Enrico Gregorio Luigi Salce

Algebra Lineare

Edizioni Libreria Progetto
Padova

Indice

Prefazione

Sebbene l'Algebra Lineare sia una delle parti più antiche di tutta la matematica, il suo corpo centrale in forma moderna si è costituito e consolidato nel XIX secolo, e alcuni rilevanti sviluppi sono stati ottenuti nella prima metà del 1900. Essa costituisce tuttora un fertile campo di indagine sia dal punto di vista teorico che per le svariate applicazioni all'interno della matematica, come in teoria degli anelli e dei moduli, e in molte altre discipline scientifiche, quali economia, statistica, demografia, informatica e diversi settori dell'ingegneria.

Esistono sul mercato librario universitario un gran numero di libri di Algebra Lineare, sia a livello elementare che avanzato, sia in lingua italiana che, soprattutto, in lingua inglese. Si può dire che, con i libri di "Calculus", quelli di Algebra Lineare sono i più diffusi testi di matematica a livello universitario, costituendo le due discipline del calcolo differenziale-integrale e di teoria delle matrici le basi matematiche di qualsivoglia applicazione alle altre discipline scientifiche.

Perché allora proporre l'$n+1$-esimo libro di Algebra Lineare? Possiamo dire che prima di tutto c'è un motivo egoistico: abbiamo sentito l'esigenza di ritagliare un programma che ci soddisfi, e i libri in commercio non ci soddisfano mai del tutto: sono troppo succinti o troppo ampi, a un livello troppo semplice o troppo elevato, e così via. Abbiamo cioè voluto un libro che trattasse proprio quello che desideriamo insegnare nei nostri corsi e l'abbiamo esposto al livello a nostro avviso più adatto alle nuove esigenze delle lauree triennali italiane, con uno sguardo attento agli sviluppi negli anni successivi e ai corsi di base delle lauree magistrali.

Il secondo autore ha alle spalle un'esperienza analoga, avendo scritto un libro sulla teoria degli autovalori, in prosecuzione di un libro scritto da Brunella Bruno sugli argomenti più basilari di Algebra Lineare. A distanza di una dozzina d'anni da quella prima esperienza, il fatto che quei libri siano andati in esaurimento, e ancor più l'entrata ormai a regime della riforma universitaria in Italia, ci hanno indotto a ripetere l'esperienza aggiornandola con i suggerimenti derivati da svariati lustri di insegnamento nella disciplina.

Questo libro parte dalle operazioni sulle matrici (che sono sempre a coefficienti reali o complessi) e termina con un capitolo contenente risultati di un certo rilievo sugli autovalori delle matrici hermitiane. Tra questi due estremi vengono trattati i classici argomenti dei sitemi di equazioni lineari, la teoria degli spazi vettoriali, quella degli spazi euclidei, la teoria dei determinanti e quella degli autovalori.

Ma, oltre ad argomenti tradizionali, abbiamo inserito alcuni aspetti di teoria delle matrici meno usuali nei testi di stampo classico, almeno italiani, di Algebra Lineare. Ne forniamo di seguito qualche esempio:

- la matrice pseudo-inversa di Moore-Penrose;
- la decomposizione in valori singolari e la decomposizione polare di una matrice;
- il teorema di Ostrowski sul confronto di autovalori di matrici congruenti;
- il teorema di Schur sul confronto diagonale-spettro di matrici hermitiane;
- il teorema di monotonicità di Weyl e il pricipio di inclusione di Poincaré per le matrici hermitiane;
- il teorema di Birkhoff sulle matrici bistocastiche;
- il collegamento tra numeri complessi e quaternioni con le matrici 2×2 a coefficienti reali e complessi, rispettivamente;
- una dimostrazione del Teorema Fondamentale dell'Algebra che fa uso, oltre che di risultati elementari sui polinomi reali, di soli strumenti di Algebra Lineare.

Il libro vuole portare gradualmente lo studente dai fatti più semplici sulle matrici a risultati complessi e profondi; perciò la difficoltà del testo aumenta col progredire dei Capitoli. Ciò comporta che il libro può proficuamente essere utilizzato in corsi e anni diversi. Per esempio, i primi quattro Capitoli (a parte qualche Paragrafo) costituiscono un corso elementare di base che può essere svolto più o meno in sessanta ore al primo anno di corso, mentre gli ultimi due Capitoli possono entrare nel programma di un corso più avanzato e occupare dalle trenta alle quaranta ore.

Ogni Capitolo è seguito da un certo numero di esercizi di tipo diverso: alcuni esercizi non sono altro che la richiesta di provare alcuni fatti di cui nel testo si è omessa la dimostrazione (o perché molto facile, o perché noiosa); altri per esemplificare la teoria, altri ancora per fornire risultati teorici di un certo rilievo a completamento di un argomento. Non compaiono in genere esercizi di tipo numerico, che saranno oggetto di una raccolta apposita.

Il libro è stato scritto tenendo anche presente i problemi degli studenti-lavoratori che non possono seguire le lezioni del docente: molte definizioni e risultati sono seguiti da esempi che ne illustrano il significato, scelti tra i più semplici possibili. Su molte spiegazioni ci si sofferma discorsivamente per aiutare la comprensione di concetti e teoremi.

La simbologia e terminologia impiegate sono quelle usuali, fatta eccezione per il concetto di 'insieme finito di vettori', sul quale però non si insiste in modo troppo formale. La fine delle dimostrazioni e degli esempi viene indicata con un quadratino.

I due autori dono docenti in corsi di laurea in Informatica, Matematica e Statistica; il libro può essere utilizzato per insegnamenti di Algebra Lineare in questi corsi, come pure in corsi di laurea della Facoltà di Ingegneria, sia nelle lauree triennali che in quelle magistrali.

A conclusione, dobbiamo sentitamente ringraziare Gemma Parmeggiani che ha iniziato con noi la fatica di questo libro e ce ne ha lasciato buone porzioni già ben rifinite. Ogni svista o errore è però a totale carico nostro e preghiamo il lettore di segnalarceli ai seguenti indirizzi:

`enrico.gregorio@univr.it` — `salce@math.unipd.it`

Padova, settembre 2005

In questa edizione sono stati corretti gli errori di stampa e alcune piccole parti. Ringraziamo tutti coloro che hanno segnalato le sviste.

Padova, febbraio 2008

Nella terza edizione abbiamo apportato altre correzioni, grazie anche alle segnalazioni dei lettori.

Padova, settembre 2010

Capitolo 1

Matrici e sistemi di equazioni lineari

Il primo obiettivo di questo Capitolo è quello di introdurre le matrici a coefficienti complessi e le loro principali operazioni: la somma di due matrici, il prodotto di uno scalare per una matrice e il prodotto righe per colonne di due matrici. In relazione a queste operazioni vengono poi studiati gli operatori di trasposizione e di H-trasposizione, nonché le decomposizioni a blocchi delle matrici, di cui sono illustrati gli esempi più usati.

Il secondo obiettivo del Capitolo è quello di presentare l'algoritmo di eliminazione di Gauss per risolvere i sistemi di equazioni lineari; è questo il metodo più antico e più semplice per risolvere un sistema lineare, ma al tempo stesso il più efficiente. Come applicazione notevole dell'eliminazione di Gauss viene presentato l'algoritmo di inversione di una matrice quadrata. Un intero paragrafo è dedicato al problema della ricerca di matrici inverse di una matrice qualunque; si introduce anche la matrice pseudo-inversa, di cui sono provate esistenza e unicità.

La parte finale del Capitolo è dedicata allo studio delle matrici elementari e al loro impiego nella decomposizione LU di una generica matrice. La decomposizione LU è uno dei pilastri portanti dell'Algebra Lineare. Le matrici elementari saranno usate nel Capitolo 4 nel corso della trattazione dei determinanti.

1. Matrici e loro operazioni

Questo paragrafo introduce le principali operazioni che si possono eseguire sulle matrici: somma e prodotto di due matrici, prodotto di una matrice per uno scalare. Queste operazioni si basano sulle usuali operazioni di somma e prodotto tra numeri, dove con "numeri" si intenderanno sempre elementi dell'insieme $\mathbb{C}$ dei numeri complessi, o, in particolare, del suo sottoinsieme $\mathbb{R}$ dei numeri reali, o del sottoinsieme $\mathbb{Q}$ dei numeri razionali. I numeri complessi saranno chiamati anche *scalari*, e saranno denotati con lettere greche: α, β, γ, eccetera.

Una *matrice* è una tabella di numeri (o di simboli che rappresentano numeri) disposti in righe e colonne; tali numeri, detti *coefficienti* (o *entrate*) della matrice, sono per comodità racchiusi usualmente tra parentesi. L'unico coefficiente della matrice che si trova nella i-esima riga e nella j-esima colonna si chiama *coefficiente di posto* (i, j). Diremo anche che una matrice con m righe ed n colonne ha *dimensioni* $m \times n$, o semplicemente che è una matrice $m \times n$.

Esempio 1.1. Le seguenti tabelle di numeri

$$\mathbf{A} = \begin{bmatrix} 1+i & 2-i \\ 3 & -i \end{bmatrix}$$

$$\mathbf{B} = \begin{bmatrix} 2 \\ -\pi \end{bmatrix}$$

$$\mathbf{C} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \end{bmatrix}$$

costituiscono esempi, rispettivamente, di matrici 2×2 a coefficienti complessi, 2×1 a coefficienti reali e 3×4 a coefficienti razionali. □

Designeremo sempre le matrici con lettere maiuscole "in nero". Una generica matrice $\mathbf{A}$ $m \times n$, in cui sono messe in evidenza la i-esima riga e la j-esima colonna, ha il seguente aspetto:

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1j} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2j} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{i1} & a_{i2} & \dots & a_{ij} & \dots & a_{in} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mj} & \dots & a_{mn} \end{bmatrix};$$

si noti che ogni coefficiente di $\mathbf{A}$ viene contrassegnato da due indici, di cui il primo dice in quale riga si trova il coefficiente e il secondo in quale colonna.

In maniera più compatta, tale matrice verrà anche denotata nel modo seguente

$$\mathbf{A} = [a_{ij}]_{j \le n}^{i \le m}$$

o più semplicemente con $\mathbf{A} = [a_{ij}]$ se le dimensioni di $\mathbf{A}$ sono note.

Introduciamo fin dall'inizio alcune speciali classi di matrici.

Matrici quadrate

Sono quelle matrici $m \times n$ per cui $m = n$, tali cioè che il numero delle righe è uguale al numero delle colonne. Tale numero viene chiamato *ordine* della matrice. Nel caso di matrici quadrate si può parlare della *diagonale (principale)* della matrice, costituita dai coefficienti di posto (i, i) $(1 \le i \le m)$, che sono detti per l'appunto *coefficienti diagonali*. Si considera anche la *diagonale secondaria*, costituita dai coefficienti di posto $(i, m - i + 1)$ $(1 \le i \le m)$. La seguente matrice

$$\begin{bmatrix} 1 & 2 & 3 \\ 5 & 6 & 7 \\ 9 & 10 & 11 \end{bmatrix}$$

è un esempio di matrice quadrata di ordine 3, con diagonale $(1,6,11)$ e diagonale secondaria $(3,6,9)$.

Matrici diagonali

Le matrici diagonali sono quelle matrici quadrate che hanno tutti i coefficienti al di fuori della diagonale uguali a 0, quindi del tipo

$$\mathbf{D} = \begin{bmatrix} d_1 & 0 & 0 & \dots & 0 \\ 0 & d_2 & 0 & \dots & 0 \\ 0 & 0 & d_3 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & d_n \end{bmatrix}.$$

Una tale matrice sarà denotata con $\mathbf{Diag}(d_1, d_2, d_3, \dots, d_n)$. Ovviamente basta un solo indice per contrassegnare i coefficienti sulla diagonale.

Matrici scalari

Una matrice scalare è una matrice diagonale in cui tutti i coefficienti diagonali sono uguali tra di loro, quindi del tipo $\mathbf{Diag}(d, d, d, \dots, d)$. Una tale matrice è individuata dal suo ordine e dal coefficiente che compare sulla diagonale. Tra tutte le matrici, le matrici scalari sono quelle che più si avvicinano ai numeri, e questo anche dal punto di vista delle operazioni (si veda l'Esercizio 1.1).

Matrici triangolari superiori

Le matrici triangolari superiori sono quelle matrici quadrate in cui i coefficienti *al di sotto* della diagonale sono nulli. Una tale matrice $\mathbf{A} = [a_{ij}]$ è pertanto definita dalle relazioni

$$a_{ij} = 0 \quad \text{per } i > j.$$

Le matrici triangolari superiori saranno spesso denotate con il simbolo $\mathbf{T}$ o con il simbolo $\mathbf{U}$ (che sta per *upper*). Una generica matrice triangolare superiore 3×3 è quindi del tipo

$$\begin{bmatrix} t_{11} & t_{12} & t_{13} \\ 0 & t_{22} & t_{23} \\ 0 & 0 & t_{33} \end{bmatrix}.$$

Se tutti i coefficienti diagonali sono uguali a 1, la matrice si chiama *uni-triangolare superiore*.

Matrici triangolari inferiori

Le matrici triangolari inferiori sono quelle matrici quadrate in cui i coefficienti *al di sopra* della diagonale sono nulli. Una tale matrice $\mathbf{A} = [a_{ij}]$ è pertanto definita dalle relazioni

$$a_{ij} = 0 \quad \text{per } i < j.$$

Una generica matrice triangolare inferiore 3×3 è quindi del tipo

$$\begin{bmatrix} t_{11} & 0 & 0 \\ t_{21} & t_{22} & 0 \\ t_{31} & t_{32} & t_{33} \end{bmatrix}.$$

Le matrici triangolari inferiore saranno spesso denotate anche con il simbolo $\mathbf{T}$ o con il simbolo $\mathbf{L}$ (che sta per *lower*). Se tutti i coefficienti diagonali sono uguali a 1, la matrice si chiama *uni-triangolare inferiore*.

Matrici nulle

Una matrice $m \times n$ in cui *tutti* i coefficienti sono uguali a 0 è detta matrice *nulla* ed è denotata col simbolo $\mathbb{O}_{mn}$; gli indici saranno omessi, e la matrice si denoterà semplicemente con $\mathbb{O}$, se sarà chiaro dal contesto quali sono le dimensioni della matrice.

Matrici riga e colonna

Una matrice $1 \times n$, quindi con una sola riga, si chiama *matrice riga*, mentre una matrice $m \times 1$, quindi con una sola colonna, si chiama *matrice colonna*. Le matrici colonna saranno chiamate anche *vettori (colonna)* (con il termine tra parentesi usualmente omesso), e denotati anche con lettere minuscole "in nero": $\mathbf{v}$, $\mathbf{u}$, $\mathbf{w}$, eccetera. Le matrici riga invece saranno chiamate *vettori riga* e denotate, per motivi che appariranno evidenti più avanti, coi seguenti simboli: $\mathbf{v}^T$, $\mathbf{u}^T$, $\mathbf{w}^T$, eccetera. I coefficienti di un vettore (riga o colonna) saranno anche chiamati *coordinate*.

Un esempio di vettore 2×1 è fornito dalla matrice $\mathbf{B}$ nell'Esempio 1.1. Un generico vettore riga con n coordinate sarà scritto nella forma

$$\mathbf{v}^T = [v_1 \ v_2 \ \dots \ v_n];$$

evidentemente, in un vettore (riga o colonna) basta un solo indice per contrassegnare le coordinate.

Vettori coordinati

Tra i vettori (colonna) ce ne sono alcuni di particolare utilità; essi sono chiamati *vettori coordinati* e sono caratterizzati dal fatto di avere tutte le coordinate nulle tranne una che è uguale a 1; se la coordinata non nulla è la i-esima, il vettore coordinato è denotato con $\mathbf{e}_i$; l'analogo vettore riga coordinato è denotato con $\mathbf{e}_i^T$. Si ha quindi

$$\mathbf{e}_i = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \qquad \mathbf{e}_i^T = [0 \ \dots \ 0 \ 1 \ 0 \ \dots \ 0]$$

dove gli 1 si trovano all'i-esimo posto.

Introduciamo ora le due più semplici operazioni che si possono eseguire sulle matrici: il prodotto per scalari e la somma.

Prodotto per scalari

Data una matrice $m \times n$ $\mathbf{A} = [a_{ij}]$ e uno scalare α, si definisce la matrice *prodotto dello scalare* α *per la matrice* $\mathbf{A}$ come quella matrice, denotata con $\alpha\mathbf{A}$, che ha come coefficiente di posto (i, j) il numero αa_{ij}; pertanto

$$\alpha\mathbf{A} = [\alpha a_{ij}].$$

Si può definire analogamente il prodotto di $\mathbf{A}$ per lo scalare α come la matrice $\mathbf{A}\alpha = [a_{ij}\alpha]$; tale matrice coincide evidentemente con $\alpha\mathbf{A}$, attesa la commutatività del prodotto tra scalari, pertanto $\alpha\mathbf{A} = \mathbf{A}\alpha$.

