3 + 5x_4 = 1 \\ 3x_1 - 9x_2 + 2x_3 + 10x_4 = 4 \end{cases}$$

Svolgimento. La matrice completa associata al sistema 2.3 è:

$$A = \begin{pmatrix} 1 & -3 & 1 & 2 & 0 \\ 2 & -6 & 1 & 5 & 1 \\ 3 & -9 & 2 & 10 & 4 \end{pmatrix}$$

Portiamola in forma a scalini per righe:

$$\begin{aligned} A \rightarrow A_1 &= \begin{pmatrix} 1 & -3 & 1 & 2 & 0 \\ 0 & 0 & -1 & 1 & 1 \\ 3 & -9 & 2 & 10 & 4 \end{pmatrix} \\ A_1 \rightarrow A_2 &= \begin{pmatrix} 1 & -3 & 1 & 2 & 0 \\ 0 & 0 & -1 & 1 & 1 \\ 0 & 0 & -1 & 4 & 4 \end{pmatrix} \\ A_2 \rightarrow A_3 &= \begin{pmatrix} 1 & -3 & 1 & 2 & 0 \\ 0 & 0 & -1 & 1 & 1 \\ 0 & 0 & 0 & 3 & 3 \end{pmatrix}. \end{aligned}$$

Il rango della matrice incompleta è tre ed è uguale al rango della matrice completa. Dunque sistema associato ad A_3 è risolubile; osserviamo che ha

come unica variabile libera x_2 . Troviamo l'espressione di queste soluzioni in funzione di x_2 ; scriviamo il sistema corrispondente alla matrice A_3 (che sappiamo essere equivalente a 2.3):

$$\begin{cases} x_1 - 3x_2 + x_3 + 2x_4 = 0 \\ -x_3 + x_4 = 1 \\ +3x_4 = 3 \end{cases} \longrightarrow \begin{cases} x_1 = 3x_2 - 2 \\ x_3 = 0 \\ x_4 = 1 \end{cases}$$

Perciò le soluzioni del sistema (2.3) sono tutti i vettori di \mathbb{Q}^4 del tipo $(3x_2 - 2, x_2, 0, 1)$ al variare di x_2 in \mathbb{Q} .

ESERCIZIO 3.10. Trovare tutte le soluzioni del seguente sistema lineare omogeneo a coefficienti in \mathbb{Z}_{11} :

$$(2.4) \quad \begin{cases} 6x + y + 4z = 0 \\ 7x + 8y + 8z = 0 \\ 10x + y + z = 0 \\ 2x + y + 7z = 0 \end{cases}$$

Svolgimento. Possiamo limitarci a ridurre a scalini la matrice incompleta corrispondente a (2.4) in quanto l'ultima colonna, che ha tutti i coefficienti uguali a 0, rimarrà immutata dopo ogni operazione di riga:

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

Per portare la matrice a scalini in questo caso risolviamo alcune congruenze. Per prima cosa troviamo l'inverso di 7 in \mathbb{Z}_{11} : tale inverso è 8 perché $7 \cdot 8 = 56 \equiv 1 \pmod{11}$. Allora moltiplichiamo la seconda riga per $8 \cdot 6$, di modo che il suo primo coefficiente a sinistra sia uguale a 6, dopodiché sottraiamo la prima riga alla seconda:

$$B \rightarrow B_1 = \begin{pmatrix} 6 & 1 & 4 \\ 0 & 9 & 6 \\ 10 & 1 & 1 \\ 2 & 1 & 7 \end{pmatrix}$$

L'inverso di 10 in \mathbb{Z}_{11} è ovviamente 10 stesso (ossia -1) quindi moltiplichiamo la terza riga per $-1 \cdot 6$ e poi sottraiamo la prima riga alla terza:

$$B_1 \rightarrow B_2 = \begin{pmatrix} 6 & 1 & 4 \\ 0 & 9 & 6 \\ 0 & 4 & 1 \\ 2 & 1 & 7 \end{pmatrix}$$

Altri simili passaggi portano alla seguente forma a scalini:

$$B_3 = \begin{pmatrix} 6 & 1 & 4 \\ 0 & 9 & 6 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

La matrice B_3 ha tre scalini, e il sistema (omogeneo) ad essa associato ha un'unica soluzione che è la soluzione identicamente nulla: $(0, 0, 0)$.

ESERCIZIO 3.11. Discutere la risolubilità del seguente sistema a coefficienti in \mathbb{Z}_{11} in dipendenza del parametro $\lambda \in \mathbb{Z}_{11}$:

$$(2.5) \quad \begin{cases} 3x + 2y - 5z = 6 \\ 5x + (2 + \lambda)y - 2z = 4 \\ 9x + 5y - 3z = 3\lambda \end{cases}$$

Svolgimento. La matrice completa associata al sistema (2.5) è:

$$A = \begin{pmatrix} 3 & 2 & -5 & 6 \\ 5 & 2 + \lambda & -2 & 4 \\ 9 & 5 & -3 & 3\lambda \end{pmatrix}.$$

Portiamola in forma a scalini; potremmo per esempio fare le seguenti mosse:

$$A \rightarrow A_1 = \begin{pmatrix} 3 & 2 & -5 & 6 \\ 0 & 6 + \lambda & -1 & 5 \\ 9 & 5 & -3 & 3\lambda \end{pmatrix}$$

$$A_1 \rightarrow A_2 = \begin{pmatrix} 3 & 2 & -5 & 6 \\ 0 & 6 + \lambda & -1 & 5 \\ 0 & -1 & 1 & 3\lambda - 7 \end{pmatrix}$$

A questo punto conviene scambiare la seconda e la terza riga,

$$A_2 \rightarrow A_3 = \begin{pmatrix} 3 & 2 & -5 & 6 \\ 0 & -1 & 1 & 3\lambda - 7 \\ 0 & 6 + \lambda & -1 & 5 \end{pmatrix}$$

e sommare alla terza riga la seconda moltiplicata per $(6 + \lambda)$:

$$A_3 \rightarrow A_4 = \begin{pmatrix} 3 & 2 & -5 & 6 \\ 0 & -1 & 1 & 3\lambda - 7 \\ 0 & 0 & 5 + \lambda & (3\lambda - 7) \cdot (6 + \lambda) + 5 \end{pmatrix}.$$

La matrice trovata è a scalini qualunque sia λ , ma dobbiamo capire esattamente quali sono i suoi pivots. Se $5 + \lambda \neq 0$ allora il sistema ha una e una sola soluzione.

Se invece $5 + \lambda = 0$ (ossia se $\lambda = -5 = 6$), abbiamo:

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

Quindi se $\lambda = 6$ il sistema (2.5) non ha soluzioni.

ESERCIZIO 3.12. Consideriamo il seguente sistema a coefficienti in \mathbb{Z}_p :

$$(2.6) \quad \begin{cases} x + 5y - 6z = 0 \\ 2x - 8y - 14z = 12 \\ -x + 7y + 10z = 0 \end{cases}$$

Discutere al variare di p tra i numeri primi la risolubilità del sistema (2.6)

Svolgimento. La matrice completa associata al sistema 2.6 è la seguente:

$$A = \begin{pmatrix} 1 & 5 & -6 & 0 \\ 2 & -8 & -14 & 12 \\ -1 & 7 & 10 & 0 \end{pmatrix}$$

Cerchiamo di portarla in forma a scalini. Le prime due mosse possono essere fatte qualunque sia p :

$$A \rightarrow A_1 = \begin{pmatrix} 1 & 5 & -6 & 0 \\ 0 & -18 & -2 & 12 \\ -1 & 7 & 10 & 0 \end{pmatrix}$$

$$A_1 \rightarrow A_2 = \begin{pmatrix} 1 & 5 & -6 & 0 \\ 0 & -18 & -2 & 12 \\ 0 & 12 & 4 & 0 \end{pmatrix}.$$

Ora vorremmo moltiplicare la terza riga per 3 e sommarle la seconda riga moltiplicata per 2. Possiamo farlo, purché il campo in questione non sia \mathbb{Z}_3 (altrimenti staremmo moltiplicando la terza riga per 0, mossa non ammissibile). Quindi tratteremo a parte il caso \mathbb{Z}_3 . Per tutti i $p \neq 3$ possiamo tranquillamente fare la mossa descritta e si ottiene:

$$A_2 \rightarrow A_3 = \begin{pmatrix} 1 & 5 & -6 & 0 \\ 0 & -18 & -2 & 12 \\ 0 & 0 & 8 & 24 \end{pmatrix}$$

Ora, se p non divide coefficienti -18 o 8 , la matrice è in forma a scalini e ha tre scalini. Si può quindi dire che se $p \neq 2$ e $p \neq 3$ allora il sistema (2.6) ha una e una sola soluzione.

Se $p = 2$ la matrice A_3 ridotta modulo 2 diventa:

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

Quindi il sistema (2.6) ha due variabili libere e dunque 4 soluzioni in $(\mathbb{Z}_2)^3$, una per ogni scelta possibile della coppia di variabili libere (y, z) . Ci resta da trattare il caso $p = 3$; torniamo alla matrice A_2 , ovvero prima della sostituzione lineare che in \mathbb{Z}_3 non potevamo effettuare. Riducendo tale matrice modulo 3, si trova

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

che può essere portata nella seguente forma a scalini:

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

Quindi il sistema (2.6) in $(\mathbb{Z}_3)^3$ ha una variabile libera e dunque 3 soluzioni, una per ogni possibile scelta della variabile libera z .

ESERCIZIO 3.13. Determinare per quale valori del parametro reale t il sistema lineare (2.7) nelle variabili x, y, z a coefficienti in \mathbb{R} è risolubile e trovarne le soluzioni:

$$(2.7) \quad \begin{cases} x + y + tz = 1 \\ x + z = 0 \\ x + y + t^3z = 3 \\ x + y + z = 0 \end{cases}$$

Svolgimento La matrice completa associata al sistema è A :

$$A = \begin{pmatrix} 1 & 1 & t & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & t^3 & 3 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

Riduciamola in forma a scalini. Notazione: useremo la notazione di scrivere tra parentesi quadra le righe. Per esempio $[2]=[1]-3[2]$ significherà che sostituiamo al posto della seconda riga, la prima riga meno tre volte la seconda.

$$A \xrightarrow{[2]=[4]-[2]} A_1 = \begin{pmatrix} 1 & 1 & t & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & t^3 & 3 \\ 1 & 1 & 1 & 0 \end{pmatrix} \xrightarrow{[3]=[3]-[4]} A_2 = \begin{pmatrix} 1 & 1 & t & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & t^3 - 1 & 3 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

$$A_2 \xrightarrow{[4]=[1]-[4]} A_3 = \begin{pmatrix} 1 & 1 & t & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & t^3 - 1 & 3 \\ 0 & 0 & t - 1 & 1 \end{pmatrix}$$

A questo punto osserviamo che $t^3 - 1 = (t - 1)(t^2 + t + 1)$ e che $t^2 + t + 1$ è diverso da zero per qualsiasi valore di $t \in \mathbb{R}$. Dunque è la mossa che consiste nel moltiplicare la quarta riga per $-(t^2 + t + 1)$ è lecita e poi, come mossa successiva, possiamo sommare alla quarta riga la terza riga. Il risultato di queste due mosse può essere sintetizzato come $[4] = [3] - (t^2 + t + 1)[4]$:

$$A_3 \xrightarrow{[4]=[3]-(t^2+t+1)[4]} A_4 = \begin{pmatrix} 1 & 1 & t & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & t^3 - 1 & 3 \\ 0 & 0 & 0 & 2 - t^2 - t \end{pmatrix}$$

Il sistema (2.7) è dunque equivalente al sistema (2.8):

$$(2.8) \quad \begin{cases} x + y + tz = 1 \\ y = 0 \\ (t^3 - 1)z = 3 \\ 0 = 2 - t^2 - t \end{cases}$$

Per essere risolubile deve essere dunque $2 - t^2 - t = 0$, ovvero:

$$t = \frac{-1 \pm \sqrt{1+8}}{2} = \begin{cases} 1 \\ -2 \end{cases}$$

Il sistema (2.7) può avere soluzioni solo per $t = 1$ o $t = -2$. Nel caso $t = 1$ però, sostituendo nel sistema (2.8), si ha che la terza equazione è $0 = 3$ e dunque anche per questo valore il sistema non ha soluzioni.

Rimane il caso $t = -2$. Sostituendo nel sistema (2.8) si ottiene:

$$\begin{cases} x - 2z = 1 \\ y = 0 \\ -9z = 3 \\ 0 = 0 \end{cases}$$

che ha una unica soluzione:

$$\begin{cases} x = \frac{1}{3} \\ y = 0 \\ z = -\frac{1}{3} \end{cases}$$

Concludendo il sistema (2.7) ammette soluzioni solo nel caso $t = 2$. Per questo valore di t la soluzione del sistema è unica.

ESERCIZIO 3.14. Trovare tutte le soluzioni in \mathbb{Q}^4 del seguente sistema lineare:

$$(2.9) \quad \begin{cases} x_1 - 3x_2 + x_3 + 2x_4 = 0 \\ 2x_1 - 6x_2 + x_3 + 5x_4 = 1 \\ 3x_1 - 9x_2 + 2x_3 + 10x_4 = 4 \end{cases}$$

Svolgimento La matrice dei coefficienti associata al sistema (2.10) è:

$$B = \begin{pmatrix} 1 & -3 & 1 & 2 & 0 \\ 2 & -6 & 1 & 5 & 1 \\ 3 & -9 & 2 & 10 & 4 \end{pmatrix}$$

Lavoriamo con sostituzioni di riga per trovare una matrice a scalini associata ad un sistema equivalente (ovvero con lo stesso insieme di soluzioni) al sistema 2.10:

$$B \xrightarrow{[2]=[2]-2[1]} B_1 = \begin{pmatrix} 1 & -3 & 1 & 2 & 0 \\ 0 & 0 & -1 & 1 & 1 \\ 3 & -9 & 2 & 10 & 4 \end{pmatrix} \xrightarrow{[3]=[3]-3[1]} B_2 = \begin{pmatrix} 1 & -3 & 1 & 2 & 0 \\ 0 & 0 & -1 & 1 & 1 \\ 0 & 0 & -1 & 4 & 4 \end{pmatrix}$$

$$B_2 \xrightarrow{[3]=[3]-[2]} B_3 = \begin{pmatrix} 1 & -3 & 1 & 2 & 0 \\ 0 & 0 & -1 & 1 & 1 \\ 0 & 0 & 0 & 3 & 3 \end{pmatrix}$$

La matrice B_3 è a scalini e il sistema corrispondente ad essa, equivalente al sistema (2.9), è il seguente:

$$(2.10) \quad \begin{cases} x_1 - 3x_2 + x_3 + 2x_4 = 0 \\ -x_3 + x_4 = 1 \\ 3x_4 = 3 \end{cases}$$

Il sistema (2.10) ha una variabile libera (che è x_2). Dunque al variare del valore di x_2 in \mathbb{Q} , si ha che le soluzioni del sistema (2.10) sono gli elementi di \mathbb{Q}^4 del tipo: $(3x_2 - 2, x_2, 0, 1)$.

ESERCIZIO 3.15. Determinare un polinomio $g(x) \in \mathbb{Q}[x]$ tale che:

$$g(1) = 10 \quad g(-1) = 2 \quad g(-2) = 1$$

Svolgimento Scegliendo un grado per il polinomio $g(x)$ e imponendo le condizioni richieste, l'esercizio si traduce nel risolvere un sistema lineare per determinare i valori dei coefficienti di $g(x)$.

- Un polinomio di grado 0 è una costante e dunque non c'è speranza di trovare $g(x)$ di grado 0 che, valutato su tre valori diversi di x , assuma tre valori distinti.
- Proviamo a vedere se esiste un polinomio di primo grado con i valori richiesti. Poniamo dunque $g(x) = ax + b$ con $a, b \in \mathbb{Q}$. Le condizioni richieste equivalgono al seguente sistema in \mathbb{Q}^2 :

$$\begin{cases} a + b = 10 \\ -a + b = 2 \\ -2a + b = 1 \end{cases}$$

La matrice dei coefficienti associata al sistema è:

$$A = \begin{pmatrix} 1 & 1 & 10 \\ -1 & 1 & 2 \\ -2 & 1 & 1 \end{pmatrix}$$

Portiamola a scalini:

$$A \xrightarrow[\substack{[2]=[1]+[2] \\ [3]=2[1]+[3]}]{\substack{[3]=[3]-\frac{3}{2}[2]}} A_1 = \begin{pmatrix} 1 & 1 & 10 \\ 0 & 2 & 12 \\ 0 & 3 & 21 \end{pmatrix} \xrightarrow{\substack{[3]=[3]-\frac{3}{2}[2]}} A_2 = \begin{pmatrix} 1 & 1 & 10 \\ 0 & 2 & 12 \\ 0 & 0 & 3 \end{pmatrix}$$

Il sistema dunque risulta non risolubile in quanto equivalente al seguente sistema:

$$\begin{cases} a + b = 10 \\ 2b = 12 \\ 0 = 3 \end{cases}$$

Questo significa che non esistono polinomi $g(x)$ di grado 1 con la proprietà richiesta di assumere i valori 10, 2 e 1 rispettivamente in 1, -1 e -2.

- Proviamo con $g(x)$ di secondo grado. Poniamo dunque $g(x) = ax^2 + bx + c$ e imponiamo le condizioni richieste ottenendo il sistema in \mathbb{Q}^3 seguente:

$$\begin{cases} a + b + c = 10 \\ a - b + c = 2 \\ 4a - 2b + c = 1 \end{cases}$$

La matrice dei coefficienti associata al sistema è:

$$A = \begin{pmatrix} 1 & 1 & 1 & 10 \\ 1 & -1 & 1 & 2 \\ 4 & -2 & 1 & 1 \end{pmatrix}$$

Portiamola a scalini:

$$A \xrightarrow{\substack{[2]=[1]-[2] \\ [3]=4[1]-[3]}} A_1 = \begin{pmatrix} 1 & 1 & 1 & 10 \\ 0 & 2 & 0 & 8 \\ 0 & 6 & 3 & 39 \end{pmatrix} \xrightarrow{[3]=[3]-3[2]} A_2 = \begin{pmatrix} 1 & 1 & 1 & 10 \\ 0 & 2 & 0 & 8 \\ 0 & 0 & 3 & 15 \end{pmatrix}$$

Questa matrice ha rango massimo e uguale a 3 (come il numero delle variabili) e dunque il sistema corrispondente ha una unica soluzione:

$$\begin{cases} a + b + c = 10 \\ 2b = 8 \\ 3c = 15 \end{cases} \longrightarrow \begin{cases} a = 1 \\ b = 4 \\ c = 5 \end{cases}$$

L'unico polinomio di secondo grado con la proprietà richiesta è dunque $g(x) = x^2 + 4x + 5$.

Generalizzando quanto visto finora (e pensando il tutto in \mathbb{R} invece che in \mathbb{Q}) si potrebbero dimostrare (o comunque ripensare in termini di algebra lineare) alcuni risultati di geometria analitica: la condizione richiesta equivale al fatto che il grafico della funzione $g(x)$ passi per i tre punti del piano $(1, 10)$, $(-1, 2)$, $(-2, 1)$.

Ora il grafico del polinomio di primo grado $ax+b$ corrisponde ad una generica retta del piano, dunque l'unica speranza che passi per tre punti è che questi siano allineati.

Il grafico del polinomio di secondo grado $ax^2 + bx + c$ corrisponde ad una generica parabola del piano. Abbiamo dimostrato che esiste una e una sola parabola del piano passante per i tre punti richiesti. Generalizzando si potrebbe dimostrare che, scelti tre punti non allineati, esiste una e una sola parabola del piano passante per i tre punti.

ESERCIZIO 3.16. Trovare tutte le soluzioni del sistema a coefficienti in \mathbb{R} :

$$\begin{cases} 2x + 2y + z + 2t = 0 \\ 2y + 3z - t = -5 \\ +y - z - t = 0 \end{cases}$$

ESERCIZIO 3.17. Trovare tutte le soluzioni del sistema a coefficienti in \mathbb{R} :

$$\begin{cases} 2x + y + z + t + w = 1 \\ 2y + 3z - t + 2w = 0 \\ 2x + y - z - t + w = 0 \\ x + y + 3z + t + w = 0 \end{cases}$$

ESERCIZIO 3.18. Trovare tutte le soluzioni del sistema a coefficienti in \mathbb{R} :

$$\begin{cases} x + 2y + z + 2t + w = 0 \\ 2y + 3z - t + 2w = 0 \\ y - z - t + w = 0 \\ 4x + y + 3z + t + w = 0 \end{cases}$$

ESERCIZIO 3.19. Consideriamo il sistema lineare a coefficienti in \mathbb{R} :

$$\begin{cases} 2x + y + mz = 1 \\ 2y + mz = 0 \\ x + my + 2z = 1 \end{cases}$$

Stabilire per quali valori del parametro reale m il seguente sistema ammette soluzioni e, per tali valori, calcolare le soluzioni.

ESERCIZIO 3.20. Consideriamo il sistema lineare a coefficienti in \mathbb{R} :

$$\begin{cases} 2x + 2y + (k - 3)z = -2 \\ x + (k - 2)y - (k + 1)z = -3 \\ x + 2y + kz = 1 \end{cases}$$

Stabilire per quali valori del parametro reale k il seguente sistema ammette soluzioni e, per tali valori, calcolare le soluzioni.

ESERCIZIO 3.21. Si consideri l'applicazione lineare $A_t : \mathbb{R}^4 \rightarrow \mathbb{R}^3$ a cui, rispetto alle basi standard, è associata la seguente matrice:

$$[A_t] = \begin{pmatrix} 1 & 1 & 2 & 1 \\ 1 & 1 & 2 & 0 \\ t & t^3 & 1+t & 1 \end{pmatrix}.$$

Trovare, se esistono, valori del parametro t per i quali si ha che $\dim \text{Ker } A_t = 2$ ed esibire, in tal caso, una base di $\text{Ker } A_t$.

Svolgimento. Dal Teorema 2.21 segue che il nucleo di A_t ha dimensione 2 se e solo se la dimensione dell'immagine di A_t è uguale a 2, in altre parole se e solo se il rango di A_t è 2. Come sappiamo, il rango si può calcolare riducendo la matrice $[A_t]$ in forma a scalini. Lo si può fare con operazioni elementari di riga, oppure con operazioni elementari di colonna, oppure, se ci interessa esclusivamente il rango, si possono usare sequenze “miste” di operazioni elementari per riga e per colonna.

In questo caso è vero che in prima battuta ci interessa il rango, ma l'esercizio chiede anche di esibire una base del nucleo di A_t per certi valori

di t , dunque di risolvere un sistema lineare. In previsione di questo, ci conviene utilizzare le mosse di riga, le uniche che non cambiano le soluzioni del sistema lineare.

Facciamo una rapida analisi della matrice in questione: le due prime righe sono sicuramente linearmente indipendenti, perciò il numero di scalini che otterremo è almeno 2 e al massimo sarà 3 (ci sono solo tre righe).

Portiamo A_t in forma a scalini

$$\begin{pmatrix} 1 & 1 & 2 & 1 \\ 1 & 1 & 2 & 0 \\ t & t^3 & 1+t & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 1 & 2 & 1 \\ 0 & 0 & 0 & -1 \\ t & t^3 & 1+t & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 1 & 2 & 1 \\ 0 & 0 & 0 & -1 \\ 0 & t^3-t & 1-t & 1-t \end{pmatrix}$$

A questo punto affinché la matrice abbia rango 2 è necessario che l'ultima riga non abbia coefficienti non nulli prima della quarta colonna, ovvero che:

$$t^3 - t = 1 - t = 0$$

e ciò accade solo per $t = 1$. Si ha quindi che A_1 è l'unica applicazione del tipo considerato che ha il nucleo di dimensione 2. Per individuare $\text{Ker } A_1$ dobbiamo risolvere il sistema omogeneo:

$$[A_1] \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Tale sistema, come sappiamo, equivale a quello con matrice a scalini per righe:

$$\begin{pmatrix} 1 & 1 & 2 & 1 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

Quindi dobbiamo risolvere il sistema trovando le variabili x e t in funzione delle variabili libere y e z :

$$\begin{cases} x + y + 2z + t = 0 \\ -t = 0 \\ 0 = 0 \end{cases}$$

Troviamo $t = 0$ e $x = -y - 2z$, quindi un generico vettore di $\text{Ker } A_1$ è della forma:

$$\begin{pmatrix} -y - 2z \\ y \\ z \\ 0 \end{pmatrix} = \begin{pmatrix} -1 \\ 1 \\ 0 \\ 0 \end{pmatrix} \cdot y + \begin{pmatrix} -2 \\ 0 \\ 1 \\ 0 \end{pmatrix} \cdot z$$

Si osserva immediatamente che i due vettori:

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

sono un insieme di generatori linearmente indipendenti (quindi una base) di $\text{Ker } A_1$.

ESERCIZIO 3.22. Sia $g : \mathbb{Q}^3 \rightarrow \mathbb{Q}^2$ definita da:

$$g(x, y, z) = (2x + y + 2z, x + y + 3z).$$

Trovare una base di $\text{Imm } g$ e di $\text{Ker } g$.

Svolgimento. La matrice associata a g nelle basi canoniche di \mathbb{Q}^3 e \mathbb{Q}^2 è:

$$[g] = \begin{pmatrix} 2 & 1 & 2 \\ 1 & 1 & 3 \end{pmatrix}$$

Portiamola in forma a scalini con operazioni di riga:

$$[g] \rightarrow \begin{pmatrix} 2 & 1 & 2 \\ 0 & 1 & 4 \end{pmatrix}$$

Gli elementi di $\text{Ker } g$ sono le soluzioni del sistema:

$$\begin{cases} 2x + y + 2z = 0 \\ y + 4z = 0 \end{cases}$$

Lo risolviamo in funzione della variabile libera z , quindi: $y = -4z$ e $x = z$. Perciò un generico elemento di $\text{Ker } g$ è della forma:

$$\begin{pmatrix} z \\ -4z \\ z \end{pmatrix} = z \begin{pmatrix} 1 \\ -4 \\ 1 \end{pmatrix}$$

Dunque $\text{Ker } g$ ha dimensione 1 e una sua base è data dal vettore:

$$\begin{pmatrix} 1 \\ -4 \\ 1 \end{pmatrix}.$$

Per il Teorema 2.21 sappiamo a questo punto che $\text{Imm } g$ ha dimensione 2. Per esibire una base di $\text{Imm } g$ basta allora scegliere due colonne linearmente indipendenti nella matrice

$$[g] = \begin{pmatrix} 2 & 1 & 2 \\ 1 & 1 & 3 \end{pmatrix}$$

Le prime due colonne, come si verifica immediatamente, sono linearmente indipendenti, dunque i vettori

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

costituiscono una base di $\text{Imm } g$.

3. Come funziona Google

NOTA: Questo paragrafo è ricavato da una delle schede di una serie intitolata “Modelli e Realtà”, a cura di A. Abbondandolo e G. Gaiffi.

Le schede sono in forma di dialogo fra due personaggi, Ilaria e Orazio.

Orazio ha appena messo in rete la sua prima pagina web, che raccoglie gli appunti su alcuni dei problemi matematici che ha affrontato insieme a Ilaria. Però non è soddisfatto.

O - Niente da fare: Google non ci trova. La nostra pagina è invisibile a chi non conosca già l'indirizzo esatto.

I - Abbi un po' di pazienza. Google ci mette un po' ad accorgersi della presenza di nuove pagine. È vero che dispone di un intero esercito di computer, che giorno e notte navigano per la rete e indicizzano tutti i documenti che trovano, ma si tratta pur sempre di parecchi miliardi di documenti. Riproverei a fare una nuova ricerca tra qualche settimana.

O - E basterà cercare “Ilaria e Orazio” per far saltare fuori la nostra pagina?

I - Su questo non sarei troppo ottimista. In rete ci saranno migliaia di documenti che contengono i nostri nomi. Dipenderà da quanta rilevanza Google attribuirà alla nostra pagina: se sarà considerata rilevante, apparirà tra le prime risposte, altrimenti finirà in fondo ad una lista lunghissima, che nessuno avrà voglia di leggere.

O - E come fa Google a decidere quanto rilevante è la nostra pagina web? Si vanno a leggere tutto quello che scriviamo?

I - No, lo fa in modo automatico, basandosi sul numero e sulla rilevanza delle altre pagine che contengono un link alla nostra. Utilizza un algoritmo che si chiama “PageRank”. Vuoi che ti spieghi come funziona?

O - Certo.

I - Immaginati un navigatore indeciso, che non sa bene quello che cerca. Parte da una pagina a caso, guarda tutti i link che questa contiene, ne sceglie uno a caso, lo segue e fa lo stesso con la nuova pagina raggiunta. E avanti così, all'infinito. Supponiamo di aver numerato tutte le pagine della rete con numeri da 1 a N e chiamiamo r_j la probabilità che ad un dato istante il navigatore indeciso si trovi sulla j -esima pagina. Il valore r_j può essere interpretato come una misura della rilevanza della pagina j -esima.

O - Sí, capisco perché: nel suo girovagare, il navigatore indeciso si troverà più spesso sulle pagine molto popolari, quelle a cui puntano numerosi link, mentre visiterà molto raramente le pagine poco segnalate. Ma la quantità r_j non dovrebbe essere funzione del tempo?

I - All'inizio della navigazione sì, ma è ragionevole supporre che dopo un po' queste probabilità si avvicinino a dei valori indipendenti dal tempo. Possiamo anche scrivere una relazione tra le varie r_j . Chiamiamo ℓ_j il numero dei link presenti nella j -esima pagina e A_i il sottoinsieme di $\{1, \dots, N\}$ che corrisponde alle pagine che puntano verso la i -esima. Affinché ad un dato

istante il navigatore si trovi sulla i -esima pagina, è necessario che all'istante precedente si trovasse in una delle pagine dell'insieme A_i . Se j è una delle pagine di questo insieme, la probabilità che all'istante precedente il navigatore fosse su j vale r_j e, in questi caso, la probabilità che segua il link che lo porta ad i è $1/\ell_j$. Quindi la probabilità r_i è data dalla somma su tutti gli elementi j di A_i di r_j moltiplicato per $1/\ell_j$. In una formula:

$$(3.1) \quad r_i = \sum_{j \in A_i} \frac{r_j}{\ell_j}, \quad \forall i \in \{1, \dots, N\}.$$

O - Non sono sicuro di aver capito. Sai che la probabilità non è il mio forte...

I - Puoi anche prescindere dal modello probabilistico del navigatore indeciso e considerare la formula che ho scritto come una definizione della rilevanza di una pagina: la rilevanza r_i della pagina i -esima è pari alla somma dei quozienti tra la rilevanza r_j di ciascuna delle pagine che ad essa puntano per il numero dei link ℓ_j di tale pagina. È come se ciascuna pagina trasmettesse una porzione della propria rilevanza alle pagine verso le quali punta. Quindi la rilevanza di una pagina non dipende solamente dal numero dei link che ad essa puntano, ma anche e soprattutto dalla rilevanza delle pagine che contengono questi link. È molto ragionevole che essere citati da una pagina molto visitata sia considerato più rilevante che essere citati da dieci pagine che non legge nessuno.

O - Ma la formula che hai scritto non è una definizione! Per sapere quanto vale r_i hai bisogno di conoscere il valore delle altre r_j : è un gatto che si morde la coda.

I - Hai ragione, ma più precisamente la (3.1) è un sistema di N equazioni lineari (una per ciascuna i) in N incognite (le r_1, \dots, r_N).