Esempio 1.2. Se $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$ sono le matrici dell'Esempio 1.1, si ha

$$i\mathbf{A} = \begin{bmatrix} i-1 & 2i+1 \\ 3i & 1 \end{bmatrix}, \qquad \pi^{-1}\mathbf{B} = \begin{bmatrix} 2\pi^{-1} \\ -1 \end{bmatrix}, \qquad -1\mathbf{C} = \begin{bmatrix} -1 & -2 & -3 & -4 \\ -5 & -6 & -7 & -8 \\ -9 & -10 & -11 & -12 \end{bmatrix} \qquad \square$$

La matrice $-1\mathbf{C}$ nell'Esempio 1.2 viene denotata più semplicemente con $-\mathbf{C}$. In generale, data la matrice $\mathbf{A} = [a_{ij}]$, si pone

$$-\mathbf{A} = [-a_{ij}];$$

$-\mathbf{A}$ si chiama *matrice opposta* di $\mathbf{A}$. Si osservi che la matrice prodotto di una data matrice per uno scalare produce una matrice delle stesse dimensioni della matrice data. L'operazione di prodotto per scalare gode delle seguenti proprietà, la cui verifica è del tutto evidente:

(p_1) $1\mathbf{A} = \mathbf{A}$;

(p_2) $0\mathbf{A} = \mathbb{O}$;

(p_3) $(\alpha\beta)\mathbf{A} = \alpha(\beta\mathbf{A})$.

Somma di matrici

Date due matrici $\mathbf{A} = [a_{ij}]$ e $\mathbf{B} = [b_{ij}]$ delle medesime dimensioni $m \times n$, si definisce come loro *somma* la matrice

$$\mathbf{A} + \mathbf{B} = [a_{ij} + b_{ij}].$$

Quindi la somma tra matrici è definita nel modo più naturale possibile, e viene detta *somma per componenti.* Sottolineiamo il fatto che, con la definizione data sopra, non si può eseguire la somma tra due matrici che hanno dimensioni diverse (cioè il numero delle righe oppure quello delle colonne, o entrambi, sono differenti).

Esempio 1.3. Date le due matrici 2×2

$$\mathbf{A} = \begin{bmatrix} i-1 & 2i+1 \\ 3i & 1 \end{bmatrix}, \qquad \mathbf{B} = \begin{bmatrix} i+1 & 2i-1 \\ i & -1 \end{bmatrix}$$

risulta

$$\mathbf{A}+\mathbf{B} = \begin{bmatrix} 2i & 4i \\ 4i & 0 \end{bmatrix}.$$ □

Esempio 1.4. La somma di due matrici scalari (rispettivamente: diagonali, triangolari superiori, triangolari inferiori) delle stesse dimensioni è ancora una matrice scalare (rispettivamente: diagonale, triangolare superiore, triangolare inferiore). □

L'operazione di somma tra matrici gode di numerose proprietà, anche in relazione a quella di prodotto per scalari, che elenchiamo di seguito. La verifica di queste proprietà è del tutto evidente.

Se $\mathbf{A}$, $\mathbf{B}$ e $\mathbf{C}$ sono tre matrici di dimensioni $m \times n$, e α, β sono scalari, allora

(S_1) $\mathbf{A}+(\mathbf{B}+\mathbf{C}) = (\mathbf{A}+\mathbf{B})+\mathbf{C}$,

(S_2) $\mathbf{A}+\mathbf{B} = \mathbf{B}+\mathbf{A}$,

(S_3) $\mathbf{A}+\mathbb{O}_{mn} = \mathbf{A}$,

(S_4) $\mathbf{A}+(-\mathbf{A}) = \mathbb{O}_{mn}$,

(pS_1) $\alpha(\mathbf{A}+\mathbf{B}) = \alpha\mathbf{A}+\alpha\mathbf{B}$,

(pS_2) $(\alpha+\beta)\mathbf{A} = \alpha\mathbf{A}+\beta\mathbf{A}$.

Si possono definire diversi tipi di prodotto tra matrici. Ad esempio, si può definire l'operazione di prodotto nel modo più semplice possibile, cioè *per componenti*, in modo analogo a quanto fatto con la somma; tale operazione è detta anche *prodotto di Hadamard-Schur*. Un altro modo più complicato è tramite il cosiddetto *prodotto di Kronecker*, o *prodotto tensoriale*. Pur essendo tali prodotti interessanti per numerose applicazioni, essi sono meno fondamentali del prodotto che ora andremo a studiare e non saranno qui trattati.

Passiamo quindi a definire l'operazione di prodotto tra due matrici di gran lunga più usata, che viene detta *prodotto righe per colonne*. Partiremo dal caso più semplice del prodotto di una sola riga per una sola colonna, per passare poi al caso generale.

Prodotto di vettore riga per vettore colonna

Dati un vettore riga $\mathbf{v}^T$ e un vettore colonna $\mathbf{u}$ con lo stesso numero di coordinate, tali cioè che le loro dimensioni siano rispettivamente $1 \times n$ e $n \times 1$, denotiamo con $v_1, v_2, \dots, v_n$ le coordinate di $\mathbf{v}^T$ e con $u_1, u_2, \dots, u_n$ le coordinate di $\mathbf{u}$. Si chiama *prodotto (riga per colonna)* dei due vettori, e lo si denota con $\mathbf{v}^T\mathbf{u}$, il numero (o matrice 1×1)

$$\mathbf{v}^T\mathbf{u} = v_1u_1 + v_2u_2 + \cdots + v_nu_n.$$

Le seguenti proprietà del prodotto di un vettore riga per un vettore colonna sono del tutto evidenti: $\mathbf{v}^T\mathbf{0} = 0$; $\mathbf{v}^T\mathbf{u} = \mathbf{u}^T\mathbf{v}$.

Esempio 1.5. Dato un vettore riga $\mathbf{v}^T = [v_1\ v_2\ \dots\ v_n]$, il prodotto di $\mathbf{v}^T$ per l'i-esimo vettore coordinato $\mathbf{e}_i$ coincide con v_i, la i-esima coordinata di $\mathbf{v}^T$. Il prodotto di $\mathbf{v}^T$ per il vettore colonna $\mathbf{u}$ che ha n coordinate tutte uguali a 1 è

$$\mathbf{v}^T\mathbf{u} = v_1 + v_2 + \ldots + v_n.$$

Il prodotto di $\mathbf{v}^T \neq \mathbf{0}^T$ per un vettore colonna $\mathbf{w} \neq \mathbf{0}$ può dare 0; per esempio, se $\mathbf{v}^T = [1\ 0]$ e $\mathbf{w} = [0\ 1]^T$. □

Prodotto di matrici righe per colonne

Consideriamo ora due matrici $\mathbf{A}$ e $\mathbf{B}$ e definiamo il loro *prodotto righe per colonne*. Va detto subito che

> *il prodotto righe per colonne di* **A** *per* **B** *è possibile solo se il numero di colonne di* **A** *coincide col numero di righe di* **B**.

Deve quindi risultare $\mathbf{A}$ di dimensioni $m \times n$ e $\mathbf{B}$ di dimensioni $n \times p$. Due matrici che si trovano in questa situazione rispetto alle dimensioni si dicono *conformi per il prodotto*.

La nozione base per definire questo prodotto è quella appena vista di prodotto di vettore riga per vettore colonna. È utile a tal fine porre in evidenza le righe della matrice $\mathbf{A}$:

$$\mathbf{A} = \begin{bmatrix} \mathbf{r}_1^T \\ \mathbf{r}_2^T \\ \dots \\ \mathbf{r}_m^T \end{bmatrix}.$$

Se $\mathbf{A} = [a_{ij}]$, allora $\mathbf{r}_i^T = [a_{i1}\ a_{i2}\ \dots\ a_{in}]$. Mettiamo anche in evidenza le colonne della matrice $\mathbf{B}$:

$$\mathbf{B} = [\mathbf{b}_1\mathbf{b}_2\ldots\mathbf{b}_p]$$

dove ciascun vettore colonna $\mathbf{b}_j$ ha n coordinate. Se $\mathbf{B} = (b_{ij})$, allora

$$\mathbf{b}_j = \begin{bmatrix} b_{1j} \\ b_{2j} \\ \dots \\ b_{nj} \end{bmatrix}.$$

Visto che il numero di coordinate di ciascun vettore riga $\mathbf{r}_i^T$ è uguale al numero delle coordinate di ciascun vettore colonna $\mathbf{b}_j$, è possibile eseguire il prodotto $\mathbf{r}_i^T\mathbf{b}_j$. La matrice prodotto righe per colonne della matrice $\mathbf{A}$ per la matrice $\mathbf{B}$, che viene denotata con $\mathbf{AB}$, è la matrice di dimensioni $m \times p$ definita nel modo seguente:

$$\mathbf{AB} = [\mathbf{r}_i^T\mathbf{b}_j]_{j\le p}^{i\le m}.$$

Esempio 1.6. Date le due matrici

$$\mathbf{A} = \begin{bmatrix} 1+i & 2-i \\ 3 & -i \end{bmatrix}, \qquad \mathbf{B} = \begin{bmatrix} i \\ -1 \end{bmatrix}$$

risulta

$$\mathbf{AB} = \begin{bmatrix} (1+i)i + (2-i)(-1) \\ 3i + i \end{bmatrix} = \begin{bmatrix} -3+2i \\ 4i \end{bmatrix},$$

mentre il prodotto **BA** non si può eseguire. □

D'ora in avanti, quando parleremo di prodotto tra due matrici, intenderemo sempre il prodotto righe per colonne. Questo modo di definire il prodotto sembra alquanto artificioso. Tale artificiosità scompare, non appena si pensi a rappresentare tramite tale prodotto un sistema di m equazioni lineari in n incognite:

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

Il sistema si può rappresentare semplicemente tramite l'uguaglianza del vettore (detto *vettore dei termini noti*)

$$\mathbf{b} = \begin{bmatrix} b_1 \\ b_2 \\ \ldots \\ b_m \end{bmatrix}$$

con il vettore che ha come coordinate i primi membri delle m equazioni

$$\begin{bmatrix} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n \\ \ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n \end{bmatrix}.$$

Quest'ultimo vettore non è altro che il risultato del prodotto righe per colonne della matrice (detta *matrice dei coefficienti*)

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{bmatrix}$$

per il vettore (detto *vettore delle incognite*)

$$\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ \ldots \\ x_n \end{bmatrix}.$$

Pertanto il sistema di equazioni si può scrivere in forma compatta, detta *forma matriciale* del sistema:

$$\mathbf{Ax} = \mathbf{b}.$$

Diamo qui di seguito le più importanti proprietà cui soddisfa il prodotto tra matrici, anche in relazione alle due operazioni di somma e di prodotto per scalari.

(P_1) Se $\mathbf{A}, \mathbf{B}$ e $\mathbf{C}$ sono tre matrici di dimensioni rispettivamente $m \times n$, $n \times p$ e $p \times q$, allora

$$\mathbf{A}(\mathbf{BC}) = (\mathbf{AB})\mathbf{C}.$$

Sia $[a_{ij}] = \mathbf{A}$, $[b_{ij}] = \mathbf{B}$ e $[c_{ij}] = \mathbf{C}$. Sia inoltre $[d_{ij}] = \mathbf{A}(\mathbf{BC})$ e $[e_{ij}] = (\mathbf{AB})\mathbf{C}$. Per la proprietà distributiva risulta:

$$d_{ij} = \sum_{1 \le h \le n} a_{ih} \sum_{1 \le k \le p} b_{hk} c_{kj} = \sum_{1 \le k \le p} c_{kj} \sum_{1 \le h \le n} a_{ih} b_{hk} = e_{ij}.$$

(P_2) Se $\mathbf{A}$ è una matrice $n \times p$, allora

$$\mathbb{O}_{mn}\mathbf{A} = \mathbb{O}_{mp}, \qquad \mathbf{A}\mathbb{O}_{pq} = \mathbb{O}_{nq}.$$

Per dare la proprietà successiva dobbiamo introdurre un nuovo tipo di matrici scalari: fissato $n \ge 1$, denotiamo con $\mathbf{I}_n$ la matrice scalare $n \times n$ che ha sulla diagonale il numero 1:

$$\mathbf{I}_n = \mathbf{Diag}(1,1,1,\dots,1) = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \end{bmatrix}.$$

Le matrici $\mathbf{I}_n$ sono chiamate *matrici identità*, per il motivo che appare chiaro dalla proprietà seguente.

(P_3) Se $\mathbf{A}$ è una matrice $n \times p$, allora

$$\mathbf{I}_n\mathbf{A} = \mathbf{A} = \mathbf{A}\mathbf{I}_p.$$

Questa proprietà è un caso particolare del seguente Esempio 1.8 e la sua dimostrazione è lasciata al lettore.

(PS_1) Se $\mathbf{A}$ è una matrice $m \times n$ e $\mathbf{B}$ e $\mathbf{C}$ sono matrici $n \times p$, allora

$$\mathbf{A}(\mathbf{B}+\mathbf{C}) = \mathbf{AB} + \mathbf{AC}.$$

Sia $[d_{ij}] = \mathbf{A}(\mathbf{B}+\mathbf{C})$ e $[e_{ij}] = \mathbf{AB} + \mathbf{AC}$. Risulta

$$d_{ij} = \sum_{1 \le k \le n} a_{ik}(b_{kj} + c_{kj}) = \sum_{1 \le k \le n} a_{ik} b_{kj} + \sum_{1 \le k \le n} a_{ik} c_{kj} = e_{ij}.$$

(PS_2) Se $\mathbf{A}$ e $\mathbf{B}$ sono matrici $m \times n$ e $\mathbf{C}$ è una matrice $n \times p$, allora

$$(\mathbf{A}+\mathbf{B})\mathbf{C} = \mathbf{AC} + \mathbf{BC}.$$

La dimostrazione è analoga a quella della proprietà precedente.

(Pp) Se $\mathbf{A}$ e $\mathbf{B}$ sono matrici conformi per il prodotto e α è uno scalare, allora

$$\alpha(\mathbf{AB}) = (\alpha\mathbf{A})\mathbf{B} = \mathbf{A}(\alpha\mathbf{B}).$$

La dimostrazione è lasciata come facile esercizio per il lettore.

Esempio 1.7. Il lettore provi come esercizio che il prodotto di matrici scalari (rispettivamente: diagonali, triangolari superiori, triangolari inferiori) dello stesso ordine è ancora una matrice scalare (rispettivamente: diagonale, triangolare superiore, triangolare inferiore), con coefficienti diagonali i prodotti dei corrispondenti coefficienti diagonali dei due fattori. □

I due seguenti esempi descrivono il risultato del prodotto di una matrice per una matrice diagonale, prima moltiplicata a sinistra (*pre-moltiplicazione*) e poi a destra (*post-moltiplicazione*).

Esempio 1.8. Siano

$$\mathbf{A} = \begin{bmatrix} \mathbf{r}_1^T \\ \mathbf{r}_2^T \\ \dots \\ \mathbf{r}_m^T \end{bmatrix}$$

una matrice $m \times n$ in cui sono in evidenza le righe e $\mathbf{D} = \mathbf{Diag}(d_1, d_2, \dots, d_m)$ una matrice diagonale. Una facile verifica mostra che

$$\mathbf{DA} = \begin{bmatrix} d_1\mathbf{r}_1^T \\ d_2\mathbf{r}_2^T \\ \dots \\ d_m\mathbf{r}_m^T \end{bmatrix},$$

quindi la pre-moltiplicazione di $\mathbf{A}$ per una matrice diagonale $\mathbf{D}$ ha l'effetto di moltiplicare ogni riga di $\mathbf{A}$ per il corrispondente elemento diagonale di $\mathbf{D}$.

Per esempio, se

$$\mathbf{A} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \end{bmatrix}$$

e $\mathbf{D} = \mathbf{Diag}(1, 2, 3)$, risulta

$$\mathbf{DA} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 10 & 12 & 14 & 16 \\ 27 & 30 & 33 & 36 \end{bmatrix}.$$ □

Esempio 1.9. Siano

$$\mathbf{A} = [\mathbf{a}_1 \ \mathbf{a}_2 \ \dots \ \mathbf{a}_n]$$

una matrice $m \times n$ in cui sono in evidenza le colonne e $\mathbf{D} = \mathbf{Diag}(d_1, d_2, \dots, d_n)$ una matrice diagonale. Si verifica che

$$\mathbf{AD} = [d_1\mathbf{a}_1 \ d_2\mathbf{a}_2 \ \dots \ d_n\mathbf{a}_n]$$

quindi la post-moltiplicazione di $\mathbf{A}$ per una matrice diagonale $\mathbf{D}$ ha l'effetto di moltiplicare ogni colonna di $\mathbf{A}$ per il corrispondente elemento diagonale di $\mathbf{D}$.

Per esempio, se la matrice $\mathbf{A}$ è quella dell'esempio precedente e se si pone $\mathbf{D} = \mathbf{Diag}(1,2,3,4)$, risulta

$$\mathbf{AD} = \begin{bmatrix} 1 & 4 & 9 & 16 \\ 5 & 12 & 21 & 32 \\ 9 & 20 & 33 & 48 \end{bmatrix}. \qquad \square$$

Una cosa da dire sul prodotto tra matrici, altrettanto importante che elencarne le proprietà, è quali sono le proprietà cui non soddisfa. A tal fine la cosa più opportuna da fare è quella di fornire esempi di prodotti di particolari matrici che non soddisfano a quelle proprietà. La proprietà più importante cui il prodotto non soddisfa è quella commutativa.