O - È vero! Anzi, si tratta di un sistema lineare omogeneo. Come tale ha sempre la soluzione banale $r_1 = r_2 = \dots = r_N = 0$. Se le righe della matrice quadrata associata sono linearmente indipendenti, ossia se la matrice ha rango uguale a N , questa è l'unica soluzione. Altrimenti, se le righe non sono linearmente indipendenti, ve ne sono infinite. Infatti in questo caso riducendo la matrice a scalini per righe si trovano delle righe uguali a 0 e degli scalini "lunghi".

I - Proprio così. La soluzione banale ovviamente non ci interessa. Vorremmo che ci fosse una soluzione non banale che, fedeli al modello probabilistico, possiamo normalizzare in modo che la somma di tutte le r_i valga 1.

O - Ma non è detto che questa soluzione ci sia! Considera questo esempio semplicissimo: una rete composta da due sole pagine, in cui la prima contiene un link alla seconda, che invece non possiede link:



In questo caso, il tuo sistema lineare è

$$\begin{cases} r_1 = 0 \\ r_2 = r_1, \end{cases}$$

che ha soltanto la soluzione $r_1 = r_2 = 0$.

I - Hai di nuovo ragione, ho dimenticato di introdurre una piccola modifica. Nel tuo esempio il problema è causato dalla seconda pagina, che non possiede link. Ripensa al navigatore indeciso: come prosegue se va a cadere in una pagina senza link? Dobbiamo aggiungere una regola che dica cosa fare in questo caso. La più semplice è questa: da una pagina senza link si va in una qualunque delle N pagine della rete con probabilità $1/N$. Se V è il sottoinsieme di $\{1, \dots, N\}$ che corrisponde alle pagine prive di link, la formula corretta è la seguente:

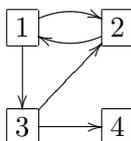
$$(3.2) \quad r_i = \sum_{j \in A_i} \frac{r_j}{\ell_j} + \frac{1}{N} \sum_{j \in V} r_j.$$

È come se si decidesse d'ufficio che le pagine senza link puntano a tutte le pagine della rete: una tale pagina trasmette una piccolissima parte della sua rilevanza ($1/N$ è un numero piccolissimo) a tutte le altre (inclusa sé stessa). Dopo questa correzione, il tuo esempio produce il sistema

$$\begin{cases} r_1 = r_2/2 \\ r_2 = r_1 + r_2/2, \end{cases}$$

che ha per soluzione generale $r_1 = s$, $r_2 = 2s$, al variare di s tra tutti i numeri reali. Imponendo la condizione di normalizzazione $r_1 + r_2 = 1$, si trova $r_1 = 1/3$ e $r_2 = 2/3$.

O - Sì, mi sembra ragionevole che la seconda pagina sia il doppio più rilevante della prima. Fammi provare con un altro esempio:



Questa volta il sistema è:

$$\begin{cases} r_1 = r_2 + r_4/4 \\ r_2 = r_1/2 + r_3/2 + r_4/4 \\ r_3 = r_1/2 + r_4/4 \\ r_4 = r_3/2 + r_4/4. \end{cases}$$

Provo a risolverlo... Ecco, la soluzione generale è

$$r_1 = 10s, \quad r_2 = 9s, \quad r_3 = 6s, \quad r_4 = 4s,$$

e normalizzando trovo

$$r_1 = 10/29, \quad r_2 = 9/29, \quad r_3 = 6/29, \quad r_4 = 4/29.$$

La quarta pagina è ovviamente la meno rilevante. Le prime due sono le più rilevanti, ma la prima lo è leggermente di più poiché beneficia per intero

della rilevanza della seconda, la quale a sua volta riceve solamente metà della rilevanza della prima. In questo esempio ho trovato una soluzione non banale, ma sei sicura che il sistema (3.2) ne abbia sempre?

I - Sì, e te lo posso dimostrare facilmente. Cerchiamo di riscrivere il sistema (3.2) utilizzando il linguaggio dei vettori e delle matrici. Se chiamiamo r il vettore (r_1, \dots, r_N) , possiamo riscrivere (3.2) come

$$(3.3) \quad r = Wr,$$

dove W è la matrice $N \times N$ in cui alla riga i -esima e alla colonna j -esima compare $1/\ell_j$ se la pagina j contiene un link verso la pagina i , $1/N$ se la pagina j non possiede link, e 0 se la pagina j contiene link che però non puntano verso la pagina i :

$$W_{i,j} = \begin{cases} 1/\ell_j & \text{se } j \in A_i, \\ 1/N & \text{se } j \in V, \\ 0 & \text{altrimenti.} \end{cases}$$

Nota che i coefficienti di questa matrice sono tutti numeri non negativi e che la somma dei coefficienti di ciascuna colonna vale 1. Le matrici con questa proprietà si chiamano “stocastiche”.

O - Fammi capire perchè vale l'ultima proprietà che hai detto... Guardare una colonna significa fissare j e far variare i da 1 a N . Se la pagina j possiede link, allora sulla colonna j -esima trovo $1/\ell_j$ per ognuna delle ℓ_j pagine i a cui punta la pagina j , e tutti gli altri coefficienti sono zero: totale 1. Se invece la pagina j non possiede link, tutti i coefficienti della colonna j -esima valgono $1/N$: di nuovo, la somma è 1.

I - Esatto, mentre invece se avessi scritto allo stesso modo il sistema (3.1), avrei avuto delle colonne con coefficienti tutti uguali a 0 e la matrice W non sarebbe stata stocastica. Come hai giustamente osservato, l'equazione (3.3) rappresenta un sistema lineare omogeneo. Posso riscriverlo come

$$(I - W)r = 0,$$

dove I è la matrice identità, ossia la matrice $N \times N$ che ha 1 sulla diagonale e 0 fuori da essa. Scritto in questa forma, vediamo che (3.3) ha soluzioni non banali se e solamente se l'applicazione lineare rappresentata da $I - W$ ha nucleo non banale, ovvero se e solo se $I - W$ ha rango strettamente minore di N . Affermo che il fatto che W sia stocastica implica che il rango di $I - W$ sia $< N$.

O - Forse ci sono! La somma dei coefficienti di ciascuna colonna di $I - W$ vale 0 (c'è esattamente un 1 che viene dalla matrice identità, a cui devo togliere la somma dei coefficienti della corrispondente colonna della matrice stocastica W). Ma questo è come dire che la somma degli N vettori riga che compongono la matrice $I - W$ è il vettore nullo. In particolare, le righe di $I - W$ sono linearmente dipendenti e sappiamo che questo implica che il rango di $I - W$ è $< N$.

I - Proprio così. Quindi l'equazione (3.3), o equivalentemente il sistema (3.2), ha sempre soluzioni non banali.

O - Però se vogliamo che la (3.3) ci dia una buona definizione della rilevanza di tutte le pagine della rete, abbiamo anche bisogno che la soluzione non banale sia unica, una volta normalizzata in modo che la somma degli r_i valga 1...

I - Hai ragione. In effetti occorre apportare un'ultima modifica per avere l'unicità. Nota infatti che se la rete consiste di due sotto-reti non collegate tra loro da alcun link, non possiamo aspettarci che la soluzione sia unica.

O - È vero. In questo caso posso costruire due soluzioni linearmente indipendenti dell'equazione (3.3) in questo modo: risolvo l'equazione relativa ad una delle due sotto-reti e la estendo ad una soluzione globale ponendo la rilevanza di ciascuna pagina dell'altra sotto-rete uguale a zero.

I - Infatti l'idea della modifica che garantisce l'unicità è proprio quella di eliminare eventuali sotto-reti isolate. Si fa così: fissiamo un parametro ϵ compreso tra 0 e 1 e definiamo

$$(3.4) \quad G = (1 - \epsilon)W + \epsilon Q,$$

dove Q è la matrice $N \times N$ che ha tutti i coefficienti uguali a $1/N$. La matrice G è ancora stocastica, ma adesso tutti i suoi coefficienti sono positivi. Si può dimostrare che questo garantisce che l'equazione

$$(3.5) \quad r = Gr$$

possiede un'unica soluzione r tale che $\sum_i r_i = 1$. L'interpretazione probabilistica dietro a questa modifica è la seguente: a ciascun passo, il navigatore indeciso segue le regole che abbiamo descritto prima - e che sono riassunte dalla matrice W - con probabilità $1 - \epsilon$, mentre con probabilità ϵ si sposta su una pagina a caso.

O - E immagino che ϵ debba essere scelto piccolo, in modo da non modificare troppo la struttura effettiva delle rete.

I - Esatto, ma non troppo piccolo, perché il termine ϵQ risulta anche utile per calcolare effettivamente la soluzione r dell'equazione (3.5).

O - Già. Avevamo tralasciato completamente questo aspetto: i computer di Google devono risolvere un sistema lineare composto da qualche miliardo di equazioni. Come ci riescono?

I - In realtà si accontentano di una soluzione approssimata. Partono da un qualsiasi vettore con coefficienti positivi aventi somma 1, ad esempio $r(0) = (1/N, \dots, 1/N)$. Gli applicano la matrice G , ottenendo il vettore $r(1) = Gr(0)$. Poi iterano il procedimento, determinando i vettori $r(2) = Gr(1)$, $r(3) = Gr(2)$, eccetera. Si può dimostrare che il fatto che la matrice stocastica G abbia tutti i coefficienti positivi implica che la successione di vettori $r(n)$ si avvicina sempre di più alla soluzione normalizzata dell'equazione (3.5). La convergenza è tanto più rapida quanto più grande è ϵ . Penso che Google scelga $\epsilon = 0,15$ ed ottenga una soluzione approssimata soddisfacente fermandosi dopo qualche decina di iterazioni. La rilevanza delle pagine della rete viene aggiornata a scadenze regolari ed il calcolo dura qualche giorno.

O - Fammi ricapitolare. I computer di Google esplorano in continuazione la rete. Le parole di ciascun documento vengono memorizzate in un database, mentre le informazioni sulla struttura della rete, ossia quali pagine contengano link a quali altre, vengono memorizzate nella matrice W . Il database serve per decidere quali documenti riportare in risposta alle varie ricerche. La matrice W è utilizzata invece per determinare una classifica assoluta di tutte le pagine, che vengono ordinate per rilevanza determinando una soluzione approssimata dell'equazione (3.5), dove la matrice G è ottenuta dalla W grazie alla formula (3.4). La rilevanza determina a sua volta l'ordine in cui Google fornisce le risposte ad una determinata ricerca.

I - Esatto. Quindi se vogliamo fare in modo che la nostra pagina abbia una rilevanza alta, dobbiamo convincere i gestori di qualche sito già rilevante - ad esempio qualche sito istituzionale sull'istruzione, o sulla divulgazione matematica - ad includerla tra i loro link.

La formula di Grassmann

1. La formula di Grassmann per le intersezioni e le somme di sottospazi.

Dati due sottospazi vettoriali A e B in \mathbb{R}^3 di dimensione 2 (dunque due piani contenenti O), di che dimensione può essere la loro intersezione?

Possono intersecarsi lungo una retta: in tal caso si nota che il sottospazio generato dai vettori di $A \cup B$, ossia $A + B$ (vedi Definizione 1.37), è tutto \mathbb{R}^3 .

Oppure vale $A = B$: allora la loro intersezione è uguale ad A (e a B) e ha dimensione 2, e anche il sottospazio $A + B$ coincide con A .

In entrambi i casi, la somma delle dimensioni di $A \cap B$ e di $A + B$ è sempre uguale a 4 (che a sua volta è uguale a $\dim A + \dim B$).

E se in \mathbb{R}^4 consideriamo un piano C e un sottospazio D di dimensione 3?¹ Possono darsi tre casi per l'intersezione: $C \cap D = \{O\}$, $\dim(C \cap D) = 1$, $C \cap D = C$. Qualunque sia il caso, si verifica sempre (esercizio!) che

$$\dim C \cap D + \dim(C + D) = 5 = \dim C + \dim D.$$

Sembra dunque che ci sia una relazione fra le dimensioni in gioco: se due sottospazi A e B di uno spazio vettoriale V si intersecano “tanto”, allora generano “poco”. Più precisamente:

$$\dim A \cap B + \dim(A + B) = \dim A + \dim B.$$

Questa formula ci dice, per esempio, che in \mathbb{R}^5 due sottospazi di dimensione 3 devono avere intersezione non banale: infatti $\dim A = \dim B = 3$ e inoltre, visto che $A + B$ è un sottospazio di \mathbb{R}^5 , $\dim A + B \leq 5$, dunque $\dim A \cap B \geq 1$.

Dimostreremo questa formula, detta *formula di Grassmann*, come applicazione del Teorema 2.21.

Premettiamo una osservazione sul prodotto cartesiano di due spazi vettoriali. Dati due spazi vettoriali V e W sul campo \mathbb{K} , sul loro prodotto cartesiano $V \times W$ c'è una struttura “naturale” di spazio vettoriale, dove la somma è definita da:

$$(v, w) + (v_1, w_1) = (v + v_1, w + w_1)$$

¹In generale, se V è uno spazio vettoriale di dimensione n e H è un sottospazio di dimensione $n - 1$ si dice che H è un *iperpiano* di V .

e il prodotto per scalare da:

$$\lambda(v, w) = (\lambda v, \lambda w).$$

Si verifica immediatamente che, se $\{v_1, v_2, \dots, v_n\}$ è una base di V e $\{w_1, \dots, w_m\}$ è una base di W , allora $\{(v_1, O), (v_2, O), \dots, (v_n, O), (O, w_1), \dots, (O, w_m)\}$ è una base² di $V \times W$, che dunque ha dimensione $n+m = (\dim V) + (\dim W)$.

TEOREMA 4.1. *Dati due sottospazi A, B di uno spazio vettoriale V sul campo \mathbb{K} , vale*

$$\dim A + \dim B = \dim A \cap B + \dim (A + B)$$

Dimostrazione. Consideriamo l'applicazione

$$\Phi : A \times B \rightarrow V$$

definita da $\Phi((a, b)) = a - b$. Si verifica (facile esercizio) che Φ è lineare. Dimosteremo il teorema studiando il nucleo e l'immagine di Φ e applicando il Teorema 2.21.

Cosa sappiamo dire del nucleo di Φ ? Per definizione

$$\text{Ker } \Phi = \{(a, b) \in A \times B \mid a - b = O\}$$

dunque

$$\text{Ker } \Phi = \{(a, b) \in A \times B \mid a = b\}$$

che equivale a scrivere:

$$\text{Ker } \Phi = \{(z, z) \in A \times B \mid z \in A \cap B\}.$$

Si nota subito che la applicazione lineare $\theta : A \cap B \rightarrow \text{Ker } \Phi$ data da $z \rightarrow (z, z)$ è iniettiva e surgettiva, dunque è un isomorfismo (vedi la Definizione 2.22). Allora il suo dominio e il suo codominio hanno la stessa dimensione, ovvero

$$\dim \text{Ker } \Phi = \dim A \cap B$$

Cosa sappiamo dire dell'immagine di Φ ? Per definizione

$$\text{Imm } \Phi = \{a - b \mid a \in A, b \in B\}$$

Visto che B , come ogni spazio vettoriale, se contiene un elemento b contiene anche il suo opposto $-b$, possiamo scrivere la seguente uguaglianza fra insiemi:

$$\{a - b \mid a \in A, b \in B\} = \{a + b \in V \mid a \in A, b \in B\} = A + B.$$

Dunque

$$\text{Imm } \Phi = A + B$$

Per il Teorema 2.21 applicato a Φ sappiamo che:

$$\dim (A \times B) = \dim \text{Ker } \Phi + \dim \text{Imm } \Phi.$$

²Una precisazione: lo O che compare nelle coppie (v_i, O) è lo O dello spazio W , mentre lo O che compare in (O, w_j) è lo O di V . Qui e altrove nel testo abbiamo scelto, per semplicità, di non aggiungere indici al vettore O .

Questa formula, viste le osservazioni fatte fin qui, si traduce come:

$$\dim A + \dim B = \dim A \cap B + \dim (A + B)$$

□

ESERCIZIO 4.2. Dare una dimostrazione della formula di Grassmann nel seguente modo: fissare una base z_1, z_2, \dots, z_k di $A \cap B$ e usare il teorema di completamento (Teorema 2.19) per completarla ad una base di A aggiungendo certi vettori v_1, v_2, \dots, v_r . Poi usare di nuovo il teorema di completamento per completare la base di $A \cap B$ ad una base di B aggiungendo certi vettori w_1, w_2, \dots, w_s . A questo punto dimostrare che i vettori $z_1, z_2, \dots, z_k, v_1, v_2, \dots, v_r, w_1, w_2, \dots, w_s$ sono una base di $A + B$.

ESERCIZIO 4.3. Dire se è possibile trovare in \mathbb{R}^4 tre sottospazi vettoriali A, B, C di dimensione 2 tali che $A \cap B = \{O\}$, $A \cap C = \{O\}$ e $B \cap C = \{O\}$.

ESERCIZIO 4.4. Dati tre sottospazi vettoriali A, B, C di uno spazio vettoriale V , dare una buona definizione di $A + B + C$ e dire se è vera la formula:

$$\begin{aligned} & \dim (A + B + C) = \\ = & \dim A + \dim B + \dim C - \dim (A \cap B) - \dim (B \cap C) - \dim (A \cap C) + \dim (A \cap B \cap C) \end{aligned}$$

2. Un metodo per calcolare l'intersezione di due sottospazi vettoriali

Fin qui abbiamo visto essenzialmente due modi di presentare un sottospazio vettoriale di uno spazio vettoriale V : come span di certi vettori ($\langle v_1, \dots, v_r \rangle$) oppure come nucleo di una applicazione lineare (ovvero come insieme delle soluzioni di un sistema lineare omogeneo).

Consideriamo due sottospazi, U e W , di V . Se entrambi sono presentati come insieme delle soluzioni di un sistema è facile calcolare $U \cap W$: basta calcolare le soluzioni del sistema 'doppio', ottenuto considerando tutte le equazioni dei due sistemi.

Per esempio se U e W in \mathbb{R}^4 sono dati rispettivamente dalle soluzioni dei sistemi S_U :

$$\begin{cases} 3x + 2y + 4w & = 0 \\ 2x + y + z + w & = 0 \end{cases}$$

e S_W :

$$\begin{cases} x + 2y + z + w & = 0 \\ x + z + w & = 0 \end{cases}$$

allora $U \cap W$ è dato dalle soluzioni del sistema:

$$\begin{cases} 3x + 2y + 4w & = 0 \\ 2x + y + z + w & = 0 \\ x + 2y + z + w & = 0 \\ x + z + w & = 0 \end{cases}$$

ESERCIZIO 4.5. Calcolare $U \cap W$ nell'esempio proposto.

Ma come possiamo calcolare $U \cap W$ se i due sottospazi sono presentati come span di certi vettori? Consideriamo per esempio U e W in \mathbb{R}^5 definiti così:

$$U = \left\langle \begin{pmatrix} 1 \\ 2 \\ 3 \\ -1 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ 4 \\ 7 \\ 2 \\ -1 \end{pmatrix} \right\rangle$$

$$W = \left\langle \begin{pmatrix} 1 \\ 2 \\ 0 \\ -2 \\ -1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \\ -1 \\ -1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ -3 \\ -6 \\ 1 \end{pmatrix} \right\rangle$$

Un metodo per calcolare $U \cap W$ è quello di esprimere U e W come soluzioni di un sistema lineare. Mostriamo come si può fare, cominciando da U .

Per prima cosa scriviamo la seguente matrice:

$$\begin{pmatrix} 1 & 2 & x_1 \\ 2 & 4 & x_2 \\ 3 & 7 & x_3 \\ -1 & 2 & x_4 \\ 2 & -1 & x_5 \end{pmatrix}$$

Le prime due colonne sono i vettori della base di U , la terza colonna è data

dal vettore $v = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix}$, dove x_1, x_2, x_3, x_4, x_5 sono dei numeri reali. Cosa

possiamo dire sul rango di questa matrice? Se il vettore v appartiene ad U significa che è combinazione lineare delle prime due colonne, dunque il rango della matrice è 2. Se il vettore non appartiene ad A allora il rango della matrice è 3, perchè la matrice è formata da tre colonne linearmente indipendenti.

Dunque il calcolo del rango della matrice può essere utilizzato per decidere se v appartiene o no ad U . Possiamo allora ridurre la matrice a scalini per righe, ottenendo:

$$\begin{pmatrix} 1 & 2 & x_1 \\ 0 & 1 & x_3 - 3x_1 \\ 0 & 0 & 2x_1 - x_2 \\ 0 & 0 & 13x_1 - 4x_3 + x_4 \\ 0 & 0 & -17x_1 + 5x_3 + x_5 \end{pmatrix}$$

Tale matrice ha lo stesso rango della matrice iniziale, e, studiando i suoi scalini, notiamo che ha rango due se e solo se i coefficienti x_1, x_2, x_3, x_4, x_5

soddisfano le equazioni

$$(2.1) \quad \begin{cases} 2x_1 - x_2 & = 0 \\ 13x_1 - 4x_3 + x_4 & = 0 \\ -17x_1 + 5x_3 + x_5 & = 0 \end{cases}$$

Dunque il vettore $v = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix}$ appartiene ad U se e solo se le sue

coordinate soddisfano il sistema (2.1). Questo equivale a dire che le soluzioni del sistema coincidono con gli elementi di U . Abbiamo raggiunto il nostro scopo, ossia abbiamo presentato il sottospazio U come insieme di soluzioni di un sistema lineare.

OSSERVAZIONE 4.6. Visto che U ha dimensione 2, un sistema le cui soluzioni coincidono con l'insieme U deve avere almeno 3 equazioni (infatti la dimensione dello spazio delle soluzioni di un sistema omogeneo, come sappiamo, è uguale al numero di variabili del sistema meno il rango della matrice; nel nostro caso le variabili sono cinque e dunque il rango deve essere tre, ovvero devono esserci almeno tre equazioni non nulle nel sistema). Questo vuol dire che nel nostro esempio abbiamo ottenuto una descrizione di U col numero minimo possibile di equazioni.

ESERCIZIO 4.7. Dimostrare che l'osservazione precedente vale in generale: quando si parte da un sottospazio U di \mathbb{K}^n di cui conosciamo una base v_1, \dots, v_r , il metodo descritto sopra permette di presentare U come lo spazio delle soluzioni di un sistema di $n - r$ equazioni, il numero minimo possibile di equazioni.

Per finire il calcolo di $U \cap W$ possiamo allo stesso modo ottenere un sistema le cui soluzioni sono tutti e soli i vettori di W :

$$\begin{cases} x_2 + x_3 + 2x_5 & = 0 \\ -10x_1 + 9x_2 - 5x_3 + 4x_4 & = 0 \end{cases}$$

A questo punto possiamo ottenere $U \cap W$ risolvendo il sistema:

$$\begin{cases} 2x_1 - x_2 & = 0 \\ 13x_1 - 4x_3 + 1x_4 & = 0 \\ -17x_1 + 5x_3 + 1x_5 & = 0 \\ x_2 + x_3 + 2x_5 & = 0 \\ -10x_1 + 9x_2 - 5x_3 + 4x_4 & = 0 \end{cases}$$

ESERCIZIO 4.8. Verificare nel dettaglio tutti i calcoli di questo paragrafo e concludere l'esercizio, indicando una base di $U \cap V$. La dimensione risulta uguale a quella prevista dalla formula di Grassmann (4.1)?

3. Somma diretta di sottospazi

Si dice che due sottospazi U e W di uno spazio vettoriale V formano una *somma diretta* se vale che $U \cap W = \{O\}$. In questo caso, come sappiamo dalla formula di Grassmann, la dimensione di $U+W$ è ‘la massima possibile’, ovvero è uguale a $\dim U + \dim W$. Vale anche il viceversa, ossia due sottospazi sono in somma diretta se e solo se $\dim(U+W) = \dim U + \dim W$. Quando siamo sicuri che $U+W$ è la somma di due sottospazi che sono in somma diretta, al posto di $U+W$ possiamo scrivere:

$$U \oplus W.$$

In particolare, per avere una base di $U \oplus W$ basta fare l’unione di una base di U con una base di W (si osserva immediatamente che i vettori di questa unione generano $U \oplus W$ e inoltre sono nel ‘giusto numero’, ossia il loro numero è $\dim U + \dim W$, vedi il Corollario 2.17).

Per esempio, in \mathbb{R}^4 , il sottospazio

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

e il sottospazio

$$W = \left\langle \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \right\rangle$$

sono in somma diretta, e una base di $U \oplus W$ è data dai tre vettori

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

ESERCIZIO 4.9. Motivare come mai è valido il seguente criterio per stabilire se, dato un sottospazio U , un certo vettore v vi appartiene o no: si controlla se U e $\langle v \rangle$ sono in somma diretta, ovvero si calcola la dimensione di $U + \langle v \rangle$ e se risulta uguale a $\dim U + 1$ allora $v \notin U$, se invece è uguale a $\dim U$ allora $v \in U$.

Dati due sottospazi U e W di uno spazio vettoriale V , può capitare che siano in somma diretta e che inoltre $U \oplus W = V$. Si dice in questo caso che i due sottospazi sono l’uno il *complementare* dell’altro. Un esempio banale di sottospazi complementari è fornito da $\{O\}$ e da V stesso, visto che vale $\{O\} \oplus V = V$. In generale è sempre possibile trovare lo spazio complementare ad un sottospazio proprio di V , come mostra il seguente esercizio.

ESERCIZIO 4.10. Dimostrare che, dato un sottospazio vettoriale proprio U di V , esiste sempre un complementare di U .

Suggerimento: prendere una base di U e completarla ad una base di V (vedi Teorema 2.19). I vettori che abbiamo aggiunto sono la base di uno spazio vettoriale complementare a U .

OSSERVAZIONE 4.11. Attenzione: un sottospazio vettoriale U di V che non è uguale a V possiede in generale molti complementari (infiniti, se il campo \mathbb{K} ha infiniti elementi). Per esempio, in \mathbb{R}^3 un piano passante per l'origine ha per complementare una qualunque retta passante per l'origine e che non giace sul piano. Come ulteriore esempio, il lettore può facilmente verificare che, in \mathbb{R}^4 , il sottospazio

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

ha come complementare

$$W_1 = \left\langle \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \right\rangle$$

ma anche

$$W_2 = \left\langle \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 2 \\ 0 \end{pmatrix} \right\rangle$$

In generale, dati k sottospazi U_1, U_2, \dots, U_k di uno spazio vettoriale V , si dice che tali sottospazi sono in somma diretta se, per ogni $i = 1, 2, \dots, k$, vale che l'intersezione di U_i con la somma di tutti gli altri è uguale a $\{O\}$, ovvero

$$U_i \cap (U_1 + \dots + \widehat{U}_i + \dots + U_k) = \{O\}$$

dove il simbolo \widehat{U}_i indica che nella somma si è saltato il termine U_i .

In tal caso per indicare $U_1 + U_2 + \dots + U_k$ si può usare la notazione:

$$U_1 \oplus U_2 \oplus \dots \oplus U_k$$

ESERCIZIO 4.12. Dimostrare che, se U_1, U_2, \dots, U_k sono in somma diretta, vale:

$$\dim (U_1 \oplus U_2 \oplus \dots \oplus U_k) = \dim U_1 + \dim U_2 + \dots + \dim U_k$$

Suggerimento. Dimostrarlo per induzione su k .

In base all'esercizio precedente, osserviamo che per trovare una base di

$$U_1 \oplus U_2 \oplus \dots \oplus U_k$$

basta scegliere una base per ognuno dei sottospazi U_i e poi fare l'unione (si vede immediatamente che questi elementi sono generatori e il loro numero è 'il numero giusto'). Se accade che

$$U_1 \oplus U_2 \oplus \cdots \oplus U_k = V$$

otterremo in tal modo una base dell'intero spazio.

4. Altri esercizi

ESERCIZIO 4.13. Trovare un complementare in \mathbb{R}^5 del sottospazio

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

ESERCIZIO 4.14. Stabilire se i due sottospazi di \mathbb{R}^4

$$U = \left\langle \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 2 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 3 \\ 2 \end{pmatrix} \right\rangle$$

e

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

sono in somma diretta.

Applicazioni lineari e matrici invertibili

1. Endomorfismi lineari invertibili

Abbiamo già incontrato nei capitoli precedenti applicazioni lineari invertibili. In questo paragrafo torniamo sull'argomento per alcuni approfondimenti; ci occuperemo in particolare di applicazioni lineari invertibili che hanno come dominio e codominio lo stesso spazio vettoriale V . Nel prossimo paragrafo descriveremo un algoritmo che, data la matrice associata ad una applicazione lineare invertibile, permette di trovare la matrice associata alla applicazione inversa.

Consideriamo uno spazio vettoriale V di dimensione n sul campo \mathbb{K} e una applicazione lineare $L : V \rightarrow V$. Una tale applicazione si dice *endomorfismo lineare di V* . Chiameremo $End(V)$ l'insieme di tutti gli endomorfismi lineari di V .

PROPOSIZIONE 5.1. *Un endomorfismo L di V è invertibile se e solo se ha rango n . La funzione inversa $L^{-1} : V \rightarrow V$ è anch'essa una applicazione lineare.*

DIMOSTRAZIONE. Supponiamo che L abbia rango n . Questo significa, per la definizione di rango (vedi Definizione 2.32), che $Imm L$ è un sottospazio di V di dimensione n ; ma allora $Imm L = V$ e dunque L è surgettiva. Inoltre, per il Teorema 2.21 sappiamo che la dimensione di $Ker L$ è 0, dunque $Ker L = \{O\}$ e L è iniettiva. In conclusione, abbiamo mostrato che L è bigettiva e dunque invertibile.

Viceversa, se L è invertibile, allora in particolare è surgettiva, dunque $Imm L = V$ e il rango di L , che è uguale a $dim Imm L$, è uguale a n .

Quanto al fatto che l'inversa L^{-1} sia anch'essa lineare, basta verificare che, per ogni $v, w \in V$ e per ogni $\lambda \in \mathbb{K}$, valga $L^{-1}(v+w) = L^{-1}(v) + L^{-1}(w)$ e $L^{-1}(\lambda v) = \lambda L^{-1}(v)$. Facciamo a titolo di esempio la prima di queste due verifiche. Visto che L è bigettiva, in particolare è iniettiva, dunque

$$L^{-1}(v + w) = L^{-1}(v) + L^{-1}(w)$$

vale se e solo se vale

$$L(L^{-1}(v + w)) = L(L^{-1}(v) + L^{-1}(w)).$$

Quest'ultima relazione si verifica facilmente. Infatti per il membro di destra abbiamo $L(L^{-1}(v + w)) = v + w$ e per il membro di sinistra, utilizzando la linearità di L , $L(L^{-1}(v) + L^{-1}(w)) = L(L^{-1}(v)) + L(L^{-1}(w)) = v + w$.

□

OSSERVAZIONE 5.2. Un endomorfismo invertibile è un caso particolare di *isomorfismo* (vedi Definizione 2.22). Il lettore può molto facilmente adattare (esercizio!) la dimostrazione precedente per ottenere un risultato che generalizza in questo senso quello precedente: dati due spazi vettoriali V e W entrambi di dimensione n e una applicazione lineare $L : V \rightarrow W$, l'applicazione L è invertibile (ossia è un isomorfismo) se e solo se ha rango n ; l'applicazione inversa L^{-1} è anch'essa lineare.

Chiameremo $GL(V)$ il sottoinsieme di $End(V)$ costituito dagli endomorfismi invertibili. Come si verifica immediatamente, $GL(V)$ è un gruppo¹ con la operazione di composizione fra funzioni \circ , chiamato il *gruppo generale lineare* su V .

ESERCIZIO 5.3. Verificare che la composizione di due applicazioni $L, T \in GL(V)$ è ancora in $GL(V)$. Completare poi tutte le altre verifiche del fatto che $GL(V)$ è un gruppo.

Se fissiamo una base di V , ad ogni endomorfismo $L \in End(V)$ viene associata una matrice $[L] \in Mat_{n \times n}(\mathbb{K})$ (per costruire $[L]$ si è usata la base scelta come base sia “in partenza” sia “in arrivo”). Se L è invertibile, consideriamo l'inversa L^{-1} e la matrice ad essa associata $[L^{-1}]$. Visto che $L \circ L^{-1} = L^{-1} \circ L = I$, il Teorema 2.26 ci assicura che in $Mat_{n \times n}(\mathbb{K})$ vale

$$[L^{-1}][L] = [L][L^{-1}] = [I] = I$$

(ricordiamo che, quando la base scelta in partenza e in arrivo è la stessa, $[I]$ è la matrice identità, che avevamo convenuto di indicare sempre col simbolo I , vedi Osservazione 1.93).

Dunque la matrice $[L]$ è invertibile e ha per inversa $[L^{-1}]$. Sempre applicando il Teorema 2.26 otteniamo il viceversa: se la matrice $[L]$ associata ad un endomorfismo lineare è invertibile allora anche L è invertibile e la sua inversa è l'applicazione associata alla matrice $[L^{-1}]$.

Alla luce di questa osservazione, la proposizione precedente ha un immediato corollario.

COROLLARIO 5.4. *Una matrice $A \in Mat_{n \times n}(\mathbb{K})$ è invertibile se e solo se il suo rango è n .*

DIMOSTRAZIONE. Data una matrice $A \in Mat_{n \times n}(\mathbb{K})$ possiamo sempre supporre che sia la matrice associata ad un certo endomorfismo lineare L di uno spazio vettoriale V di dimensione n su cui è stata fissata una base. Dalla osservazione che precede il corollario sappiamo che A è invertibile se e solo se L è invertibile. Dalla Proposizione 5.1 sappiamo che L è invertibile se e solo se ha rango n . Dal Teorema 2.46 e dalla osservazione che lo segue sappiamo che il rango di A è uguale al rango di L .

□

¹Il lettore può trovare la definizione di gruppo nelle dispense della prima parte del corso.

2. Il metodo per trovare l'inversa (se esiste) di una matrice quadrata

Come abbiamo visto nel paragrafo precedente, il problema di trovare una inversa di $L \in \text{End}(V)$ si può tradurre nel problema di trovare l'inversa in $\text{Mat}_{n \times n}(\mathbb{K})$ di una matrice data. Molto spesso questa traduzione è utile nelle applicazioni; dedichiamo questo paragrafo alla descrizione di un metodo concreto per trovare l'inversa di una matrice $A \in \text{Mat}_{n \times n}(\mathbb{K})$. Cominciamo con un esempio.

2.1. Un esempio. Consideriamo la matrice $A = \begin{pmatrix} 3 & 2 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$ che ha rango 3, dunque è invertibile, e calcoliamo la sua inversa. Per prima cosa formiamo la matrice

$$(A \ I) = \begin{pmatrix} 3 & 2 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Ora con delle operazioni elementari di riga portiamola in forma a scalini per righe ridotta, per esempio nel seguente modo: si sottrae alla prima riga la terza moltiplicata per 3

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

poi si somma alla prima riga la seconda

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

A questo punto si permutano le righe e si ottiene:

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

Per ottenere la forma a scalini ridotta, moltiplichiamo l'ultima riga per $\frac{1}{2}$

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

sottraiamo alla seconda riga la terza riga

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

infine sottraiamo alla prima riga la seconda:

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

La matrice

$$B = \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} & \frac{3}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{3}{2} \end{pmatrix}$$

è l'inversa di A , come il lettore può immediatamente verificare.

2.2. Come mai il metodo funziona? Descriviamo di nuovo, da un punto di vista più generale, il metodo illustrato dall'esempio e spieghiamo come mai funziona. Consideriamo una matrice $A \in Mat_{n \times n}(\mathbb{K})$ e cerchiamo la sua inversa; dato il Corollario 5.4 possiamo supporre che A abbia rango n .

Per prima cosa creiamo una matrice $n \times 2n$ “ponendo accanto” le colonne di A e quelle di I . Indicheremo tale matrice col simbolo:

$$(A \ I).$$

Adesso possiamo agire con operazioni elementari di riga in modo da ridurre la matrice in forma a scalini per righe ridotta. Poichè A ha rango n , anche $(A \ I)$ ha rango n . Un modo per rendersene conto è il seguente: il rango di $(A \ I)$ è minore o uguale a n visto che ha n righe, ed è maggiore o uguale a n , visto che si individuano facilmente n colonne linearmente indipendenti (quelle che provengono da A , oppure quelle che provengono da I).

Allora quando la matrice $(A \ I)$ viene ridotta in forma a scalini per righe ridotta, deve avere esattamente n scalini, dunque deve avere la forma:

$$(I \ B).$$

Affermiamo che la matrice B (quadrata, di formato $n \times n$) che si ricava dalla matrice precedente è proprio l'inversa di A che cercavamo.

Infatti agire con operazioni di riga equivale, come sappiamo dal Paragrafo 5 del Capitolo 2, a moltiplicare a sinistra la matrice $(A \ I)$ per una matrice invertibile U di formato $n \times n$, dunque:

$$U(A \ I) = (I \ B).$$

Per come è definito il prodotto righe per colonne,

$$U(A \ I) = (UA \ UI)$$

(per rendersene conto può essere utile osservare che la colonna i -esima di $U(A \ I)$ è uguale a UC_i , dove C_i è la colonna i -esima di $(A \ I)$).

Dalle due uguaglianze precedenti ricaviamo

$$(UA \quad UI) = (I \quad B)$$

ossia le relazioni $UA = I$ e $UI = B$ che ci dicono che U è l'inversa di A e che $U = B$, come avevamo annunciato.

OSSERVAZIONE 5.5. La relazione $UA = I$, ossia $BA = I$, ci dice solo che B è l'inversa sinistra di A . Ma possiamo mostrare facilmente che B coincide con l'inversa di A e dunque vale anche $AB = I$. Infatti l'inversa di A deve esistere (ed è unica²), visto che A è invertibile. Chiamiamola K ; tale matrice K deve soddisfare per definizione $AK = KA = I$. Ora moltiplichiamo entrambi i membri della relazione $BA = I$, a destra, per K : $BAK = IK$. Usando la proprietà associativa del prodotto in $Mat_{n \times n}(\mathbb{K})$ otteniamo, visto che $AK = I$:

$$B = K,$$

ossia B è l'inversa di A .

OSSERVAZIONE 5.6. Se la matrice A da cui siamo partiti non fosse stata invertibile, ossia se avesse avuto rango minore di n , il procedimento descritto per trovare l'inversa (ovviamente) non avrebbe funzionato: infatti nella riduzione a scalini non avremmo trovato n pivots nella parte di sinistra della matrice e non saremmo riusciti a portare $(A \quad I)$ nella forma $(I \quad B)$.

ESERCIZIO 5.7. Dimostrare che una matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Mat_{2 \times 2}(\mathbb{K})$ è invertibile se e solo se $ad - bc \neq 0$. Calcolare, in tal caso, l'inversa.

Nota: il risultato sarà la matrice:

$$\frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

3. Cambiamento di base nel caso degli endomorfismi lineari

Sia V uno spazio vettoriale di dimensione finita n sul campo \mathbb{K} e sia $L \in End(V)$. Supponiamo di avere due basi di V , una data dai vettori v_1, v_2, \dots, v_n e l'altra dai vettori e_1, e_2, \dots, e_n . In questo paragrafo studieremo la relazione che lega le matrici associate a L rispetto a tali basi,

$$[L]_{v_1, v_2, \dots, v_n} \quad \text{e} \quad [L]_{e_1, e_2, \dots, e_n}$$

²L'insieme delle matrici $n \times n$ invertibili è un gruppo rispetto alla moltiplicazione, come possiamo facilmente ricavare, per esempio, dal fatto che $GL(V)$ è un gruppo (vedi Esercizio 5.3). Ricordiamo che in un gruppo l'inverso di un elemento è unico: se b e c sono inversi di a e se indichiamo con e l'elemento neutro, dalla relazione $ab = e$ si ricava, moltiplicando a sinistra per c , $cab = ce$. A questo punto, utilizzando la proprietà associativa e il fatto che $ca = e$, si ottiene $b = c$.

Per prima cosa scriviamo ogni vettore v_i come combinazione lineare dei vettori della base e_1, e_2, \dots, e_n :

$$v_1 = a_{11}e_1 + a_{21}e_2 + \dots + a_{n1}e_n$$

$$v_2 = a_{12}e_1 + a_{22}e_2 + \dots + a_{n2}e_n$$

.....

$$v_n = a_{1n}e_1 + a_{2n}e_2 + \dots + a_{nn}e_n$$

Osserviamo a questo punto che la matrice associata all'endomorfismo identità $I \in \text{End}(V)$ prendendo come base in partenza v_1, v_2, \dots, v_n e come base in arrivo e_1, e_2, \dots, e_n è la seguente:

$$[I] \begin{matrix} v_1, v_2, \dots, v_n \\ e_1, e_2, \dots, e_n \end{matrix} = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{pmatrix}$$

Infatti nella prima colonna abbiamo scritto i coefficienti di $I(v_1)$ (che è uguale a v_1) rispetto alla base e_1, e_2, \dots, e_n , nella seconda colonna i coefficienti di $I(v_2) = v_2$ e così via... La matrice appena trovata è una *matrice di cambiamento di base* e la chiameremo M . Osserviamo subito che M è invertibile. Infatti pensiamo alla composizione di endomorfismi $I \circ I$ ovvero $V \xrightarrow{I} V \xrightarrow{I} V$ e consideriamo il primo spazio V e l'ultimo muniti della base v_1, v_2, \dots, v_n , mentre lo spazio V al centro lo consideriamo con la base e_1, e_2, \dots, e_n . Applicando il Teorema 2.26 otteniamo:

$$[I \circ I] \begin{matrix} v_1, v_2, \dots, v_n \\ v_1, v_2, \dots, v_n \end{matrix} = [I] \begin{matrix} e_1, e_2, \dots, e_n \\ v_1, v_2, \dots, v_n \end{matrix} [I] \begin{matrix} v_1, v_2, \dots, v_n \\ e_1, e_2, \dots, e_n \end{matrix}$$

Visto che $I \circ I = I$ possiamo riscrivere

$$[I] \begin{matrix} v_1, v_2, \dots, v_n \\ v_1, v_2, \dots, v_n \end{matrix} = [I] \begin{matrix} e_1, e_2, \dots, e_n \\ v_1, v_2, \dots, v_n \end{matrix} [I] \begin{matrix} v_1, v_2, \dots, v_n \\ e_1, e_2, \dots, e_n \end{matrix}$$

Ora la matrice al membro di sinistra è, come sappiamo, la matrice identità I , mentre la matrice più a destra è M , dunque:

$$I = [I] \begin{matrix} e_1, e_2, \dots, e_n \\ v_1, v_2, \dots, v_n \end{matrix} M$$

Questo ci permette di concludere che M è invertibile e che $M^{-1} = [I] \begin{matrix} e_1, e_2, \dots, e_n \\ v_1, v_2, \dots, v_n \end{matrix}$.

A questo punto possiamo enunciare il teorema che descrive la relazione fra le matrici associate a L rispetto alle due diverse basi:

TEOREMA 5.8. *Con le notazioni introdotte sopra, vale:*

$$[L] \begin{matrix} v_1, v_2, \dots, v_n \\ v_1, v_2, \dots, v_n \end{matrix} = M^{-1} [L] \begin{matrix} e_1, e_2, \dots, e_n \\ e_1, e_2, \dots, e_n \end{matrix} M$$

DIMOSTRAZIONE. Consideriamo la composizione di endomorfismi $I \circ L \circ I$ e applichiamo il Teorema 2.26:

$$V \xrightarrow{I} V \xrightarrow{L} V \xrightarrow{I} V$$

$v_i \quad e_i \quad e_i \quad v_i$

(sotto ogni copia di V il simbolo e_i oppure v_i indica quale base abbiamo scelto). Otteniamo³:

$$[I \circ L \circ I] \begin{matrix} v_1, v_2, \dots, v_n \\ v_1, v_2, \dots, v_n \end{matrix} = [I] \begin{matrix} e_1, e_2, \dots, e_n \\ v_1, v_2, \dots, v_n \end{matrix} [L] \begin{matrix} e_1, e_2, \dots, e_n \\ e_1, e_2, \dots, e_n \end{matrix} [I] \begin{matrix} v_1, v_2, \dots, v_n \\ e_1, e_2, \dots, e_n \end{matrix}$$

Visto che $I \circ L \circ I = L$ la formula appena ottenuta si può riscrivere come:

$$[L] \begin{matrix} v_1, v_2, \dots, v_n \\ v_1, v_2, \dots, v_n \end{matrix} = M^{-1} [L] \begin{matrix} e_1, e_2, \dots, e_n \\ e_1, e_2, \dots, e_n \end{matrix} M$$

□

Ricordiamo che il problema di trovare la matrice associata a L rispetto ad una base se si conosce la matrice associata rispetto ad un'altra base può essere affrontato anche senza scrivere le matrici M e M^{-1} , come mostra l'Esempio 1.90, ma il teorema appena dimostrato ha una grande importanza dal punto di vista teorico, come vedremo nei prossimi capitoli.

Per esempio, nell'Esercizio 1.106 abbiamo definito l'applicazione *traccia*

$$\mathcal{T} : Mat_{n \times n}(\mathbb{K}) \rightarrow \mathbb{K}$$

nel seguente modo:

$$\mathcal{T}((a_{ij})) = a_{11} + a_{22} + \dots + a_{nn}.$$

È naturale chiedersi se, dato un endomorfismo $L \in End(V)$, la funzione traccia dia lo stesso valore su tutte le matrici che si possono associare a V , in altre parole se vale:

$$\mathcal{T} \left(\begin{matrix} [L] & & & \\ & v_1, v_2, \dots, v_n & & \\ & & & \\ & & & v_1, v_2, \dots, v_n \end{matrix} \right) = \mathcal{T} \left(\begin{matrix} [L] & & & \\ & e_1, e_2, \dots, e_n & & \\ & & & \\ & & & e_1, e_2, \dots, e_n \end{matrix} \right)$$

per ogni scelta delle basi e_1, e_2, \dots, e_n e v_1, v_2, \dots, v_n .

³Il Teorema 2.26 si riferisce alla composizione di due applicazioni lineari, ma la versione con tre applicazioni lineari si ricava subito usando la proprietà associativa e applicando due volte il teorema.

La risposta è sì: la traccia non dipende dalla base scelta e dunque possiamo anche considerarla come applicazione lineare da $End(V)$ a \mathbb{K} . Per mostrarlo, innanzitutto utilizziamo il Teorema 5.8 e scriviamo:

$$\mathcal{T} \left(\begin{array}{c} [L] \\ v_1, v_2, \dots, v_n \\ v_1, v_2, \dots, v_n \end{array} \right) = \mathcal{T} \left(\begin{array}{ccc} M^{-1}[L] & & M \\ e_1, e_2, \dots, e_n & & \\ e_1, e_2, \dots, e_n & & \end{array} \right)$$

A questo punto ricordiamo che per ogni $A, B \in Mat_{n \times n}(\mathbb{K})$ vale $\mathcal{T}(AB) = \mathcal{T}(BA)$ (vedi l'Esercizio 1.106), dunque:

$$\begin{aligned} \mathcal{T} \left(\left(\begin{array}{c} M^{-1}[L] \\ e_1, e_2, \dots, e_n \\ e_1, e_2, \dots, e_n \end{array} \right) M \right) &= \mathcal{T} \left(M \left(\begin{array}{c} M^{-1}[L] \\ e_1, e_2, \dots, e_n \\ e_1, e_2, \dots, e_n \end{array} \right) \right) = \\ &= \mathcal{T} \left(\begin{array}{ccc} MM^{-1}[L] & & \\ e_1, e_2, \dots, e_n & & \\ e_1, e_2, \dots, e_n & & \end{array} \right) = \mathcal{T} \left(\begin{array}{c} [L] \\ e_1, e_2, \dots, e_n \\ e_1, e_2, \dots, e_n \end{array} \right) \end{aligned}$$

Questa catena di uguaglianze conduce, come avevamo annunciato, a:

$$\mathcal{T} \left(\begin{array}{c} [L] \\ v_1, v_2, \dots, v_n \\ v_1, v_2, \dots, v_n \end{array} \right) = \mathcal{T} \left(\begin{array}{c} [L] \\ e_1, e_2, \dots, e_n \\ e_1, e_2, \dots, e_n \end{array} \right)$$

4. Altri esercizi

ESERCIZIO 5.9. Trovare, se esiste, l'inversa della seguente matrice a coefficienti in \mathbb{R} :

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

ESERCIZIO 5.10. Trovare, se esiste, l'inversa della seguente matrice a coefficienti in \mathbb{R} :

$$\begin{pmatrix} -11 & 2 & 2 \\ -1 & 0 & 1 \\ 6 & -1 & -1 \end{pmatrix}$$

ESERCIZIO 5.11. Trovare, se esistono, le inverse delle matrici degli Esercizi 5.9 e 5.10, lette stavolta come matrici a coefficienti in \mathbb{Z}_2 .

ESERCIZIO 5.12. Trovare, se esistono, le inverse delle matrici degli Esercizi 5.9 e 5.10, lette come matrici a coefficienti in \mathbb{Z}_3 .

ESERCIZIO 5.13. Dimostrare che se una matrice $A \in Mat_{n \times n}(\mathbb{R})$ ha tutti i coefficienti in \mathbb{Z} ed è invertibile, allora la sua inversa ha coefficienti in \mathbb{Q} .

ESERCIZIO 5.14. Sia $L : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ l'applicazione lineare la cui matrice rispetto alla base standard è

$$[L] = \begin{pmatrix} 2 & -\frac{1}{2} & -\frac{1}{2} \\ 0 & \frac{5}{2} & \frac{1}{2} \\ 0 & \frac{1}{2} & \frac{5}{2} \end{pmatrix}$$

Consideriamo adesso la base di \mathbb{R}^3 data dai vettori $v_1 = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$, $v_2 =$

$\begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$, $v_3 = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$. Calcolare le matrici M e M^{-1} di cambiamento di base fra la base standard e la base v_1, v_2, v_3 e scrivere la matrice associata a L rispetto alla base v_1, v_2, v_3 .

ESERCIZIO 5.15. Sia $L : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ l'applicazione lineare la cui matrice rispetto alla base standard è

$$[L] = \begin{pmatrix} 1 & 2 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 2 \end{pmatrix}$$

Consideriamo adesso la base di \mathbb{R}^3 data dai vettori $v_1 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$, $v_2 =$

$\begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$, $v_3 = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$. Calcolare la matrice associata a L rispetto alla base v_1, v_2, v_3 in due modi: direttamente (come nell'Esempio 1.90) e attraverso il calcolo delle matrici di cambiamento di base M e M^{-1} .

Informazioni sul determinante

In questo capitolo daremo alcune informazioni sulla funzione *determinante*. Alcuni teoremi non verranno dimostrati nel corso, ma utilizzeremo gli enunciati. Il lettore interessato può trovare le dimostrazioni per esempio in [Ab].

1. Definizione del determinante di una matrice quadrata

Il determinante è una funzione

$$\text{Det} : \text{Mat}_{n \times n}(\mathbb{K}) \rightarrow \mathbb{K}$$

Per alleggerire la notazione talvolta indicheremo con $|a_{ij}|$ oppure con $\text{Det}(a_{ij})$ o con $\text{Det} A$ - invece che con $\text{Det}((a_{ij}))$ o $\text{Det}(A)$ - il determinante di una matrice $A = (a_{ij})$.

Il determinante è definito ricorsivamente, al crescere di n , nel seguente modo:

- (1) il determinante di una matrice 1×1 è uguale all'unico coefficiente della matrice:

$$\text{Det}(a) = a$$

- (2) dato $n \geq 2$, il determinante di una matrice $A = (a_{ij})$ di formato $n \times n$ può essere ottenuto come combinazione lineare dei coefficienti di una qualunque riga, diciamo la i -esima, tramite la seguente formula:

$$(1.1) \quad \text{Det} A = (-1)^{1+i} a_{i1} \text{Det} A_{i1} + (-1)^{2+i} a_{i2} \text{Det} A_{i2} + \cdots + (-1)^{i+n} a_{in} \text{Det} A_{in}$$

dove A_{ij} indica la matrice (quadrata) di formato $(n-1) \times (n-1)$ che si ottiene da A cancellando la riga i -esima e la colonna j -esima.

OSSERVAZIONE 6.1. Dalla definizione possiamo immediatamente ricavare la seguente formula per il determinante di una matrice 2×2 :

$$\text{Det} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$$

OSSERVAZIONE 6.2. Il determinante si può ottenere anche come combinazione lineare dei coefficienti di una qualunque colonna, diciamo la j -esima, tramite la seguente formula:

$$(1.2) \quad \text{Det} A = (-1)^{1+j} a_{1j} \text{Det} A_{1j} + (-1)^{2+j} a_{2j} \text{Det} A_{2j} + \cdots + (-1)^{j+n} a_{nj} \text{Det} A_{nj}$$

Ovviamente il fatto che sia equivalente calcolare il determinante a partire da una qualunque riga o da una qualunque colonna va dimostrato, ma noi abbiamo deciso di omettere questa dimostrazione.

ESEMPIO 6.3. Data in $Mat_{3 \times 3}(\mathbb{R})$ la matrice

$$A = \begin{pmatrix} 3 & 2 & 5 \\ 2 & 0 & 1 \\ 4 & 2 & 6 \end{pmatrix}$$

per calcolare il determinante si sceglie una riga e poi si applica la formula (1.1) (oppure si sceglie una colonna e poi si applica la (1.2)). Per esempio, scegliamo la seconda riga:

$$\begin{aligned} \text{Det } A &= -2\text{Det} \begin{pmatrix} 2 & 5 \\ 2 & 6 \end{pmatrix} + 0\text{Det} \begin{pmatrix} 3 & 5 \\ 4 & 6 \end{pmatrix} - \text{Det} \begin{pmatrix} 3 & 2 \\ 4 & 2 \end{pmatrix} = \\ &= -2(12 - 10) - (6 - 8) = -4 + 2 = -2 \end{aligned}$$

OSSERVAZIONE 6.4. Nel caso delle matrici 3×3 il determinante si può calcolare anche mediante la seguente *regola di Sarrus*¹. Data

$$B = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$$

si forma la seguente matrice 3×5

$$\begin{pmatrix} a & b & c & a & b \\ d & e & f & d & e \\ g & h & i & g & h \end{pmatrix}$$

dopodiché si sommano i tre prodotti dei coefficienti che si trovano sulle tre diagonali che scendono da sinistra a destra e si sottraggono i tre prodotti dei coefficienti che si trovano sulle tre diagonali che salgono da sinistra a destra:

$$\text{Det } B = aei + bfg + cdh - gec - hfa - idb$$

Verifichiamo che nel caso della matrice

$$A = \begin{pmatrix} 3 & 2 & 5 \\ 2 & 0 & 1 \\ 4 & 2 & 6 \end{pmatrix}$$

la regola di Sarrus dia lo stesso risultato -2 che abbiamo già calcolato:

$$3 \cdot 0 \cdot 6 + 2 \cdot 1 \cdot 4 + 5 \cdot 2 \cdot 2 - 4 \cdot 0 \cdot 5 - 2 \cdot 1 \cdot 3 - 6 \cdot 2 \cdot 2 = 8 + 20 - 6 - 24 = -2.$$

ESERCIZIO 6.5. Dimostrare che il determinante di una matrice (a_{ij}) triangolare superiore (ossia tale che $a_{ij} = 0$ se $i > j$) è uguale al prodotto dei coefficienti che si trovano sulla diagonale. Lo stesso per una matrice triangolare inferiore.

¹La regola prende nome dal matematico francese Pierre Frederic Sarrus (1798-1861).

2. Il determinante e il calcolo del rango di una matrice

Data una matrice $A = (a_{ij}) \in Mat_{n \times m}(\mathbb{K})$ e dato un numero intero positivo k minore o uguale al minimo fra m e n , possiamo scegliere k righe fra le n righe (diciamo che scegliamo le righe i_1, i_2, \dots, i_k) e k colonne fra le m colonne (diciamo che scegliamo le colonne j_1, j_2, \dots, j_k).

DEFINIZIONE 6.6. Data la scelta di k righe e k colonne come sopra, chiamiamo *minore di A di formato $k \times k$* la matrice ottenuta da A cancellando tutti i coefficienti eccetto quelli che giacciono contemporaneamente su una delle righe e su una delle colonne scelte, in altre parole cancellando tutti i coefficienti eccetto gli a_{ij} per cui $i \in \{i_1, i_2, \dots, i_k\}$ e $j \in \{j_1, j_2, \dots, j_k\}$.

OSSERVAZIONE 6.7. Da una matrice $n \times m$ è possibile ricavare $\binom{n}{k} \binom{m}{k}$ minori di formato $k \times k$.

I determinanti dei minori possono essere utilizzati per calcolare il rango di una matrice $n \times m$, come risulta dal seguente teorema.

TEOREMA 6.8. *Data una matrice $A = (a_{ij}) \in Mat_{n \times m}(\mathbb{K})$, supponiamo che esista un minore di formato $k \times k$ il cui determinante è diverso da 0. Allora il rango di A è maggiore o uguale a k . Se $k = n$ oppure $k = m$ allora il rango di A è uguale a k . Se $k < n$ e $k < m$ e tutti i determinanti dei minori di formato $(k+1) \times (k+1)$ sono uguali a 0 allora il rango di A è uguale a k .*

OSSERVAZIONE 6.9. Se una matrice quadrata $n \times n$ ha determinante diverso da zero, allora per il teorema precedente ha rango n e dunque è invertibile. Sempre per il teorema vale anche il viceversa: se una matrice $n \times n$ ha determinante uguale a 0, allora il suo rango è strettamente minore di n e dunque la matrice non è invertibile. Nel caso 2×2 , data

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

con determinante diverso da zero, ossia $ad - bc \neq 0$, l'inversa (vedi Esercizio 5.7) si scrive esplicitamente come:

$$A^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

ESEMPIO 6.10. La matrice

$$\begin{pmatrix} 3 & 9 & 4 & 7 & 12 \\ 1 & \mathbf{3} & \mathbf{2} & 0 & \mathbf{5} \\ 1 & \mathbf{2} & \mathbf{0} & 0 & \mathbf{1} \\ 1 & \mathbf{4} & \mathbf{2} & 7 & \mathbf{6} \end{pmatrix}$$

ha rango maggiore o uguale a 3 in quanto contiene un minore 3×3 (quello individuato dalle righe seconda, terza e quarta e dalle colonne seconda, terza e quinta, ovvero dai coefficienti in grassetto) che ha determinante diverso da 0 (è uguale a -2, come abbiamo calcolato nel paragrafo precedente).

Inoltre, poiché tutti i minori 4×4 hanno determinante uguale a zero, la matrice ha rango esattamente 3. Quest'ultima verifica richiede il controllo del determinante di 5 minori. È più rapido osservare che la prima riga è uguale alla somma delle altre tre righe, dunque il rango è minore o uguale a 3: poiché dal calcolo del determinante del minore 3×3 sappiamo che il rango è maggiore o uguale a 3, allora è esattamente 3.

Il calcolo del rango attraverso il Teorema 6.8 può richiedere molte verifiche, ed è in generale meno conveniente della riduzione di Gauss. Il seguente teorema può comunque aiutare a ridurre i determinanti da calcolare:

TEOREMA 6.11 (Teorema degli orlati). *Data una matrice $A = (a_{ij}) \in \text{Mat}_{n \times m}(\mathbb{K})$, supponiamo che esista un minore K di formato $k \times k$ (con $k < n$ e $k < m$) il cui determinante è diverso da 0. Se sono uguali a 0 tutti i determinanti dei minori di formato $(k+1) \times (k+1)$ che si ottengono aggiungendo una riga e una colonna a quelle scelte per formare il minore K , allora il rango di A è uguale a k , altrimenti è strettamente maggiore di k .*

Dunque se abbiamo un minore di formato $k \times k$ con determinante diverso da 0 e vogliamo decidere se la matrice ha rango k oppure ha rango strettamente maggiore di k basta controllare $(n-k)(m-k)$ minori di formato $(k+1) \times (k+1)$, non tutti i $\binom{n}{k+1}\binom{m}{k+1}$ minori di formato $(k+1) \times (k+1)$. Per rendersi conto del ‘risparmio’, anche con matrici piccole, consideriamo una matrice A di formato 5×6 e supponiamo di conoscere un minore 3×3 con determinante diverso da 0. Per controllare se la matrice ha rango 3 basta controllare i determinanti dei 6 minori 4×4 che si ottengono “orlando” il minore dato con una riga e una colonna in più; non occorre calcolare i determinanti di tutti i 75 minori 4×4 di A .

3. Il teorema di Binet

Il determinante non è una applicazione lineare (a parte il caso banale delle matrici 1×1). In particolare in generale $\text{Det}(A+B) \neq \text{Det}(A) + \text{Det}(B)$. Vale invece il seguente:

TEOREMA 6.12 (Teorema di Binet²). *Siano $A, B \in \text{Mat}_{n \times n}(\mathbb{K})$. Allora*

$$\text{Det}(AB) = \text{Det}(A)\text{Det}(B)$$

Come prima applicazione osserviamo

COROLLARIO 6.13. *Se $M \in \text{Mat}_{n \times n}(\mathbb{K})$ è una matrice invertibile, allora*

$$\text{Det}(M^{-1}) = \frac{1}{\text{Det}(M)}$$

DIMOSTRAZIONE. Calcoliamo $\text{Det}(M^{-1}M)$. Per il Teorema di Binet vale $\text{Det}(M^{-1}M) = \text{Det}(M^{-1})\text{Det}(M)$. D'altra parte $M^{-1}M = I$ e $\text{Det}(I) = 1$. □

²Il nome deriva dal matematico francese Jacques Philippe Marie Binet (1786-1856).

Grazie al Teorema di Binet possiamo osservare che, dato un endomorfismo $L \in \text{End}(V)$, il determinante assume lo stesso valore su tutte le matrici che si associano a V al variare delle basi dello spazio, ossia vale:

$$\text{Det} \begin{pmatrix} [L] & v_1, v_2, \dots, v_n \\ v_1, v_2, \dots, v_n \end{pmatrix} = \text{Det} \begin{pmatrix} [L] & e_1, e_2, \dots, e_n \\ e_1, e_2, \dots, e_n \end{pmatrix}$$

per ogni scelta di due basi e_1, e_2, \dots, e_n e v_1, v_2, \dots, v_n di V .