Esempio 1.10. Il prodotto di due matrici quadrate non gode in generale della proprietà commutativa. Prendiamo per esempio due generiche matrici 2×2:

$$\mathbf{A} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \qquad \mathbf{A}' = \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}.$$

Allora risulta

$$\mathbf{AA}' = \begin{bmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{bmatrix}, \qquad \mathbf{A}'\mathbf{A} = \begin{bmatrix} a'a + b'c & a'b + b'd \\ c'a + d'c & c'b + d'd \end{bmatrix}$$

per cui $\mathbf{AA}' = \mathbf{A}'\mathbf{A}$ se e solo se

$$bc' = b'c, \quad ab' + bd' = a'b + b'd, \quad ca' + dc' = c'a + d'c.$$

Il lettore trovi esempi numerici opportuni di matrici 2×2 $\mathbf{A}$ e $\mathbf{A}'$ che non commutano, tali cioè che $\mathbf{AA}' \neq \mathbf{A}'\mathbf{A}$. $\square$

Data una matrice quadrata $\mathbf{A}$, se ne possono considerare le potenze successive:

$$\mathbf{A}^0 = \mathbf{I}, \qquad \mathbf{A}^1 = \mathbf{A}, \qquad \mathbf{A}^2 = \mathbf{AA}, \qquad \mathbf{A}^3 = \mathbf{AAA}, \qquad \dots$$

Col crescere dell'esponente k, la matrice $\mathbf{A}^k$ può diventare più complicata oppure più semplice rispetto ad $\mathbf{A}$, come mostrano i tre esempi seguenti.

Esempio 1.11. Si consideri la matrice 3×3:

$$\mathbf{A} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

che ha cinque coefficienti nulli. Il lettore verifichi che nelle successive potenze $\mathbf{A}^2$, $\mathbf{A}^3$ e $\mathbf{A}^4$ i coefficienti nulli diminuiscono progressivamente, e che $\mathbf{A}^k$ non ha coefficienti nulli per ogni $k \geq 5$. $\square$

Esempio 1.12. Si consideri la matrice 3×3:

$$\mathbf{P} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

Si verifichi che $\mathbf{P}^3 = \mathbf{I}_3$. Quindi le successive potenze di $\mathbf{P}$ riproducono ciclicamente le prime tre potenze. □

Esempio 1.13. Si consideri la matrice 3×3:

$$\mathbf{J} = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

Il lettore verifichi che $\mathbf{J}^2$ ha un unico coefficiente non nullo uguale a 1 e che $\mathbf{J}^k = \mathbb{O}$ per ogni $k \geq 3$. Questo esempio prova anche che in generale il prodotto di matrici non nulle può annullarsi. □

Due matrici $\mathbf{A}$ e $\mathbf{B}$ si possono sia sommare che moltiplicare tra di loro se e solo se sono quadrate dello stesso ordine n. Denoteremo con $\mathrm{M}_n(\mathbb{C})$ l'insieme di tutte le matrici a coefficienti complessi di ordine n, dotato delle operazioni di prodotto per scalari, somma e prodotto (righe per colonne). Chiameremo $\mathrm{M}_n(\mathbb{C})$ l'*algebra* delle matrici complesse $n \times n$. Analogamente, per le matrici a coefficienti reali o razionali, useremo le notazioni $\mathrm{M}_n(\mathbb{R})$ e $\mathrm{M}_n(\mathbb{Q})$ e parleremo dell'algebra delle matrici reali o razionali di ordine n.

Altre notazioni universalmente usate sono quelle di $\mathbb{C}^n$ e $\mathbb{C}_n$, che denotano rispettivamente l'insieme dei vettori colonna e dei vettori riga con n coordinate, dotati del prodotto per scalari e della somma. Analogamente, per i vettori a coordinate reali (o razionali), useremo le notazioni $\mathbb{R}^n$ (o $\mathbb{Q}^n$) e $\mathbb{R}_n$ (o $\mathbb{Q}_n$).

Infine, denoteremo con $\mathrm{M}_{n\times p}(\mathbb{C})$ (rispettivamente, con $\mathrm{M}_{n\times p}(\mathbb{R})$ e $\mathrm{M}_{n\times p}(\mathbb{Q})$) l'insieme delle matrici $n \times p$ a coefficienti complessi (rispettivamente, reali e razionali).

2. Trasposte e *H*-trasposte, decomposizioni a blocchi

Data una matrice $m \times n$ $\mathbf{A} = [a_{ij}]$, si chiama *trasposta* di $\mathbf{A}$, e la si indica con $\mathbf{A}^T$, la matrice che si ottiene da $\mathbf{A}$ scambiandone le righe con le colonne. Pertanto, il coefficiente di posto (i, j) della matrice trasposta $\mathbf{A}^T$ coincide con a_{ji}. È evidente dalla definizione che la trasposta $\mathbf{A}^T$ ha dimensioni $n \times m$.

Esempio 2.1. Riprendiamo le matrici dell'Esempio 1.1 cui affianchiamo le rispettive trasposte:

$$\mathbf{A} = \begin{bmatrix} 1+i & 2-i \\ 3 & -i \end{bmatrix}, \qquad \mathbf{A}^T = \begin{bmatrix} 1+i & 3 \\ 2-i & -i \end{bmatrix};$$

$$\mathbf{B} = \begin{bmatrix} 2 \\ -\pi \end{bmatrix}, \qquad \mathbf{B}^T = [2 \ -\pi];$$

$$\mathbf{C} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \end{bmatrix}, \qquad \mathbf{C}^T = \begin{bmatrix} 1 & 5 & 9 \\ 2 & 6 & 10 \\ 3 & 7 & 11 \\ 4 & 8 & 12 \end{bmatrix}. \qquad \square$$

Esempio 2.2. La matrice trasposta di un vettore colonna $\mathbf{v}$ non è altro che il vettore riga $\mathbf{v}^T$, che è stato denotato in questo modo nel paragrafo precedente proprio per usare la notazione della trasposizione. $\square$

Per le informazioni basilari sull'operazione di coniugazione dei numeri complessi rimandiamo all'Appendice A.

La matrice *coniugata* della matrice $\mathbf{A} = [a_{ij}]$, denotata con $\overline{\mathbf{A}}$, è la matrice ottenuta coniugando tutti i coefficienti di $\mathbf{A}$:

$$\overline{\mathbf{A}} = [\overline{a}_{ij}].$$

Evidentemente la coniugata di una matrice reale coincide con la matrice stessa, e la matrice coniugata di $\overline{\mathbf{A}}$ coincide con $\mathbf{A}$ stessa. Eseguendo prima l'operazione di trasposizione e poi quella di coniugazione sulla matrice $\mathbf{A}$ si ottiene la medesima matrice che invertendo l'ordine delle due operazioni; tale matrice si denota con $\mathbf{A}^H$ e si chiama matrice *H-trasposta* di $\mathbf{A}$. Si ha pertanto

$$\mathbf{A}^H = \overline{\mathbf{A}}^T = \overline{\mathbf{A}^T}.$$

Il simbolo "H" deriva dal matematico francese Hermite. Ovviamente, se $\mathbf{A}$ è una matrice reale, $\mathbf{A}^H = \mathbf{A}^T$.

Esempio 2.3. La matrice H-trasposta della matrice $\mathbf{A}$ dell'Esempio 1.1 è

$$\mathbf{A}^H = \begin{bmatrix} 1-i & 3 \\ 2+i & i \end{bmatrix}.$$

Le matrici H-trasposte delle matrici $\mathbf{B}$ e $\mathbf{C}$ dello stesso Esempio 1.1 coincidono con $\mathbf{B}^T$ e $\mathbf{C}^T$, rispettivamente. $\square$

Elenchiamo di seguito le principali proprietà di cui godono le matrici trasposte e H-trasposte; le dimostrazioni di queste proprietà sono tutte banali, a eccezione di quella della proprietà (T_4).

Siano $\mathbf{A}$ e $\mathbf{B}$ matrici delle medesime dimensioni, $\mathbf{C}$ una matrice conforme ad $\mathbf{A}$ per il prodotto, e α uno scalare. Allora

(T_1) $(\alpha\mathbf{A})^T = \alpha\mathbf{A}^T$;

(T_2) $(\mathbf{A}+\mathbf{B})^T = \mathbf{A}^T + \mathbf{B}^T$;

(T_3) $(\mathbf{A}^T)^T = \mathbf{A}$;

(T_4) $(\mathbf{A}\mathbf{C})^T = \mathbf{C}^T\mathbf{A}^T$;

(H_1) $(\alpha\mathbf{A})^H = \overline{\alpha}\mathbf{A}^H$;

(H_2) $(\mathbf{A}+\mathbf{B})^H = \mathbf{A}^H + \mathbf{B}^H$;

(H_3) $(\mathbf{A}^H)^H = \mathbf{A}$;

(H_4) $(\mathbf{A}\mathbf{C})^H = \mathbf{C}^H\mathbf{A}^H$.

Dimostriamo la (T_4). Sia $\mathbf{A} = [a_{ij}]_{j\le n}^{i\le m}$ e $\mathbf{C} = [c_{jh}]_{h\le p}^{j\le n}$. L'elemento di posto (i, j) di $(\mathbf{AC})^T$ coincide con quello di posto (j, i) di $\mathbf{AC}$, che è $\sum_{1\le h\le n} a_{jh}c_{hi}$. D'altra parte, l'elemento di posto (i, j) di $\mathbf{C}^T\mathbf{A}^T$ è dato dal prodotto della i-esima riga di $\mathbf{C}^T$ per la j-esima colonna di $\mathbf{A}^T$, quindi è $\sum_{1\le h\le n} c_{hi}a_{jh}$, da cui l'asserto.

È importante rilevare che nelle proprietà (T_4) e (H_4) l'ordine dei due fattori viene invertito passando alle trasposte e H-trasposte. La proprietà (H_4) si ricava immediatamente dalla proprietà (T_4) e dal fatto che $\overline{\mathbf{AC}} = \overline{\mathbf{A}}\,\overline{\mathbf{C}}$, il che risulta evidente non appena si ricordi che il coniugato di somma e prodotto di due numeri complessi è la somma e, rispettivamente, il prodotto dei loro coniugati.

Matrici simmetriche ed hermitiane

Tra tutte le matrici quadrate, quelle che coincidono con la loro trasposta rivestono un particolare interesse; esse vengono chiamate matrici *simmetriche*. Pertanto, una matrice $n \times n$ $\mathbf{A}$ è simmetrica se $\mathbf{A} = \mathbf{A}^T$. In altri termini, una matrice quadrata risulta simmetrica quando, ruotata di mezzo giro attorno alla sua diagonale, coincide con sé stessa.

La matrice $\mathbf{A}$ è invece detta *hermitiana* se coincide con la sua H-trasposta, cioè se $\mathbf{A} = \mathbf{A}^H$.

È evidente che per le matrici reali le due nozioni di matrice simmetrica e di matrice hermitiana vengono a coincidere, giacché la coniugazione non modifica una matrice reale. Invece una matrice complessa non reale può risultare simmetrica senza essere hermitiana, e viceversa.

Mentre i coefficienti diagonali di una matrice simmetrica possono essere del tutto arbitrari, quelli di una matrice hermitiana devono essere numeri reali, perché devono coincidere con i loro coniugati.

Ci sono altri due tipi importanti di matrici, collegate alle operazioni di trasposizione e H-trasposizione. Diremo che una matrice $\mathbf{A}$ è *anti-simmetrica* se $\mathbf{A} = -\mathbf{A}^T$; diremo invece che è *anti-hermitiana* se $\mathbf{A} = -\mathbf{A}^H$.

Segue immediatamente dalla definizione che gli elementi diagonali di una matrice anti-simmetrica sono nulli, mentre gli elementi diagonali di una matrice anti-hermitiana sono tutti immaginari, cioè del tipo ir, con $r \in \mathbb{R}$.

Esempio 2.4. Le seguenti quattro matrici offrono esempi, ordinatamente, di matrice simmetrica, hermitiana, anti-simmetrica e anti-hermitiana:

$$\mathbf{A} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & 6 \end{bmatrix} \qquad \text{simmetrica;}$$

$$\mathbf{B} = \begin{bmatrix} 2 & 1-i & i \\ 1+i & 0 & 3+2i \\ -i & 3-2i & 3 \end{bmatrix} \qquad \text{hermitiana;}$$

$$\mathbf{C} = \begin{bmatrix} 0 & 2 & 3 \\ -2 & 0 & 4 \\ -3 & -4 & 0 \end{bmatrix} \qquad \text{anti-simmetrica;}$$

$$\mathbf{D} = \begin{bmatrix} i & 1-i & i \\ -1-i & 0 & 3+2i \\ i & -3+2i & -2i \end{bmatrix} \qquad \text{anti-hermitiana.}$$

□

In analogia con la forma algebrica di un numero complesso, per cui ogni numero $z \in \mathbb{C}$ si scrive in uno e un solo modo come $z = a + ib$, con a e b numeri reali (a è detto parte reale e ib parte immaginaria di z), per ogni matrice complessa quadrata si ha la seguente decomposizione.

Proposizione 2.5. *Ogni matrice complessa quadrata* $\mathbf{A}$ *si scrive in uno e un solo modo nella forma* $\mathbf{A} = \mathbf{B} + \mathbf{C}$, *con* $\mathbf{B}$ *matrice hermitiana e* $\mathbf{C}$ *matrice anti-hermitiana.*

Dimostrazione. Si ponga $\mathbf{B} = (\mathbf{A} + \mathbf{A}^H)/2$ e $\mathbf{C} = (\mathbf{A} - \mathbf{A}^H)/2$. Una verifica diretta mostra che $\mathbf{B}$ è hermitiana, $\mathbf{C}$ è anti-hermitiana e $\mathbf{A} = \mathbf{B} + \mathbf{C}$. Quanto all'unicità, se $\mathbf{A} = \mathbf{B}' + \mathbf{C}'$, con $\mathbf{B}'$ hermitiana e $\mathbf{C}'$ anti-hermitiana, risulta

$$\mathbf{B} - \mathbf{B}' = \mathbf{C}' - \mathbf{C}.$$

Ma $\mathbf{B} - \mathbf{B}'$ risulta hermitiana, mentre $\mathbf{C}' - \mathbf{C}$ risulta anti-hermitiana; l'unica matrice contemporaneamente hermitiana e anti-hermitiana è la matrice nulla, percio $\mathbf{B} = \mathbf{B}'$ e $\mathbf{C} = \mathbf{C}'$. □

Le matrici $\mathbf{B}$ e $\mathbf{C}$ che compaiono nella Proposizione 2.5 si chiamano, rispettivamente, *parte hermitiana* e *parte anti-hermitiana* della matrice complessa $\mathbf{A}$ (se $\mathbf{A}$ è una matrice reale, allora la parte hermitiana risulta reale simmetrica e la parte anti-hermitiana risulta reale anti-simmetrica). Esiste un motivo ben preciso per cui c'è analogia tra matrici hermitiane e numeri reali da un lato e matrici anti-hermitiane e numeri immaginari dall'altro, che potrà essere compreso solo al Capitolo 6 quando avremo a disposizione la teoria degli autovalori.

L'analogia con i numeri complessi cade se si chiede alla parte hermitiana di commutare con la parte anti-hermitiana, come invece accade per a e ib nel numero complesso $z = a + ib$. Ciò infatti caratterizza una particolare classe di matrici, chiamate normali, come mostra la seguente Proposizione. Una matrice $\mathbf{A}$ si dice *normale* se

$\mathbf{AA}^H = \mathbf{A}^H\mathbf{A}$, cioè se $\mathbf{A}$ commuta con la sua H-trasposta. Le matrici normali sono molto importanti per un'altra loro proprietà, che si vedrà al Capitolo 6 nel Teorema Spettrale.

Proposizione 2.6. *Sia* $\mathbf{A} = \mathbf{B}+\mathbf{C}$ *la decomposizione della matrice quadrata* $\mathbf{A}$ *nella parte hermitiana* $\mathbf{B}$ *e nella parte anti-hermitiana* $\mathbf{C}$. *Allora* $\mathbf{BC} = \mathbf{CB}$ *se e solo se* $\mathbf{A}$ *è normale.*

Dimostrazione. Poiché $\mathbf{A}^H = \mathbf{B}^H+\mathbf{C}^H = \mathbf{B}-\mathbf{C}$, si ha che $\mathbf{AA}^H = \mathbf{B}^2-\mathbf{BC}+\mathbf{CB}-\mathbf{C}^2$, mentre $\mathbf{A}^H\mathbf{A} = \mathbf{B}^2+\mathbf{BC}-\mathbf{CB}-\mathbf{C}^2$. Perciò $\mathbf{AA}^H = \mathbf{A}^H\mathbf{A}$ se e solo se $-\mathbf{BC}+\mathbf{CB} = \mathbf{BC}-\mathbf{CB}$, se e solo se $\mathbf{BC} = \mathbf{CB}$. □

Esempio 2.7. Data la matrice complessa

$$\mathbf{A} = \begin{bmatrix} 1+i & 2-i \\ 3 & -i \end{bmatrix}$$

la sua decomposizione in parte hermitiana e parte anti-hermitiana è:

$$\mathbf{A} = [(\mathbf{A}+\mathbf{A}^H)/2] + [(\mathbf{A}-\mathbf{A}^H)/2] = \frac{1}{2}\begin{bmatrix} 2 & 5-i \\ 5+i & 0 \end{bmatrix} + \frac{1}{2}\begin{bmatrix} 2i & -1-i \\ 1-i & -2i \end{bmatrix};$$

il lettore verifichi che parte hermitiana e parte anti-hermitiana non commutano, ovvero che $\mathbf{A}$ non è normale. □

Diamo alcune proprietà cui soddisfano le matrici simmetriche ed hermitiane, anti-simmetriche e anti-hermitiane. La loro verifica è lasciata come esercizio.

(a) La somma di due matrici simmetriche, hermitiane, anti-simmetriche o anti-hermitiane è dello stesso tipo.

(b) Se $\mathbf{A}$ è una matrice simmetrica (risp., hermitiana) e α è uno scalare (risp., un numero reale), allora $\alpha\mathbf{A}$ è una matrice simmetrica (risp., hermitiana).

(c) Se $\mathbf{A}$ è una matrice anti-simmetrica (risp., anti-hermitiana) e α è uno scalare (risp., un numero reale), allora $\alpha\mathbf{A}$ è una matrice anti-simmetrica (risp., anti-hermitiana).

(d) $\mathbf{A}$ è una matrice hermitiana se e solo se $i\mathbf{A}$ è una matrice anti-hermitiana.

(e) Il prodotto di due matrici simmetriche (risp., hermitiane) è una matrice simmetrica (risp., hermitiana) se e solo se le due matrici commutano tra di loro.
È importante rilevare che il prodotto di due matrici simmetriche (risp., hermitiane) che non commutano tra di loro non risulta mai una matrice simmetrica (risp., hermitiana). La proprietà seguente prende in considerazione una matrice del tutto arbitraria, e da essa ricava due matrici simmetriche, oppure hermitiane, che risulteranno molto usate in futuro (si veda, per esempio, il Paragrafo 4 del Capitolo 6).

(f) Sia $\mathbf{X}$ una matrice complessa $m \times n$. Le matrici quadrate $\mathbf{XX}^T$ e $\mathbf{X}^T\mathbf{X}$ sono entrambi simmetriche e le matrici $\mathbf{XX}^H$ e $\mathbf{X}^H\mathbf{X}$ sono entrambi hermitiane.

Si osservi che le matrici $\mathbf{XX}^T$ e $\mathbf{X}^T\mathbf{X}$ hanno in generale dimensioni del tutto differenti. Vediamo un esempio.

Esempio 2.8. Sia $\mathbf{v}^T = [v_1\ v_2\ \dots\ v_n]$ un vettore riga con n coordinate. Allora la matrice $\mathbf{v}\mathbf{v}^T$ è una matrice simmetrica $n \times n$, con $v_i v_j$ come coefficiente di posto (i, j), mentre la matrice $\mathbf{v}^T\mathbf{v}$ ha dimensioni 1×1, giacché è lo scalare $\sum_{i \le n} v_i^2$. Ad esempio, se $\mathbf{v}^T = [1\ 0\ 2\ -1]$, $\mathbf{v}^T\mathbf{v} = 6$, mentre

$$\mathbf{v}\mathbf{v}^T = \begin{bmatrix} 1 & 0 & 2 & -1 \\ 0 & 0 & 0 & 0 \\ 2 & 0 & 4 & -2 \\ -1 & 0 & -2 & 1 \end{bmatrix}. \qquad \square$$

Sottomatrici

Data una matrice $m \times n$ $\mathbf{A}$, se ne possono considerare delle sue "porzioni". Per esempio, se scegliamo ad arbitrio alcune righe e alcune colonne di $\mathbf{A}$, i coefficienti che stanno nella intersezione di queste righe e colonne formano quella che si chiama una *sottomatrice* di $\mathbf{A}$. La matrice $\mathbf{A}$ è naturalmente una sottomatrice di sé stessa; le sottomatrici diverse da $\mathbf{A}$ sono dette sottomatrici *proprie*.

Esempio 2.9. Si consideri la seguente matrice 4×4:

$$\mathbf{A} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{bmatrix}.$$

Ciascuna delle seguenti matrici è sottomatrice di $\mathbf{A}$:

$$\begin{bmatrix} 1 & 2 \\ 9 & 10 \end{bmatrix}; \quad \begin{bmatrix} 1 & 3 & 4 \\ 9 & 11 & 12 \end{bmatrix}; \quad \begin{bmatrix} 2 & 4 \\ 6 & 8 \\ 14 & 16 \end{bmatrix}; \quad \begin{bmatrix} 5 & 6 & 7 & 8 \\ 13 & 14 & 15 & 16 \end{bmatrix}. \qquad \square$$

Tra le sottomatrici di una matrice quadrata risultano particolarmente utili e usate le *sottomatrici principali*, che si ottengono scegliendo righe e colonne (la cui intersezione produce la sottomatrice) con gli stessi indici. È facile convincersi che i coefficienti diagonali di una sottomatrice principale sono coefficienti diagonali anche nella matrice originaria.

Esempio 2.10. Nessuna delle sottomatrici della matrice $\mathbf{A}$ considerate nel precedente esempio è una sottomatrice principale. Le seguenti sottomatrici invece lo sono:

$$\begin{bmatrix} 1 & 3 \\ 9 & 11 \end{bmatrix}; \quad \begin{bmatrix} 6 & 7 \\ 10 & 11 \end{bmatrix}; \quad \begin{bmatrix} 6 & 7 & 8 \\ 10 & 11 & 12 \\ 14 & 15 & 16 \end{bmatrix}. \qquad \square$$

In certi casi (per esempio nello studio delle matrici hermitiane definite positive (si veda il Capitolo 6) si considerano solo le sottomatrici principali ottenute intersecando le prime k righe e colonne, dove k varia da 1 all'ordine n della matrice; esse vengono chiamate *sottomatrici principali k-esime*. Naturalmente la matrice stessa è la sottomatrice principale n-esima di sé stessa.

Esempio 2.11. Nessuna delle sottomatrici considerate nell'Esempio 2.10 è una sottomatrice principale k-esima della matrice $\mathbf{A}$. Lo sono invece tutte e sole le seguenti matrici:

$$[1]; \quad \begin{bmatrix} 1 & 2 \\ 5 & 6 \end{bmatrix}; \quad \begin{bmatrix} 1 & 2 & 3 \\ 5 & 6 & 7 \\ 9 & 10 & 11 \end{bmatrix}; \quad \mathbf{A}. \qquad \square$$

Decomposizioni a blocchi

Un'altra maniera di considerare "porzioni" di matrici è quella di *decomporre a blocchi* una matrice; questa operazione si esegue tracciando delle righe orizzontali e verticali che "tagliano" la matrice in sottomatrici, ciascuna delle quali è formata dalla intersezione di righe e colonne consecutive ed è chiamata *blocco*. Si ottengono così delle righe e delle colonne di blocchi, e si parla di *dimensioni a blocchi* della matrice. Di seguito sono riportati due diversi modi di decomporre a blocchi la matrice dell'Esempio 2.9.

$$\mathbf{A} = \left[\begin{array}{cc|cc} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ \hline 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{array}\right] = \begin{bmatrix} \mathbf{A}_{11} & \mathbf{A}_{12} \\ \mathbf{A}_{21} & \mathbf{A}_{22} \end{bmatrix}$$

dove è evidente quali sono i quattro blocchi $\mathbf{A}_{ij}$. La matrice $\mathbf{A}$ così decomposta ha dimensioni a blocchi 2×2;

$$\mathbf{A} = \left[\begin{array}{c|cc|c} 1 & 2 & 3 & 4 \\ \hline 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ \hline 13 & 14 & 15 & 16 \end{array}\right] = \begin{bmatrix} \mathbf{A}'_{11} & \mathbf{A}'_{12} & \mathbf{A}'_{13} \\ \mathbf{A}'_{21} & \mathbf{A}'_{22} & \mathbf{A}'_{23} \\ \mathbf{A}'_{31} & \mathbf{A}'_{32} & \mathbf{A}'_{33} \end{bmatrix}$$

dove è chiaro quali sono i nove blocchi $\mathbf{A}'_{ij}$. La matrice $\mathbf{A}$ così decomposta ha dimensioni a blocchi 3×3.

L'utilità delle decomposizioni a blocchi sta nel fatto che sulle matrici si possono eseguire le operazioni di somma e prodotto (righe per colonne) *per blocchi*, cioè considerando i blocchi come fossero dei coefficienti. Naturalmente ciò è possibile solo se sono rispettati i seguenti requisiti:

(B_1) le dimensioni a blocchi delle due matrici devono essere le stesse nella somma a blocchi, e conformi per il prodotto nel prodotto a blocchi;

(B_2) le coppie di blocchi delle due matrici che si sommano tra di loro devono essere delle stesse dimensioni, e quelle che si moltiplicano tra di loro devono essere conformi rispetto al prodotto.

Una volta che tali requisiti sono soddisfatti, si può *operare a blocchi*, ottenendo lo stesso risultato che operando sui coefficienti. La giustificazione di questo fatto è del tutto evidente per la somma, mentre, per quanto riguarda il prodotto, dipende essenzialmente dalla proprietà associativa della somma.

Esempio 2.12. Il prodotto a blocchi delle due matrici decomposte a blocchi

$$\mathbf{A} = \left[\begin{array}{c|cc|c} 1 & 2 & 3 & 1 \\ \hline 0 & -1 & 0 & -2 \\ 3 & 0 & 1 & 2 \end{array}\right] = \begin{bmatrix} \mathbf{A}_{11} & \mathbf{A}_{12} & \mathbf{A}_{13} \\ \mathbf{A}_{21} & \mathbf{A}_{22} & \mathbf{A}_{23} \end{bmatrix}, \quad \mathbf{B} = \left[\begin{array}{c|c} 2 & 0 \\ \hline -1 & 2 \\ 0 & -1 \\ \hline 3 & -1 \end{array}\right] = \begin{bmatrix} \mathbf{B}_{11} & \mathbf{B}_{12} \\ \mathbf{B}_{21} & \mathbf{B}_{22} \\ \mathbf{B}_{31} & \mathbf{B}_{32} \end{bmatrix}$$

produce la matrice

$$\begin{aligned} \mathbf{AB} &= \begin{bmatrix} \mathbf{A}_{11}\mathbf{B}_{11} + \mathbf{A}_{12}\mathbf{B}_{21} + \mathbf{A}_{13}\mathbf{B}_{31} & \mathbf{A}_{11}\mathbf{B}_{12} + \mathbf{A}_{12}\mathbf{B}_{22} + \mathbf{A}_{13}\mathbf{B}_{32} \\ \mathbf{A}_{21}\mathbf{B}_{11} + \mathbf{A}_{22}\mathbf{B}_{21} + \mathbf{A}_{23}\mathbf{B}_{31} & \mathbf{A}_{21}\mathbf{B}_{12} + \mathbf{A}_{22}\mathbf{B}_{22} + \mathbf{A}_{23}\mathbf{B}_{32} \end{bmatrix} \\ &= \left[\begin{array}{c|c} 3 & 0 \\ \hline -5 & 0 \\ 12 & -3 \end{array}\right]. \end{aligned}$$

□

La notazione usuale per una matrice decomposta a blocchi di dimensioni a blocchi $m \times n$ è la seguente:

$$\mathbf{A} = \begin{bmatrix} \mathbf{A}_{11} & \mathbf{A}_{12} & \dots & \mathbf{A}_{1n} \\ \mathbf{A}_{21} & \mathbf{A}_{22} & \dots & \mathbf{A}_{2n} \\ \dots & \dots & \dots & \dots \\ \mathbf{A}_{m1} & \mathbf{A}_{m2} & \dots & \mathbf{A}_{mn} \end{bmatrix}.$$

Se ciascun blocco $\mathbf{A}_{ij}$ ha dimensioni $m_i \times n_j$, le dimensioni della matrice $\mathbf{A}$ sono $m \times n$, dove $m = \sum_i m_i$ e $n = \sum_j n_j$.

Molte definizioni date per le matrici si estendono in modo ovvio alle matrici a blocchi. Così, la matrice a blocchi $m \times n$ $\mathbf{A} = (\mathbf{A}_{ij})$ si dice *triangolare superiore a blocchi* se $\mathbf{A}_{ij} = \mathbb{O}$ per $i > j$. Analogamente si hanno le nozioni di matrice triangolare inferiore a blocchi e matrice diagonale a blocchi. Per queste ultime a volte si usa, anziché l'ovvia notazione $\mathbf{Diag}(\mathbf{A}_1, \mathbf{A}_2, \dots, \mathbf{A}_n)$, la notazione alternativa

$$\mathbf{A}_1 \oplus \mathbf{A}_2 \oplus \cdots \oplus \mathbf{A}_n.$$

Anche l'operazione di trasposizione (e di H-trasposizione) si può eseguire a blocchi: basta scambiare tra di loro le righe e le colonne di blocchi, avendo l'avvertenza di trasporre (e di coniugare) ciascun blocco. Per esempio, data la matrice a blocchi

$$\mathbf{A} = \begin{bmatrix} \mathbf{A}_{11} & \mathbf{A}_{12} & \mathbf{A}_{13} \\ \mathbf{A}_{21} & \mathbf{A}_{22} & \mathbf{A}_{23} \end{bmatrix}$$

la matrice trasposta è:

$$\mathbf{A}^T = \begin{bmatrix} \mathbf{A}_{11}^T & \mathbf{A}_{21}^T \\ \mathbf{A}_{12}^T & \mathbf{A}_{22}^T \\ \mathbf{A}_{13}^T & \mathbf{A}_{23}^T \end{bmatrix}.$$

Per ottenere la matrice H-trasposta a blocchi basta sostituire l'operatore ^{T} con l'operatore ^{H}.

Un modo di decomporre a blocchi una matrice che viene molto usato anche nelle dimostrazioni di risultati teorici, è quello di mettere in evidenza la prima riga e la prima colonna (oppure l'ultima riga e l'ultima colonna); diremo allora che la matrice è *in forma bordata*. Una generica matrice $m \times n$ $\mathbf{A}$ in forma bordata ha questo aspetto:

$$\mathbf{A} = \begin{bmatrix} a & \mathbf{u}^T \\ \mathbf{v} & \mathbf{B} \end{bmatrix}$$

dove a è il coefficiente di posto $(1,1)$, $\mathbf{u}^T$ è la prima riga privata del primo coefficiente, $\mathbf{v}$ è la prima colonna privata del primo coefficiente, e $\mathbf{B}$ si ottiene da $\mathbf{A}$ eliminando prima riga e prima colonna.

Chiudiamo questo paragrafo mostrando alcune rilevanti conseguenze che si ricavano da decomposizioni a blocchi di matrici fatte in modo opportuno.

Consideriamo due matrici $\mathbf{A}$ e $\mathbf{B}$ conformi per il prodotto, diciamo di dimensioni rispettivamente $m \times n$ e $n \times p$. Mettiamo in evidenza in entrambe righe e colonne:

$$\mathbf{A} = \begin{bmatrix} \mathbf{r}_1^T \\ \mathbf{r}_2^T \\ \dots \\ \mathbf{r}_m^T \end{bmatrix} = [\mathbf{a}_1\ \mathbf{a}_2\ \dots\ \mathbf{a}_n], \qquad \mathbf{B} = \begin{bmatrix} \mathbf{s}_1^T \\ \mathbf{s}_2^T \\ \dots \\ \mathbf{s}_n^T \end{bmatrix} = [\mathbf{b}_1\ \mathbf{b}_2\ \dots\ \mathbf{b}_p].$$

Si hanno quindi per ciascuna matrice due diverse decomposizioni a blocchi, la prima a blocchi riga e la seconda a blocchi colonna. Possiamo perciò eseguire la moltiplicazione a blocchi in due modi diversi.

(I) Usando per $\mathbf{A}$ la decomposizione a blocchi riga e per $\mathbf{B}$ la decomposizione a blocchi colonna, si ottiene

$$\mathbf{AB} = (\mathbf{r}_i^T \mathbf{b}_j)_{j \le p}^{i \le m}$$

che non è altro che la definizione di prodotto righe per colonne.

(II) Usando per $\mathbf{A}$ la decomposizione a blocchi colonna e per $\mathbf{B}$ la decomposizione a blocchi riga si ottiene

$$\mathbf{AB} = \sum_{i \le n} \mathbf{a}_i \mathbf{s}_i^T$$

che esprime il prodotto di $\mathbf{A}$ per $\mathbf{B}$ come somma di n matrici, ciascuna prodotto di un vettore colonna per un vettore riga.

Si può anche eseguire la moltiplicazione prima considerando $\mathbf{A}$ come un unico blocco e decomponendo $\mathbf{B}$ in blocchi colonna. Si ricava allora

$$\mathbf{A}[\mathbf{b}_1\ \mathbf{b}_2\ \dots\ \mathbf{b}_p] = [\mathbf{Ab}_1\ \mathbf{Ab}_2\ \dots\ \mathbf{Ab}_p].$$

Simmetricamente, si può considerare $\mathbf{B}$ come un unico blocco e decomporre $\mathbf{A}$ in blocchi riga. Si ricava allora

$$\begin{bmatrix} \mathbf{r}_1^T \\ \mathbf{r}_2^T \\ \dots \\ \mathbf{r}_m^T \end{bmatrix} \mathbf{B} = \begin{bmatrix} \mathbf{r}_1^T\mathbf{B} \\ \mathbf{r}_2^T\mathbf{B} \\ \dots \\ \mathbf{r}_m^T\mathbf{B} \end{bmatrix}.$$

Quanto appena visto si può esprimere nel modo seguente.