Infatti, per il Teorema 5.8 possiamo scrivere:

$$\text{Det} \begin{pmatrix} [L] & v_1, v_2, \dots, v_n \\ v_1, v_2, \dots, v_n \end{pmatrix} = \text{Det} \begin{pmatrix} M^{-1}[L] & e_1, e_2, \dots, e_n & M \\ e_1, e_2, \dots, e_n & & \end{pmatrix}$$

A questo punto, per il Teorema di Binet e per il Corollario 6.13, possiamo concludere che

$$\begin{aligned} & \text{Det} \begin{pmatrix} [L] & v_1, v_2, \dots, v_n \\ v_1, v_2, \dots, v_n \end{pmatrix} = \\ & = \text{Det}(M^{-1}) \text{Det} \begin{pmatrix} [L] & e_1, e_2, \dots, e_n \\ e_1, e_2, \dots, e_n \end{pmatrix} \text{Det}(M) = \\ & = \text{Det} \begin{pmatrix} [L] & e_1, e_2, \dots, e_n \\ e_1, e_2, \dots, e_n \end{pmatrix} \end{aligned}$$

4. Proprietà del determinante rispetto alle mosse di riga e di colonna

Studiamo come cambia il determinante se facciamo una operazione elementare di riga o di colonna su una matrice $A \in \text{Mat}_{n \times n}(\mathbb{K})$. Ricordiamo che le operazioni elementari di colonna sono di tre tipi:

- si somma alla colonna i la colonna j moltiplicata per uno scalare λ ;
- si moltiplica la colonna s per uno scalare $k \neq 0$;
- si permutano fra di loro due colonne, diciamo la i e la j .

Una operazione del primo tipo corrisponde a moltiplicare A a destra per la matrice $n \times n$ (chiamata $M_{ij\lambda}$ nel Paragrafo 4 del Capitolo 2) che ha tutti 1 sulla diagonale, e 0 in tutte le altre caselle eccetto che nella casella identificata da “riga j , colonna i ”, dove troviamo λ . La matrice M_{ij} è triangolare e il suo determinante è uguale a 1, dunque $\text{Det}(AM_{ij})$ è uguale a $\text{Det}(A)$ per il Teorema di Binet.

Analogamente, si osserva che una operazione di colonna del terzo tipo ha come effetto quello di cambiare il segno del determinante.

Quanto alle operazioni del secondo tipo, dalla definizione stessa di determinante si ricava che, se si moltiplica una colonna per uno scalare $k \neq 0$, anche il determinante della matrice risulterà moltiplicato per k (per convincersene basta calcolare il determinante proprio a partire da quella colonna).

Considerazioni analoghe valgono, ovviamente, per le operazioni elementari di riga.

Una conseguenza di queste osservazioni è che se vogliamo solo sapere se il determinante di una certa matrice è uguale a 0 oppure no (come capita quando ci interessa solo calcolare il rango, oppure in altre situazioni che incontreremo nei prossimi capitoli) possiamo, prima di calcolarlo, fare alcune operazioni di riga e/o di colonna. Di solito questo risulta utile se con tali operazioni otteniamo una riga, o una colonna, con molti coefficienti uguali a 0, facilitando il calcolo.

5. Altri esercizi

ESERCIZIO 6.14. Dimostrare che il determinante della seguente *matrice di Vandermonde*³ di formato $n \times n$ (con $n \geq 2$)

$$\begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ b_1 & b_2 & b_3 & \dots & b_n \\ b_1^2 & b_2^2 & b_3^2 & \dots & b_n^2 \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ b_1^{n-1} & b_2^{n-1} & b_3^{n-1} & \dots & b_n^{n-1} \end{pmatrix}$$

è uguale a $\prod_{i < j} (b_j - b_i)$, ossia al prodotto di tutte le possibili differenze fra i b_i (col segno opportuno, come risulta dalla formula). In particolare, se i b_i sono a due a due distinti, il determinante è diverso da 0 e la matrice è invertibile.

ESERCIZIO 6.15. Ripensare al fatto che una matrice di Vandermonde interviene nel metodo, illustrato nella prima parte del corso, per trovare una formula per le successioni definite per ricorrenza lineare e a coefficienti costanti.

ESERCIZIO 6.16. Sia A una matrice 2×2 a valori in \mathbb{R} .

- (1) Dimostrare che esiste una matrice B , di formato 2×2 , a valori in \mathbb{R} , diversa dalla matrice nulla, tale che $AB = 0$ se e solo se il determinante di A è uguale a 0.
- (2) Il risultato precedente è vero anche per le matrici $n \times n$?

ESERCIZIO 6.17. Sia L un endomorfismo lineare dello spazio vettoriale V , sia A la matrice corrispondente all'endomorfismo L in una base fissata

³Il nome deriva dal matematico francese Alexandre-Theophile Vandermonde (1735-1796)

di V e sia $\text{Det}(A) = 0$. Dire, giustificando la risposta, quali delle seguenti affermazioni sono vere e quali false:

- (1) L'endomorfismo L non è surgettivo.
- (2) $\text{Ker } L = \{O\}$.
- (3) In una riduzione a scalini per righe di A almeno una riga è nulla.
- (4) La matrice A ha almeno uno 0 sulla diagonale principale.
- (5) Esiste una base \mathcal{B} di V per cui la matrice associata ad L rispetto a \mathcal{B} ha la prima colonna tutta di zeri.

Diagonalizzazione di endomorfismi lineari

1. Autovalori e autovettori di un endomorfismo lineare

Sia $T : V \rightarrow V$ un endomorfismo lineare dello spazio vettoriale V sul campo \mathbb{K} .

DEFINIZIONE 7.1. Un vettore $v \in V - \{O\}$ si dice un autovettore di T se

$$T(v) = \lambda v$$

per un certo $\lambda \in \mathbb{K}$.

In altre parole un autovettore di T è un vettore **diverso da O** dello spazio V che ha la seguente proprietà: la T lo manda in un multiplo di sé stesso.

DEFINIZIONE 7.2. Se $v \in V - \{O\}$ è un autovettore di T tale che

$$T(v) = \lambda v$$

allora lo scalare $\lambda \in \mathbb{K}$ si dice autovalore di T relativo a v (e viceversa si dirà che v è un autovettore relativo all'autovalore λ).

Si noti che l'autovalore può essere $0 \in \mathbb{K}$: se per esempio T non è iniettiva, ossia $\text{Ker } T \supsetneq \{O\}$, tutti gli elementi $w \in (\text{Ker } T) - \{O\}$ soddisfano

$$T(w) = O = 0 w$$

ossia sono autovettori relativi all'autovalore 0.

DEFINIZIONE 7.3. Dato $\lambda \in \mathbb{K}$ chiamiamo l'insieme

$$V_\lambda = \{v \in V \mid T(v) = \lambda v\}$$

autospazio relativo a λ .

ESERCIZIO 7.4. Verificare che un autospazio V_λ è un sottospazio vettoriale di V .

OSSERVAZIONE 7.5. In particolare abbiamo notato poco fa che $V_0 = \text{Ker } T$.

Anche se abbiamo definito l'autospazio V_λ per qualunque $\lambda \in \mathbb{K}$, in realtà V_λ è sempre uguale a $\{O\}$ a meno che λ non sia un autovalore. Questo è dunque il caso interessante: se λ è un autovalore di T allora V_λ è costituito da O e da tutti gli autovettori relativi a λ .

Perché per noi sono importanti autovettori e autovalori ?

Supponiamo che V abbia dimensione n e pensiamo a cosa succederebbe se riuscissimo a trovare una base di V , $\{v_1, v_2, \dots, v_n\}$, composta solo da autovettori di T .

Avremmo, per ogni $i = 1, 2, \dots, n$,

$$T(v_i) = \lambda_i v_i$$

per certi autovalori λ_i (sui quali non abbiamo informazioni, per esempio potrebbero anche essere tutti uguali $\lambda_1 = \dots = \lambda_n$).

Come sarebbe fatta la matrice

$$[T] \begin{matrix} v_1, v_2, \dots, v_n \\ v_1, v_2, \dots, v_n \end{matrix}$$

associata a T rispetto a questa base ?

Ricordandosi come si costruiscono le matrici osserviamo che la prima colonna conterrebbe il vettore $T(v_1)$ scritto in termini della base $\{v_1, v_2, \dots, v_n\}$, ossia

$$T(v_1) = \lambda_1 v_1 + 0v_2 + 0v_3 + 0v_4 + \dots + 0v_n$$

la seconda il vettore $T(v_2) = 0v_1 + \lambda_2 v_2 + 0v_3 + \dots + 0v_n$ e così via. Quindi la matrice sarebbe diagonale:

$$[T] \begin{matrix} v_1, v_2, \dots, v_n \\ v_1, v_2, \dots, v_n \end{matrix} = \begin{pmatrix} \lambda_1 & 0 & 0 & \dots & 0 & 0 \\ 0 & \lambda_2 & 0 & \dots & 0 & 0 \\ 0 & 0 & \lambda_3 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \lambda_{n-1} & 0 \\ 0 & 0 & 0 & \dots & 0 & \lambda_n \end{pmatrix}$$

Ora, una matrice diagonale è per noi "leggibilissima"; a colpo d'occhio possiamo sapere tutto di T : il suo rango (dunque anche la dimensione del nucleo), quali sono esattamente i vettori di $\text{Ker } T$, quali sono (se esistono) i sottospazi in cui T si comporta come l'identità, ossia i sottospazi costituiti dai vettori di V che T lascia fissi...

Dunque studiamo gli autovalori e gli autovettori di T nella speranza di trovare "basi buone" che ci permettano di conoscere bene il comportamento di T .

Ma esistono sempre queste "basi buone", ossia basi costituite solo da autovettori di T ? NO, non sempre. Se per un certo endomorfismo T esiste una base buona si dice che T è *diagonalizzabile*, altrimenti T è *non diagonalizzabile*.

ESEMPIO 7.6. Consideriamo l'endomorfismo $R_\theta : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ dato da una *rotazione* di angolo θ con centro l'origine. Si verifica immediatamente

che, rispetto alla base standard di \mathbb{R}^2 , questo endomorfismo è rappresentato dalla matrice

$$[R_\theta] = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$$

Per esempio, nel caso di una rotazione di 60° (ovvero $\frac{\pi}{3}$), abbiamo:

$$[R_{\frac{\pi}{3}}] = \begin{pmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix}$$

Nel caso in cui $0 < \theta < \pi$, non ci sono vettori $v \neq O$ che vengono mandati in un multiplo di se stessi, visto che tutti i vettori vengono ruotati di un angolo che non è nullo e non è di 180° . Dunque non ci sono autovettori e autovalori.

Nel caso $\theta = 0$ la rotazione è l'identità, dunque tutti i vettori $v \neq O$ sono autovettori relativi all'autovalore 1, e $V_1 = \mathbb{R}^2$.

Nel caso $\theta = \pi$ la rotazione è uguale a $-I$, dunque tutti i vettori $v \neq O$ sono autovettori relativi all'autovalore -1, e $V_{-1} = \mathbb{R}^2$.

ESEMPIO 7.7. Consideriamo l'endomorfismo $T : \mathbb{C}^2 \rightarrow \mathbb{C}^2$ che, rispetto alla base standard di \mathbb{C}^2 , è rappresentato dalla matrice

$$[T] = \begin{pmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix}$$

Si tratta della stessa matrice che nell'esempio precedente era associata alla rotazione di $\frac{\pi}{3}$ nel piano reale ma stavolta, visto che stiamo considerando uno spazio vettoriale complesso, riusciamo a trovare autovettori e autovalori per T . Si verifica infatti (esercizio!) che il vettore $\begin{pmatrix} \iota \\ 1 \end{pmatrix}$ è un autovettore relativo all'autovalore $\frac{1+\iota\sqrt{3}}{2}$ e che il vettore $\begin{pmatrix} -\iota \\ 1 \end{pmatrix}$ è un autovettore relativo all'autovalore $\frac{1-\iota\sqrt{3}}{2}$. Poiché i due vettori sono linearmente indipendenti sul campo \mathbb{C} , costituiscono una base. Dunque T è diagonalizzabile e

$$V_{\frac{1+\iota\sqrt{3}}{2}} = \left\langle \begin{pmatrix} \iota \\ 1 \end{pmatrix} \right\rangle$$

$$V_{\frac{1-\iota\sqrt{3}}{2}} = \left\langle \begin{pmatrix} -\iota \\ 1 \end{pmatrix} \right\rangle$$

$$\mathbb{C}^2 = V_{\frac{1-\iota\sqrt{3}}{2}} \oplus V_{\frac{1+\iota\sqrt{3}}{2}}.$$

2. Il polinomio caratteristico di un endomorfismo

Vogliamo trovare dei criteri semplici che ci permettano di decidere se un endomorfismo è diagonalizzabile o no. Un buon primo passo è quello di avere un metodo che, dato un endomorfismo $T : V \rightarrow V$ e posto $n = \dim V$, ci permetta di decidere se uno scalare $\lambda \in \mathbb{K}$ è o no un autovalore di T . Entrano qui in gioco i polinomi e le loro radici.

Innanzitutto osserviamo che, perché $\lambda \in \mathbb{K}$ sia un autovalore, secondo la definizione bisogna che esista un $v \in V - \{O\}$ tale che

$$T(v) = \lambda v.$$

Questo si può riscrivere anche come

$$T(v) - \lambda I(v) = O$$

dove $I : V \rightarrow V$ è l'identità. Riscriviamo ancora:

$$(T - \lambda I)(v) = O$$

Abbiamo scoperto che, se T possiede un autovalore λ , allora l'endomorfismo $T - \lambda I$ non è iniettivo: infatti manda il vettore v in O . Dunque, se scegliamo una base qualunque per V e costruiamo la matrice $[T]$ associata a T , la matrice $[T - \lambda I] = [T] - \lambda I$ dovrà avere determinante uguale a 0 (vedi l'Osservazione 6.9):

$$\det([T] - \lambda I) = 0 = \det(\lambda I - [T])$$

dove come consuetudine abbiamo indicato con I anche la matrice identità.

Questa osservazione è la premessa per la seguente definizione:

DEFINIZIONE 7.8. Dato un endomorfismo lineare $T : V \rightarrow V$ con $n = \dim V$, scegliamo una base per V e costruiamo la matrice $[T]$ associata a T rispetto a tale base. Il polinomio caratteristico $P_T(t) \in \mathbb{K}[t]$ dell'endomorfismo T è definito da:

$$P_T(t) = \det(t[I] - [T]).$$

OSSERVAZIONE 7.9. 1) Perché la definizione data abbia senso innanzitutto bisogna verificare che $\det(t[I] - [T])$ sia veramente un polinomio. Questo si può dimostrare facilmente per induzione sulla dimensione n di V . Sempre per induzione si può dimostrare un po' di più, ossia che $P_T(t)$ è un polinomio di grado n con coefficiente direttore 1: $P_T(t) = t^n + \dots$. Provate a fare questi esercizi!

2) È fondamentale inoltre che la definizione appena data non dipenda dalla base scelta di V : non sarebbe una definizione buona se con la scelta di due basi diverse ottenessimo due polinomi caratteristici diversi.

Questo problema per fortuna non si verifica. Infatti, se scegliamo due basi b e b' di V , come sappiamo dal Teorema 5.8, le due matrici $[T]_b$ e $[T]_{b'}$

$[T]_{b'}$ sono legate dalla seguente relazione: esiste una matrice $[B]$ invertibile tale che

$$[T]_{b'} = [B]^{-1} [T]_{b'} [B]$$

Usando il teorema di Binet (Teorema 6.12) a questo punto verifichiamo che

$$\begin{aligned} \det \begin{pmatrix} tI - [T]_{b'} & \\ & b' \end{pmatrix} &= \det \begin{pmatrix} tI - [B]^{-1} [T]_{b'} [B] & \\ & b' \end{pmatrix} = \det \left([B]^{-1} \begin{pmatrix} tI - [T]_{b'} & \\ & b' \end{pmatrix} [B] \right) = \\ &= \det([B]^{-1}) \det \begin{pmatrix} tI - [T]_{b'} & \\ & b' \end{pmatrix} \det([B]) = \det \begin{pmatrix} tI - [T]_{b'} & \\ & b' \end{pmatrix} \end{aligned}$$

Abbiamo dunque mostrato che $P_T(t) = \det(tI - [T])$ non dipende dalla scelta della base.

ESERCIZIO 7.10. Grazie all'osservazione precedente, sappiamo in particolare che i coefficienti di $p_T(t)$ non dipendono dalla base scelta. Chiamiamo dunque

$$C_r : \text{End}(V) \rightarrow \mathbb{K}$$

la funzione che, ad ogni endomorfismo T associa il coefficiente di t^r in $P_T(t)$. Dimostrare che C_{n-1} è uguale a meno la traccia ossia $C_{n-1}(T) = -\mathcal{T}(T)$ (per la funzione traccia vedi il Paragrafo 3 del Capitolo 5) e che C_0 è uguale, a meno del segno, al determinante ossia $C_0(T) = \pm \text{Det}(T)$. Il polinomio caratteristico ci fornisce dunque l'esempio di altre funzioni che, come il determinante e la traccia, coinvolgono i coefficienti di una matrice $[T]$ ma in realtà non dipendono dalla base scelta.

ESERCIZIO 7.11. Usando le stesse notazioni dell'esercizio precedente, calcolare la funzione C_1 nel caso in cui $\dim V = 3$, ossia in cui la matrice $[T]$ sia 3×3 .

Possiamo a questo punto enunciare il teorema principale che spiega l'utilità del polinomio caratteristico ai fini del problema della diagonalizzazione.

TEOREMA 7.12. *Considerato T come sopra, vale che uno scalare $\lambda \in \mathbb{K}$ è un autovalore di T se e solo se λ è una radice di $P_T(t)$, ossia se e solo se $P_T(\lambda) = 0$*

DIMOSTRAZIONE. Abbiamo già visto (l'osservazione prima della definizione del polinomio caratteristico) che se λ è un autovalore di T allora $\det(\lambda I - [T]) = P_T(\lambda) = 0$.

Resta dunque da dimostrare il viceversa. Supponiamo che $\det(\lambda I - [T]) = P_T(\lambda) = 0$: allora l'applicazione lineare $\lambda I - T$ non è iniettiva. Dunque

esiste $v \in V - \{O\}$ tale che $(\lambda I - T)(v) = 0$. Questo si può riscrivere anche come

$$T(v) = \lambda v$$

Abbiamo trovato un autovettore che ha autovalore λ e quindi abbiamo mostrato, come volevamo, che λ è un autovalore di T . \square

ESEMPIO 7.13. Consideriamo l'endomorfismo T dell'Esempio 7.7. Il suo polinomio caratteristico risulta $P_T(t) = t^2 - t + 1$ (verificare!). Questo polinomio ha due radici in \mathbb{C} , ovvero $\frac{1-i\sqrt{3}}{2}$ e $\frac{1+i\sqrt{3}}{2}$, che in effetti, come sappiamo, sono gli autovalori di T .

Notiamo che $t^2 - t + 1$ non ha invece radici in \mathbb{R} , coerentemente col fatto, osservato nell'Esempio 7.6, che la rotazione $R_{\frac{\pi}{3}}$ del piano reale non ammette autovettori.

ESERCIZIO 7.14. Sia $F : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ l'applicazione lineare definita, nella base standard di \mathbb{R}^2 , dalla matrice:

$$[F] = \begin{pmatrix} -1 & 0 \\ 2 & 1 \end{pmatrix}$$

Calcolare $P_F(t)$.

ESERCIZIO 7.15. Sia $F : \mathbb{C}^3 \rightarrow \mathbb{C}^3$ l'applicazione lineare definita, nella base standard di \mathbb{C}^3 , dalla matrice:

$$[F] = \begin{pmatrix} -1 & 0 & 2 \\ 2i & 1 & 2i \\ 1 & 0 & 0 \end{pmatrix}$$

Calcolare $P_F(t)$.

ESERCIZIO 7.16. Sia $F : \mathbb{C}^4 \rightarrow \mathbb{C}^4$ l'applicazione lineare definita, nella base standard di \mathbb{C}^4 , dalla matrice:

$$[F] = \begin{pmatrix} -1 & 0 & 2 & 0 \\ 0 & 1 & 2i & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 3 & 0 & 0 \end{pmatrix}$$

Calcolare $P_F(t)$.

3. Una strategia per scoprire se un endomorfismo è diagonalizzabile

In questo paragrafo descriviamo una strategia in quattro passi che ci permette di scoprire se un endomorfismo $T : V \rightarrow V$, dove V è uno spazio vettoriale sul campo \mathbb{K} di dimensione n , è diagonalizzabile, e, in caso sia diagonalizzabile, di trovare una base che lo diagonalizza, ossia una base di V fatta tutta da autovettori di T . La nostra strategia sarà la seguente:

- PASSO 1. Data T , troviamo gli autovalori di T utilizzando il polinomio caratteristico.
- PASSO 2. Supponiamo di aver trovato gli autovalori $\lambda_1, \lambda_2, \dots, \lambda_k$: a questo punto scopriamo chi sono i relativi autospazi $V_{\lambda_1}, V_{\lambda_2}, \dots, V_{\lambda_k}$.
- PASSO 3. Un teorema (vedi Teorema 7.19) ci assicurerà che gli autospazi $V_{\lambda_1}, V_{\lambda_2}, \dots, V_{\lambda_k}$ sono in somma diretta (vedi Paragrafo 3 del Capitolo 4). Quindi se

$$V_{\lambda_1} \oplus V_{\lambda_2} \oplus \dots \oplus V_{\lambda_k} = V$$

allora è possibile trovare una base “buona”, fatta da autovettori di T e T è diagonalizzabile. Per scrivere una base “buona” basta scegliere una base per ogni V_{λ_i} e poi fare l’unione. Altrimenti, se

$$V_{\lambda_1} \oplus V_{\lambda_2} \oplus \dots \oplus V_{\lambda_k} \subsetneq V$$

T non è diagonalizzabile.

- PASSO 4. Se T è risultata diagonalizzabile, usando la base trovata si scrive la matrice diagonale $[T]$.

Vediamo i dettagli passo per passo.

3.1. Passo 1. Di questo ci siamo già occupati nel paragrafo precedente: per sapere quali sono gli autovalori di un endomorfismo T possiamo calcolare il polinomio caratteristico $P_T(t)$ e trovare le sue radici in \mathbb{K} .

3.2. Passo 2. Supponiamo dunque di aver scoperto che T ha i seguenti autovalori: $\lambda_1, \lambda_2, \dots, \lambda_k$, tutti distinti fra loro. Vogliamo individuare gli autospazi $V_{\lambda_1}, V_{\lambda_2}, \dots, V_{\lambda_k}$.

Per questo basterà risolvere dei sistemi lineari: per ogni $i = 1, 2, \dots, k$, l’autospazio V_{λ_i} è costituito per definizione dai vettori $v \in V$ tali che $T(v) = \lambda_i v$, ossia, scelta una base di V e dunque trovata la matrice $[T]$, dalle soluzioni del sistema lineare

$$([T] - \lambda_i I) \begin{pmatrix} x_1 \\ x_2 \\ \dots \\ \dots \\ x_{n-1} \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \dots \\ \dots \\ 0 \\ 0 \end{pmatrix}$$

3.3. Passo 3. Cominciamo col dimostrare il seguente teorema.

TEOREMA 7.17. *Dato un endomorfismo lineare $T : V \rightarrow V$, siano $\lambda_1, \lambda_2, \dots, \lambda_k$ degli autovalori di T distinti fra loro. Consideriamo ora degli autovettori $v_1 \in V_{\lambda_1}, v_2 \in V_{\lambda_2}, \dots, v_k \in V_{\lambda_k}$. Allora $\{v_1, v_2, \dots, v_k\}$ è un insieme di vettori linearmente indipendenti.*

OSSERVAZIONE 7.18. Spesso ci si riferisce a questo teorema con la frase: “autovettori relativi ad autovalori distinti sono linearmente indipendenti”.

DIMOSTRAZIONE. Procediamo per induzione su k . Per $k = 1$ l’enunciato è banale perché $\{v_1\}$ è un insieme di vettori linearmente indipendenti (c’è un vettore solo... ed è diverso da O perché è un autovettore). Supponiamo di aver dimostrato che l’enunciato è vero fino al caso di $k - 1$ vettori e cerchiamo di dimostrarlo per k . Supponiamo allora di avere un insieme di vettori $\{v_1, v_2, \dots, v_k\}$ come nelle ipotesi e che valga:

$$(3.1) \quad a_1v_1 + a_2v_2 + \dots + a_kv_k = O$$

Per mostrare che $\{v_1, v_2, \dots, v_k\}$ è un insieme di vettori linearmente indipendenti dobbiamo mostrare che questo può accadere solo quando $a_1 = a_2 = \dots = a_k = 0$.

Dalla equazione scritta ne ricaviamo due in due modi diversi. Prima applichiamo T ad entrambi i membri e per linearità otteniamo

$$a_1T(v_1) + a_2T(v_2) + \dots + a_kT(v_k) = O$$

che svolgendo il calcolo diventa

$$a_1\lambda_1v_1 + a_2\lambda_2v_2 + \dots + a_k\lambda_kv_k = O$$

Poi invece moltiplichiamo l’equazione per λ_k ottenendo:

$$a_1\lambda_kv_1 + a_2\lambda_kv_2 + \dots + a_k\lambda_kv_k = O$$

Per sottrazione da queste due equazioni ricaviamo:

$$a_1(\lambda_k - \lambda_1)v_1 + a_2(\lambda_k - \lambda_2)v_2 + \dots + a_{k-1}(\lambda_k - \lambda_{k-1})v_{k-1} = O$$

Ma questa è una combinazione lineare dei $k - 1$ vettori $\{v_1, v_2, \dots, v_{k-1}\}$ uguale a O : per ipotesi induttiva tutti i coefficienti devono essere uguali a 0 . Visto che gli scalari $\lambda_k - \lambda_i$ sono tutti diversi da zero (gli autovalori in questione sono distinti fra loro per ipotesi) questo implica che $a_1 = a_2 = \dots = a_{k-1} = 0$. Sostituendo nella equazione iniziale (3.1), notiamo che deve essere anche $a_k = 0$. \square

Il seguente teorema è un rafforzamento del precedente.

TEOREMA 7.19. *Dato un endomorfismo lineare $T : V \rightarrow V$, siano $\lambda_1, \lambda_2, \dots, \lambda_k$ degli autovalori di T distinti fra loro. Allora gli autospazi $V_{\lambda_1}, V_{\lambda_2}, \dots, V_{\lambda_k}$ sono in somma diretta.*

DIMOSTRAZIONE. Ricordiamo (vedi Paragrafo 3 del Capitolo 4) che dire che gli autospazi $V_{\lambda_1}, V_{\lambda_2}, \dots, V_{\lambda_k}$ sono in somma diretta vuol dire che se ne prendiamo uno qualunque, diciamo V_{λ_1} tanto per fissare la notazione, la sua intersezione con la somma di tutti gli altri è banale, ossia

$$V_{\lambda_1} \cap (V_{\lambda_2} + \dots + V_{\lambda_k}) = \{O\}.$$

Supponiamo per assurdo che non sia così, e che ci sia un vettore $w \neq O$ tale che

$$w \in V_{\lambda_1} \cap (V_{\lambda_2} + \dots + V_{\lambda_k})$$

Allora possiamo scrivere w in due modi:

$$w = v_1 \in V_{\lambda_1} - \{O\}$$

perché $w \in V_{\lambda_1}$, e

$$w = v_2 + v_3 + \dots + v_k$$

(dove i $v_j \in V_{\lambda_j}$ per ogni j) visto che $w \in V_{\lambda_2} + \dots + V_{\lambda_k}$. Alcuni dei vettori v_j potrebbero essere uguali a O , ma non tutti (se fossero tutti uguali a O allora anche w sarebbe uguale a O). Diciamo che, a meno di riordinamenti, i vettori diversi da zero siano v_2, \dots, v_s , con $s \leq k$.

Dunque vale:

$$v_1 = w = v_2 + v_3 + \dots + v_s$$

Da questa uguaglianza ricaviamo la relazione

$$v_1 - v_2 - v_3 - \dots - v_s = O$$

che rivela che gli autovettori $\{v_1, \dots, v_s\}$ sono linearmente dipendenti, assurdo perché contraddice il Teorema 7.17 (si tratta di autovettori relativi ad autovalori distinti). \square

Nelle ipotesi del teorema precedente sappiamo allora (vedi Esercizio 4.12), che la dimensione della somma degli autospazi è “la massima possibile”, ossia

$$\dim (V_{\lambda_1} \oplus V_{\lambda_2} \oplus \dots \oplus V_{\lambda_k}) = \dim V_{\lambda_1} + \dim V_{\lambda_2} + \dots + \dim V_{\lambda_k}$$

Osserviamo che abbiamo dunque già ottenuto un criterio per dire se T è diagonalizzabile o no. Infatti, se

$$\dim V_{\lambda_1} + \dim V_{\lambda_2} + \dots + \dim V_{\lambda_k} = n = \dim V$$

allora

$$V_{\lambda_1} \oplus V_{\lambda_2} \oplus \dots \oplus V_{\lambda_k} = V$$

e quindi è possibile trovare una base “buona”, fatta da autovettori di T , insomma T è diagonalizzabile.

Per scrivere una simile base “buona”, come sappiamo dal Paragrafo 3 del Capitolo 4, basta scegliere una base per ogni V_{λ_i} e poi fare l’unione.

Altrimenti, se

$$(3.2) \quad \dim V_{\lambda_1} + \dim V_{\lambda_2} + \dots + \dim V_{\lambda_k} < n = \dim V$$

T non è diagonalizzabile. Infatti non è possibile trovare una base di autovettori: se la trovassimo contraddiremmo la (3.2).

3.4. Passo 4. Se l'endomorfismo T è diagonalizzabile, scegliamo dunque una base di autovettori nel modo descritto al Passo 3, e avremo una matrice associata $[T]$ che risulterà diagonale. Manteniamo le notazioni introdotte al Passo 3: allora sulla diagonale troveremo $\dim V_{\lambda_1}$ coefficienti uguali a λ_1 , $\dim V_{\lambda_2}$ coefficienti uguali a λ_2 , \dots , $\dim V_{\lambda_k}$ coefficienti uguali a λ_k .

Il rango di T sarà uguale al numero dei coefficienti non zero che troviamo sulla diagonale di $[T]$, la dimensione del nucleo sarà uguale al numero dei coefficienti uguali a zero che troviamo sulla diagonale di $[T]$.

4. Il criterio della molteplicità algebrica e della molteplicità geometrica

Nel paragrafo precedente abbiamo descritto un algoritmo che ci permette di decidere se un endomorfismo è diagonalizzabile o no. In questo paragrafo faremo una osservazione che ci permetterà di riformulare questo algoritmo e di individuare alcune “scorciatoie”.

Consideriamo come al solito un endomorfismo $T : V \rightarrow V$, dove V è uno spazio vettoriale sul campo \mathbb{K} con $n = \dim V$.

Calcoliamo il suo polinomio caratteristico e fattorizziamolo in $\mathbb{K}[t]$. Otterremo una espressione del tipo:

$$P_T(t) = (t - \lambda_1)^{a_1} (t - \lambda_2)^{a_2} \dots (t - \lambda_k)^{a_k} f(t)$$

dove $\lambda_1, \lambda_2, \dots, \lambda_k$ sono gli autovalori di T in \mathbb{K} e sono tutti distinti fra loro, e $f(t)$ o è 1 oppure è un polinomio irriducibile in $\mathbb{K}[t]$ di grado > 1 .

Se la T è diagonalizzabile, allora esiste una base b di V in cui la matrice associata $[T]_b$ ha forma diagonale e sulla diagonale compaiono $\lambda_1, \lambda_2, \dots, \lambda_k$.

Più esattamente, per ogni $i = 1, 2, \dots, k$, λ_i compare $\dim V_{\lambda_i}$ volte. Dunque in questo caso possiamo ricalcolare il polinomio caratteristico P_T usando $[T]_b$:

$$P_T(t) = \text{Det} (tI - [T]_b)$$

Si tratta di calcolare il determinante di una matrice diagonale e si osserva allora che P_T si spezza nel prodotto di fattori lineari:

$$P_T(t) = (t - \lambda_1)^{\dim V_{\lambda_1}} (t - \lambda_2)^{\dim V_{\lambda_2}} \dots (t - \lambda_k)^{\dim V_{\lambda_k}}$$

il che dimostra che il fattore $f(t)$ è 1.