Proposizione 2.13. *Nel prodotto (righe per colonne)* $\mathbf{AB}$ *di due matrici:*

(a) *la j-esima colonna di* $\mathbf{AB}$ *coincide con il prodotto* $\mathbf{Ab}_j$ *di* $\mathbf{A}$ *per la j-esima colonna* $\mathbf{b}_j$ *di* $\mathbf{B}$*;*

(b) *la i-esima riga di* $\mathbf{AB}$ *coincide con il prodotto* $\mathbf{r}_i^T\mathbf{B}$ *della i-esima riga* $\mathbf{r}_i^T$ *di* $\mathbf{A}$ *per* $\mathbf{B}$. □

Casi particolari del modo descritto in (II) di eseguire il prodotto si hanno quando la matrice $\mathbf{A}$ è un vettore riga $\mathbf{u}^T$, oppure la matrice $\mathbf{B}$ è un vettore (colonna) $\mathbf{v}$. Nel primo caso si ottiene

$$\mathbf{u}^T\mathbf{B} = u_1\mathbf{s}_1^T + u_2\mathbf{s}_2^T + \ldots + u_n\mathbf{s}_n^T$$

e nel secondo caso si ottiene

$$\mathbf{Av} = v_1\mathbf{a}_1 + v_2\mathbf{a}_2 + \ldots + v_n\mathbf{a}_n$$

dove naturalmente gli scalari u_i e v_j sono le coordinate di $\mathbf{u}^T$ e di $\mathbf{v}$, rispettivamente; il che si esprime anche dicendo che $\mathbf{u}^T\mathbf{B}$ è combinazione lineare delle righe di $\mathbf{B}$ con coefficienti le coordinate di $\mathbf{u}^T$, e che $\mathbf{Av}$ è combinazione lineare delle colonne di $\mathbf{A}$ con coefficienti le coordinate di $\mathbf{v}$.

Se come vettori riga e colonna prendiamo i vettori coordinati $\mathbf{e}_i^T$ ed $\mathbf{e}_j$, rispettivamente, si ricava immediatamente la seguente

Proposizione 2.14. *Siano* $\mathbf{A}$ *una matrice $m \times n$,* $\mathbf{e}_i^T$ *un vettore coordinato riga ($i \leq m$) ed* $\mathbf{e}_j$ *un vettore coordinato colonna ($j \leq n$). Allora* $\mathbf{e}_i^T\mathbf{A}$ *coincide con la i-esima riga di* $\mathbf{A}$ *mentre* $\mathbf{Ae}_j$ *coincide con la j-esima colonna di* $\mathbf{A}$. □

3. Eliminazione di Gauss per sistemi di equazioni lineari

L'algoritmo di Eliminazione di Gauss (che in breve denoteremo con EG) presentato in questo Paragrafo per risolvere i sistemi di equazioni lineari, attribuito a Gauss (e quindi fatto risalire alla fine del XVIII secolo), ha un suo antesignano nell'algoritmo denominato Fang Ch'eng, che si trova nel libro cinese "Nove capitoli sull'arte matematica", risalente al III secolo A.C.; esso è quindi una antichissima conoscenza dell'umanità. L'idea alla base dell'algoritmo è molto semplice: eliminare progressivamente (da qui il nome di "eliminazione") nelle successive equazioni del sistema sempre più incognite, ottenendo un sistema equivalente a quello di partenza (cioè con le medesime soluzioni), ma che si può risolvere molto facilmente con un metodo di "sostituzione all'indietro".

Il modo moderno di presentare la EG consiste nell'operare direttamente sulla matrice dei coefficienti del sistema, cui si aggiunge come ultima colonna la colonna dei termini noti, cioè su quella che si chiama *matrice aumentata* (o ampliata) del sistema. La matrice del sistema semplificato, cui si perviene al termine della EG, si chiama *forma ridotta (di Gauss)* della matrice aumentata del sistema.

Dato il sistema in m equazioni ed n incognite nella sua forma generale vista nel Paragrafo 1

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

che in forma matriciale si scrive

$$\mathbf{A}\mathbf{x} = \mathbf{b},$$

dove $\mathbf{A}$ è la matrice dei coefficienti e $\mathbf{b}$ è il vettore dei termini noti, la matrice aumentata del sistema è la matrice a blocchi

$$[\mathbf{A}\ \mathbf{b}].$$

Ricordiamo fatti ben noti riguardanti i sistemi di equazioni lineari: si ottiene un sistema equivalente a quello dato (cioè con esattamente le stesse soluzioni) se si opera sulle sue equazioni in uno dei tre seguenti modi:

(i) una equazione viene moltiplicata per uno scalare non nullo;

(ii) una equazione viene sostituita con la sua somma con un'altra equazione del sistema moltiplicata per uno scalare non nullo;

(iii) si scambiano tra di loro due equazioni.

Applicando ripetutamente queste tre operazioni, dette *operazioni elementari*, si possono eliminare progressivamente le incognite nelle successive equazioni. Osserviamo inoltre che per ciascuna operazione elementare ne esiste un'altra che riporta la matrice ottenuta nella sua configurazione originale; pertanto queste due operazioni sono una l'inversa dell'altra.

Gli esempi che seguono servono meglio di ogni discorso generale a illustrare come ciò avviene. Nel primo esempio manterremo ancora l'usuale forma del sistema (con le incognite e le somme) e la modificheremo con la EG; tradurremo poi i vari passaggi nella forma matriciale. Dall'esempio successivo opereremo direttamente sulle matrici aumentate.

Esempio 3.1. Si consideri il sistema 3×3 (cioè di tre equazioni in tre incognite)

$$\begin{cases} 2x_1 + 6x_2 + 3x_3 = 4 \\ x_1 - 2x_2 + \frac{1}{2}x_3 = 1 \\ -x_1 + x_2 - \frac{1}{2}x_3 = \frac{2}{5} \end{cases}$$

che ha come matrice aumentata

$$[\mathbf{A}\ \mathbf{b}] = \left[\begin{array}{ccc|c} 2 & 6 & 3 & 4 \\ 1 & -2 & \frac{1}{2} & 1 \\ -1 & 1 & -\frac{1}{2} & \frac{2}{5} \end{array}\right].$$

Moltiplichiamo la prima equazione per 1/2 ottenendo il sistema equivalente

$$\begin{cases} x_1 + 3x_2 + \dfrac{3}{2}x_3 = 2 \\ x_1 - 2x_2 + \dfrac{1}{2}x_3 = 1 \\ -x_1 + \quad x_2 - \dfrac{1}{2}x_3 = \dfrac{2}{5}. \end{cases}$$

Sommando ora alla seconda equazione la prima moltiplicata per -1, e sommando alla terza equazione la prima moltiplicata per 1, si ricava il nuovo sistema equivalente

$$\begin{cases} x_1 + \quad 3x_2 + \dfrac{3}{2}x_3 = \ 2 \\ \qquad -5x_2 - \quad x_3 = -1 \\ \qquad\quad 4x_2 + \quad x_3 = \dfrac{12}{5}. \end{cases}$$

Moltiplichiamo in questo sistema la seconda equazione per $-1/5$, ottenendo il sistema equivalente

$$\begin{cases} x_1 + 3x_2 + \dfrac{3}{2}x_3 = \ 2 \\ \qquad\quad x_2 + \dfrac{1}{5}x_3 = \ \dfrac{1}{5} \\ \qquad 4x_2 + \quad x_3 = \dfrac{12}{5}. \end{cases}$$

Nel sistema così modificato, sommando alla terza equazione la seconda moltiplicata per -4, si ricava il sistema equivalente

$$\begin{cases} x_1 + 3x_2 + \dfrac{3}{2}x_3 = 2 \\ \qquad\quad x_2 + \dfrac{1}{5}x_3 = \dfrac{1}{5} \\ \qquad\qquad\quad \dfrac{1}{5}x_3 = \dfrac{8}{5}. \end{cases}$$

Infine, moltiplicando la terza equazione per 5, si perviene al sistema equivalente

$$\begin{cases} x_1 + 3x_2 + \dfrac{3}{2}x_3 = 2 \\ \qquad\quad x_2 + \dfrac{1}{5}x_3 = \dfrac{1}{5} \\ \qquad\qquad\qquad x_3 = 8. \end{cases}$$

A questo punto la EG è terminata. Le soluzioni del sistema si possono facilmente trovare partendo dalla terza equazione, che fornisce il valore di x_3, poi sostituendo tale valore nella seconda equazione e ricavando il valore di x_2, poi sostituendo tali valori nella prima equazione e ricavando il valore di x_1. Si dice che si esegue la *sostituzione all'indietro*. Si ricava così la soluzione:

$$x_3 = 8, \qquad x_2 = -\frac{7}{5}, \qquad x_1 = -\frac{29}{5}.$$

Scriviamo le matrici aumentate dei sistemi ottenuti modificando quello originario

$$\left[\begin{array}{ccc|c} 1 & 3 & \frac{3}{2} & 2 \\ 1 & -2 & \frac{1}{2} & 1 \\ -1 & 1 & -\frac{1}{2} & \frac{2}{5} \end{array}\right]; \quad \left[\begin{array}{ccc|c} 1 & 3 & \frac{3}{2} & 2 \\ 0 & -5 & -1 & -1 \\ 0 & 4 & 1 & \frac{12}{5} \end{array}\right]; \quad \left[\begin{array}{ccc|c} 1 & 3 & \frac{3}{2} & 2 \\ 0 & 1 & \frac{1}{5} & \frac{1}{5} \\ 0 & 4 & 1 & \frac{12}{5} \end{array}\right];$$
$$\left[\begin{array}{ccc|c} 1 & 3 & \frac{3}{2} & 2 \\ 0 & 1 & \frac{1}{5} & \frac{1}{5} \\ 0 & 0 & \frac{1}{5} & \frac{8}{5} \end{array}\right]; \quad \left[\begin{array}{ccc|c} 1 & 3 & \frac{3}{2} & 2 \\ 0 & 1 & \frac{1}{5} & \frac{1}{5} \\ 0 & 0 & 1 & 8 \end{array}\right] = [\mathbf{U}\ \mathbf{c}].$$

Si può notare che le operazioni fatte sulle equazioni dei sistemi si potevano fare direttamente sulle righe delle matrici aumentate, rendendo più semplici le notazioni. Abbiamo denotato la matrice a blocchi ottenuta alla fine con $[\mathbf{U}\ \mathbf{c}]$; $\mathbf{U}$ si chiama forma ridotta (di Gauss) della matrice $\mathbf{A}$, e $[\mathbf{U}\ \mathbf{c}]$ è forma ridotta della matrice aumentata $[\mathbf{A}\ \mathbf{b}]$. Si noti che la matrice $\mathbf{U}$ è uni-triangolare superiore. □

Esempio 3.2. Modifichiamo leggermente il sistema dell'esempio precedente, aggiungendo una incognita:

$$\begin{cases} 2x_1 + 6x_2 + 3x_3 + 2x_4 = 4 \\ x_1 - 2x_2 + \frac{1}{2}x_3 + \frac{9}{4}x_4 = 1 \\ -x_1 + x_2 - \frac{1}{2}x_3 - x_4 = \frac{2}{5}. \end{cases}$$

Il sistema ha come matrice aumentata

$$[\mathbf{B}\ \mathbf{b}] = \left[\begin{array}{cccc|c} 2 & 6 & 3 & 2 & 4 \\ 1 & -2 & \frac{1}{2} & \frac{9}{4} & 1 \\ -1 & 1 & -\frac{1}{2} & -1 & \frac{2}{5} \end{array}\right].$$

Le medesime operazioni elementari eseguite nell'Esempio 3.1 producono successivamente le matrici

$$\left[\begin{array}{cccc|c} 1 & 3 & \frac{3}{2} & 1 & 2 \\ 1 & -2 & \frac{1}{2} & \frac{9}{4} & 1 \\ -1 & 1 & -\frac{1}{2} & -1 & \frac{2}{5} \end{array}\right]; \quad \left[\begin{array}{cccc|c} 1 & 3 & \frac{3}{2} & 1 & 2 \\ 0 & -5 & -1 & \frac{5}{4} & -1 \\ 0 & 4 & 1 & 0 & \frac{12}{5} \end{array}\right];$$

$$\left[\begin{array}{cccc|c} 1 & 3 & \frac{3}{2} & 1 & 2 \\ 0 & 1 & \frac{1}{5} & -\frac{1}{4} & \frac{1}{5} \\ 0 & 4 & 1 & 0 & \frac{12}{5} \end{array}\right]; \quad \left[\begin{array}{cccc|c} 1 & 3 & \frac{3}{2} & 1 & 2 \\ 0 & 1 & \frac{1}{5} & -\frac{1}{4} & \frac{1}{5} \\ 0 & 0 & \frac{1}{5} & 1 & \frac{8}{5} \end{array}\right];$$

$$\left[\begin{array}{cccc|c} 1 & 3 & \frac{3}{2} & 1 & 2 \\ 0 & 1 & \frac{1}{5} & -\frac{1}{4} & \frac{1}{5} \\ 0 & 0 & 1 & 5 & 8 \end{array}\right] = [\mathbf{V}\ \mathbf{c}].$$

L'ultima riga di $[\mathbf{V}\ \mathbf{c}]$ corrisponde all'equazione

$$x_3 + 5x_4 = 8.$$

Diamo all'incognita x_4 un qualunque valore h; ne risulta

$$x_3 = 8 - 5h, \quad x_2 = -\frac{7}{5} + \frac{5}{4}h, \quad x_1 = -\frac{29}{5} + \frac{11}{4}h;$$

pertanto il sistema ha infinite soluzioni dipendenti dal parametro h, che è conveniente scrivere in questa forma:

$$\begin{bmatrix} -\frac{29}{5} \\ -\frac{7}{5} \\ 8 \\ 0 \end{bmatrix} + h \begin{bmatrix} \frac{11}{4} \\ \frac{5}{4} \\ -5 \\ 1 \end{bmatrix}. \qquad \square$$

Le matrici in forma ridotta **U** e **V** cui si è pervenuti nei due esempi precedenti hanno una configurazione che viene detta *a scala per righe*; essa è caratterizzata dal fatto che ogni riga a partire dalla seconda ha un numero di zeri iniziali superiore alla riga precedente (qualora questa non sia la riga nulla, nel qual caso è essa stessa nulla).

Per un sistema che ha la matrice aumentata in forma a scala per righe è chiaro che le soluzioni, qualora esistano, si trovano facilmente con la sostituzione all'indietro, dando possibilmente valori arbitrari a certe variabili. Vediamo ora un esempio di un sistema che non ha soluzioni.

Esempio 3.3. Modifichiamo in altro modo il sistema del'Esempio 3.1, cambiando il coefficiente della variabile x_3 nella terza equazione. Consideriamo quindi il sistema

$$\begin{cases} 2x_1 + 6x_2 + \ \ 3x_3 = 4 \\ \ \ x_1 - 2x_2 + \ \frac{1}{2}x_3 = 1 \\ -x_1 + \ \ x_2 - \frac{7}{10}x_3 = \frac{2}{5} \end{cases}$$

che ha come matrice aumentata

$$[\mathbf{A}' \ \mathbf{b}] = \left[\begin{array}{ccc|c} 2 & 6 & 3 & 4 \\ 1 & -2 & \frac{1}{2} & 1 \\ -1 & 1 & -\frac{7}{10} & \frac{2}{5} \end{array}\right].$$

Le operazioni elementari eseguite nell'Esempio 3.1 producono le matrici

$$\left[\begin{array}{ccc|c} 1 & 3 & \frac{3}{2} & 2 \\ 1 & -2 & \frac{1}{2} & 1 \\ -1 & 1 & -\frac{7}{10} & \frac{2}{5} \end{array}\right]; \quad \left[\begin{array}{ccc|c} 1 & 3 & \frac{3}{2} & 2 \\ 0 & -5 & -1 & -1 \\ 0 & 4 & \frac{4}{5} & \frac{12}{5} \end{array}\right];$$

$$\left[\begin{array}{ccc|c} 1 & 3 & \frac{3}{2} & 2 \\ 0 & 1 & \frac{1}{5} & \frac{1}{5} \\ 0 & 4 & \frac{4}{5} & \frac{12}{5} \end{array}\right]; \quad \left[\begin{array}{ccc|c} 1 & 3 & \frac{3}{2} & 2 \\ 0 & 1 & \frac{1}{5} & \frac{1}{5} \\ 0 & 0 & 0 & \frac{8}{5} \end{array}\right];$$

$$\left[\begin{array}{ccc|c} 1 & 3 & \frac{3}{2} & 2 \\ 0 & 1 & \frac{1}{5} & \frac{1}{5} \\ 0 & 0 & 0 & 1 \end{array}\right] = [\mathbf{U}' \ \mathbf{c}].$$

L'ultima riga corrisponde all'equazione

$$0x_3 = 1$$

che evidentemente non ha soluzione. Quindi il sistema $\mathbf{A}'\mathbf{x} = \mathbf{b}$ non ha soluzioni. □

Nei tre esempi precedenti non si è mai resa necessaria l'operazione elementare (iii) di scambio di due equazioni. Vediamo allora un esempio in cui bisogna eseguire tale operazione.

Esempio 3.4. Consideriamo il sistema $\mathbf{C}\mathbf{x} = \mathbf{d}$, dove

$$[\mathbf{C} \ \mathbf{d}] = \left[\begin{array}{cccc|c} 1 & 2 & 2 & 1 & 1 \\ 1 & 2 & 2 & 2 & 2 \\ 2 & 5 & -1 & 3 & 4 \end{array}\right].$$

Sommando alla seconda riga l'opposto della prima, e alla terza riga la prima moltiplicata per -2, si ricava la matrice

$$\left[\begin{array}{cccc|c} 1 & 2 & 2 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & -5 & 1 & 2 \end{array}\right].$$

È evidente che per trasformare la matrice in forma a scala per righe bisogna scambiare tra di loro la seconda e la terza riga; con questo scambio di righe si ha la matrice

$$[\mathbf{W}\,\mathbf{w}] = \left[\begin{array}{cccc|c} 1 & 2 & 2 & 1 & 1 \\ 0 & 1 & -5 & 1 & 2 \\ 0 & 0 & 0 & 1 & 1 \end{array}\right]$$

che è in forma ridotta. La variabile cui diamo in questo caso un valore arbitrario k è x_3; le soluzioni dipendenti da tale parametro sono, come si verifica facilmente

$$x_1 = -2 - 12k; \quad x_2 = 1 + 5k; \quad x_3 = k; x_4 = 1$$

che vanno convenientemente scritte nella forma

$$\begin{bmatrix} -2 \\ 1 \\ 0 \\ 1 \end{bmatrix} + k \begin{bmatrix} -12 \\ 5 \\ 1 \\ 0 \end{bmatrix}.$$ □

Osservando il diverso comportamento delle matrici in forma ridotta cui si perviene nei quattro esempi precedenti, si capisce subito da cosa dipende il fatto che un sistema abbia una e una sola soluzione, oppure infinite soluzioni, oppure nessuna soluzione; non esitono infatti altre possibilità (si dice anche che i sistemi di equazioni lineari sono di tipo 0, 1, ∞).

È utile a tal fine introdurre la seguente definizione: in una matrice in forma a scala per righe una colonna si dice *dominante* se contiene il primo coefficiente non nullo di qualche riga. Le variabili corrispondenti alle colonne dominanti sono pure chiamate *variabili dominanti*. Le variabili del sistema corrispondenti alle colonne non dominanti della forma ridotta si chiamano *variabili libere*.

Guardando agli esempi precedenti, nell'Esempio 3.1 sono colonne dominanti di $[\mathbf{U}\,\mathbf{c}]$ le prime tre, mentre l'ultima colonna non è dominante. Nell'Esempio 3.2 sono colonne dominanti di $[\mathbf{V}\,\mathbf{c}]$ le prime tre, mentre le ultime due colonne non lo sono. Nell'Esempio 3.3 sono colonne dominanti di $[\mathbf{U}'\,\mathbf{c}]$ le prime due e l'ultima, mentre la terza colonna non lo è. Nell'Esempio 3.4 sono colonne dominanti di $[\mathbf{W}\,\mathbf{w}]$ la prima, la seconda e la quarta, mentre la terza e la quinta colonna non lo sono.

Possiamo allora dire che per la forma ridotta $[\mathbf{U}\,\mathbf{c}]$ della matrice aumentata $[\mathbf{A}\,\mathbf{b}]$ di un generico sistema $\mathbf{Ax} = \mathbf{b}$ accade uno e uno solo dei tre casi seguenti.

[1] Tutte le colonne sono dominanti tranne l'ultima (corrispondente alla colonna dei termini noti); in tal caso il sistema ammette una e una sola soluzione.

[∞] L'ultima colonna non è dominante ed esiste almeno un'altra colonna non dominante; in tal caso il sistema ammette infinite soluzioni, che dipendono da tanti parametri quante sono le variabili libere.

[0] L'ultima colonna è dominante; in tal caso il sistema non ammette soluzioni.

Se $\mathbf{A}$ è una matrice non nulla $m \times n$, il caso [1] può accadere solo se $m \geq n$, il caso [∞] solo se $n > 1$, mentre il caso [0] può accadere qualunque siano m ed n. Osserviamo che la EG, così come la abbiamo descritta, è un algoritmo che non lascia discrezionalità se, quando necessitano scambi di righe, si fissa *a priori* il modo in cui lo scambio va eseguito, per esempio impiegando la prima riga utile successiva a quella da scambiare; per altro, ogni altro scambio con righe utili è legittimo.

Esplicitiamo meglio cosa si intende con "riga utile". Uno scambio di righe si rende necessario quando si vuole eliminare una certa variabile x_j nelle equazioni a partire da una di esse, diciamo dalla i-esima; se il coefficiente di x_j nella i-esima equazione è 0, si cerca nella matrice aumentata una riga al di sotto della i-esima in cui il coefficiente di x_j è diverso da 0. Una qualunque di queste è una "riga utile" al fine di eseguire lo scambio con la riga i-esima. Può però accadere che in tutte le righe al di sotto della i-esima il coefficiente di x_j sia uguale a 0. In tal caso la colonna j-esima della matrice aumentata non ha bisogno di nessuna modifica e si passa quindi alla colonna successiva, cioè alla variabile x_{j+1}.

Vogliamo schematizzare la forma che una generica matrice in forma ridotta $[\mathbf{U}\ \mathbf{c}]$ assume quando si è giunti al termine della EG, a partire dalla matrice aumentata di un sistema lineare.

Nel caso [1], in cui il sistema $m \times n$ ammette una e una sola soluzione, la forma ridotta è del tipo

$$[\mathbf{U}\ \mathbf{c}] = \left[\begin{array}{cccccc|c} 1 & + & + & \dots & + & + & c_1 \\ 0 & 1 & + & \dots & + & + & c_2 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & + & c_{n-1} \\ 0 & 0 & 0 & \dots & 0 & 1 & c_n \\ 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & 0 & 0 \end{array}\right]$$

dove i simboli "+" stanno a indicare coefficienti non specificati.

Nel caso [∞], in cui il sistema ammette infinite soluzioni, la forma ridotta è del tipo

$$[\mathbf{U}\ \mathbf{c}] = \left[\begin{array}{ccccccc|c} \mathbf{0}^T & 1 & ++ & + & ++ & + & ++ & c_1 \\ \mathbf{0}^T & 0 & \mathbf{0}^T & 1 & ++ & + & ++ & c_2 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \mathbf{0}^T & 0 & \mathbf{0}^T & 0 & \mathbf{0}^T & 1 & ++ & c_k \\ \mathbf{0}^T & 0 & \mathbf{0}^T & 0 & \mathbf{0}^T & 0 & \mathbf{0}^T & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \mathbf{0}^T & 0 & \mathbf{0}^T & 0 & \mathbf{0}^T & 0 & \mathbf{0}^T & 0 \end{array}\right]$$

dove compare effettivamente qualcuno dei vettori riga $\mathbf{0}^T$ in qualcuna delle prime k righe (ovvero, ci sono variabili libere) e ci sono $k \leq n$ righe non nulle.

Infine, nel caso [0], in cui il sistema non ammette soluzioni, la forma a scala per righe è del tipo

$$[\mathbf{U}\ \mathbf{c}] = \left[\begin{array}{ccccccc|c} \mathbf{0}^T & 1 & ++ & + & ++ & + & ++ & c_1 \\ \mathbf{0}^T & 0 & \mathbf{0}^T & 1 & ++ & + & ++ & c_2 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \mathbf{0}^T & 0 & \mathbf{0}^T & 0 & \mathbf{0}^T & 1 & ++ & c_k \\ \mathbf{0}^T & 0 & \mathbf{0}^T & 0 & \mathbf{0}^T & 0 & \mathbf{0}^T & c_{k+1} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \mathbf{0}^T & 0 & \mathbf{0}^T & 0 & \mathbf{0}^T & 0 & \mathbf{0}^T & 0 \end{array}\right]$$

dove c_{k+1} è diverso da 0.

Nella EG si possono anche non eseguire le moltiplicazioni che rendono uguali a 1 i primi coefficienti non nulli di ogni riga; in tal caso i numeri $d_i \neq 0$ che compaiono come primi coefficienti non nulli di ogni riga si chiamano *pivot*, per il fatto che vengono impiegati per annullare gli elementi della loro colonna che si trovano sotto di loro.

Il numero k di righe non nulle nella forma ridotta $\mathbf{U}$ (che nel caso [1] coincide con n) si chiama *rango* di $\mathbf{U}$; si noti che il rango di $\mathbf{U}$ coincide col numero delle sue colonne dominanti.

La definizione di rango di una matrice generica che daremo più avanti è del tutto diversa da quella data ora per una matrice in forma ridotta, ma risulterà a essa equivalente. Seguirà da quanto vedremo sugli spazi vettoriali che ogni forma ridotta cui si perviene al termine della EG a partire da una data matrice ha sempre lo stesso rango. Si può pertanto definire il rango di una generica matrice $\mathbf{A} \neq \mathbb{O}$ come il numero di righe non nulle comune a tutte le forme ridotte di $\mathbf{A}$.

Esempio 3.5. Consideriamo il sistema $\mathbf{Ax} = \mathbf{b}$, dove

$$[\mathbf{A}\ \mathbf{b}] = \left[\begin{array}{cccc|c} 0 & 0 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 \\ 1 & -1 & 2 & 0 & \alpha \end{array}\right]$$

e dove α è un parametro, cioè un simbolo che può assumere un arbitrario valore numerico. La prima riga non si può usare per porre 0 nella prima colonna al di sotto del coefficiente di posto $(1,1)$; si può scambiare la prima riga con la seconda oppure con la terza. Nel primo caso la EG porge successivamente le tre matrici

$$\left[\begin{array}{cccc|c} 1 & -1 & 1 & -1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & -1 & 2 & 0 & \alpha \end{array}\right]; \quad \left[\begin{array}{cccc|c} 1 & -1 & 1 & -1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & \alpha-1 \end{array}\right];$$

$$\left[\begin{array}{cccc|c} 1 & -1 & 1 & -1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & \alpha-2 \end{array}\right].$$

Nel secondo caso invece la EG porge successivamente le tre matrici

$$\left[\begin{array}{cccc|c} 1 & -1 & 2 & 0 & \alpha \\ 1 & -1 & 1 & -1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{array}\right]; \quad \left[\begin{array}{cccc|c} 1 & -1 & 2 & 0 & \alpha \\ 0 & 0 & -1 & -1 & 1-\alpha \\ 0 & 0 & 1 & 1 & 1 \end{array}\right];$$
$$\left[\begin{array}{cccc|c} 1 & -1 & 2 & 0 & \alpha \\ 0 & 0 & 1 & 1 & \alpha-1 \\ 0 & 0 & 0 & 0 & 2-\alpha \end{array}\right].$$

Si perviene quindi a due forme ridotte differenti di $[\mathbf{A}\ \mathbf{b}]$. Però in entrambi le forme ridotte il sistema ha soluzione se e solo se $\alpha = 2$, e in tal caso la prima forma ridotta porge con la sostituzione all'indietro le soluzioni

$$x_4 = k, \quad x_3 = 1-k, \quad x_2 = h, \quad x_1 = 1 + k - (1-k) + h$$

mentre la seconda forma ridotta porge le soluzioni

$$x_4 = k, \quad x_3 = 1-k, \quad x_2 = h, \quad x_1 = 2 - 2(1-k) + h;$$

i due insiemi di soluzioni evidentemente coincidono, giacché $1+k-(1-k)+h = 2k+h = 2-2(1-k)+h$. □

4. Matrici inverse e matrice pseudo-inversa

Dato un numero complesso z, esiste un test semplicissimo per vedere se z ammette un inverso, cioè un numero z' tale che $zz' = 1$: basta e occorre che z sia diverso da 0. Tale numero z' è inoltre univocamente individuato da z, per il fatto che vale la "legge dell'annullamento del prodotto" (che dice che il prodotto di numeri non nulli è non nullo): $zz' = 1 = zz''$ implica $z(z' - z'') = 0$, implica $z' = z''$.

Il problema della invertibilità per le matrici è più complesso. Anzitutto, essendo la moltiplicazione non commutativa, occorre distinguere tra inversa destra e inversa sinistra: data la matrice $m \times n$ $\mathbf{A}$, si chiama *inversa destra* di $\mathbf{A}$ una matrice $\mathbf{R}$ tale che $\mathbf{AR} = \mathbf{I}_m$; si chiama *inversa sinistra* di $\mathbf{A}$ una matrice $\mathbf{L}$ tale che $\mathbf{LA} = \mathbf{I}_n$ (i simboli $\mathbf{R}$ ed $\mathbf{L}$ stanno a indicare le iniziali dei termini inglesi "right" e "left"). Notiamo subito che sia $\mathbf{R}$ che $\mathbf{L}$ sono matrici $n \times m$.

Una matrice che sia contemporaneamente inversa destra e inversa sinistra della matrice $\mathbf{A}$ si chiama *inversa bilatera*, o più semplicemente *l'inversa* di $\mathbf{A}$, e ciò per il buon motivo che essa, se esiste, è unica, come prova la seguente proposizione.

Proposizione 4.1. *Sia* $\mathbf{A}$ *una matrice* $m \times n$. *Se* $\mathbf{A}$ *ha sia inversa destra* $\mathbf{R}$ *che inversa sinistra* $\mathbf{L}$, *allora* $\mathbf{R} = \mathbf{L}$. *Ne consegue che* $\mathbf{R} = \mathbf{L}$ *è l'unica inversa (destra, sinistra e bilatera) di* $\mathbf{A}$.

Dimostrazione. $\mathbf{L} = \mathbf{L}\mathbf{I}_m = \mathbf{L}(\mathbf{AR}) = (\mathbf{LA})\mathbf{R} = \mathbf{I}_n\mathbf{R} = \mathbf{R}$. □

La matrice inversa della matrice $\mathbf{A}$, qualora esista, viene denotata con $\mathbf{A}^{-1}$. Vedremo tra poco che $\mathbf{A}^{-1}$ può esistere solo nel caso in cui $\mathbf{A}$ è quadrata; in tal caso la matrice $\mathbf{A}$ si dice *invertibile* (o anche *non-singolare*). È importante rilevare che il termine *invertibile* non si può riferire a matrici dotate solo di inversa destra o sinistra.

Oltre al problema di distinguere tra inverse destre e sinistre, esiste anche il problema che non basta più che una matrice sia diversa dalla matrice nulla perché sia dotata di inversa. Inoltre, come terzo problema, si ha anche la possibilità che una matrice ammetta più di una inversa destra o sinistra, cosa prevedibile per il fatto che la "legge dell'annullamento del prodotto" non vale per il prodotto tra matrici, come si è visto nell'Esempio 1.13.

I seguenti semplici esempi convinceranno subito dell'esistenza di queste possibilità.

Esempio 4.2. Il vettore riga $\mathbf{v}^T = [a\ b]$, con a e b non entrambi nulli, è una matrice con infinite inverse destre e nessuna inversa sinistra. Infatti, se $\mathbf{u} = \left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right]$, risulta

$$\mathbf{v}^T\mathbf{u} = 1 \iff ax + by = 1$$

e tale equazione nelle incognite x e y ha infinite soluzioni. Inoltre, $\mathbf{u}\mathbf{v}^T = \mathbf{I}_2$ comporta che

$$xa = 1, \quad xb = 0, \quad ya = 0, \quad yb = 1,$$

il che è evidentemente assurdo. □

Esempio 4.3. La matrice 2×2

$$\mathbf{A} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$$

non ha nè inversa destra nè inversa sinistra. Se infatti esistesse una matrice

$$\mathbf{X} = \begin{bmatrix} x & y \\ z & w \end{bmatrix}$$

per cui $\mathbf{XA} = \mathbf{I}_2$, risulterebbe $x + y = 1$ e $x + y = 0$, che è manifestamente assurdo; se invece risultasse $\mathbf{AX} = \mathbf{I}_2$, si avrebbe $x + z = 1$ e $x + z = 0$, pure assurdo. □

Stabiliamo preliminarmente un collegamento tra l'esistenza di soluzioni di un sistema lineare $\mathbf{Ax} = \mathbf{b}$ e l'esistenza di inverse della matrice dei coefficienti $\mathbf{A}$.

Se la matrice $\mathbf{A}$ ammette una inversa destra $\mathbf{R}$, il vettore $\mathbf{Rb}$ risulta essere una soluzione, perché $\mathbf{A}(\mathbf{Rb}) = (\mathbf{AR})\mathbf{b} = \mathbf{Ib} = \mathbf{b}$.

Se invece la matrice $\mathbf{A}$ ammette una inversa sinistra $\mathbf{L}$, e se il sistema ammette soluzioni, allora la soluzione è unica: infatti, da $\mathbf{Au} = \mathbf{b} = \mathbf{Av}$, moltiplicando a sinistra ambo i membri per $\mathbf{L}$ si ricava che $\mathbf{u} = \mathbf{LAu} = \mathbf{Lb} = \mathbf{LAv} = \mathbf{v}$.

Possiamo pertanto enunciare il seguente risultato, in cui il punto (c) segue ovviamente dai punti (a) e (b).

Proposizione 4.4. *Il sistema di equazioni lineari* $\mathbf{Ax} = \mathbf{b}$

(a) *ammette almeno una soluzione se la matrice* **A** *ammette inversa destra;*
(b) *ammette al più una soluzione se la matrice* **A** *ammette inversa sinistra;*
(c) *ammette una e una sola soluzione se la matrice* **A** *ammette inversa bilatera.* □

Osserviamo che nel punto (c) la soluzione è $\mathbf{A}^{-1}\mathbf{b}$. Osserviamo inoltre che i tre punti considerati nella precedente proposizione forniscono condizioni che sono solo sufficienti per l'esistenza e l'unicità di soluzioni, e questo per il fatto che il vettore **b** è fissato. Proveremo invece che, se $\mathbf{Ax} = \mathbf{b}$ ha soluzione per ogni vettore **b**, allora **A** ammette inversa destra (Teorema 4.10), mentre, se il particolare sistema $\mathbf{Ax} = \mathbf{0}$ ha al più una soluzione, allora **A** ammette inversa sinistra (Teorema 4.12).

Inverse destre e sinistre

Affrontiamo per primo il problema dell'esistenza di inverse destre e di inverse sinistre. Per le matrici quadrate si ha una situazione del tutto particolare. Infatti, la seguente Proposizione 4.6 mostra che, non appena la matrice quadrata **A** ha una inversa destra (risp., sinistra), questa è anche inversa sinistra (risp., destra). La sua prova inaugura una tecnica dimostrativa per induzione che fa uso della forma bordata delle matrici; questa tecnica sarà ampiamente usata in seguito. Faremo inoltre uso del punto (i) del lemma seguente, che si riferisce al primo passo dell'eliminazione di Gauss sulla matrice **A**; il lemma sarà dimostrato nel Paragrafo 6.