In sintesi:

PROPOSIZIONE 7.20. *Se l'endomorfismo T è diagonalizzabile sul campo \mathbb{K} , allora il suo polinomio caratteristico $P_T(t)$ si fattorizza come prodotto di fattori lineari in $\mathbb{K}[t]$:*

$$P_T(t) = (t - \lambda_1)^{\dim V_{\lambda_1}} (t - \lambda_2)^{\dim V_{\lambda_2}} \cdots (t - \lambda_k)^{\dim V_{\lambda_k}}$$

Dunque se nella fattorizzazione di P_T rimane un fattore irriducibile $f(T)$ di grado > 1 possiamo concludere che T non è diagonalizzabile. Ma cosa possiamo dire del viceversa? Se P_T si fattorizza come prodotto di fattori lineari in $\mathbb{K}[t]$ allora T è diagonalizzabile? NO, in generale non è vero. Basta considerare per esempio l'applicazione lineare $L : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ che nelle basi standard è rappresentata dalla matrice

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

Il polinomio caratteristico è $P_L(t) = (t-2)^2$ ma l'applicazione non è diagonalizzabile: possiamo verificarlo applicando il criterio del paragrafo precedente, infatti L ha il solo autospazio V_2 e se ne calcoliamo la dimensione scopriamo che $\dim V_2 = 1 < 2 = \dim \mathbb{R}^2$.

Prima di enunciare il nuovo criterio diamo qualche definizione:

DEFINIZIONE 7.21. Data T come sopra con polinomio caratteristico

$$P_T(t) = (t - \lambda_1)^{a_1} (t - \lambda_2)^{a_2} \cdots (t - \lambda_k)^{a_k} f(t)$$

dove $f(t)$ o è 1 oppure è un polinomio irriducibile in $\mathbb{K}[t]$ di grado > 1 , diremo che, per ogni $i = 1, 2, \dots, k$, a_i è la *molteplicità algebrica* dell'autovalore λ_i . Chiameremo invece *molteplicità geometrica* dell'autovalore λ_i il numero intero positivo $\dim V_{\lambda_i}$.

PROPOSIZIONE 7.22. *Dati $T : V \rightarrow V$ e*

$$P_T(t) = (t - \lambda_1)^{a_1} (t - \lambda_2)^{a_2} \cdots (t - \lambda_k)^{a_k} f(t)$$

come sopra, per ogni autovalore λ_i vale che la sua molteplicità geometrica è minore o uguale alla sua molteplicità algebrica:

$$\dim V_{\lambda_i} \leq a_i$$

DIMOSTRAZIONE. Nella proposizione precedente abbiamo già visto che se l'applicazione T è diagonalizzabile, allora vale

$$\dim V_{\lambda_i} = a_i \quad \forall i = 1, 2, \dots, k$$

Se invece T non è diagonalizzabile, ricordando che gli autospazi sono in somma diretta

$$V_{\lambda_1} \oplus V_{\lambda_2} \oplus \cdots \oplus V_{\lambda_k}$$

possiamo cominciare a costruire una base di V prendendo una base per ogni V_{λ_i} e facendo l'unione b' . Poiché in questo caso

$$\dim V_{\lambda_1} \oplus V_{\lambda_2} \oplus \cdots \oplus V_{\lambda_k} < \dim V$$

b' non è ancora una base di V , ma è solo un insieme di vettori linearmente indipendenti; possiamo allora, per il teorema di completamento (Teorema 2.19), scegliere degli elementi s_1, \dots, s_r tali che $b = b' \cup \{s_1, \dots, s_r\}$ sia una base. Rispetto a questa base la matrice di T ha la seguente forma:

$$[T]_{\substack{b \\ b}} = \begin{pmatrix} \lambda_1 & 0 & & & & & * & \dots & * & * \\ 0 & \lambda_1 & & & & & * & \dots & * & * \\ 0 & 0 & \dots & & & & & & & \\ 0 & 0 & & \dots & \dots & & & & & \\ \dots & \dots & & & & & & & & \\ \dots & \dots & & & & & & & & \\ \dots & & & & & & & & & \\ & & & & \dots & & 0 & & & \\ & & & & & & \lambda_k & 0 & * & \dots & * & * \\ & & & & & & & \lambda_k & * & \dots & * & * \\ & & & & & & & 0 & * & \dots & * & * \\ \dots & \dots & & & & & & 0 & * & \dots & * & * \\ 0 & 0 & & & & & & 0 & * & \dots & * & * \\ 0 & 0 & & & & & & 0 & * & \dots & * & * \end{pmatrix}$$

ossia ha una parte diagonale, dove troviamo λ_1 ripetuto $\dim V_{\lambda_1}$ volte, λ_2 ripetuto $\dim V_{\lambda_2}$ volte... λ_k ripetuto $\dim V_{\lambda_k}$ volte, e poi sulle ultime r colonne, che corrispondono a $T(s_1), T(s_2), \dots, T(s_r)$ non sappiamo dire nulla.

Osserviamo però che, sviluppando il determinante di $tI - [T]_{\substack{b \\ b}}$ a partire

dalla prima colonna, poi dalla seconda, poi dalla terza, e così via otteniamo:

$$P_T(t) = \text{Det} (tI - [T]_{\substack{b \\ b}}) = (t - \lambda_1)^{\dim V_{\lambda_1}} (t - \lambda_2)^{\dim V_{\lambda_2}} \dots (t - \lambda_k)^{\dim V_{\lambda_k}} \text{Det } M$$

dove M è il minore $r \times r$ che sta nell'angolo in basso a destra di $tI - [T]_{\substack{b \\ b}}$.

Ricordiamo ora la fattorizzazione in irriducibili per P_T

$$P_T(t) = (t - \lambda_1)^{a_1} (t - \lambda_2)^{a_2} \dots (t - \lambda_k)^{a_k} f(t)$$

L'unicità di tale fattorizzazione ci dice che la potenza massima di $(t - \lambda_1)$ che divide $P_T(t)$ è a_1 . Dunque, qualunque polinomio sia $\text{Det } M$, possiamo dire che, per ogni $i = 1, 2, \dots, k$, $\dim V_{\lambda_i} \leq a_i$. \square

Le disuguaglianze appena dimostrate implicano subito il risultato principale di questa sezione:

TEOREMA 7.23 (Criterio delle molteplicità algebrica e geometrica.). *Da-to un endomorfismo lineare $T : V \rightarrow V$ di uno spazio vettoriale V (di di-mensione finita n) sul campo \mathbb{K} , siano $\lambda_1, \lambda_2, \dots, \lambda_k$ gli autovalori (distinti fra loro) di T in \mathbb{K} . Allora T è diagonalizzabile se e solo se P_T si fattorizza*

come prodotto di fattori lineari e, per ogni autovalore λ_i , la sua molteplicità algebrica e quella geometrica sono uguali.

DIMOSTRAZIONE. Abbiamo già visto, nelle dimostrazioni delle proposizioni precedenti, che se T è diagonalizzabile allora P_T si fattorizza come prodotto di fattori lineari e, per ogni i

$$\text{molteplicità algebrica di } \lambda_i = \dim V_{\lambda_i}.$$

Viceversa, se P_T si fattorizza come prodotto di fattori lineari

$$P_T(t) = (t - \lambda_1)^{a_1} (t - \lambda_2)^{a_2} \cdots (t - \lambda_k)^{a_k}$$

e, per ogni autovalore λ_i , la sua molteplicità algebrica a_i e quella geometrica sono uguali, allora calcoliamo

$$\dim V_{\lambda_1} \oplus V_{\lambda_2} \oplus \cdots \oplus V_{\lambda_k}$$

Tale dimensione è uguale a

$$\sum_{i=1}^k \dim V_{\lambda_i}$$

ma per la nostra ipotesi

$$\sum_{i=1}^k \dim V_{\lambda_i} = \sum_{i=1}^k a_i$$

che è uguale al grado del polinomio caratteristico P_T , e dunque a $n = \dim V$. Allora

$$\dim V_{\lambda_1} \oplus V_{\lambda_2} \oplus \cdots \oplus V_{\lambda_k} = V$$

e T è diagonalizzabile come volevamo dimostrare. \square

ESERCIZIO 7.24. Dato un endomorfismo lineare $T : V \rightarrow V$ di uno spazio vettoriale V sul campo \mathbb{K} , dimostrare che se un autovalore di T ha molteplicità algebrica uguale a 1 allora anche la sua molteplicità geometrica è uguale a 1.

5. Esempi

ESEMPIO 7.25. Sia $T : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ un endomorfismo lineare la cui matrice rispetto alla base standard è:

$$[T] = \begin{pmatrix} 0 & 3 & 0 \\ 1 & -2 & 0 \\ 1 & -3 & 1 \end{pmatrix}$$

Vogliamo capire se è diagonalizzabile o no, e, se lo è, vogliamo trovare una base composta da autovettori. Innanzitutto calcoliamo il polinomio caratteristico:

$$P_T(t) = \det \left(tI - \begin{pmatrix} 0 & 3 & 0 \\ 1 & -2 & 0 \\ 1 & -3 & 1 \end{pmatrix} \right) = \det \begin{pmatrix} t & -3 & 0 \\ -1 & t+2 & 0 \\ -1 & 3 & t-1 \end{pmatrix} = (t-1)^2(t+3)$$

Gli autovalori sono dunque 1 e -3 . La molteplicità algebrica di -3 è uguale a 1 e coincide con la sua molteplicità geometrica. Ripetiamo infatti in questo caso particolare il ragionamento che alcuni lettori avranno già utilizzato per risolvere l'Esercizio 7.24: infatti la molteplicità geometrica di -3 è ≥ 1 (visto che -3 è autovalore¹), e per la Proposizione 7.22 deve essere minore o uguale alla molteplicità algebrica, quindi è esattamente 1 e coincide con la molteplicità algebrica.

Dunque, volendo applicare il criterio del Teorema 7.23, dobbiamo studiare l'autovalore 1, che ha molteplicità algebrica 2, e controllare se la sua molteplicità geometrica è uguale a 2 o no. La molteplicità geometrica di 1 è la dimensione dell'autospazio $V_1 = Ker(1I - T)$, dunque dobbiamo calcolare la dimensione di:

$$Ker \left(1I - \begin{pmatrix} 0 & 3 & 0 \\ 1 & -2 & 0 \\ 1 & -3 & 1 \end{pmatrix} \right) = Ker \begin{pmatrix} 1 & -3 & 0 \\ -1 & 3 & 0 \\ -1 & 3 & 0 \end{pmatrix}$$

Si osserva subito che la matrice ha rango uguale a 1, di conseguenza la dimensione del Ker è uguale a 2. Anche per quel che riguarda l'autovalore 1 la molteplicità geometrica risulta uguale alla molteplicità algebrica, dunque l'applicazione T è diagonalizzabile.

Per trovare una base formata da autovettori, dobbiamo scegliere una base di V_1 e una base di V_{-3} e fare l'unione. Cominciamo col trovare una base di V_1 , ossia una base di

$$Ker(1I - T) = Ker \begin{pmatrix} 1 & -3 & 0 \\ -1 & 3 & 0 \\ -1 & 3 & 0 \end{pmatrix}$$

Risolvendo il sistema 'a occhio', si vede subito che una possibile base è data dai vettori $\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 3 \\ 1 \\ 0 \end{pmatrix}$.

Per trovare una base di V_{-3} che, come sappiamo, ha dimensione 1, basta individuare un vettore non nullo in

$$V_{-3} = Ker \left(-3I - \begin{pmatrix} 0 & 3 & 0 \\ 1 & -2 & 0 \\ 1 & -3 & 1 \end{pmatrix} \right) = Ker \begin{pmatrix} -3 & -3 & 0 \\ -1 & -1 & 0 \\ -1 & 3 & -4 \end{pmatrix}$$

Anche in questo caso il sistema associato si risolve immediatamente: è facile osservare che il vettore $\begin{pmatrix} -1 \\ 1 \\ 1 \end{pmatrix}$ costituisce una base di V_{-3} .

¹La molteplicità geometrica di un autovalore è sempre ≥ 1 , visto che, per definizione, l'autospazio relativo a tale autovalore non è banale.

Dunque una base che diagonalizza l'endomorfismo T è data dai vettori

$$v_1 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, v_2 = \begin{pmatrix} 3 \\ 1 \\ 0 \end{pmatrix}, v_3 = \begin{pmatrix} -1 \\ 1 \\ 1 \end{pmatrix}.$$

La matrice di T rispetto a tale base è data da

$$[T]_{v_1, v_2, v_3}^{v_1, v_2, v_3} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -3 \end{pmatrix}$$

ESEMPIO 7.26. Si consideri l'applicazione lineare $F_a : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ che, rispetto alla base standard, ha matrice:

$$[F_a] = \begin{pmatrix} a & 0 & 0 \\ 1 & a & 1 \\ 0 & -1 & 2 \end{pmatrix}$$

Vogliamo studiare, al variare del parametro $a \in \mathbb{R}$, la diagonalizzabilità di F_a . Per prima cosa calcoliamo il polinomio caratteristico $P_{F_a}(t)$:

$$\begin{aligned} P_{F_a}(t) &= \det \left(tI - \begin{pmatrix} a & 0 & 0 \\ 1 & a & 1 \\ 0 & -1 & 2 \end{pmatrix} \right) = \det \begin{pmatrix} t-a & 0 & 0 \\ -1 & t-a & -1 \\ 0 & 1 & t-2 \end{pmatrix} = \\ &= (t-a)(t^2 - (a+2)t + 2a + 1) \end{aligned}$$

Ora osserviamo che il polinomio $t^2 - (a+2)t + 2a + 1$ ha radici

$$\frac{a+2 \pm \sqrt{a^2 - 4a}}{2}$$

Tali radici sono reali se e solo se $a^2 \geq 4a$ ovvero se e solo se $a \geq 4$ oppure $a \leq 0$. Visto che il campo in cui stiamo cercando gli autovalori è \mathbb{R} , per il Teorema 7.23 possiamo intanto concludere che: *se $0 < a < 4$ l'endomorfismo F_a non è diagonalizzabile.*

Se invece $a \geq 4$ oppure $a \leq 0$, abbiamo tre autovalori reali:

$$\frac{a+2 - \sqrt{a^2 - 4a}}{2}, \quad \frac{a+2 + \sqrt{a^2 - 4a}}{2}, \quad a$$

e la prima cosa che ci conviene fare è calcolare le loro molteplicità algebriche, ossia capire se per qualche valore di a questi autovalori coincidono. Infatti, per i valori di a per cui questi tre autovalori sono a due a due distinti possiamo subito dire, in base al Teorema 7.23, che F_a è diagonalizzabile: gli autovalori hanno molteplicità algebrica uguale a 1, e dunque (vedi Esercizio 7.24), anche molteplicità geometrica uguale a 1.

Affrontiamo il problema della coincidenza studiando separatamente le tre possibili uguaglianze:

$$\frac{a+2 - \sqrt{a^2 - 4a}}{2} = \frac{a+2 + \sqrt{a^2 - 4a}}{2}$$

$$\frac{a + 2 - \sqrt{a^2 - 4a}}{2} = a$$

$$\frac{a + 2 + \sqrt{a^2 - 4a}}{2} = a$$

La prima di queste uguaglianze è vera se e solo se

$$-\sqrt{a^2 - 4a} = \sqrt{a^2 - 4a}$$

ovvero se e solo se $\sqrt{a^2 - 4a} = 0$ ovvero se e solo se $a = 0$ oppure $a = 4$. Invece si verifica subito che le uguaglianze

$$\frac{a + 2 - \sqrt{a^2 - 4a}}{2} = a$$

$$\frac{a + 2 + \sqrt{a^2 - 4a}}{2} = a$$

non sono mai vere, qualunque sia il valore di a .

Dunque i casi che richiedono attenzione sono solo $a = 0$ e $a = 4$; possiamo trarre una seconda conclusione: *se $a > 4$ oppure $a < 0$ l'endomorfismo F_a è diagonalizzabile.*

Studiamo infine i due casi rimasti: per quel che riguarda $a = 0$, gli autovalori di F_0 sono 0 e 1 e il polinomio caratteristico $P_{F_0}(t)$ è $t(t-1)^2$. Per capire se F_0 è diagonalizzabile bisogna calcolare la molteplicità geometrica di 1, ossia calcolare

$$\dim V_1 = \dim \text{Ker} \left(1I - \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & -1 & 2 \end{pmatrix} \right) = \dim \text{Ker} \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & -1 \\ 0 & 1 & -1 \end{pmatrix}$$

La matrice ha rango 2, dunque il Ker ha dimensione 1. La molteplicità geometrica dell'autovalore 1 è uguale a 1, mentre la molteplicità algebrica è uguale a 2: l'endomorfismo F_0 non è diagonalizzabile.

Per quel che riguarda $a = 4$, gli autovalori di F_4 sono 4 e 3 e il polinomio caratteristico $P_{F_4}(t)$ è $(t-4)(t-3)^2$. Per capire se F_4 è diagonalizzabile bisogna calcolare la molteplicità geometrica di 3, ossia calcolare

$$\dim V_3 = \dim \text{Ker} \left(3I - \begin{pmatrix} 4 & 0 & 0 \\ 1 & 4 & 1 \\ 0 & -1 & 2 \end{pmatrix} \right) = \det \begin{pmatrix} -1 & 0 & 0 \\ -1 & -1 & -1 \\ 0 & 1 & 1 \end{pmatrix}$$

come nel caso precedente, il Ker ha dimensione 1 e risulta che l'endomorfismo F_4 non è diagonalizzabile.

6. Altri esercizi

ESERCIZIO 7.27. Sia $A : \mathbb{R}^4 \rightarrow \mathbb{R}^4$ l'applicazione lineare che nella base standard è rappresentata dalla matrice

$$[A] = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 \\ 1 & 0 & 2 & 0 \end{pmatrix}$$

Dire se A è diagonalizzabile. Descrivere gli autovalori e gli autospazi di A .

ESERCIZIO 7.28. Sia $F : \mathbb{C}^3 \rightarrow \mathbb{C}^3$ l'applicazione lineare definita, nella base standard di \mathbb{C}^3 , dalla matrice:

$$[F] = \begin{pmatrix} -1 & 0 & 1 \\ 2 & 1 & 2i \\ 1 & 0 & 0 \end{pmatrix}$$

Dire se F è diagonalizzabile e, se lo è, trovare una base di autovettori [nota: ricordiamo che stiamo lavorando sul campo \mathbb{C}].

ESERCIZIO 7.29. Consideriamo l'endomorfismo lineare L_a di \mathbb{R}^3 dipendente dal parametro reale a e definito da:

$$L_a(x, y, z) = (ax + y + z, x + ay + z, -x + y + az)$$

- (1) Discutere la diagonalizzabilità di L_a al variare del parametro reale a .
- (2) Determinare, se esiste, una base di \mathbb{R}^3 di autovettori per L_0 .

ESERCIZIO 7.30. Sia $T : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ l'endomorfismo la cui matrice rispetto alla base standard è

$$\begin{pmatrix} 9 & 6 & 9 \\ 3 & 12 & 9 \\ 3 & 6 & 15 \end{pmatrix}$$

Dire se T è diagonalizzabile e, se lo è, trovare una base fatta da autovettori.

ESERCIZIO 7.31. a) Si consideri l'endomorfismo $A : \mathbb{C}^2 \rightarrow \mathbb{C}^2$ a cui nella base standard è associata la matrice

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

Trovare gli autovettori di A e dire se A è diagonalizzabile.

b) Si consideri l'endomorfismo $B : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ a cui nella base standard è associata la matrice

$$\begin{pmatrix} 1 & b \\ b & 1 \end{pmatrix}$$

- i) Per quali valori di $b \in \mathbb{R}$ è diagonalizzabile?
- ii) Sia k un intero positivo. Si trovino, in funzione di k e del parametro b , gli autovalori dell'endomorfismo B^k .

ESERCIZIO 7.32. Consideriamo l'applicazione lineare $A_a : \mathbb{R}^4 \rightarrow \mathbb{R}^4$ definita rispetto alla base standard dalla seguente matrice:

$$[A_a] = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & a & 0 \\ 1 & 0 & 1 & -1 \end{pmatrix}$$

Dire se esistono, e in caso affermativo trovare quali, valori del parametro $a \in \mathbb{R}$ per cui A_a è diagonalizzabile. Determinare inoltre gli autovettori di A_{-1} .

ESERCIZIO 7.33. Sia $F_a : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ l'applicazione lineare la cui matrice associata rispetto alla base canonica è la seguente:

$$[F_a] = \begin{pmatrix} 1 & 2 & 1 \\ 0 & -1 & -1 \\ 0 & 1 & a+1 \end{pmatrix}$$

- (1) Determinare per quali valori del parametro a la matrice $[F_a]$ è invertibile.
- (2) Trovare i valori di a per i quali F_a è diagonalizzabile.
- (3) Trovare, se esiste, una base di autovettori di F_a quando $a = 1/2$.

ESERCIZIO 7.34. Sia $T_a : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ l'endomorfismo lineare che, rispetto alla base standard di \mathbb{R}^3 , è rappresentato dalla seguente matrice:

$$\begin{pmatrix} 1 & 2-a & 1 \\ 0 & a & 0 \\ -1 & 7a & a \end{pmatrix}$$

Per quali valori di $a \in \mathbb{R}$ l'endomorfismo T_a è diagonalizzabile ?

ESERCIZIO 7.35. Sia $T_a : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ l'endomorfismo lineare che, rispetto alla base standard di \mathbb{R}^3 , è rappresentato dalla seguente matrice:

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

a) Per quali valori di $a \in \mathbb{R}$ l'endomorfismo T_a è diagonalizzabile ?

b) Trovare, per ogni a per cui T_a è diagonalizzabile, una base di \mathbb{R}^3 costituita da autovettori di T_a .

ESERCIZIO 7.36. Sia $T_a : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ l'endomorfismo lineare che, rispetto alla base standard di \mathbb{R}^3 , è rappresentato dalla seguente matrice:

$$\begin{pmatrix} 2a-1 & 3a-1 & 1 \\ 0 & 4a-1 & 0 \\ -1 & 1 & a+1 \end{pmatrix}$$

Per quali valori di $a \in \mathbb{R}$ l'endomorfismo T_a è diagonalizzabile ?

ESERCIZIO 7.37. Sia $T_k : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ l'applicazione lineare che, rispetto alla base standard di \mathbb{R}^3 , è rappresentata dalla seguente matrice:

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

a) Per quali valori di $k \in \mathbb{R}$ T_k è diagonalizzabile ?

b) Nei casi in cui T_k è diagonalizzabile, trovare una base fatta da autovettori.

ESERCIZIO 7.38. Sia $T_a : \mathbb{R}^4 \rightarrow \mathbb{R}^4$ l'endomorfismo lineare che, rispetto alla base standard di \mathbb{R}^4 , è rappresentato dalla seguente matrice:

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

a) Per quali valori di $a \in \mathbb{R}$ l'endomorfismo T_a è diagonalizzabile ?

b) Trovare, per ogni a per cui T_a è diagonalizzabile, una base di \mathbb{R}^4 costituita da autovettori di T_a .

ESERCIZIO 7.39. Sia V uno spazio vettoriale di dimensione finita n sul campo \mathbb{K} e sia $T : V \rightarrow V$ un endomorfismo lineare. Dimostrare che esiste in $\mathbb{K}[t]$ un polinomio

$$f(t) = a_{n^2}t^{n^2} + \cdots + a_1t + a_0$$

di grado minore o uguale a n^2 tale che

$$f(T) = a_{n^2}T^{n^2} + \cdots + a_1T + a_0I$$

è l'endomorfismo nullo.

ESERCIZIO 7.40 (Teorema di Cayley-Hamilton). Sia V uno spazio vettoriale di dimensione finita n sul campo \mathbb{K} e sia $T : V \rightarrow V$ un endomorfismo lineare. Il teorema di Cayley-Hamilton afferma che l'endomorfismo $P_T(T)$ è l'endomorfismo nullo. Dimostrare questo teorema nel caso $n = 2$ e $n = 3$.

ESERCIZIO 7.41. Dimostrare, come sopra, il teorema di Cayley-Hamilton nel caso $n = 2$ e $n = 3$ supponendo di sapere in più che l'endomorfismo T ammette un autovalore. La dimostrazione si semplifica?

ESERCIZIO 7.42. Un endomorfismo lineare $T : V \rightarrow V$ si dice *nilpotente* se per un certo intero positivo n vale che $T^n = T \circ T \circ T \cdots \circ T$ è l'endomorfismo nullo.² Dimostrare che se T è nilpotente allora ha un unico autovalore: $\lambda = 0$.

²Analogamente, una matrice quadrata A si dice *nilpotente* se per un certo intero positivo n vale che A^n è la matrice nulla.

ESERCIZIO 7.43. Nel caso in cui V sia uno spazio vettoriale sul campo \mathbb{C} dimostrare il viceversa dell'enunciato dell'esercizio precedente, ossia che se T ha un unico autovalore, uguale a 0, allora T è nilpotente. Se il campo è \mathbb{R} e si sa che T ha un unico autovalore reale, uguale a 0, allora si può concludere che T è nilpotente?

ESERCIZIO 7.44. Sia V uno spazio vettoriale di dimensione 4 sul campo \mathbb{K} e sia $T : V \rightarrow V$ un endomorfismo lineare che, rispetto ad una certa base, è rappresentato dalla matrice:

$$[T] = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

L'endomorfismo T è nilpotente? È diagonalizzabile?

ESERCIZIO 7.45. Sia $T : V \rightarrow V$ un endomorfismo lineare e sia λ un autovalore. Dimostrare che, per un ogni intero positivo n , λ^n è un autovalore di T^n .

ESERCIZIO 7.46. Sia V uno spazio vettoriale di dimensione finita sul campo \mathbb{K} e sia $T : V \rightarrow V$ un endomorfismo lineare diverso da I e da $-I$. Supponiamo che valga $T^2 = I$. Individuare gli autovalori di T e dimostrare che T è diagonalizzabile.

ESERCIZIO 7.47 (Proiezione lineare su un sottospazio). Sia V uno spazio vettoriale di dimensione finita sul campo \mathbb{K} e sia $T : V \rightarrow V$ un endomorfismo lineare diverso da I e dall'endomorfismo nullo. Supponiamo che valga $T^2 = T$. Dimostrare che T è diagonalizzabile e ha due autovalori, 1 e 0. Osservare che questo equivale a dire che T è una *proiezione lineare* di V su V_1 : T manda V surgettivamente su V_1 e lascia fissi tutti i vettori di V_1 . Sia v_1, v_2, \dots, v_n una base che diagonalizza T , con $V_1 = \langle v_1, v_2, \dots, v_i \rangle$ e $V_0 = \langle v_{i+1}, \dots, v_n \rangle$: scrivendo i vettori rispetto a questa base, la T è l'applicazione tale che

$$[T] \begin{pmatrix} a_1 \\ \dots \\ a_i \\ a_{i+1} \\ \dots \\ a_n \end{pmatrix} = \begin{pmatrix} a_1 \\ \dots \\ a_i \\ 0 \\ \dots \\ 0 \end{pmatrix}$$

ESERCIZIO 7.48 (Diagonalizzazione simultanea di endomorfismi che commutano). Sia V uno spazio vettoriale di dimensione finita n sul campo \mathbb{K} e siano T ed S due endomorfismi lineari diagonalizzabili. Dimostrare che, se vale

$$T \circ S = S \circ T$$

allora esiste una base di V che diagonalizza S e T *simultaneamente*.

Suggerimento. Cominciare con l'osservare che, se λ è un autovalore per S e V_λ è il suo autospazio, allora $T(V_\lambda) \subseteq V_\lambda$.

ESERCIZIO 7.49. Trovare, se possibile, una base di \mathbb{R}^2 che diagonalizza simultaneamente gli endomorfismi T ed S che, nella base standard, sono rappresentati rispettivamente dalle matrici:

$$[T] = \begin{pmatrix} 2 & 1 \\ 3 & 0 \end{pmatrix} \quad [S] = \begin{pmatrix} 5 & 2 \\ 6 & 1 \end{pmatrix}$$

Alcune osservazioni sulla fattorizzazione dei polinomi

Abbiamo già incontrato nei precedenti capitoli lo spazio vettoriale $\mathbb{K}[x]$ dato dai polinomi a coefficienti in un campo \mathbb{K} . Quando si considera anche la moltiplicazione fra polinomi, tale spazio vettoriale acquista una struttura di anello commutativo con identità, che avete cominciato a studiare nel primo semestre del corso (avete studiato la divisione euclidea e teorema della radice). Nella fattorizzazione del polinomio caratteristico di un endomorfismo questa struttura entra di nuovo in gioco; per questo motivo le dedichiamo un breve approfondimento.

1. Polinomi irriducibili e teorema di fattorizzazione unica

In questo paragrafo, che tratterà della fattorizzazione di polinomi, considereremo (per motivi che diverranno chiari nel corso del paragrafo stesso) anche polinomi a coefficienti in \mathbb{Z} , ovvero in un anello che non è un campo. Cercheremo di sottolineare le differenze principali nei due casi, una per esempio è che in $\mathbb{Z}[x]$ non è più vero che tutti i polinomi di grado 0 (ovvero le costanti non nulle) sono invertibili: gli unici polinomi invertibili sono il polinomio 1 e il polinomio -1 (per le altre costanti a non esiste un polinomio di grado 0 b in $\mathbb{Z}[x]$ tale che $a \cdot b = 1$). Useremo la notazione $A[x]$ quando considereremo il caso allargato di polinomi a coefficienti in un anello A commutativo, con unità e privo di divisori di zero.¹ I casi che ci interesseranno saranno essenzialmente quelli dei polinomi a coefficienti in $\mathbb{Z}, \mathbb{Z}_p, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, dunque tutti del tipo descritto e, a parte \mathbb{Z} , tutti campi.

Cominciamo introducendo il concetto di polinomio irriducibile in $A[x]$, che avrà lo stesso ruolo del concetto di numero primo in \mathbb{Z} .

DEFINIZIONE 8.1. Dato un polinomio $p(x)$ di $A[x]$ con A anello, se esistono due polinomi $f(x)$ e $g(x)$ in $A[x]$ entrambi non invertibili e tali che

$$p(x) = f(x) \cdot g(x)$$

il prodotto $f(x) \cdot g(x)$ si dice **una fattorizzazione** di $p(x)$ in $A[x]$.

A questo punto possiamo caratterizzare quelli che vogliamo chiamare polinomi irriducibili in $A[x]$:

¹Si dice in tal caso che A è un dominio. Per esempio l'anello \mathbb{Z} è un dominio, mentre l'anello \mathbb{Z}_{15} non lo è.

DEFINIZIONE 8.2. Sia $f(x)$ un polinomio di $A[x]$ non invertibile. Il polinomio $f(x)$ si dice **riducibile** (o fattorizzabile) in $A[x]$ se in $A[x]$ esiste almeno una fattorizzazione di $f(x)$. Altrimenti il polinomio $f(x)$ si dice **irriducibile**.