Lemma 4.5. *Data una qualunque matrice* **A**

(i) *esiste una matrice invertibile* **E** *tale che* **EA** *ha la seguente forma bordata*

$$\mathbf{EA} = \begin{bmatrix} a & \mathbf{x}^T \\ \mathbf{0} & \mathbf{X} \end{bmatrix};$$

(ii) *esiste una matrice invertibile* **F** *tale che* $\mathbf{FA} = \mathbf{U}$, *dove* **U** *è una forma ridotta di* **A**. □

Proposizione 4.6. *Sia* **A** *una matrice quadrata di ordine n. Allora una inversa destra di* **A** *è anche inversa sinistra, e viceversa.*

Dimostrazione. Sia $\mathbf{AR} = \mathbf{I}_n$ e ragioniamo per induzione su n. Se $n = 1$ l'asserto è ovvio. Sia allora $n > 1$ e l'asserto vero per $n-1$. Usiamo la forma bordata di **EA** data dal Lemma 4.5, che vale per una opportuna matrice invertibile **E**. Osserviamo che

$$\mathbf{AR} = \mathbf{I}_n \implies \mathbf{EAR} = \mathbf{E} \implies \mathbf{EARE}^{-1} = \mathbf{EE}^{-1} = \mathbf{I}_n.$$

Decomponiamo anche $\mathbf{RE}^{-1}$ in forma bordata

$$\mathbf{RE}^{-1} = \begin{bmatrix} b & \mathbf{y}^T \\ \mathbf{z} & \mathbf{Y} \end{bmatrix}.$$

Dall'uguaglianza

$$\begin{bmatrix} a & \mathbf{x}^T \\ \mathbf{0} & \mathbf{X} \end{bmatrix} \begin{bmatrix} b & \mathbf{y}^T \\ \mathbf{z} & \mathbf{Y} \end{bmatrix} = \begin{bmatrix} 1 & \mathbf{0}^T \\ \mathbf{0} & \mathbf{I}_{n-1} \end{bmatrix}$$

si ricavano le uguaglianze

$$ab + \mathbf{x}^T\mathbf{z} = 1, \quad a\mathbf{y}^T + \mathbf{x}^T\mathbf{Y} = \mathbf{0}^T, \quad \mathbf{Xz} = \mathbf{0}, \quad \mathbf{XY} = \mathbf{I}_{n-1}.$$

Poiché le matrici $\mathbf{X}$ e $\mathbf{Y}$ hanno ordine $n-1$, per l'ipotesi induttiva risulta $\mathbf{YX} = \mathbf{I}_{n-1}$, quindi $\mathbf{Y} = \mathbf{X}^{-1}$ e $\mathbf{z} = \mathbf{I}_{n-1}\mathbf{z} = \mathbf{YXz} = \mathbf{Y0} = \mathbf{0}$. Ne consegue che $ab = 1$ e $\mathbf{y}^T = -a^{-1}\mathbf{x}^T\mathbf{X}^{-1}$, quindi

$$\mathbf{RE}^{-1} = \begin{bmatrix} a^{-1} & -a^{-1}\mathbf{x}^T\mathbf{X}^{-1} \\ \mathbf{0} & \mathbf{X}^{-1} \end{bmatrix}.$$

Basta allora a questo punto eseguire la moltiplicazione $\mathbf{RA} = \mathbf{RE}^{-1}\mathbf{EA}$ a blocchi:

$$\begin{aligned} \begin{bmatrix} a^{-1} & -a^{-1}\mathbf{x}^T\mathbf{X}^{-1} \\ \mathbf{0} & \mathbf{X}^{-1} \end{bmatrix} \begin{bmatrix} a & \mathbf{x}^T \\ \mathbf{0} & \mathbf{X} \end{bmatrix} &= \begin{bmatrix} a^{-1}a & a^{-1}\mathbf{x}^T - a^{-1}\mathbf{x}^T\mathbf{X}^{-1}\mathbf{X} \\ \mathbf{0} & \mathbf{X}^{-1}\mathbf{X} \end{bmatrix} \\ &= \begin{bmatrix} 1 & \mathbf{0}^T \\ \mathbf{0} & \mathbf{I}_{n-1} \end{bmatrix} \end{aligned}$$

per ottenere che $\mathbf{RA} = \mathbf{I}_n$.

Per quanto riguarda il viceversa, se $\mathbf{LA} = \mathbf{I}_n$, usando quanto appena visto si ricava:

$$\begin{aligned} \mathbf{LA} = \mathbf{I}_n \implies (\mathbf{LA})^T = \mathbf{I}_n^T \implies \mathbf{A}^T\mathbf{L}^T = \mathbf{I}_n \implies \\ \implies \mathbf{L}^T\mathbf{A}^T = \mathbf{I}_n \implies (\mathbf{AL})^T = \mathbf{I}_n \implies \mathbf{AL} = \mathbf{I}_n. \end{aligned}$$ □

Il risultato che segue mostra come una matrice può avere inversa destra solo se è "orizzontale", cioè con un numero di colonne non inferiore a quello delle righe.

Proposizione 4.7. *Sia* $\mathbf{A}$ *una matrice* $m \times n$ *dotata di inversa destra. Allora* $m \le n$.

Dimostrazione. Sia $\mathbf{AR} = \mathbf{I}_m$. Se fosse $m > n$ si potrebbero decomporre a blocchi $\mathbf{A}$ ed $\mathbf{R}$ nel modo seguente

$$\mathbf{A} = \begin{bmatrix} \mathbf{A}_1 \\ \mathbf{A}_2 \end{bmatrix}; \qquad \mathbf{R} = [\mathbf{R}_1\ \mathbf{R}_2]$$

con $\mathbf{A}_1$ ed $\mathbf{R}_1$ blocchi quadrati di ordine n. Moltiplicando $\mathbf{A}$ ed $\mathbf{R}$ a blocchi e uguagliando a $\mathbf{I}_m$, pure decomposta a blocchi in modo conforme, si ottiene:

$$\mathbf{A}_1\mathbf{R}_1 = \mathbf{I}_n, \quad \mathbf{A}_1\mathbf{R}_2 = \mathbb{O}, \quad \mathbf{A}_2\mathbf{R}_1 = \mathbb{O}, \quad \mathbf{A}_2\mathbf{R}_2 = \mathbf{I}_{m-n}.$$

Dalla Proposizione 4.6 sappiamo che $\mathbf{A}_1\mathbf{R}_1 = \mathbf{R}_1\mathbf{A}_1$, quindi

$$\mathbf{A}_2\mathbf{R}_1 = \mathbb{O} \implies \mathbf{A}_2\mathbf{R}_1\mathbf{A}_1 = \mathbb{O} \implies \mathbf{A}_2 = \mathbb{O},$$

che contraddice l'uguaglianza $\mathbf{A}_2\mathbf{R}_2 = \mathbf{I}_{m-n}$. □

Come immediata conseguenza si ricava il risultato simmetrico per le inverse sinistre di matrici $m \times n$, che mostra come esse possono esistere solo per matrici "verticali", cioè con un numero di righe non inferiore a quello delle colonne.

Corollario 4.8. *Sia* $\mathbf{A}$ *una matrice* $m \times n$ *dotata di inversa sinistra. Allora* $m \geq n$.

Dimostrazione. $\mathbf{A}$ ammette come inversa sinistra la matrice $\mathbf{L}$ se e solo se $\mathbf{A}^T$ ammette come inversa destra la matrice $\mathbf{L}^T$. Si applichi allora ad $\mathbf{A}^T$ la Proposizione 4.7. □

Diamo un'altra diretta conseguenza dei due ultimi risultati e della Proposizione 4.1.

Corollario 4.9. *Se una matrice* $\mathbf{A}$ *ha inversa destra e inversa sinistra, allora è una matrice quadrata invertibile.*

Dimostrazione. Sia $\mathbf{A}$ $m \times n$. Per la Proposizione 4.7 risulta $m \leq n$ e per il Corollario 4.8 risulta $m \geq n$, quindi $m = n$. La Proposizione 4.1 assicura poi che $\mathbf{A}$ è invertibile. □

Diamo ora il risultato che contiene le principali caratterizzazioni delle matrici che ammettono inversa destra.

Teorema 4.10. *Per una matrice* $m \times n$ $\mathbf{A}$, *le seguenti proprietà sono equivalenti:*

(a) $\mathbf{A}$ *ammette inversa destra;*

(b) *il sistema* $\mathbf{A}\mathbf{x} = \mathbf{b}$ *ammette almeno una soluzione per ogni scelta del vettore* $\mathbf{b}$*;*

(c) $\mathbf{A}$ *ha rango* m.

Dimostrazione. (a) ⇒ (b) Segue dalla Proposizione 4.4 (a).

(b) ⇒ (c) Se per assurdo $\mathbf{A}$ avesse rango $< m$, una sua forma ridotta $\mathbf{U}$ avrebbe l'ultima riga nulla. Indicato al solito con $\mathbf{e}_m$ l'm-esimo vettore coordinato con m coordinate, nella matrice $[\mathbf{U}\ \mathbf{e}_m]$ l'ultima colonna sarebbe dominante quindi si sarebbe nel caso [0] del Paragrafo precedente e il sistema con matrice aumentata $[\mathbf{U}\ \mathbf{e}_m]$ non avrebbe soluzioni. Procedendo a ritroso, a partire dalla matrice $[\mathbf{U}\ \mathbf{e}_m]$, con le operazioni elementari inverse di quelle eseguite sulla matrice $\mathbf{A}$ per ottenere la forma ridotta $\mathbf{U}$, si perviene alla matrice aumentata $[\mathbf{A}\ \mathbf{b}]$ di un sistema $\mathbf{A}\mathbf{x} = \mathbf{b}$, equivalente al sistema $\mathbf{U}\mathbf{x} = \mathbf{e}_m$, che non ha soluzione, il che è assurdo. Quindi $\mathbf{A}$ ha rango m.

(c) ⇒ (a) Si tratta di provare che esiste una matrice $n \times m$ $\mathbf{R} = [\mathbf{r}_1\ \mathbf{r}_2\ \dots\ \mathbf{r}_m]$, di cui sono state messe in evidenza le colonne, tale che $\mathbf{A}\mathbf{R} = \mathbf{I}_m$, cioè $\mathbf{A}\mathbf{r}_j = \mathbf{e}_j$ per ogni $j \leq m$. Bisogna trovare quindi soluzioni per ciascuno dei sistemi $\mathbf{A}\mathbf{x}_j = \mathbf{e}_j$. La EG sulle matrici aumentate $[\mathbf{A}\ \mathbf{e}_j]$ produce le forme ridotte $[\mathbf{U}\ \mathbf{c}_j]$ in cui l'ultima colonna non è mai dominante, giacché l'ultima riga di $\mathbf{U}$ non è nulla. Pertanto i sistemi considerati hanno soluzione e la matrice $\mathbf{R}$ esiste. □

L'equivalenza di (a) e (c) nel Teorema 4.10 e la Proposizione 4.6 hanno una conseguenza immediata.

Corollario 4.11. *Una matrice quadrata di ordine* m *è invertibile se e solo se ha rango* m. □

Il risultato simmetrico del precedente per le matrici che ammettono inversa sinistra è fornito dal teorema seguente.

Teorema 4.12. *Per una matrice* $m \times n$ $\mathbf{A}$, *le seguenti proprietà sono equivalenti:*

(a) $\mathbf{A}$ *ammette inversa sinistra;*
(b) *il sistema* $\mathbf{Ax} = \mathbf{0}$ *ammette solo la soluzione nulla;*
(c) $\mathbf{A}$ *ha rango* n*;*
(d) *la matrice* $\mathbf{A}^H\mathbf{A}$ *è invertibile.*

Dimostrazione. (a) $\Rightarrow$ (b) Segue dalla Proposizione 4.4 (b).

(b) $\Leftrightarrow$ (c) $\mathbf{A}$ ha rango $< n$ se e solo se la matrice aumentata $[\mathbf{A}\ \mathbf{0}]$ ha forma ridotta $[\mathbf{U}\ \mathbf{0}]$ con meno di n righe non nulle. Ciò equivale al fatto che almeno una colonna di $\mathbf{U}$ non è dominante, cioè il sistema $\mathbf{Ax} = \mathbf{0}$ ricade nel caso $[\infty]$ del Paragrafo 3 e ha infinite soluzioni (oltre a quella nulla).

(c) $\Rightarrow$ (d) Essendo $\mathbf{A}^H\mathbf{A}$ matrice quadrata di ordine n, per il Corollario 4.11 è sufficiente provare che essa ha rango n. Per l'implicazione (b) $\Rightarrow$ (c) applicata alla matrice $\mathbf{A}^H\mathbf{A}$, basta provare che il sistema $\mathbf{A}^H\mathbf{Ax} = \mathbf{0}$ ammette solo la soluzione nulla. Sia $\mathbf{v}$ una soluzione; risulta allora $\mathbf{v}^H\mathbf{A}^H\mathbf{Av} = 0$. Posto $\mathbf{Av} = \mathbf{y} = (y_1\ \dots\ y_m)^T$, si ha $\mathbf{y}^H\mathbf{y} = 0$; ma $\mathbf{y}^H\mathbf{y} = \overline{y}_1 y_1 + \cdots + \overline{y}_m y_m = 0$ implica che $y_i = 0$ per ogni i (perché $\overline{y}_i y_i$ è un numero reale ≥ 0 per ogni i) e quindi $\mathbf{y} = \mathbf{0}$. Ma allora $\mathbf{Av} = \mathbf{0}$ e da (b) segue che $\mathbf{v} = \mathbf{0}$, come desiderato.

(d) $\Rightarrow$ (a) Una inversa sinistra di $\mathbf{A}$ è $(\mathbf{A}^H\mathbf{A})^{-1}\mathbf{A}^H$. □

Per completare la caratterizzazione delle matrici che ammettono inversa destra, manca l'analogo del punto (d) del Teorema 4.12, che però siamo ora in grado di dimostrare.

Corollario 4.13. *Una matrice* $m \times n$ $\mathbf{A}$ *ha inversa destra se e solo se la matrice* $\mathbf{AA}^H$ *è invertibile.*

Dimostrazione. Se $\mathbf{A}$ ha inversa destra, allora $\mathbf{A}^H$ ha inversa sinistra. Per il Teorema 4.12, $(\mathbf{A}^H)^H\mathbf{A}^H$ è invertibile. Ma $(\mathbf{A}^H)^H\mathbf{A}^H = \mathbf{AA}^H$, da cui l'asserto.

Viceversa, se $\mathbf{AA}^H$ è invertibile, una inversa destra di $\mathbf{A}$ è $\mathbf{A}^H(\mathbf{AA}^H)^{-1}$. □

È utile osservare che nelle condizioni sulle matrici $\mathbf{AA}^H$ e $\mathbf{A}^H\mathbf{A}$ nel Teorema 4.10 e nel Corollario 4.13 non si può sostituire la matrice H-trasposta $\mathbf{A}^H$ con la matrice trasposta $\mathbf{A}^T$, naturalmente a meno che $\mathbf{A}$ non sia una matrice reale. Infatti, pure essendo $\mathbf{A}$ non nulla, può risultare $\mathbf{AA}^T = \mathbb{O}$ (e analogamente $\mathbf{A}^T\mathbf{A} = \mathbb{O}$), come mostra il seguente esempio.

Esempio 4.14. Si consideri il vettore riga

$$\mathbf{A} = [1+i \ \ 1-i]$$

per il quale risulta

$$\mathbf{A}^T = \begin{bmatrix} 1+i \\ 1-i \end{bmatrix}, \qquad \mathbf{A}^H = \begin{bmatrix} 1-i \\ 1+i \end{bmatrix}.$$

Un facile calcolo mostra che

$$\mathbf{AA}^T = 1 - 1 + 2i + 1 - 1 - 2i = 0,$$
$$\mathbf{AA}^H = (1+i)(1-i) + (1-i)(1+i) = 4.$$

□

I due Teoremi 4.10 e 4.12 congiuntamente con la Proposizione 4.6 e il Corollario 4.13 porgono come immediata conseguenza il seguente teorema, in cui il punto (e) impiega la nozione di determinante, che sarà introdotta nel Capitolo 4, ed è pertanto inserito qui a puro titolo informativo.

Teorema 4.15. *Sia* $\mathbf{A}$ *una matrice quadrata di ordine* n. *Le seguenti proprietà sono equivalenti:*

(a) $\mathbf{A}$ *è invertibile;*

(b) *il sistema* $\mathbf{Ax} = \mathbf{b}$ *ammette almeno una soluzione per ogni scelta del vettore* $\mathbf{b}$*;*

(c) *il sistema* $\mathbf{Ax} = \mathbf{0}$ *ha come unica soluzione* $\mathbf{x} = \mathbf{0}$*;*

(d) $\mathbf{A}$ *ha rango* n*;*

(e) *il determinante di* $\mathbf{A}$ *è diverso da* 0. □

Il modo più semplice per vedere se una matrice quadrata è invertibile risulta quello fornito nel punto (d) del Teorema 4.15: si controlla che una forma ridotta della matrice non abbia righe nulle. L'algoritmo di inversione presentato nel prossimo Paragrafo permetterà poi di trovare esplicitamente l'inversa.

Le proprietà delle matrici inverse di matrici quadrate sono raccolte nel seguente elenco; le facili dimostrazioni sono lasciate come esercizio.