OSSERVAZIONE 8.3. Un modo equivalente di dire che un polinomio $f(x)$ di $A[x]$ è irriducibile (ed è quello che solitamente viene richiamato negli esercizi e nelle dimostrazioni) è affermare che qualsiasi scrittura di $f(x)$ come prodotto di polinomi di $A[x]$:

$$f(x) = g(x)h(x)$$

implica che uno dei due polinomi sia invertibile in $A[x]$. Ovvero nel caso di polinomi a coefficienti in un campo \mathbb{K} , essendo gli invertibili tutti e soli i polinomi di grado 0 (le costanti), $f(x)$ è irriducibile in $\mathbb{K}[x]$ se e solo se $f(x)$ ha grado maggiore o uguale a 1 e non può essere scritto come prodotto di due polinomi (non necessariamente distinti) di grado maggiore di 0.

Cominciamo a discutere qualche proprietà sulla irriducibilità che vale nei $\mathbb{K}[x]$ (ma in generale, vedremo, non vale per gli $A[x]$).

PROPOSIZIONE 8.4. *Negli anelli di polinomi $\mathbb{K}[x]$, con \mathbb{K} campo, tutti i polinomi di grado 1 sono irriducibili.*

DIMOSTRAZIONE. Supponiamo che il polinomio $f(x) \in \mathbb{K}[x]$ di grado 1 sia il prodotto di due polinomi $g(x)$ e $h(x)$ di $\mathbb{K}[x]$:

$$f(x) = g(x)h(x)$$

Per le proprietà del grado del prodotto di polinomi abbiamo che:

$$1 = \deg(f(x)) = \deg(g(x)) + \deg(h(x))$$

Ovvero uno dei due polinomi deve avere grado 0. E sappiamo che in $\mathbb{K}[x]$ tutti i polinomi di grado 0 sono invertibili. \square

OSSERVAZIONE 8.5. Mostriamo, ad esempio, che in $\mathbb{Z}[x]$ esistono polinomi di primo grado riducibili. Consideriamo $f(x) = 2x - 4$, possiamo scriverlo come $2 \cdot (x - 2)$ ed i polinomi 2 e $x - 2$ non sono invertibili in $\mathbb{Z}[x]$.

DEFINIZIONE 8.6. Un polinomio $f(x) = \sum_{i=0}^n a_i x^i$ in $\mathbb{Z}[x]$ si dice **primitivo** se il massimo comun divisore tra i suoi coefficienti a_0, a_1, \dots, a_n è uguale a 1.

La definizione di polinomio primitivo ci permette di individuare i polinomi irriducibili di primo grado in $\mathbb{Z}[x]$ (e dunque di mostrare che, per esempio, il polinomio $x - 2$ è irriducibile in $\mathbb{Z}[x]$).

PROPOSIZIONE 8.7. *In $\mathbb{Z}[x]$ i polinomi di primo grado sono irriducibili se e solo se sono primitivi.*

DIMOSTRAZIONE. Se $f(x) = ax + b \in \mathbb{Z}[x]$ di primo grado è il prodotto di due polinomi, allora, per la proprietà del grado², deve essere il prodotto di un polinomio di primo grado $h(x) = sx + t$, per un polinomio di grado 0, ovvero una costante $c \in \mathbb{Z}$. Questo, per la definizione di uguaglianza tra polinomi significa che $c \cdot s = a$ e $c \cdot t = b$, dunque che c è un divisore comune dei coefficienti di $f(x)$. Dunque esiste c non invertibile (ovvero diverso da 1 o -1), e quindi una fattorizzazione di $f(x)$ (ovvero $c \cdot h(x)$) se e solo se $f(x)$ non è primitivo. \square

Abbiamo dunque discusso l'irriducibilità dei polinomi di grado 1 in $\mathbb{K}[x]$ e in $\mathbb{Z}[x]$. Per quanto riguarda i polinomi di grado maggiore di 1, una discussione importante è quella che lega la irriducibilità di un polinomio $f(x)$ in $\mathbb{K}[x]$ di grado $n > 1$ al fatto che esso abbia radici in \mathbb{K} . Dal teorema di Ruffini segue che se $f(x)$ ha una radice α in \mathbb{K} allora è riducibile. Infatti si ha che il polinomio $(x - \alpha)$ divide $f(x)$:

$$\underbrace{f(x)}_{\text{grado} > 1} = g(x) \cdot \underbrace{(x - \alpha)}_{\text{grado} = 1}$$

Inoltre, per le proprietà del grado, $g(x)$ ha grado maggiore di 0, ovvero non è invertibile.

Viceversa in generale **non è vero** che se un polinomio di grado maggiore di 1 non ha radici allora è irriducibile. Ad esempio il polinomio $x^4 + 2x^2 + 1$ di $\mathbb{R}[x]$ è riducibile in $\mathbb{R}[x]$:

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

ma non ha radici in \mathbb{R} (non esiste nessun numero reale che elevato al quadrato è uguale a -1).

L'unica cosa certa è che un polinomio che non ha radici in \mathbb{K} allora non ha fattori di grado 1 nella sua fattorizzazione in $\mathbb{K}[x]$. Da questo segue che:

COROLLARIO 8.8. *Un polinomio $f(x) \in \mathbb{K}[x]$ di grado 2 e 3 è riducibile se e solo se ha una radice in \mathbb{K} .*

DIMOSTRAZIONE. Abbiamo osservato che, in generale, un polinomio di grado $n > 1$ che ha una radice in \mathbb{K} è riducibile in $\mathbb{K}[x]$. Viceversa se un polinomio di grado 2 o 3 è riducibile allora, sfruttando le proprietà del grado del prodotto di polinomi, necessariamente nel primo caso ($n = 2$) deve essere il prodotto di due fattori di grado 1, mentre nel secondo caso ($n = 3$) può essere il prodotto di un polinomio di grado 1 per un polinomio di grado 2 o il prodotto di tre polinomi di grado 1. Ovvero abbiamo stabilito che i polinomi di grado 2 o 3 riducibili hanno necessariamente un fattore di grado 1 e il teorema di Ruffini ci dice che avere un fattore di grado 1 in $\mathbb{K}[x]$ equivale ad avere una radice in \mathbb{K} . \square

²Le proprietà del grado continuano a valere in $A[x]$ con A dominio, come potete facilmente verificare.

Gli elementi irriducibili di $\mathbb{K}[x]$ hanno molte analogie con i numeri primi di \mathbb{Z} . Un primo risultato importante è quello che ci dice che *se un polinomio irriducibile divide un prodotto di polinomi, allora divide uno dei due fattori*. Enunciamo questo risultato nel seguente teorema, la cui dimostrazione, lasciata come esercizio, coinvolge, analogamente a quello che accade in \mathbb{Z} , il lemma di Bezout.

TEOREMA 8.9 (Primalità di un polinomio irriducibile). *Se $p(x)$ è un polinomio irriducibile in $\mathbb{K}[x]$ dove \mathbb{K} è un campo, e $p(x) \mid f(x) \cdot g(x)$ (dove $f(x), g(x) \in \mathbb{K}[x]$), allora o vale $p(x) \mid f(x)$ o vale $p(x) \mid g(x)$.*

Vale anche l'analogo del teorema di fattorizzazione unica (la dimostrazione è un esercizio caldamente consigliato; è una applicazione del teorema di primalità: si procede in maniera del tutto simile alla dimostrazione della fattorizzazione unica in \mathbb{Z}).

TEOREMA 8.10 (Teorema di fattorizzazione unica per polinomi). *Ogni polinomio di grado ≥ 1 in $\mathbb{K}[x]$ (dove \mathbb{K} è un campo) è irriducibile o si fattorizza come prodotto di polinomi irriducibili. Inoltre, se*

$$f(x) = p_1(x) \cdot p_2(x) \cdot \dots \cdot p_s(x) = q_1(x) \cdot q_2(x) \cdot \dots \cdot q_t(x)$$

sono due fattorizzazioni del polinomio $f(x)$ come prodotto di irriducibili, allora vale che $s = t$ e che i polinomi $p_i(x)$ e i polinomi $q_j(x)$ sono a due a due associati.

Nel teorema di fattorizzazione unica per polinomi i $p_i(x)$ non sono necessariamente distinti. Proprio come nel caso della fattorizzazione tra gli interi, possiamo scrivere la fattorizzazione di un polinomio *accorpando* i fattori uguali e usando le potenze. Si scriverà dunque

$$h(x) = a \cdot q_1^{r_1}(x) \cdot q_2^{r_2}(x) \cdot \dots \cdot q_t^{r_t}(x)$$

dove a è il coefficiente direttivo di $h(x)$, i $q_j(x)$ sono i polinomi irriducibili distinti monici³ della fattorizzazione di $h(x)$, gli r_i sono i numeri naturali positivi che evidenziano quante volte ricorre il polinomio $q_i(x)$ nella fattorizzazione di $h(x)$.⁴

Avendo questa fattorizzazione è molto facile individuare, proprio come avveniva in \mathbb{Z} , il *M.C.D.* di due polinomi (se non si conosce già una fattorizzazione, in generale è invece più conveniente. Se infatti consideriamo un polinomio $g(x)$ e la sua fattorizzazione in irriducibili:

$$g(x) = b \cdot p_1^{s_1}(x) p_2^{s_2}(x) \cdot \dots \cdot p_j^{r_j}(x)$$

allora il *M.C.D.* ($h(x), g(x)$) si otterrà facendo il prodotto degli irriducibili che compaiono sia fra i $p_m(x)$ che fra i $q_n(x)$, ciascuno preso col minimo esponente fra i due esponenti che troviamo nelle due fattorizzazioni.

³Un polinomio monico è un polinomio in cui il coefficiente del termine di grado più alto è uguale a 1, tipo $f(x) = x^4 + 6x^3 + x + 6$ in $\mathbb{R}[x]$.

⁴Detto in formule r_i è quel numero naturale tale che $q_i(x)^{r_i}$ divide $h(x)$ e $q_i(x)^{r_i+1}$ non divide $h(x)$.

ESEMPIO 8.11. Consideriamo in $\mathbb{Q}[x]$,

$$h(x) = (x - 1)^2(x^2 - 5)^3(x^4 - 7x + 7)$$

e

$$g(x) = (x - 1)^7(x^2 - 5)(x^5 + 11x^2 + 11)^2$$

e supponiamo di sapere che i fattori che compaiono nelle fattorizzazioni sono irriducibili (presto discuteremo un criterio che permette di verificarlo facilmente); allora il *M.C.D.* $(h(x), g(x))$ è

$$(x - 1)^2(x^2 - 5)$$

Gli altri *M.C.D.* $(h(x), g(x))$, come sappiamo, sono tutti i polinomi associati a $(x - 1)^2(x^2 - 5)$.

OSSERVAZIONE 8.12. L'unicità della fattorizzazione in $\mathbb{K}[x]$ è a meno dell'ordine dei fattori e di moltiplicazione per invertibili, cioè le costanti. Ovvero la fattorizzazione $(x - 1) \cdot (x - 2)$ del polinomio $x^2 - 3x + 2$ potrebbe essere scritta anche $(x - 2) \cdot (x - 1)$, ma questa fattorizzazione la consideriamo identica alla precedente, abbiamo cambiato solo l'ordine dei fattori. Così come consideriamo identica la fattorizzazione $\frac{1}{2} \cdot (x - 1) \cdot 2 \cdot (x - 2)$, in quanto abbiamo solo moltiplicato per invertibili (il cui prodotto è 1) i due fattori irriducibili.

Anche in questo caso osserviamo l'analogia con l'unicità della fattorizzazione in primi dei numeri in \mathbb{Z} . Il numero 21 è uguale a $7 \cdot 3$; noi consideriamo identica (perchè cambiamo solo l'ordine) la fattorizzazione $3 \cdot 7$, ma anche la fattorizzazione che si può ottenere moltiplicando per invertibili il cui prodotto totale sia 1. Gli invertibili in \mathbb{Z} sono 1 e -1 . Dunque 21 lo possiamo fattorizzare anche come $-1 \cdot 3 \cdot (-1) \cdot 7$ ovvero come $-3 \cdot (-7)$.

OSSERVAZIONE 8.13. Il teorema di fattorizzazione unica vale per ogni $\mathbb{K}[x]$ con \mathbb{K} campo. Per la dimostrazione usiamo il teorema di primalità che a sua volta si dimostra tramite il teorema di Bezout che vale in $\mathbb{K}[x]$ con K campo. Cosa succede se l'insieme dei coefficienti A è un anello ma non un campo? Vale la fattorizzazione unica? La risposta è "dipende"... Si può infatti dimostrare che il teorema di fattorizzazione unica vale anche in $\mathbb{Z}[x]$, ma anche mostrare esempi di anelli (che non sono campi) per cui il teorema di fattorizzazione unica non vale. Consideriamo ad esempio l'insieme $\mathbb{Z}_{30}[x]$ ed il polinomio $x^2 - 1$. Facendo i conti si può verificare che:

$$x^2 - 1 = (x - 1)(x - 29) = (x - 19)(x - 11)$$

Queste sono due distinte fattorizzazioni in irriducibili.

2. Fattorizzazione in $\mathbb{C}[x]$, $\mathbb{R}[x]$, $\mathbb{Q}[x]$

Affrontiamo ora il problema della fattorizzazione nell'anello dei polinomi $\mathbb{K}[x]$, variando \mathbb{K} tra uno dei seguenti campi: \mathbb{C} , \mathbb{R} , \mathbb{Q} .

2.1. Fattorizzazione in $\mathbb{C}[x]$. Il campo \mathbb{C} dei numeri complessi ha una proprietà molto importante per quanto riguarda le radici di polinomi a coefficienti in \mathbb{C} , proprietà che non a caso si chiama **teorema fondamentale dell'algebra** e di cui noi riportiamo solo l'enunciato (la dimostrazione di questo risultato esula dagli obiettivi di questo testo).

TEOREMA 8.14 (Teorema fondamentale dell'algebra). *Ogni polinomio $f(x)$ a coefficienti in \mathbb{C} di grado maggiore di zero ammette almeno una radice in \mathbb{C} .*

Usando il teorema fondamentale dell'algebra e il teorema di Ruffini abbiamo una caratterizzazione completa degli irriducibili in \mathbb{C} . Infatti una immediata conseguenza è che:

COROLLARIO 8.15. *Ogni polinomio $f \in \mathbb{C}[x]$ di grado $n > 0$ è il prodotto di n fattori di primo grado in $\mathbb{C}[x]$.*

DIMOSTRAZIONE. Procediamo per induzione sul grado n di f . Se f è di primo grado la tesi segue immediatamente. Sia ora $f(x) = \sum_{i=0}^n a_i x^i$ con $a_i \in \mathbb{C}$ e $a_n \neq 0$, $n > 1$. Possiamo scrivere $f(x) = a_n g(x)$ con $g(x)$ monico. Sia α radice di $g(x)$, la cui esistenza è assicurata dal Teorema 8.14 allora:

$$f(x) = a_n(x - \alpha)g_1(x) \quad \text{con} \quad \deg(g_1) = n - 1$$

quindi g_1 e di conseguenza f si scrivono come prodotto di fattori di grado 1. \square

Dal Corollario 8.15 segue che:

In $\mathbb{C}[x]$ un polinomio è irriducibile se e solo se è di primo grado
 In $\mathbb{C}[x]$ quindi fattorizzare un polinomio equivale a trovarne le radici perchè tutti i suoi fattori irriducibili sono di grado 1. Dobbiamo cioè essere in grado di risolvere equazioni polinomiali a coefficienti complessi, cosa che può essere anche molto complicata. Prima di vedere un esempio, sottolineiamo il fatto che la ricerca di radici complesse è importante, come vedremo, anche per la fattorizzazione in $\mathbb{R}[x]$.

ESEMPIO 8.16. Fattorizzare il polinomio $x^2 + 4x + 5 \in \mathbb{C}[x]$ come prodotto di irriducibili.

Dobbiamo trovare le radici complesse del polinomio $x^2 + 4x + 5$, ovvero le soluzioni complesse dell'equazione

$$(2.1) \quad x^2 + 4x + 5 = 0$$

La formula risolutiva dell'equazione di secondo grado ci permette di trovare le soluzioni complesse (anche se il delta è negativo!):

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Nel nostro caso:

$$x_{1,2} = \frac{-4 \pm 2i}{2} = -2 \pm i$$

Quindi il polinomio $x^2 + 4x + 5 \in \mathbb{C}[x]$ si fattorizza in irriducibili come:

$$(x - (-2 + i)) \cdot (x - (-2 - i))$$

Per riprova possiamo calcolarci questo prodotto osservando che:

$$(x - (-2 + i)) \cdot (x - (-2 - i)) = ((x + 2) + i) \cdot ((x + 2) - i)$$

E questo sappiamo essere un prodotto notevole (ovvero la differenza di quadrati):

$$((x + 2) + i) \cdot ((x + 2) - i) = (x + 2)^2 - i^2 = x^2 + 4x + 5$$

Per la ricerca di radici complesse in polinomi a coefficienti reali (e dunque utile sia per la fattorizzazione in $\mathbb{C}[x]$ che in $\mathbb{R}[x]$) è importante ricordare la funzione coniugio da \mathbb{C} in \mathbb{C} :

DEFINIZIONE 8.17. Chiamiamo funzione **coniugio** la funzione da \mathbb{C} in \mathbb{C} che al numero complesso $a + ib$ associa $\overline{a + ib} = a - ib$.

ESERCIZIO 8.18. Usando la definizione dimostrare le seguenti proprietà della funzione coniugio:

- (1) I suoi punti fissi, ovvero gli $z \in \mathbb{C}$ tali che $\bar{z} = z$, sono tutti e soli i numeri reali.
- (2) Il coniugio della somma è la somma dei coniugi, ovvero per ogni $z, w \in \mathbb{C}$ $\overline{z + w} = \bar{z} + \bar{w}$.
- (3) Il coniugio del prodotto è il prodotto dei coniugi, ovvero per ogni $z, w \in \mathbb{C}$ $\overline{z \cdot w} = \bar{z} \cdot \bar{w}$.
- (4) Il prodotto di un numero complesso per il suo coniugato è un numero reale, ovvero per ogni $z \in \mathbb{C}$ si ha che $z \cdot \bar{z} \in \mathbb{R}$.

Il coniugio permette di dimostrare una interessante proprietà delle radici complesse di un polinomio a coefficienti reali (**ATTENZIONE:** sottolineiamo il fatto che tra le ipotesi che stiamo considerando c'è che i coefficienti del polinomio siano reali), ovvero che se z è una radice di un polinomio $p(x)$ a coefficienti reali, allora \bar{z} è una radice di $p(x)$. Questo è ovvio, ma non è di nessuna utilità, se z è reale in quanto $\bar{z} = z$, ma è invece importante nel caso in cui $z \in \mathbb{C} - \mathbb{R}$:

PROPOSIZIONE 8.19. Sia $f(x) \in \mathbb{R}[x] \subset \mathbb{C}[x]$ e sia $\alpha \in \mathbb{C}$ una radice di f . Allora anche $\bar{\alpha}$ è una radice di f .

DIMOSTRAZIONE. sia $f(x) = \sum_{i=0}^n a_i x^i$ con $a_i \in \mathbb{R}$. Per ipotesi:

$$0 = f(\alpha) = \sum_{i=0}^n a_i \alpha^i$$

quindi, dall'enunciato dell'Esercizio 8.18, segue che:

$$\bar{0} = \overline{\sum_{i=0}^n a_i \alpha^i} = \sum_{i=0}^n \overline{a_i \alpha^i} = \sum_{i=0}^n a_i \bar{\alpha}^i = \sum_{i=0}^n a_i \bar{\alpha}^i$$

Cioè $f(\bar{\alpha}) = \bar{0} = 0$. □

Nel prossimo esercizio useremo il risultato della Proposizione 8.19 per fattorizzare un polinomio a coefficienti reali in $\mathbb{C}[x]$.

ESERCIZIO 8.20. Sapendo che $f(x) = x^4 - 4x^3 + 3x^2 + 14x + 26$ ha radice $3 + 2i$, fattorizzare il polinomio in $\mathbb{C}[x]$.

Risoluzione. Il polinomio considerato è a coefficienti interi, quindi in particolare reali. Allora possiamo applicare la Proposizione 8.19 e concludere che anche $3 - 2i$ è radice del polinomio; da questo segue che $(x - (3 + 2i)) \cdot (x - (3 - 2i)) = x^2 - 6x + 13$ divide $f(x)$:

$$\begin{array}{r}
 x^4 \quad -4x^3 \quad +3x^2 \quad +14x \quad +26 \quad | \quad x^2 - 6x + 13 \\
 x^4 \quad -6x^3 \quad +13x^2 \quad \quad | \quad x^2 + 2x + 2 \\
 \quad 2x^3 \quad -10x^2 \quad +14x \quad +26 \\
 \quad 2x^3 \quad -12x^2 \quad +26x \\
 \quad 2x^2 \quad -12x \quad +26 \\
 \quad 2x^2 \quad -12x \quad +26 \\
 \quad 0
 \end{array}$$

Quindi:

$$f(x) = \underbrace{(x - (3 + 2i)) \cdot (x - (3 - 2i))}_{x^2 - 6x + 13} \cdot (x^2 + 2x + 2)$$

E per completare la fattorizzazione in $\mathbb{C}[x]$ resta da fattorizzare il polinomio $x^2 + 2x + 2$.

Calcoliamo le radici del polinomio attraverso la formula risolutiva delle equazioni di secondo grado:

$$x_{1,2} = \frac{-2 \pm \sqrt{-4}}{2} = \frac{-2 \pm 2i}{2} = \frac{2 \cdot (-1 \pm i)}{2} = -1 \pm i$$

Per cui la fattorizzazione di $f(x)$ è data da:

$$(x - (3 + 2i)) \cdot (x - (3 - 2i)) \cdot (x + (1 + i)) \cdot (x + (1 - i))$$

OSSERVAZIONE 8.21. Osserviamo, senza ancora aver parlato di fattorizzazione in $\mathbb{R}[x]$, che la fattorizzazione in $\mathbb{C}[x]$ del polinomio $f(x) = x^4 - 4x^3 + 3x^2 + 14x + 26$ dell'Esercizio 8.20 fornisce indicazioni importanti sulla fattorizzazione dello stesso polinomio in $\mathbb{R}[x]$.

2.2. Fattorizzazione in $\mathbb{R}[x]$. Anche in $\mathbb{R}[x]$ si possono caratterizzare i polinomi irriducibili attraverso il grado, utilizzando quello che sappiamo della fattorizzazione in $\mathbb{C}[x]$.

Consideriamo un generico polinomio $f(x) \in \mathbb{R}[x]$ di grado n . In particolare $f(x)$ può essere visto come elemento di $\mathbb{C}[x]$ e indichiamo con z_1, \dots, z_r le sue radici complesse e con m_1, \dots, m_r le loro rispettive molteplicità⁵. La

⁵Sappiamo, dal Corollario 8.15, che $\sum_{i=1}^r m_i = n$, ma in generale $r \leq n$. È $r = n$ solo se $f(x)$ ha tutte radici distinte in $\mathbb{C}[x]$.

fattorizzazione di $f(x)$ in $\mathbb{C}[x]$ è dunque la seguente:

$$(2.2) \quad \prod_{i=1}^r (x - z_i)^{m_i}$$

Come si passa dalla fattorizzazione in $\mathbb{C}[x]$ a quella in $\mathbb{R}[x]$? Si osserva che se $z_i \in \mathbb{R}$ allora $(x - z_i)^{m_i}$ è un fattore di $f(x)$ in $\mathbb{R}[x]$, mentre se $z_i \in \mathbb{C} - \mathbb{R}$, allora il fattore $(x - z_i)^{m_i}$ non appartiene a $\mathbb{R}[x]$, ma sappiamo che esiste un'altra radice z_j di $f(x)$ tale che $z_j = \bar{z}_i$ e $m_i = m_j$.

Dunque, nella fattorizzazione 2.2, è presente il fattore

$$((x - z_i) \cdot (x - \bar{z}_i))^{m_i}$$

L'osservazione chiave è che il fattore di secondo grado $(x - z_i) \cdot (x - \bar{z}_i)$ è un polinomio reale. Infatti sia $z = a + ib$, $a, b \in \mathbb{R}$ e $b \neq 0$, allora:

$$(x - \underbrace{(a + ib)}_z) \cdot (x - \underbrace{(a - ib)}_{\bar{z}}) = x^2 - 2ax + a^2 + b^2$$

Come anticipato, i coefficienti del polinomio $(1, -2a + a^2 + b^2)$ sono reali. Riassumendo, date le radici complesse z_1, \dots, z_r di $f(x)$, se z_i è un numero reale allora $x - z_i$ è un fattore irriducibile di primo grado di $f(x)$ (ripetuto m_i volte) della fattorizzazione in $\mathbb{R}[x]$, se z_i non è un numero reale (ovvero $z_i = a + ib$ con $b \neq 0$) allora $(x - z_i) \cdot (x - \bar{z}_i)$ è un fattore di secondo grado della fattorizzazione in $\mathbb{R}[x]$ (ripetuto m_i volte) ed è irriducibile. Quest'ultima proprietà deriva dal fatto che, essendo di secondo grado, o è irriducibile o è il prodotto di due fattori di primo grado. Ma questa seconda opzione possiamo escluderla in quanto, dal teorema di Ruffini sappiamo che i fattori di primo grado sono associati ad una radice nel campo, e sappiamo, per ipotesi, che le radici del polinomio (che sono z e \bar{z}) non sono reali ($b \neq 0$).⁶ Dunque la fattorizzazione 2.2 di $f(x)$ in $\mathbb{C}[x]$ fatta di tutti fattori di grado 1, si *trasforma* in una fattorizzazione in $\mathbb{R}[x]$ di $f(x)$ tenendo inalterati i fattori con radici reali e *accorpando* in fattori irriducibili di secondo grado quelli corrispondenti a radici non reali (moltiplicando $x - z$ per $x - \bar{z}$).

Abbiamo scoperto che:

PROPOSIZIONE 8.22. *Ogni polinomio di grado maggiore di 2 in $\mathbb{R}[x]$ è riducibile.*

DIMOSTRAZIONE. Infatti in $\mathbb{C}[x]$ il polinomio $f(x)$ ha $n = \deg(f(x))$ radici (non necessariamente distinte)⁷ z_1, \dots, z_n . Se una di queste n radici è reale, allora $f(x)$ ha un fattore di grado 1 e dunque è riducibile, altrimenti se sono tutte radici complesse non reali, $f(x)$ è divisibile per il polinomio reale di secondo grado $(x - z_1) \cdot (x - \bar{z}_1)$:

$$f(x) = (x - z_1) \cdot (x - \bar{z}_1) \cdot h(x)$$

⁶Si poteva anche esprimere questa osservazione utilizzando il Corollario 8.8: un polinomio di grado 2 è irriducibile se e solo se non ha radici nel campo.

⁷Potrebbe essere anche tutte uguali e dunque una radice di molteplicità n .

E per la proprietà del grado del prodotto di polinomi, $h(x)$ ha grado maggiore di 1 e dunque non è invertibile. \square

Per concludere la piena caratterizzazione degli irriducibili in $\mathbb{R}[x]$, sapendo che (Proposizione 8.4) in ogni campo i polinomi di grado 1 sono irriducibili, ci resta da approfondire il caso dei polinomi di grado 2. Ma questo è molto semplice, infatti dal Corollario 8.8, sappiamo che $f(x) \in \mathbb{K}[x]$ di grado 2 è riducibile se e solo se ha una radice in \mathbb{K} . Nel caso di $\mathbb{K} = \mathbb{R}$ è noto dalla scuola superiore che, se $f(x) = ax^2 + bx + c$ è un generico polinomio reale di grado 2, allora $f(x)$ ha radici in \mathbb{R} se e solo se:

$$b^2 - 4ac \geq 0$$

Abbiamo dunque la completa caratterizzazione degli irriducibili in $\mathbb{R}[x]$:

In $\mathbb{R}[x]$ un polinomio è irriducibile se e solo è di primo grado oppure di secondo grado (del tipo $ax^2 + bx + c$ con $a \neq 0$) con $\Delta = b^2 - 4ac$ minore di zero.

Abbiamo dunque un *algoritmo* molto rapido per sapere se un polinomio $f(x)$ è riducibile in $\mathbb{R}[x]$ (basta guardare il grado ed eventualmente calcolare il delta nel caso il grado sia 2). Ma sapere che un polinomio $f(x)$ è riducibile non implica che la sua fattorizzazione in fattori irriducibili sia semplice da trovare.

ESERCIZIO 8.23. Fattorizzare il polinomio $x^4 - 2x^2 - 3 \in \mathbb{R}[x]$.

Questo polinomio è di grado 4 ed è dunque riducibile in $\mathbb{R}[x]$: o è il prodotto di quattro polinomi di grado 1 (4 radici reali non necessariamente distinte), o il prodotto di un polinomio di grado 2 e due di grado 1 (2 radici reali non necessariamente distinte e 2 complesse coniugate) o il prodotto di due polinomi di grado 2 (4 radici complesse a due a due coniugate e non necessariamente distinte). Come si evince da questa prima analisi sarebbe fondamentale riuscire a determinarne le radici complesse. Esiste una formula risolutiva per le equazioni di quarto grado, ma non la conosciamo e dunque cerchiamo di agire diversamente, osservando che il polinomio considerato è, in un certo senso, *particolare*: non ha termini di grado dispari. Possiamo quindi, con la semplice sostituzione $x^2 = t$, ottenere un polinomio di grado 2 associato a quello di partenza: $t^2 - 2t - 3$. Cerchiamo di fattorizzare questo polinomio in $\mathbb{R}[t]$. Dalla formula risolutiva delle equazioni di secondo grado otteniamo:

$$t_{1,2} = \frac{2 \pm \sqrt{16}}{2}$$

Ovvero $t^2 - 2t - 3 = (t - 3) \cdot (t + 1)$. Quindi:

$$x^4 - 2x^2 - 3 \underset{x^2=t}{=} t^2 - 2t - 3 = (t - 3) \cdot (t + 1) \underset{t=x^2}{=} (x^2 - 3) \cdot (x^2 + 1)$$

In questo caso è facile vedere che $x^2 + 1$ è irriducibile in $\mathbb{R}[x]$ (ha radici complesse i e $-i$), mentre $x^2 - 3 = (x - \sqrt{3}) \cdot (x + \sqrt{3})$. Concludendo si ha

che la fattorizzazione in irriducibili di $x^4 - 2x^2 - 3 \in \mathbb{R}[x]$ è data da:

$$(x - \sqrt{3}) \cdot (x + \sqrt{3}) \cdot (x^2 + 1)$$

2.3. Fattorizzazione in $\mathbb{Q}[x]$. In $\mathbb{Q}[x]$, a differenza di quanto visto per $\mathbb{C}[x]$ e $\mathbb{R}[x]$, vedremo che per ogni naturale n esistono polinomi di grado n irriducibili.

Una prima osservazione importante viene offerta dal Lemma di Gauss enunciato (senza dimostrazione) qui sotto: nel caso di un polinomio primitivo a coefficienti interi, la sua irriducibilità in $\mathbb{Q}[x]$ è equivalente alla sua irriducibilità in $\mathbb{Z}[x]$. Questo è un risultato per niente banale e scontato: infatti, per esempio, se è vero che è ovvio che un polinomio $f(x) \in \mathbb{K}[x]$, riducibile in $\mathbb{K}[x]$, è riducibile in qualsiasi campo \mathbb{L} che contenga strettamente \mathbb{K} (basta considerare la stessa fattorizzazione, infatti i polinomi di $\mathbb{K}[x]$ sono in particolare polinomi di $\mathbb{L}[x]$), il viceversa non è in generale vero. Ad esempio qualsiasi polinomio di secondo grado irriducibile in $\mathbb{R}[x]$ (ad esempio $x^2 + 1$) è riducibile in $\mathbb{C}[x]$ (nel caso di $x^2 + 1$ è uguale a $(x - i) \cdot (x + i)$).

LEMMA 8.24 (Lemma di Gauss). *Sia $f(x) \in \mathbb{Z}[x]$. Se $f(x) = a(x)b(x)$ in $\mathbb{Q}[x]$ allora possiamo trovare due polinomi $a_1(x) \in \mathbb{Z}[x]$, associato a $a(x)$, e $b_1 \in \mathbb{Z}[x]$, associato a $b(x)$, tali che*

$$f(x) = a_1(x)b_1(x)$$

Riassumendo, $g(x) \in \mathbb{Q}[x]$ è riducibile se e solo se il polinomio primitivo a coefficienti interi $f(x)$ ad esso associato è riducibile in $\mathbb{Z}[x]$. Abbiamo in definitiva ridotto la fattorizzazione in $\mathbb{Q}[x]$ a quella in $\mathbb{Z}[x]$ con notevoli vantaggi come vedremo da qui in avanti.

Cominciamo mostrando un primo criterio molto utile per riconoscere (e costruire) polinomi irriducibili in $\mathbb{Q}[x]$.

TEOREMA 8.25 (Criterio di Eisenstein). *Sia*

$$f(x) = \sum_{i=0}^n a_i x^i$$

un polinomio primitivo di grado maggiore di 1 a coefficienti interi. Se esiste un numero primo p tale che:

- (1) p NON divide il coefficiente direttivo a_n ,
- (2) p divide tutti gli a_i con $i < n$,
- (3) p^2 non divide il termine noto a_0 ,

allora $f(x)$ è irriducibile in $\mathbb{Z}[x]$, e dunque - per il lemma di Gauss - in $\mathbb{Q}[x]$.

DIMOSTRAZIONE. Supponiamo che $f(x)$ sia uguale al prodotto dei due polinomi $g(x) = \sum_{i=0}^r b_i x^i$ e $h(x) = \sum_{i=0}^s c_i x^i$ di $\mathbb{Z}[x]$, entrambi di grado maggiore o uguale a 1. Da $f(x) = g(x)h(x)$ e dalla definizione di uguaglianza tra polinomi, segue che tutti i coefficienti del polinomio a destra sono uguali a tutti i coefficienti del polinomio a sinistra. Facendo i conti, otteniamo un

sistema dove gli $n+1$ coefficienti a_i di $f(x)$ sono espressi tramite i coefficienti di $g(x)$ e $h(x)$ come segue⁸:

$$(2.3) \quad a_i = \sum_{j=0}^i b_j \cdot c_{i-j}$$

Partiamo *dal basso* del sistema 2.3: $a_0 = b_0c_0$. Per ipotesi p divide a_0 , ma p^2 non divide a_0 : questo significa che p divide uno tra b_0 e c_0 , ma non entrambi. Il ruolo dei b_i e dei c_i è simmetrico quindi possiamo, senza perdere di generalità, supporre che p divida b_0 e non c_0 .

A questo punto la seconda equazione del sistema 2.3 è $a_1 = b_1c_0 + b_0c_1$, che diventa:

$$b_1c_0 = a_1 - b_0c_1$$

Ora sappiamo che p divide a_1 (ipotesi), p divide b_0 (appena stabilito) e dunque p divide b_1c_0 . Sappiamo anche che p non divide c_0 e di conseguenza divide b_1 .

Iterando questo procedimento si ottiene che p divide ogni b_i e di conseguenza divide $a_n = b_n c_n$: ma questo è contro l'ipotesi. L'assurdo nasce dal fatto di aver supposto che $f(x)$, che verifica le tre condizioni del criterio di Eisenstein, possa essere scritto come prodotto di due polinomi di grado maggiore o uguale a 1. \square

Come detto il criterio di Eisenstein permette di costruire polinomi irriducibili in $\mathbb{Q}[x]$ e addirittura permette di trovarne *infiniti* per ogni grado $n > 0$:

COROLLARIO 8.26. *In $\mathbb{Q}[x]$ esistono polinomi irriducibili di grado $n > 0$ qualsiasi.*

DIMOSTRAZIONE. Basta considerare il polinomio $x^n - 2$ ed applicare Eisenstein con primo $p = 2$. Infatti 2 divide il termine noto (2), ma il quadrato di p (4) non divide il termine noto. E infine 2 non divide il coefficiente direttivo (1). Lo stesso ragionamento permette di dimostrare che $x^n - p$, per un qualsiasi primo p , è irriducibile. \square

Un altro punto importante per fattorizzare in $\mathbb{Q}[x]$ un polinomio $f(x)$ a coefficienti interi è il fatto che la conoscenza del coefficiente direttivo e del termine noto di $f(x)$ permette di limitare la ricerca delle *possibili* radici razionali di $f(x)$ (e dunque, in termini di fattorizzabilità, dei possibili fattori di grado 1 di $f(x)$) ad un insieme finito di numeri razionali. Per la precisione:

PROPOSIZIONE 8.27. *Se $f(x) \in \mathbb{Z}[x]$ e r/s (ridotto ai minimi termini, ovvero con $(r, s) = 1$) è una radice in \mathbb{Q} , allora r divide il termine noto e s divide il coefficiente direttivo di $f(x)$.*

⁸Esclusivamente per semplicità di notazione consideriamo anche i coefficienti nulli di $g(x)$ e $h(x)$ dei termini di grado maggiore rispettivamente di r e s . Ovvero $b_j = 0$ se $j > r$ e $c_t = 0$ se $t > s$.

DIMOSTRAZIONE. Sia $f(x) = \sum_{j=0}^m b_j x^j$ a coefficienti interi, l'ipotesi che r/s sia radice equivale a:

$$\sum_{i=0}^n b_i \left(\frac{r}{s}\right)^i = 0$$

Moltiplicando tutto per s^n si ottiene:

$$(2.4) \quad b_n r^n + \underbrace{b_{n-1} r^{n-1} s + \dots + b_0 s^n}_{\text{è un multiplo di } s} = 0$$

Per cui $s|b_n r^n$, ma essendo $(s, r) = 1$ questo implica $s|b_n$. Analogamente se raccogliamo in 2.4 r , otteniamo che r deve dividere $b_0 s^n$, ma essendo $(r, s) = 1$ questo implica che $r|b_0$. \square

ESEMPIO 8.28. Consideriamo il polinomio $f(x) = x^4 + 3x^3 + x^2 - 6x - 6$. Dalla Proposizione 8.27 segue che se r/s è una radice razionale, allora r divide -6 e s divide 1 . Ovvero sappiamo che le uniche radici razionali possibili di $f(x)$ sono da ricercare nell'insieme finito:

$$A = \{\pm 1, \pm 2, \pm 3, \pm 6\}$$

Sostituendo in $f(x)$ non si trova 0 in nessuno di questi casi, dunque $f(x)$ non ha radici razionali.

ATTENZIONE: questo non significa che $f(x)$ sia irriducibile! Sappiamo solo che $f(x)$ non ha fattori di grado 1, ma potrebbe essere il prodotto di due fattori irriducibili di grado 2.

ESERCIZIO 8.29. Il polinomio dell'esempio precedente è irriducibile in $\mathbb{Q}[x]$?

Suggerimento: se non vi riesce leggete più avanti...

La Proposizione 8.27 è di fondamentale importanza in quanto limita ad un insieme finito e ristretto la ricerca di possibili radici razionali (e quindi fattori irriducibili di grado 1) di un polinomio a coefficienti interi. Questo permette per esempio di avere un algoritmo per discutere l'irriducibilità di polinomi di grado 2 e 3 in $\mathbb{Q}[x]$, infatti un polinomio di questo tipo o è irriducibile o ha una radice razionale.

ESERCIZIO 8.30. Dire se $f(x) = x^3 - x^2 - 8x + 12$ è irriducibile in $\mathbb{Q}[x]$.

Risoluzione. I divisori del termine noto sono $\{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$, i divisori del coefficiente del termine di grado massimo sono $\{\pm 1\}$ quindi le possibili radici razionali sono: $\{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$. Proviamo a calcolare la funzione polinomiale $f(x)$ per questi valori fino a che non troviamo una radice; se non la troviamo vuol dire che $f(x)$ è irriducibile in $\mathbb{Q}[x]$:

$$f(1) = 4 \neq 0 \quad f(-1) = 18 \neq 0 \quad f(2) = 0$$

Dunque $f(x)$ è riducibile e ha $(x - 2)$ come fattore di grado 1.

A questo punto si potrebbe continuare a cercare altre radici razionali per vedere se ci sono altri fattori di $f(x)$ di grado 1 diversi da $(x - 2)$, ma

forse nel caso di un polinomio di grado 3 conviene procedere dividendo $f(x)$ per $(x - 2)$ in modo da trovare un fattore di grado 2 che sappiamo dire se è riducibile o meno in $\mathbb{Q}[x]$ attraverso la formula risolutiva delle equazioni di secondo grado:

$$\begin{array}{cccc|c} x^3 & -x^2 & -8x & +12 & x - 2 \\ x^3 & -2x^2 & & & x^2 + x - 6 \\ & x^2 & -8x & +12 & | \\ & x^2 & -2x & & | \\ & & -6x & +12 & | \\ & & -6x & +12 & | \\ & & & 0 & | \end{array}$$

Quindi $f(x) = (x - 2) \cdot (x^2 + x - 6)$. Si tratta di vedere se $x^2 + x - 6 = 0$ ha o meno due soluzioni razionali. Dalla formula risolutiva si ottiene:

$$x_{1,2} = \frac{-1 \pm \sqrt{25}}{2} = \frac{-1 \pm 5}{2}$$

E quindi $x^2 + x - 6$ è riducibile in $\mathbb{Q}[x]$ e si fattorizza come $(x + 3) \cdot (x - 2)$. La fattorizzazione in irriducibili di $x^3 - x^2 - 8x + 12$ in $\mathbb{Q}[x]$ è dunque data da:

$$x^3 - x^2 - 8x + 12 = (x - 2)^2 \cdot (x + 3)$$

A questo punto cominciamo ad avere diversi strumenti per la fattorizzazione in $\mathbb{Q}[x]$: innanzitutto sappiamo che ci possiamo ridurre ad un polinomio, associato a quello di partenza, primitivo e a coefficienti interi. Sui polinomi primitivi a coefficienti interi conosciamo un criterio *diretto* di irriducibilità (Eisenstein). Inoltre, la fattorizzazione è molto più semplice in $\mathbb{Z}[x]$. Cerchiamo di capire perché riprendendo in mano il polinomio $f(x)$ dell'Esempio 8.28. Abbiamo già visto che non ha radici, dunque se è fattorizzabile è il prodotto di due polinomi di grado 2 (che per il lemma di Gauss possiamo supporre a coefficienti interi).

Consideriamo due generici polinomi di grado 2 in $\mathbb{Z}[x]$:

$$\begin{aligned} g(x) &= ax^2 + bx + c \\ h(x) &= dx^2 + ex + f \end{aligned}$$

Per quanto osservato sopra, $f(x) = x^4 + 3x^3 + x^2 - 6x - 6$ è fattorizzabile se e solo se è il prodotto di due polinomi di grado 2, ovvero se e solo se esiste una soluzione del seguente sistema di 5 equazioni a coefficienti interi:

$$\begin{cases} 1 = a \cdot d \\ 3 = a \cdot e + b \cdot d \\ 1 = a \cdot f + b \cdot e + c \cdot d \\ -6 = b \cdot f + c \cdot e \\ -6 = c \cdot f \end{cases}$$

Sapere che, pur cercando la fattorizzazione in $\mathbb{Q}[x]$, possiamo risolvere in \mathbb{Z} è di grande aiuto. Infatti risolvere *algoritmicamente* questo sistema in \mathbb{Z} è possibile: ogni singola equazione infatti può avere solo un numero finito (anche uguale a 0) di soluzioni intere; studiando tutti i casi possibili e *risalendo* il sistema o si determina una soluzione intera o altrimenti si deduce che il sistema è irrisolvibile e dunque $f(x)$ è irriducibile in $\mathbb{Z}[x]$ e di conseguenza in $\mathbb{Q}[x]$. Questo procedimento di fattorizzazione in $\mathbb{Z}[x]$ risolvendo il sistema per casi è noto come **metodo della forza bruta**. Applichiamo questo metodo al nostro sistema: vedremo così concretamente i vantaggi di sapere di potersi limitare a cercare soluzioni intere del sistema. Da $1 = a \cdot d$ ad esempio, segue che o $a = d = 1$ oppure $a = d = -1$ (ma se $f(x) = g(x) \cdot h(x)$, allora $f(x) = -g(x) \cdot (-h(x))$ e dunque possiamo considerare $a = d = 1$). Andiamo dunque a riscriverci il nostro sistema:

$$\begin{cases} 1 = a \cdot d \\ 3 = a \cdot e + b \cdot d \\ 1 = a \cdot f + b \cdot e + c \cdot d \\ -6 = b \cdot f + c \cdot e \\ -6 = c \cdot f \end{cases} \leftrightarrow \begin{cases} a = d = 1 \\ 3 = e + b \\ 1 = f + b \cdot e + c \\ -6 = b \cdot f + c \cdot e \\ -6 = c \cdot f \end{cases}$$

Da $-6 = c \cdot f$ si ottiene che o $c = 1$ e $f = -6$, o $c = -1$ e $f = 6$, o $c = 2$ e $f = -3$ o infine $c = -2$ e $f = 3$ (essendo $g(x)$ e $h(x)$ dello stesso grado generici, il loro ruolo è completamente simmetrico e dunque non è necessario considerare anche i casi speculari tipo $c = 6$ e $f = -1$). Otteniamo dunque 4 sistemi con meno variabili. Bisogna studiarli tutti:

$$\begin{cases} a = d = 1 \\ 3 = e + b \\ 1 = -6 + b \cdot e + 1 \\ -6 = -6b + e \\ c = 1 \\ f = -6 \end{cases} \quad \begin{cases} a = d = 1 \\ 3 = e + b \\ 1 = 6 + b \cdot e - 1 \\ -6 = 6b - e \\ c = -1 \\ f = 6 \end{cases}$$

$$\begin{cases} a = d = 1 \\ 3 = e + b \\ 1 = -3 + b \cdot e + 2 \\ -6 = -3b + 2e \\ c = 2 \\ f = -3 \end{cases} \quad \begin{cases} a = d = 1 \\ 3 = e + b \\ 1 = 3 + b \cdot e - 2 \\ -6 = 3b - 2e \\ c = -2 \\ f = 3 \end{cases}$$

È facile verificare che i primi tre sistemi non hanno soluzioni intere (portano rispettivamente alle seguenti equazioni irrisolvibili in \mathbb{Z} : $5e = 12$, $7b = -3$, $5e = 3$), mentre l'ultimo ha soluzione (con $b = 0$ ed $e = 3$). Dunque esiste una fattorizzazione di $f(x)$ in $\mathbb{Q}[x]$ (nonostante $f(x)$ non abbia radici razionali):

$$\underbrace{x^4 + 3x^3 + x^2 - 6x - 6}_{f(x)} = \underbrace{(x^2 - 2)}_{g(x)} \underbrace{(x^2 + 3x + 3)}_{h(x)}$$

3. Esercizi

ESERCIZIO 8.31. Sia $g(x) \in \mathbb{R}[x]$ il polinomio

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

- (1) Fattorizzare $g(x)$ in prodotto di polinomi irriducibili.
- (2) Considerato il polinomio

$$f_a(x) = x^4 - 2ax^2 + 2ax - 1$$

dimostrare che, per ogni $a \in \mathbb{R}$, un M.C.D. tra $g(x)$ e $f_a(x)$ è il polinomio $x - 1$.

Risoluzione. Sappiamo che il polinomio $g(x)$ è riducibile in $\mathbb{R}[x]$, in quanto ha grado 3. Questo in particolare significa che $g(x)$ ha una radice reale. Osserviamo che non abbiamo studiato formule risolutive delle equazioni di terzo grado, quindi con i nostri strumenti possiamo trovare questa radice solo se è razionale (il polinomio che stiamo considerando in $\mathbb{R}[x]$ è a coefficienti interi): possiamo cioè provare tutte le possibili radici razionali che otteniamo dai divisori del coefficiente direttivo e del termine noto.

Però leggendo il testo dell'esercizio non abbiamo bisogno nemmeno di questo passaggio, infatti se dobbiamo mostrare che $x - 1$ è un M.C.D. di $g(x)$ con un altro polinomio, allora $x - 1$ dovrà essere un divisore di $g(x)$ (e quindi 1 una radice di $g(x)$). Andiamo a verificare che $x - 1$ è un fattore irriducibile di $g(x)$: che sia irriducibile è certo, visto che è di grado 1; dobbiamo mostrare che effettivamente è un divisore di $g(x)$ (se così non fosse potremmo intanto concludere che l'affermazione della seconda parte dell'esercizio è falsa). In realtà si vede subito che $x - 1$ è un divisore perchè $g(1) = 1 - 2 + 2 - 1 = 0$, ma a noi per la fattorizzazione interessa comunque dividere i due polinomi:

$$\begin{array}{cccc|c} x^3 & -2x^2 & +2x & -1 & x-1 \\ x^3 & -x^2 & & & x^2-x+1 \\ & -x^2 & +2x & -1 & \\ & -x^2 & +x & & \\ & & x & -1 & \\ & & & 0 & \end{array}$$

Abbiamo trovato che $g(x) = (x-1) \cdot (x^2 - x + 1)$, a questo punto verifichiamo se $x^2 - x + 1$ è riducibile o meno in $\mathbb{R}[x]$ attraverso il calcolo del delta: essendo negativo ($\Delta = 1 - 4 = -3$) il polinomio è irriducibile in $\mathbb{R}[x]$ e quindi la fattorizzazione cercata è proprio:

$$g(x) = (x - 1) \cdot (x^2 - x + 1).$$

A questo punto per dimostrare che $x - 1$ è un M.C.D. ($g(x), f_a(x)$) cominciamo mostrando che $x - 1$ divide $f_a(x)$ per ogni $a \in \mathbb{R}$ (e quindi è un fattore comune). Basta osservare che $f_a(1) = 1 - 2a + 2a - 1 = 0$. Ora se mostriamo che $x^2 - x + 1$ non è un divisore di $f_a(x)$ per qualsiasi scelta di a in \mathbb{R} , abbiamo la tesi. Procediamo dunque calcolando il resto della divisione di $f_a(x)$ per $x^2 - x + 1$, che sarà un polinomio $r_a(x)$ che dipenderà dal coefficiente a .

Dovremo osservare che $r_a(x)$ non è uguale al polinomio nullo qualsiasi sia la scelta di a in \mathbb{R} :

$$\begin{array}{cccc|c}
 x^4 & & -2ax^2 & +2ax & -1 & x^2 - x + 1 \\
 x^4 & -x^3 & +x^2 & & & x^2 + x - 2a \\
 & x^3 & +x^2 \cdot (-1 - 2a) & +2ax & -1 & \\
 & x^3 & -x^2 & +x & & \\
 & & -2a \cdot x^2 & +x \cdot (2a - 1) & -1 & \\
 & & -2a \cdot x^2 & +2a \cdot x & -2a & \\
 & & & -x & -1 + 2a &
 \end{array}$$

Osserviamo che il polinomio resto $r_a(x)$ è sempre di grado 1 qualsiasi sia la scelta di a in \mathbb{R} : in particolare non sarà mai uguale al polinomio nullo.

ESERCIZIO 8.32. Dato il polinomio $g(x) = 4x^3 + 5x^2 + 3x + 1$ fattorizzarlo in prodotto di irriducibili in $\mathbb{Q}[x]$ e in $\mathbb{Z}_{13}[x]$.

Risoluzione. Sappiamo che un polinomio di grado 3 è sicuramente riducibile in $\mathbb{R}[x]$ o in $\mathbb{C}[x]$, ma non conosciamo un algoritmo per trovare questa fattorizzazione. In $\mathbb{Q}[x]$ e in $\mathbb{Z}_p[x]$ un polinomio di grado 3 non sappiamo se è riducibile o no, ma abbiamo un algoritmo finito per rispondere a questa domanda e per trovare un'eventuale fattorizzazione in irriducibili del polinomio stesso. Questo perchè, come già osservato, la riducibilità di un polinomio di grado 3 è equivalente all'esistenza di una radice nel campo. Nel caso della riducibilità in $\mathbb{Q}[x]$ se il polinomio è a coefficienti interi (come $g(x)$) la Proposizione 8.27 permette di limitare le possibili radici razionali ad un insieme finito (tramite il calcolo dei divisori del termine noto e del coefficiente direttivo), mentre nel caso della riducibilità in $\mathbb{Z}_p[x]$ il numero delle possibili radici è ovviamente finito in quanto è finito il campo dei coefficienti.

I divisori del coefficiente direttivo sono $\{\pm 1, \pm 2 \pm 4\}$ mentre quelli del termine noto sono $\{\pm 1\}$, quindi le possibili radici razionali di $g(x)$ sono i numeri: $\{\pm \frac{1}{2}, \pm \frac{1}{4}, \pm 1\}$. Proviamoli, ma prima osserviamo che il polinomio $g(x)$ ha tutti coefficienti positivi e quindi non potrà avere radici positive. Ci possiamo dunque limitare a provare, tra le possibili radici razionali, quelle negative:

$$\begin{aligned}
 g(-\frac{1}{4}) &= -\frac{1}{16} + \frac{5}{16} - \frac{3}{4} + 1 = \frac{1}{2} \\
 g(-1) &= -4 + 5 - 3 + 1 = -1 \\
 g(-\frac{1}{2}) &= -\frac{1}{2} + \frac{5}{4} - \frac{3}{2} + 1 = \frac{1}{4}
 \end{aligned}$$

$g(x)$ non ha dunque radici razionali e quindi è irriducibile in $\mathbb{Q}[x]$.

Per quanto riguarda $\mathbb{Z}_{13}[x]$ valutando $g(x)$ per tutti gli elementi del campo si può verificare se esistono una o più radici. In questo caso troviamo $g(1) = 13 = 0$, quindi $g(x)$ è riducibile in $\mathbb{Z}_{13}[x]$ perché ha una radice e dunque per

Ruffini è divisibile per $x - 1$:

$$\begin{array}{r|l}
 4x^3 & +5x^2 & +3x & +1 & | & x - 1 \\
 4x^3 & -4x^2 & & & | & 4x^2 + 9x + 12 \\
 & 9x^2 & +3x & +1 & & \\
 & 9x^2 & -9x & & & \\
 & & 12x & +1 & & \\
 & & 12x & -12 & & \\
 & & & +13 & & \\
 & & & 0 & &
 \end{array}$$

Dunque $g(x) = (x - 1) \cdot (4x^2 + 9x + 12)$ in $\mathbb{Z}_{13}[x]$, si tratta di vedere se $4x^2 + 9x + 12$ è irriducibile o meno in $\mathbb{Z}_{13}[x]$. Per questo si può procedere in due modi: o si provano tutti gli elementi di $\mathbb{Z}_{13}[x]$ alla ricerca di un'eventuale radice, oppure si usa la seguente osservazione:

OSSERVAZIONE 8.33. La formula per la risoluzione delle equazioni di secondo grado vale in ogni campo \mathbb{K} (e quindi in particolare per campi finiti).

DIMOSTRAZIONE. Supponiamo di dover risolvere:

$$(3.1) \quad ax^2 + bx + c = 0$$

con a, b, c appartenenti ad un qualsiasi campo \mathbb{K} e $a \neq 0$ (questo per garantire che effettivamente stiamo risolvendo un'equazione di secondo grado). Ripercorriamo i passi che portano alla formula risolutiva delle equazioni reali di secondo grado per far vedere che le uniche cose che usiamo sono le proprietà di campo di \mathbb{R} :

(1) Sommiamo ad entrambi i membri di 3.1 l'opposto di c :

$$(3.2) \quad ax^2 + bx = -c$$

(2) Moltiplichiamo entrambi i membri per l'inverso di a che indichiamo con a^{-1} (sappiamo che esiste in \mathbb{K} l'inverso di $a \neq 0$):

$$(3.3) \quad x^2 + a^{-1} \cdot bx = a^{-1} \cdot (-c)$$

(3) Aggiungiamo ad entrambi i membri di 3.3 $[(2a)^2]^{-1} \cdot b^2$:

$$(3.4) \quad x^2 + a^{-1} \cdot bx + [(2a)^2]^{-1} \cdot b^2 = a^{-1} \cdot (-c) + [(2a)^2]^{-1} \cdot b^2$$

(4) È facile vedere (sfruttando la commutatività in \mathbb{K}) che il primo membro di 3.4 non è nient'altro che $(x + (2a)^{-1} \cdot b)^2$, si ha dunque:

$$(x + (2a)^{-1} \cdot b)^2 = a^{-1} \cdot (-c) + [(2a)^2]^{-1} \cdot b^2$$

che ha soluzione in \mathbb{K} se e solo se:

$$a^{-1} \cdot (-c) + [(2a)^2]^{-1} \cdot b^2 = [(2a)^2]^{-1} \cdot (b^2 - 4a \cdot c)$$

è un quadrato in \mathbb{K} .

Per concludere, basta osservare che $a \neq 0$ è un quadrato in \mathbb{K} se e solo se a^{-1} è un quadrato in \mathbb{K} e quindi $[(2a)^2]^{-1}$ è sempre un quadrato. Perciò l'equazione 3.1 ha soluzione in \mathbb{K} se e solo se $b^2 - 4a \cdot c$ (che solitamente indichiamo con Δ) è un quadrato in \mathbb{K} . Se in \mathbb{K} esiste radice di Δ e Δ è diverso da zero, allora ne esistono esattamente 2 distinte⁹. Le soluzioni dell'equazione 3.1 in questo caso sono allora due distinte e si ottengono sommando $-(2a)^{-1} \cdot b$ alle radici di Δ . \square

Il Δ in questo caso è uguale a $81 - 192 = -111$ che in \mathbb{Z}_{13} è equivalente a 6. Dobbiamo controllare se 6 è un quadrato in \mathbb{Z}_{13} :

$$0^2 = 0, 1^2 = 1, 2^2 = 4, 3^2 = 9, 4^2 = 16 = 3, 5^2 = 25 = 12, 6^2 = 10$$

E qui ci possiamo fermare perchè in \mathbb{Z}_{13} $7 = -6, 8 = -5, 9 = -4, 10 = -3, 11 = -2, 12 = -1$ e quindi i loro quadrati sono identici. Si può dunque concludere che 6 non è un quadrato in \mathbb{Z}_{13} e quindi $4x^2 + 9x + 12$ è irriducibile in $\mathbb{Z}_{13}[x]$.

ESERCIZIO 8.34. Fattorizzare il polinomio $f(x) = x^5 + x^2 + 1$ in $\mathbb{Q}[x]$.

Risoluzione. Il polinomio $f(x)$ non ha radici in $\mathbb{Q}[x]$. Infatti dalla Proposizione 8.27 sappiamo che le uniche possibili radici razionali di $f(x)$ sono 1 e -1 , ma valutando il polinomio in questi due valori si ottiene:

$$f(1) = 3 \quad f(-1) = 1$$

Il teorema di Ruffini ci dice dunque che $f(x)$ non ha fattori lineari in $\mathbb{Q}[x]$. A questo punto o $f(x)$ è irriducibile o è il prodotto di due polinomi irriducibili rispettivamente di secondo e terzo grado. Procediamo con il metodo della forza bruta (osserviamo che possiamo prendere i due eventuali polinomi fattore monici):

$$\begin{aligned} x^5 + x^2 + 1 &= (x^3 + ax^2 + bx + c)(x^2 + dx + e) = \\ &= x^5 + (a+d)x^4 + (e+ad+b)x^3 + (ae+bd+c)x^2 + (be+cd)x + ce \end{aligned}$$

Abbiamo dunque il seguente sistema a coefficienti interi:

$$\begin{cases} a + d = 0 \\ e + ad + b = 0 \\ ae + bd + c = 1 \\ be + cd = 0 \\ ce = 1 \end{cases}$$

Da $ce = 1$ seguono due possibilità $c = e = 1$ oppure $c = e = -1$, in entrambi i casi si ha $b = a = -d$. Sostituendo in $e + ad + b = 0$ si ottiene, nel caso $e = 1$:

$$a^2 - a - 1 = 0$$

⁹Supponiamo $\Delta \neq 0$ abbia radice in \mathbb{K} allora l'equazione $x^2 = \Delta$ è equivalente a

$$(x - \sqrt{\Delta}) \cdot (x + \sqrt{\Delta}) = 0$$

che in un campo, dove non ci sono divisori di zero, ha esattamente due soluzioni distinte $\sqrt{\Delta}$ e $-\sqrt{\Delta}$.

e nel caso $e = -1$:

$$a^2 - a + 1 = 0$$

In entrambi i casi non esistono soluzioni intere. Dunque il metodo della forza bruta ci dice che il polinomio $f(x)$ è irriducibile in $\mathbb{Q}[x]$.

ESERCIZIO 8.35. Fattorizzare il polinomio $f(x) = x^4 - 1$ in $\mathbb{Z}_5[x]$.

Risoluzione. Il polinomio $f(x)$ ha 1 come radice, dunque per il teorema di Ruffini è divisibile per $x - 1$. Osserviamo prima di proseguire che il risultato della divisione restituirà $f(x)$ come prodotto di $x - 1$ per un polinomio $g(x)$ di terzo grado. Per completare la fattorizzazione di $f(x)$ dovremo dunque studiare la riducibilità di $g(x)$ che, essendo di terzo grado, è equivalente alla ricerca di radici in $\mathbb{Z}_5[x]$ del polinomio suddetto. Procediamo ora con la divisione di $f(x)$ per $x - 1$:

$$\begin{array}{r|l}
 x^4 & -1 \\
 x^4 & -x^3 \\
 & x^3 \\
 & x^3 & -x^2 \\
 & & x^2 \\
 & & x^2 & -x \\
 & & & x \\
 & & & x \\
 & & & 0
 \end{array}
 \quad \left| \begin{array}{l}
 x - 1 \\
 x^3 + x^2 + x + 1 \\
 \\
 \\
 \\
 \\
 \\
 \\
 \\
 \end{array} \right.$$

Dunque:

$$x^4 - 1 = (x - 1) \underbrace{(x^3 + x^2 + x + 1)}_{g(x)}$$

Valutiamo se $g(x)$ ha radici in \mathbb{Z}_5 :

$$g(0) = 1 \quad g(1) = 4 \quad g(2) = 15 = 0 \quad g(3) = 40 = 0 \quad g(4) = 85 = 0$$

Perciò da Ruffini segue che $g(x)$ è fattorizzabile come:

$$g(x) = (x - 2)(x - 3)(x - 4)$$

Concludendo:

$$f(x) = (x - 1)(x - 2)(x - 3)(x - 4)$$

Osserviamo che potevamo arrivare alla conclusione in maniera molto più rapida sfruttando le proprietà degli \mathbb{Z}_p ed in particolare il piccolo teorema di Fermat. Infatti sappiamo che il polinomio $x^5 - x$ si annulla per ogni valore di \mathbb{Z}_5 e basta osservare che:

$$x^5 - x = x(x^4 - 1)$$

Ovvero $x^4 - 1$ si annulla in tutti gli elementi di \mathbb{Z}_5 tranne che in 0 e dunque è fattorizzabile proprio come:

$$f(x) = (x - 1)(x - 2)(x - 3)(x - 4)$$

ESERCIZIO 8.36. Sia $p(x) = x^4 - 4x^3 + 6x^2 - 4x + 5$. Sapendo che $2 + i$ è una radice complessa del polinomio $p(x)$ fattorizzarlo in $\mathbb{R}[x]$ e in $\mathbb{C}[x]$.

Risoluzione. Se $\alpha = 2 + i$ è radice, allora (Proposizione 8.19) anche il suo complesso coniugato $\bar{\alpha} = 2 - i$ è radice di $p(x)$. Dunque il polinomio è divisibile per:

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

Eseguiamo la divisione:

$$\begin{array}{r|l} x^4 & -4x^3 & +6x^2 & -4x & +5 & | & x^2 - 4x + 5 \\ x^4 & -4x^3 & +5x^2 & & & | & x^2 + 1 \\ & & x^2 & -4x & +5 & | & \\ & & x^2 & -4x & +5 & | & \\ & & & & 0 & | & \end{array}$$

Abbiamo dunque trovato che:

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

che è la fattorizzazione in irriducibili in $\mathbb{R}[x]$, infatti entrambi i polinomi di secondo grado non hanno soluzioni reali. Visto che $x^2 + 1$ ha come radici complesse i e $-i$ la fattorizzazione in irriducibili di $p(x)$ in $\mathbb{C}[x]$ è:

$$p(x) = (x - (2 + i))(x - (2 - i))(x - i)(x + i)$$

ESERCIZIO 8.37. Fattorizzare il polinomio $x^4 + 4x^3 - 19x^2 + 8x - 42$ come prodotto di irriducibili in $\mathbb{R}[x]$, $\mathbb{Q}[x]$, $\mathbb{Z}_3[x]$, $\mathbb{Z}_{13}[x]$.

ESERCIZIO 8.38. Fattorizzare il polinomio $x^4 - 4x^3 + x^2 + 8x - 6$ come prodotto di irriducibili in $\mathbb{R}[x]$, $\mathbb{Q}[x]$, $\mathbb{Z}_7[x]$, $\mathbb{Z}_{11}[x]$.

ESERCIZIO 8.39. Consideriamo il polinomio

$$p(x) = x^4 - x^3 - x^2 - x - 2$$

Fattorizzare $p(x)$ come prodotto di irriducibili in $\mathbb{R}[x]$, $\mathbb{C}[x]$, $\mathbb{Z}_3[x]$.

ESERCIZIO 8.40. Fattorizzare il polinomio $f(x) = x^6 - x^5 - 2x^4 - 2x^2 + 2x + 4$ come prodotto di irriducibili in $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$, $\mathbb{Z}_2[x]$, $\mathbb{Z}_3[x]$.

ESERCIZIO 8.41. Dimostrare che per ogni $p \in \mathbb{N}$ primo, il polinomio:

$$\sum_{i=0}^{p-1} x^i$$

è irriducibile in $\mathbb{Q}[x]$.

Prodotti scalari e spazi euclidei

1. Prodotto scalare

DEFINIZIONE 9.1. Sia V uno spazio vettoriale sul campo \mathbb{K} , dove $\mathbb{K} = \mathbb{R}$ o $\mathbb{K} = \mathbb{C}$. Un *prodotto scalare* è una funzione che ad ogni coppia di vettori u, v appartenenti a V associa lo scalare $\langle u, v \rangle \in \mathbb{K}$, con le seguenti proprietà:

- (1) $\langle au_1 + bu_2, v \rangle = a\langle u_1, v \rangle + b\langle u_2, v \rangle$, per ogni $u_1, u_2, v \in V$ e per ogni $a, b \in \mathbb{K}$;
- (2) $\langle u, v \rangle = \overline{\langle v, u \rangle}$ per ogni $u, v \in V$ (dove $\overline{\langle v, u \rangle}$ indica il numero complesso coniugato di $\langle v, u \rangle$);
- (3) per ogni $u \in V$ vale $\langle u, u \rangle \geq 0$ e $\langle u, u \rangle = 0$ vale se e solo se $u = O$.

Uno spazio vettoriale reale V munito di un prodotto scalare si dice *spazio euclideo*.

Osserviamo che, per la proprietà (2), il prodotto scalare $\langle u, u \rangle$ è sempre un numero reale, dunque ha senso la disuguaglianza che compare nella proprietà (3).

Per ogni vettore $u \in V$, scriveremo

$$\|u\| = \sqrt{\langle u, u \rangle}$$

e diremo che $\|u\|$ è la *norma* di u .

OSSERVAZIONE 9.2. Dalle proprietà (1) e (2) segue che

$$\langle u, av_1 + bv_2 \rangle = \bar{a}\langle u, v_1 \rangle + \bar{b}\langle u, v_2 \rangle$$

Se il campo \mathbb{K} è \mathbb{R} ovviamente tutti i simboli di coniugazione complessa che compaiono nelle formule precedenti possono essere ignorati.

L'esempio principale di prodotto scalare è dato dal prodotto scalare standard in \mathbb{R}^n . Dati due vettori u, v , rappresentati, rispetto alla base standard,

dalle colonne $u = \begin{pmatrix} a_1 \\ a_2 \\ \dots \\ a_n \end{pmatrix}$ e $v = \begin{pmatrix} b_1 \\ b_2 \\ \dots \\ b_n \end{pmatrix}$ il prodotto scalare standard è il

seguinte:

$$\langle u, v \rangle = a_1b_1 + a_2b_2 + \dots + a_nb_n$$

OSSERVAZIONE 9.3. Il prodotto scalare standard estende a tutti gli spazi \mathbb{R}^n un concetto che in \mathbb{R}^2 e \mathbb{R}^3 ci è già familiare. Potete facilmente verificare

che in questi casi per esempio $\|u\|$ coincide con quella che avete chiamato lunghezza del vettore u e che $\|v - u\|$ coincide con la distanza fra i vettori u e v . Inoltre $\langle u, v \rangle = 0$ se e solo se u e v sono ortogonali fra loro. Potete anche già osservare in \mathbb{R}^2 che vale la seguente relazione:

$$\langle u, v \rangle = \|u\| \|v\| \cos \theta$$

dove θ è l'angolo compreso fra i vettori u e v . Dimostreremo più in generale questa relazione fra qualche paragrafo.

Ecco altri due esempi di prodotto scalare:

ESEMPIO 9.4. In \mathbb{C}^n , dati i vettori

$$u = \begin{pmatrix} a_1 \\ a_2 \\ \dots \\ a_n \end{pmatrix}, \quad v = \begin{pmatrix} b_1 \\ b_2 \\ \dots \\ b_n \end{pmatrix}$$

scritti rispetto alla base standard, abbiamo il prodotto scalare

$$\langle u, v \rangle = a_1 \bar{b}_1 + a_2 \bar{b}_2 + \dots + a_n \bar{b}_n$$

ESEMPIO 9.5. Nello spazio vettoriale delle funzioni continue reali nell'intervallo $[a, b]$,¹ abbiamo il seguente prodotto scalare:

$$\langle f, g \rangle = \int_a^b f(t)g(t)dt$$

2. Ortogonalità

Sia V uno spazio vettoriale munito di un prodotto scalare. Estendiamo il concetto di perpendicolarità che ci è noto in \mathbb{R}^2 e \mathbb{R}^3 dando la seguente definizione:

DEFINIZIONE 9.6. Due vettori $u, v \in V$ sono detti *ortogonali* se

$$\langle u, v \rangle = 0$$

Notiamo che se due vettori verificano $\langle u, v \rangle = 0$ vale anche che $\langle v, u \rangle = \overline{\langle u, v \rangle} = 0$ dunque il concetto di ortogonalità non dipende dall'ordine con cui stiamo considerando i due vettori. Inoltre dalla definizione si ricava subito che il vettore O è ortogonale a tutti i vettori di V :

$$\langle O, v \rangle = \langle 0O, v \rangle = 0 \langle O, v \rangle = 0$$

Sia U un sottospazio di V . L'insieme dato dai vettori di V che sono ortogonali ad ogni vettore di U si indica con U^\perp :

$$U^\perp = \{v \in V \mid \langle v, u \rangle = 0 \forall u \in U\}$$

¹Questo spazio vettoriale, a differenza di tutti gli altri spazi considerati in queste dispense, non ha una base finita; si tratta dunque di uno spazio vettoriale di dimensione infinita.

Si verifica facilmente che U^\perp è un sottospazio vettoriale di V , chiamato il *sottospazio ortogonale* a U .

ESERCIZIO 9.7. Fare questa verifica.

DEFINIZIONE 9.8. Un insieme $\{u_1, \dots, u_r\}$ di vettori si dice *ortogonale* se i suoi elementi sono vettori a due a due ortogonali fra loro. L'insieme $\{u_1, \dots, u_r\}$ si dice *ortonormale* se è ortogonale e se per ogni i vale $\|u_i\| = 1$.

ESEMPIO 9.9. Nello spazio euclideo \mathbb{R}^n con il prodotto scalare standard, i vettori della base standard ($u_1 = \begin{pmatrix} 1 \\ 0 \\ \dots \\ 0 \end{pmatrix}$ etc...) costituiscono un insieme ortonormale.

TEOREMA 9.10. Sia V uno spazio vettoriale munito di un prodotto scalare. Un insieme ortonormale di vettori $\{u_1, \dots, u_r\}$ è linearmente indipendente e, per ogni $v \in V$, il vettore

$$w = v - \langle v, u_1 \rangle u_1 - \langle v, u_2 \rangle u_2 - \dots - \langle v, u_r \rangle u_r$$

è ortogonale ad ognuno degli u_i , dunque appartiene a $\text{Span}(u_1, \dots, u_r)^\perp$.

DIMOSTRAZIONE. Supponiamo di avere una combinazione lineare degli u_i uguale a O :

$$a_1 u_1 + \dots + a_r u_r = O$$

Per dimostrare la lineare indipendenza dei vettori u_1, \dots, u_r dobbiamo dimostrare che per ogni i vale $a_i = 0$.

Fissato un i , consideriamo il prodotto scalare di entrambi i membri dell'uguaglianza con u_i :

$$\langle a_1 u_1 + \dots + a_r u_r, u_i \rangle = \langle O, u_i \rangle$$

ovvero

$$a_1 \langle u_1, u_i \rangle + \dots + a_r \langle u_r, u_i \rangle = 0$$

Vista la ortonormalità dell'insieme $\{u_1, \dots, u_r\}$ questo implica $a_i = 0$.

Ripetendo questa considerazione per ogni $i = 1, \dots, r$ si dimostra che i vettori u_1, \dots, u_r sono linearmente indipendenti.

Verifichiamo adesso che w è ortogonale a u_i per ogni i :

$$\begin{aligned} \langle w, u_i \rangle &= \langle v, u_i \rangle - \langle v, u_1 \rangle \langle u_1, u_i \rangle - \dots - \langle v, u_r \rangle \langle u_r, u_i \rangle = \\ &= \langle v, u_i \rangle - \langle v, u_1 \rangle 0 - \dots - \langle v, u_i \rangle 1 - \dots - \langle v, u_r \rangle 0 = 0 \end{aligned}$$

□

Il teorema appena dimostrato è l'ingrediente principale del procedimento di ortogonalizzazione di Gram-Schmidt, che permette di ottenere una base ortonormale "modificando" una base data.

TEOREMA 9.11 (Procedimento di ortogonalizzazione di Gram-Schmidt).
 Sia V uno spazio vettoriale munito di un prodotto scalare, e sia v_1, \dots, v_n una qualunque base di V . Allora esiste una base u_1, \dots, u_n di V che è ortonormale e tale che, per ogni $i = 1, \dots, n$, $u_i \in \text{Span}(v_1, \dots, v_i)$.

DIMOSTRAZIONE. Per prima cosa poniamo $u_1 = \frac{v_1}{\|v_1\|}$. L'insieme $\{u_1\}$ è ortonormale.

Come secondo passo consideriamo il vettore $v_2 - \langle v_2, u_1 \rangle u_1$: questo vettore è diverso da O per la lineare indipendenza di v_1, v_2 e per il Teorema 9.10, applicato riferendosi all'insieme ortonormale $\{u_1\}$, è ortogonale a u_1 . Inoltre appartiene al sottospazio $\text{Span}(v_1, v_2)$.

È dunque un buon candidato per essere il nostro u_2 ; l'unico problema è che non ha norma 1. Per rimediare a questo basta moltiplicarlo per un opportuno scalare. Poniamo dunque :

$$u_2 = \frac{v_2 - \langle v_2, u_1 \rangle u_1}{\|v_2 - \langle v_2, u_1 \rangle u_1\|}$$

Per le osservazioni precedenti, l'insieme $\{u_1, u_2\}$ è ortonormale.

Facciamo un ulteriore passo, per illustrare meglio il procedimento. A questo punto consideriamo il vettore $v_3 - \langle v_3, u_1 \rangle u_1 - \langle v_3, u_2 \rangle u_2$. Questo vettore è diverso da O (altrimenti v_3 apparterebbe a $\text{Span}(v_1, v_2)$ contro l'ipotesi che v_1, v_2, \dots, v_n è una base) e per il Teorema 9.10, applicato riferendosi all'insieme ortonormale $\{u_1, u_2\}$, è ortogonale a $\text{Span}(u_1, u_2)$.

Inoltre, visto che u_1 e u_2 appartengono a $\text{Span}(v_1, v_2)$, il vettore $v_3 - \langle v_3, u_1 \rangle u_1 - \langle v_3, u_2 \rangle u_2$ appartiene a $\text{Span}(v_1, v_2, v_3)$ e ha dunque tutte le proprietà da noi richieste, eccetto quella di avere norma 1.

Come sopra, poniamo dunque:

$$u_3 = \frac{v_3 - \langle v_3, u_1 \rangle u_1 - \langle v_3, u_2 \rangle u_2}{\|v_3 - \langle v_3, u_1 \rangle u_1 - \langle v_3, u_2 \rangle u_2\|}$$

Una semplice dimostrazione per induzione ci mostra che possiamo proseguire questo procedimento ricorsivo fino a compiere n passi e definire u_n come

$$u_n = \frac{v_n - \langle v_n, u_1 \rangle u_1 - \langle v_n, u_2 \rangle u_2 - \dots - \langle v_n, u_{n-1} \rangle u_{n-1}}{\|v_n - \langle v_n, u_1 \rangle u_1 - \langle v_n, u_2 \rangle u_2 - \dots - \langle v_n, u_{n-1} \rangle u_{n-1}\|}$$

L'insieme $\{u_1, \dots, u_n\}$ sarà ortonormale e tale che, per ogni i , $u_i \in \text{Span}(v_1, \dots, v_i)$.

In particolare, i vettori u_1, \dots, u_n sono una base di V , visto che per il Teorema 9.10 sono linearmente indipendenti e $n = \dim V$.

□

Il teorema appena dimostrato dimostra in particolare che ogni spazio V munito di un prodotto scalare ha una base ortonormale.

ESERCIZIO 9.12. Applicare il procedimento di ortogonalizzazione alla seguente base di \mathbb{R}^2 :

$$v_1 = \begin{pmatrix} 2 \\ 2 \end{pmatrix}, \quad v_2 = \begin{pmatrix} 3 \\ -1 \end{pmatrix}$$

ESERCIZIO 9.13. Trovare una base ortonormale di \mathbb{R}^3 il cui primo vettore sia $(\frac{1}{3}, \frac{2}{3}, \frac{2}{3})$.

OSSERVAZIONE 9.14 (Angolo fra due vettori in \mathbb{R}^n). Consideriamo $V = \mathbb{R}^n$ munito del prodotto scalare standard. Siano u e v due vettori linearmente indipendenti di \mathbb{R}^n . Come sappiamo dal Teorema 9.10, applicato partendo dall'insieme ortonormale di vettori dato da un solo vettore, ossia $\{\frac{u}{\|u\|}\}$, il vettore

$$w = v - \left\langle v, \frac{u}{\|u\|} \right\rangle \frac{u}{\|u\|}$$

è ortogonale a $\frac{u}{\|u\|}$. Possiamo riscrivere questa relazione così

$$v = w + \left\langle v, \frac{u}{\|u\|} \right\rangle \frac{u}{\|u\|}$$

e ci accorgiamo che ci indica che nel piano $Span(u, v)$ i vettori $O, z = \left\langle v, \frac{u}{\|u\|} \right\rangle \frac{u}{\|u\|}, v$ determinano un triangolo rettangolo, con l'ipotenusa di lunghezza $\|v\|$ e i due cateti di lunghezza rispettivamente $\|w\|$ e $|\langle v, \frac{u}{\|u\|} \rangle| = \frac{|\langle v, u \rangle|}{\|u\|}$ (vedi Figura 1).

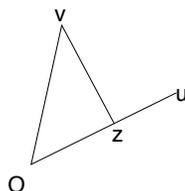


FIGURA 1. Dati due vettori $u, v \in \mathbb{R}^n$, i vettori $O, z = \left\langle v, \frac{u}{\|u\|} \right\rangle \frac{u}{\|u\|}, v$ determinano un triangolo rettangolo, visto che $w = v - \left\langle v, \frac{u}{\|u\|} \right\rangle \frac{u}{\|u\|}$ è ortogonale alla retta generata da u .

Chiamiamo θ l'angolo compreso fra l'ipotenusa e il cateto di lunghezza $\frac{|\langle v, u \rangle|}{\|u\|}$, ovvero l'angolo compreso fra u e v (andrebbe indicato quale dei due angoli stiamo considerando, ma siccome ne prenderemo il coseno non occorre in realtà precisare). Come sappiamo dalla geometria elementare vale

$$\|v\| \cos \theta = \frac{|\langle v, u \rangle|}{\|u\|}$$

da cui ricaviamo la relazione

$$\|u\| \|v\| \cos \theta = |\langle v, u \rangle|$$

a cui avevamo già accennato nella Osservazione 9.3. Come potete facilmente verificare, tale relazione vale anche se u e v non sono linearmente indipendenti, dunque vale per qualsiasi coppia di vettori in \mathbb{R}^n .

Introducendo il prodotto scalare standard, abbiamo dunque “recuperato” la trigonometria all’interno dell’algebra lineare.

3. La disuguaglianza di Cauchy-Schwarz

Dato un prodotto scalare $\langle \cdot, \cdot \rangle$ su V , abbiamo il seguente teorema:

TEOREMA 9.15 (Disuguaglianza di Cauchy-Schwarz). *Per ogni coppia di vettori $u, v \in V$ vale*

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

DIMOSTRAZIONE. Cominciamo osservando che se $v = O$, la disuguaglianza diventa $0 \leq 0$ dunque è vera.

Supponiamo dunque $v \neq O$, e calcoliamo, usando le proprietà del prodotto scalare, il quadrato della norma del vettore $u - \langle u, v \rangle tv$, dove $t \in \mathbb{R}$.

$$\begin{aligned} \|u - \langle u, v \rangle tv\|^2 &= \langle u - \langle u, v \rangle tv, u - \langle u, v \rangle tv \rangle = \\ &= \langle u, u \rangle - \overline{\langle u, v \rangle} t \langle u, v \rangle - \langle u, v \rangle t \langle v, u \rangle + \overline{\langle u, v \rangle} \langle u, v \rangle t^2 \langle v, v \rangle = \\ &= \|u\|^2 - 2t(|\langle u, v \rangle|)^2 + (|\langle u, v \rangle|)^2 t^2 \|v\|^2 \end{aligned}$$

Osserviamo che $\|u - \langle u, v \rangle tv\|^2 \geq 0$ dunque possiamo scrivere

$$\|u\|^2 - 2t(|\langle u, v \rangle|)^2 + (|\langle u, v \rangle|)^2 t^2 \|v\|^2 \geq 0$$

Questo vale per qualsiasi $t \in \mathbb{R}$. Scegliendo adesso $t = \frac{1}{\|v\|^2}$ ricaviamo:

$$\|u\|^2 - \frac{(|\langle u, v \rangle|)^2}{\|v\|^2} \geq 0$$

da cui si ottiene la tesi. □

ESEMPIO 9.16. Nel caso in cui V sia \mathbb{R}^n col prodotto scalare standard, la disuguaglianza di Cauchy-Schwarz si traduce così. Dati

$$u = \begin{pmatrix} a_1 \\ a_2 \\ \dots \\ a_n \end{pmatrix}, \quad v = \begin{pmatrix} b_1 \\ b_2 \\ \dots \\ b_n \end{pmatrix}$$

vale

$$|a_1 b_1 + a_2 b_2 + \dots + a_n b_n| \leq (a_1^2 + \dots + a_n^2)(b_1^2 + \dots + b_n^2)$$

che può essere pensata anche, svincolandosi dai vettori e dagli spazi vettoriali, come una disuguaglianza che riguarda due qualsiasi n -uple a_1, \dots, a_n e b_1, \dots, b_n di numeri reali.

ESEMPIO 9.17. Nel caso in cui V sia lo spazio delle funzioni continue reali definite sull'intervallo $[0, 1]$, col prodotto scalare descritto nell'Esempio 9.5, la disuguaglianza di Cauchy-Schwarz si traduce nella seguente importante disuguaglianza fra integrali:

$$\left(\int_0^1 f(t)g(t)dt \right)^2 \leq \int_0^1 f(t)^2 dt \int_0^1 g(t)^2 dt$$

4. Sottospazi ortogonali

Sia V , come nei paragrafi precedenti, uno spazio vettoriale munito di prodotto scalare.

PROPOSIZIONE 9.18. *Sia U un sottospazio vettoriale di V . Allora esiste una base ortonormale di U che è un sottoinsieme di una base ortonormale di V .*

DIMOSTRAZIONE. Partiamo da una qualunque base v_1, \dots, v_r di U , ed estendiamo ad una base v_1, \dots, v_n di V (usando il Teorema 2.19). Ora utilizziamo il procedimento di ortogonalizzazione di Gram-Schmidt alla base v_1, \dots, v_n : otteniamo una base ortonormale u_1, \dots, u_n di V , con la proprietà che i vettori u_1, \dots, u_r appartengono a $\text{Span}(v_1, \dots, v_r)$, ossia a U . Dunque u_1, \dots, u_r è una base ortonormale di U , che è un sottoinsieme di una base ortonormale di V , come volevamo. □

TEOREMA 9.19. *Sia U un sottospazio vettoriale di V . Allora V si decompone come somma diretta di U e di U^\perp :*

$$V = U \oplus U^\perp$$

In particolare vale che $\dim U^\perp = \dim V - \dim U$.

DIMOSTRAZIONE. Osserviamo innanzitutto che $U \cap U^\perp = \{O\}$, dunque i due sottospazi sono in somma diretta.

Infatti se $v \in U \cap U^\perp$ allora $\langle v, v \rangle = 0$ (in altre parole, visto che $v \in U^\perp$, v deve essere ortogonale a tutti i vettori di U , fra cui se stesso). Ma per la proprietà (3) del prodotto scalare da $\langle v, v \rangle = 0$ si ricava $v = O$.

Non ci resta che dimostrare che $U + U^\perp = V$, ossia che ogni vettore di V può essere scritto come somma di un vettore di U e di un vettore di U^\perp . Poniamo $r = \dim U$. Per la Proposizione 9.18 sappiamo che esiste una base ortonormale u_1, \dots, u_n di V tale che i primi r vettori u_1, \dots, u_r sono una base ortonormale di U .

Un qualunque vettore $v \in V$ può essere scritto come combinazione lineare dei vettori di questa base:

$$v = a_1 u_1 + \dots + a_r u_r + a_{r+1} u_{r+1} + \dots + a_n u_n$$

Osserviamo a questo punto che $a_1 u_1 + \dots + a_r u_r \in U$ come osservato sopra, mentre $a_{r+1} u_{r+1} + \dots + a_n u_n \in U^\perp$ per la ortonormalità della base u_1, \dots, u_n ,

dunque la scrittura

$$v = (a_1u_1 + \cdots + a_ru_r) + (a_{r+1}u_{r+1} + \cdots + a_nu_n)$$

esprime v come somma di un vettore di U e di un vettore di U^\perp . □

ESERCIZIO 9.20. Sia V uno spazio vettoriale di dimensione finita munito di un prodotto scalare e sia U un sottospazio vettoriale di V . Dimostrare che $(U^\perp)^\perp = U$.

OSSERVAZIONE 9.21 (Ortogonalità e sistemi lineari). Consideriamo $V = \mathbb{R}^n$ munito del prodotto scalare standard. Dato un sottospazio W , con base

$$w_1, \dots, w_r, \text{ dove } w_1 = \begin{pmatrix} a_1 \\ a_2 \\ \dots \\ a_n \end{pmatrix}, w_2 = \begin{pmatrix} b_1 \\ b_2 \\ \dots \\ b_n \end{pmatrix}, \text{ etc... se pensiamo a come si}$$

scrive il prodotto scalare ci rendiamo conto i vettori di W^\perp sono esattamente le soluzioni del sistema

$$\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \dots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \dots \\ 0 \end{pmatrix}$$

ESERCIZIO 9.22. Dimostrare che, dato un sottospazio U di uno spazio V munito di un prodotto scalare, e data una base ortonormale u_1, \dots, u_n di V tale che i primi r vettori u_1, \dots, u_r sono una base ortonormale di U , la mappa $T : V \rightarrow V$ data da $T(v) = v - \langle v, u_1 \rangle u_1 - \langle v, u_2 \rangle u_2 - \cdots - \langle v, u_r \rangle u_r$ è lineare, ha per immagine U^\perp e ha nucleo uguale a U . Dimostrare inoltre che $T^2 = T$ (dunque, in base all'Esercizio 7.47 possiamo dire che T è una proiezione di V su U^\perp ; in particolare T viene chiamata la *proiezione ortogonale* di V su U).

5. Esercizi

ESERCIZIO 9.23. Sia V lo spazio vettoriale delle funzioni continue reali nell'intervallo $[-\pi, \pi]$, munito del prodotto scalare:

$$\langle f, g \rangle = \int_{-\pi}^{\pi} f(t)g(t)dt$$

Verificare che il seguente sottoinsieme è ortogonale:

$$1, \cos t, \cos 2t, \dots, \sin t, \sin 2t, \dots$$

[Attenzione, come vedete si tratta di un insieme infinito: del resto lo spazio vettoriale che stiamo considerando è, a differenza di tutti gli altri spazi considerati in queste dispense, di dimensione infinita. L'insieme proposto

è molto importante in matematica, in particolare nella teoria delle *serie di Fourier*.]

ESERCIZIO 9.24. Dato uno spazio vettoriale V munito di un prodotto scalare, dimostrare che la norma soddisfa la seguente *disuguaglianza triangolare*:

$$\|u + v\| \leq \|u\| + \|v\|$$

ESERCIZIO 9.25. Si consideri \mathbb{R}^4 munito del prodotto scalare standard. Dato il sottospazio W generato dai vettori $(1, -2, 3, 3)$ e $(3, -5, 4, 4)$, trovare una base del sottospazio W^\perp .

ESERCIZIO 9.26. Si consideri \mathbb{R}^4 munito del prodotto scalare standard. Dato il sottospazio W generato dai vettori $(1, -2, 3, 3)$ e $(3, -5, 4, 4)$, trovare una base ortonormale di W usando il procedimento di ortogonalizzazione di Gram-Schmidt.

ESERCIZIO 9.27. Si consideri \mathbb{R}^4 munito del prodotto scalare standard. Dato il sottospazio W generato dai vettori $(1, 1, 0, 0)$ e $(0, 1, 1, 0)$, $(0, 0, 1, 1)$, trovare una base ortonormale di W usando il procedimento di ortogonalizzazione di Gram-Schmidt.

ESERCIZIO 9.28. Si consideri \mathbb{C}^3 munito del prodotto scalare descritto nell'Esempio 9.4. Sia W il sottospazio generato dai vettori $(1, \iota, 1)$ e $(1 + \iota, -0, 1)$. Trovare una base ortonormale per W .

Indice analitico

- $Det(a_{ij})$, 125
- $End(V)$, 115
- $GL(V)$, 116

- addizione tra matrici, 35
- addizione vettoriale, 5
- applicazione identità, 43
- applicazione lineare, 32
- autospazio relativo ad un autovalore, 133
- autovalore di un endomorfismo, 133
- autovettore di un endomorfismo, 133

- base di uno spazio vettoriale, 26

- chiusura per l'addizione vettoriale, 7
- chiusura per la moltiplicazione scalare, 7
- coefficienti di una combinazione lineare di vettori, 21
- combinazione lineare, 21
- complementare di un sottospazio vettoriale, 112
- coniugio su \mathbb{C} , 161
- criterio della molteplicità algebrica e geometrica, 144
- criterio di Eisenstein, 165

- determinante di una matrice, 125
- dimensione di uno spazio vettoriale, 29
- dipendenza lineare, 24
- disuguaglianza di Cauchy-Schwarz, 181
- disuguaglianza triangolare, 184

- endomorfismo diagonalizzabile, 134
- endomorfismo lineare, 115
- endomorfismo nilpotente, 151

- forma a scalini per colonne, 51
- forma a scalini per colonne ridotta, 53
- forma a scalini per righe, 66

- forma a scalini per righe ridotta, 67

- generatori di uno spazio vettoriale, 22
- gruppo generale lineare, 116

- indipendenza lineare, 24
- insieme ortonormale di vettori, 179
- isomorfismo lineare, 62

- legge di annullamento, 10
- legge di cancellazione, 10
- lemma di Gauss, 165

- matrice, 35
- matrice associata ad una applicazione lineare, 40
- matrice di cambiamento di base, 120
- matrice di Vandermonde, 130
- matrice identità, 43
- matrice nilpotente, 151
- minore di una matrice, 127
- molteplicità algebrica di un autovalore, 143
- molteplicità geometrica di un autovalore, 143
- moltiplicazione scalare, 5
- moltiplicazione scalare nello spazio delle matrici, 35

- norma di un vettore, 177
- nucleo di una applicazione lineare, 32

- operazioni elementari sulle colonne, 49
- operazioni elementari sulle righe, 66

- pivot, 51
- polinomi
 - fattorizzazione, 155
 - metodo della forza bruta, 169
 - polinomio irriducibile, 156
 - polinomio primitivo, 156
 - polinomio riducibile, 156

teorema di fattorizzazione unica per
 polinomi, 158
 polinomio caratteristico di un
 endomorfismo, 136
 procedimento di ortogonalizzazione di
 Gram-Schmidt, 180
 prodotto esterno, 7
 prodotto riga per colonna tra matrici,
 36
 prodotto scalare, 5, 177
 profondità di una colonna, 50
 profondità di una riga, 66
 proiezione lineare, 152
 proiezione ortogonale, 184

 rango di una applicazione lineare, 65
 rango di una matrice, 71
 regola di Sarrus, 126
 rotazione, 134

 scalare, 6
 serie di Fourier, 184
 somma diretta di sottospazi, 112
 somma vettoriale, 5
 sottospazio generato da un insieme di
 vettori, 22
 sottospazio ortogonale, 179
 sottospazio proprio, 12
 sottospazio vettoriale, 12
 Span di vettori, 22
 spazio euclideo, 177
 spazio vettoriale somma, 20

 Teorema di Binet, 128
 Teorema di Cayley-Hamilton, 151
 teorema fondamentale dell'algebra, 160
 traccia di un endomorfismo, 121
 traccia di una matrice, 48

 vettore, 6
 vettori ortogonali, 178

Bibliografia

- [Ab] M. Abate, *Algebra Lineare*, McGraw-Hill.
- [C] L.Childs, *Algebra: un'introduzione concreta*, ETS, 1991.
- [DM-D] P. Di Martino, *Algebra*, Pisa University Press, 2013.
- [H] I.N.Herstein, *Algebra*, Editori Riuniti, 1988.
- [R] K. H. Rosen, *Discrete mathematics and its applications*, Mc Graw-Hill, 2003.
- [AlgGauss] <http://marekrychlik.com/cgi-bin/gauss.cgi>
- [WIMS] <http://wims.unice.fr/wims/wims.cgi>