Siano $\mathbf{A}$ e $\mathbf{B}$ matrici quadrate invertibili di ordine n. Allora:

(a) $\mathbf{AB}$ è invertibile e $(\mathbf{AB})^{-1} = \mathbf{B}^{-1}\mathbf{A}^{-1}$.

(b) $\mathbf{A}^{-1}$ è invertibile e $(\mathbf{A}^{-1})^{-1} = \mathbf{A}$.

(c) $\mathbf{A}^T$ e $\mathbf{A}^H$ sono invertibili e $(\mathbf{A}^T)^{-1} = (\mathbf{A}^{-1})^T$, $(\mathbf{A}^H)^{-1} = (\mathbf{A}^{-1})^H$.

È utile infine sapere cosa accade per le inverse di matrici triangolari e per matrici decomposte a blocchi. Nei due esempi seguenti vengono date informazioni su tali inverse.

Esempio 4.16. Una matrice triangolare superiore (risp., inferiore) $\mathbf{T} = (t_{ij})$ è invertibile se e solo se tutti i coefficienti diagonali t_{ii} sono diversi da zero. Se ciò accade, la matrice inversa $\mathbf{T}^{-1}$ è ancora triangolare superiore (risp., inferiore) e ha come coefficienti diagonali gli inversi dei corrispondenti coefficienti diagonali di $\mathbf{T}$. La dimostrazione si esegue facilmente per induzione sull'ordine della matrice.

Lo stesso vale per matrici triangolari a blocchi, con blocchi diagonali quadrati, sostituendo le condizioni sui coefficienti diagonali con analoghe condizioni sui blocchi diagonali. In particolare, data la matrice triangolare a blocchi

$$\mathbf{T} = \begin{bmatrix} \mathbf{X} & \mathbf{Y} \\ \mathbb{O} & \mathbf{V} \end{bmatrix}$$

con $\mathbf{X}$ e $\mathbf{V}$ blocchi quadrati invertibili, risulta

$$\mathbf{T}^{-1} = \begin{bmatrix} \mathbf{X}^{-1} & -\mathbf{X}^{-1}\mathbf{Y}\mathbf{V}^{-1} \\ \mathbb{O} & \mathbf{V}^{-1} \end{bmatrix}.$$

Infatti
$$\begin{bmatrix}\mathbf{X} & \mathbf{Y}\\ \mathbb{O} & \mathbf{V}\end{bmatrix}\begin{bmatrix}\mathbf{X}^{-1} & -\mathbf{X}^{-1}\mathbf{Y}\mathbf{V}^{-1}\\ \mathbb{O} & \mathbf{V}^{-1}\end{bmatrix}=\begin{bmatrix}\mathbf{X}\mathbf{X}^{-1} & -\mathbf{X}\mathbf{X}^{-1}\mathbf{Y}\mathbf{V}^{-1}+\mathbf{Y}\mathbf{V}^{-1}\\ \mathbb{O} & \mathbf{V}\mathbf{V}^{-1}\end{bmatrix}$$
e l'ultima matrice a blocchi è evidentemente la matrice identità. □

L'esempio seguente tratta il caso non banale più semplice di matrici inverse, quello 2×2. Si confronti con l'Esempio 4.3.

Esempio 4.17. La matrice 2×2
$$\mathbf{A}=\begin{bmatrix}a & b\\ c & d\end{bmatrix}$$
ha inversa se e solo se $\Delta = ad - bc \neq 0$, e in tal caso l'inversa è la matrice
$$\mathbf{A}^{-1}=\Delta^{-1}\begin{bmatrix}d & -b\\ -c & a\end{bmatrix}.$$
La verifica che, nel caso in cui $\Delta \neq 0$, la suddetta matrice è l'inversa di $\mathbf{A}$ è immediata. Il fatto che l'invertibilità di $\mathbf{A}$ comporta che $\Delta \neq 0$ si vede nel modo seguente. Se
$$\begin{bmatrix}a & b\\ c & d\end{bmatrix}\begin{bmatrix}x & y\\ z & w\end{bmatrix}=\mathbf{I}_2$$
allora $ax+bz=1$, $cx+dz=0$ e $cy+dw=1$. Nel caso in cui $c\neq 0$, sottraendo dalla prima uguaglianza moltiplicata per c la seconda moltiplicata per a si ricava $(bc-ad)z=c$; nel caso in cui $d\neq 0$, sottraendo dalla prima uguaglianza moltiplicata per d la seconda moltiplicata per b si ricava $(ad-bc)x=d$. Poiché non può essere $c=0=d$, perché $cy+dw=1$, in ogni caso risulta $\Delta\neq 0$.

Si vedrà al Capitolo 4 che il numero Δ è il determinante della matrice $\mathbf{A}$. □

Pseudo-inversa

Si è visto che una matrice ha inversa—destra, sinistra o bilatera—solo in casi particolari. Esiste una nozione che generalizza quella di matrice inversa che è applicabile a una qualunque matrice, ed è quella di matrice pseudo-inversa. Il lettore è avvertito del fatto che sono state date molteplici nozioni che generalizzano quella di matrice inversa; quella che presentiamo qui prende anche il nome di "pseudo-inversa di Moore-Penrose" (dall'americano E. H. Moore, che la introdusse negli anni '30, e dall'inglese R. Penrose, che la divulgò negli anni '50).

Data una qualunque matrice $m\times n$ $\mathbf{A}$, si chiama *pseudo-inversa* di $\mathbf{A}$ una matrice $\mathbf{A}^+$ che soddisfa alle quattro condizioni:
$$\mathbf{A}\mathbf{A}^+\mathbf{A}=\mathbf{A},\qquad \mathbf{A}^+\mathbf{A}\mathbf{A}^+=\mathbf{A}^+,\qquad \mathbf{A}\mathbf{A}^+=(\mathbf{A}\mathbf{A}^+)^H,\qquad \mathbf{A}^+\mathbf{A}=(\mathbf{A}^+\mathbf{A})^H.$$
Si osservi che la matrice $\mathbf{A}^+$ ha necessariamente dimensioni $n\times m$. Naturalmente si pone il problema dell'esistenza di una tale matrice $\mathbf{A}^+$, e, qualora essa esista, si pone il problema della sua unicità. Cominciamo col problema dell'unicità.

Proposizione 4.18. *Sia* $\mathbf{A}$ *una matrice* $m \times n$ *e siano* $\mathbf{B}$ *e* $\mathbf{C}$ *due matrici che soddisfano alle quattro condizioni cui deve soddisfare una matrice pseudo-inversa. Allora* $\mathbf{B} = \mathbf{C}$.

Dimostrazione. Useremo nel seguito, oltre alle proprietà delle matrici H-trasposte, tutte le quattro condizioni cui soddisfano $\mathbf{B}$ e $\mathbf{C}$; il lettore controlli a ogni passaggio quale delle condizioni viene impiegata:

$$\begin{aligned}
\mathbf{B} &= \mathbf{BAB} = (\mathbf{BA})^H\mathbf{B} \\
&= \mathbf{A}^H\mathbf{B}^H\mathbf{B} = (\mathbf{ACA})^H\mathbf{B}^H\mathbf{B} \\
&= \mathbf{A}^H\mathbf{C}^H\mathbf{A}^H\mathbf{B}^H\mathbf{B} = (\mathbf{CA})^H(\mathbf{BA})^H\mathbf{B} \\
&= \mathbf{CABAB} = \mathbf{CAB} \\
&= \mathbf{CACAB} = \mathbf{C}(\mathbf{AC})^H(\mathbf{AB})^H \\
&= \mathbf{CC}^H\mathbf{A}^H\mathbf{B}^H\mathbf{A}^H = \mathbf{CC}^H(\mathbf{ABA})^H \\
&= \mathbf{CC}^H\mathbf{A}^H = \mathbf{C}(\mathbf{AC})^H \\
&= \mathbf{CAC} = \mathbf{C}.
\end{aligned}$$ □

Per quanto riguarda l'esistenza della pseudo-inversa, la prima cosa da farsi è quella di esaminare cosa accade nei tre casi, già studiati nella prima parte di questo Paragrafo, in cui esiste l'inversa bilatera, oppure esistono inverse destre o inverse sinistre.

(i) Supponiamo che la matrice $\mathbf{A}$ sia invertibile, quindi quadrata. È immediato verificare che $\mathbf{A}^{-1}$ soddisfa alle quattro condizioni della pseudo-inversa, perciò $\mathbf{A}^+ = \mathbf{A}^{-1}$.

(ii) Supponiamo che la matrice $\mathbf{A}$ non sia quadrata e abbia inversa destra; quindi risulta $m < n$. Il Teorema 4.12 (d) assicura che esiste la matrice $\mathbf{A}^H(\mathbf{AA}^H)^{-1}$, che è ovviamente inversa destra di $\mathbf{A}$. Vogliamo verificare che

$$\mathbf{A}^+ = \mathbf{A}^H(\mathbf{AA}^H)^{-1}.$$

Poiché ogni inversa destra soddisfa banalmente a tre delle condizioni richieste, basta controllare che $\mathbf{A}^H(\mathbf{AA}^H)^{-1}\mathbf{A}$ è hermitiana. Si ha infatti

$$(\mathbf{A}^H(\mathbf{AA}^H)^{-1}\mathbf{A})^H = \mathbf{A}^H((\mathbf{AA}^H)^{-1})^H\mathbf{A} = \mathbf{A}^H(\mathbf{AA}^H)^{-1}\mathbf{A}.$$

Si può verificare direttamente (si veda l'Esercizio 1.26), o dedurre dalla Proposizione 4.18, che $\mathbf{A}^H(\mathbf{AA}^H)^{-1}$ è l'unica tra le infinite inverse destre $\mathbf{R}$ di $\mathbf{A}$ a soddisfare alla condizione che $\mathbf{RA}$ è hermitiana.

(iii) Supponiamo che la matrice $\mathbf{A}$ non sia quadrata e abbia inversa sinistra; quindi risulta $m > n$. Con ragionamento in tutto analogo al precedente, partendo dal Teorema 4.11 (d) si prova che

$$\mathbf{A}^+ = (\mathbf{A}^H\mathbf{A})^{-1}\mathbf{A}^H.$$

L'esistenza della matrice pseudo-inversa nel caso di una matrice qualunque $\mathbf{A}$ si deduce agevolmente dai due precedenti casi (ii) e (iii), una volta che si sappia decomporre la matrice $\mathbf{A}$ in modo opportuno.

Proposizione 4.19. *Sia* $\mathbf{A}$ *una matrice* $m \times n$ *e sia* $\mathbf{A} = \mathbf{BC}$ *una sua fattorizzazione tale che* $\mathbf{B}$ *ammette inversa sinistra e* $\mathbf{C}$ *ammette inversa destra. Allora* $\mathbf{A}^+$ *esiste e risulta*

$$\mathbf{A}^+ = \mathbf{C}^+\mathbf{B}^+ = \mathbf{C}^H(\mathbf{C}\mathbf{C}^H)^{-1}(\mathbf{B}^H\mathbf{B})^{-1}\mathbf{B}^H.$$

Dimostrazione. Dai casi (ii) e (iii) precedentemente esaminati sappiamo che

$$\mathbf{B}^+ = (\mathbf{B}^H\mathbf{B})^{-1}\mathbf{B}^H, \qquad \mathbf{C}^+ = \mathbf{C}^H(\mathbf{C}\mathbf{C}^H)^{-1}.$$

Si tratta allora di verificare le uguaglianze

$$\mathbf{BC} = \mathbf{BCC}^+\mathbf{B}^+\mathbf{BC}, \qquad \mathbf{C}^+\mathbf{B}^+ = \mathbf{C}^+\mathbf{B}^+\mathbf{BCC}^+\mathbf{B}^+$$

che risultano ovvie, essendo $\mathbf{B}^+$ inversa sinistra di $\mathbf{B}$ e $\mathbf{C}^+$ inversa destra di $\mathbf{C}$; bisogna inoltre verificare che sono hermitiane le matrici $\mathbf{BCC}^+\mathbf{B}^+$ e $\mathbf{C}^+\mathbf{B}^+\mathbf{BC}$, il che è pure ovvio, perché

$$\mathbf{BCC}^+\mathbf{B}^+ = \mathbf{BB}^+, \qquad \mathbf{C}^+\mathbf{B}^+\mathbf{BC} = \mathbf{C}^+\mathbf{C}. \qquad \square$$

Va osservato che se si ha una arbitraria fattorizzazione $\mathbf{A} = \mathbf{BC}$ della matrice $\mathbf{A}$, non è vero che $\mathbf{A}^+ = \mathbf{C}^+\mathbf{B}^+$; si vedano però le proprietà (pi$_6$) e (pi$_7$) elencate di seguito.

Vedremo al termine del Paragrafo 6 che una generica matrice $\mathbf{A}$ ha sempre fattorizzazioni soddisfacenti all'ipotesi della Proposizione 4.19, che saranno chiamate "decomposizioni a rango pieno". Possiamo perciò concludere con il seguente risultato.

Teorema 4.20. *Data una qualunque matrice* $\mathbf{A}$*, la sua pseudo-inversa* $\mathbf{A}^+$ *esiste ed è unica.* $\square$

Diamo un semplice esempio di matrice pseudo-inversa.

Esempio 4.21. Si consideri la matrice 2×3

$$\mathbf{A} = \begin{bmatrix} 4 & 0 & 2 & 6 \\ 2 & 0 & 1 & 3 \end{bmatrix}.$$

È immediato verificare che vale la fattorizzazione

$$\mathbf{A} = \begin{bmatrix} 2 \\ 1 \end{bmatrix} [2\ 0\ 1\ 3]$$

dove la matrice $\mathbf{B} = \left[\begin{smallmatrix} 2 \\ 1 \end{smallmatrix}\right]$ ha inversa sinistra e la matrice $\mathbf{C} = [2\ 0\ 1\ 3]$ ha inversa destra. Un facile calcolo mostra che

$$\mathbf{B}^+ = (\mathbf{B}^H\mathbf{B})^{-1}\mathbf{B}^H = \left([2\ 1]\begin{bmatrix} 2 \\ 1 \end{bmatrix}\right)^{-1}[2\ 1] = [2/5\ 1/5]$$

$$\mathbf{C}^+ = \mathbf{C}^H(\mathbf{C}\mathbf{C}^H)^{-1} = \begin{bmatrix} 2 \\ 0 \\ 1 \\ 3 \end{bmatrix}\left([2\ 0\ 1\ 3]\begin{bmatrix} 2 \\ 0 \\ 1 \\ 3 \end{bmatrix}\right)^{-1} = \begin{bmatrix} 2/14 \\ 0 \\ 1/14 \\ 3/14 \end{bmatrix}.$$

Pertanto la pseudo-inversa di $\mathbf{A}$ risulta essere:

$$\mathbf{A}^{+} = \begin{bmatrix} 2/14 \\ 0 \\ 1/14 \\ 3/14 \end{bmatrix} [2/5\ 1/5] = \begin{bmatrix} 4/70 & 2/70 \\ 0 & 0 \\ 2/70 & 1/70 \\ 6/70 & 3/70 \end{bmatrix} = 70^{-1}\mathbf{A}^{T}. \qquad \square$$

Forniamo di seguito alcune proprietà della matrice psudo-inversa, la cui verifica, sempre molto facile, è lasciata come esercizio.

(pi$_1$) $(\mathbf{A}^{+})^{+} = \mathbf{A}$;

(pi$_2$) $(\mathbf{A}^{+})^{H} = (\mathbf{A}^{H})^{+}$;

(pi$_3$) $\mathbb{O}_{mn}^{+} = \mathbb{O}_{nm}$;

(pi$_4$) $(\alpha\mathbf{A})^{+} = \alpha^{-1}\mathbf{A}^{+}$ per ogni scalare $\alpha \neq 0$;

(pi$_5$) $\mathbf{A}^{H} = \mathbf{A}^{+}\mathbf{A}\mathbf{A}^{H} = \mathbf{A}^{H}\mathbf{A}\mathbf{A}^{+}$;

(pi$_6$) se $\mathbf{A} = \mathbf{B}\mathbf{C}$ con $\mathbf{B}$ soddisfacente all'uguaglianza $\mathbf{B}^{H}\mathbf{B} = \mathbf{I}$, allora $\mathbf{A}^{+} = \mathbf{C}^{+}\mathbf{B}^{H}$;

(pi$_7$) se $\mathbf{A} = \mathbf{B}\mathbf{C}$ con $\mathbf{C}$ soddisfacente all'uguaglianza $\mathbf{C}\mathbf{C}^{H} = \mathbf{I}$, allora $\mathbf{A}^{+} = \mathbf{C}^{H}\mathbf{B}^{+}$.

A chiusura del Paragrafo, osserviamo che la proprietà della matrice pseudo-inversa $\mathbf{A}^{+}$ di una matrice $m \times n$ $\mathbf{A}$ che più la avvicina all'inversa è la seguente: l'applicazione $f_{\mathbf{A}}\colon \mathbb{C}^{n} \to \mathbb{C}^{m}$ indotta dalla moltiplicazione per $\mathbf{A}$ e l'applicazione $f_{\mathbf{A}^{+}}\colon \mathbb{C}^{m} \to \mathbb{C}^{n}$ indotta dalla moltiplicazione per $\mathbf{A}^{+}$ sono due funzioni che risultano una l'inversa dell'altra se ristrette rispettivamente allo spazio delle righe $C(\mathbf{A}^{H})$ e allo spazio delle colonne $C(\mathbf{A})$ di $\mathbf{A}$ (si veda il Paragrafo 4 del Capitolo 2). Per verificare questa proprietà è sufficiente sapere che $\mathbf{y} \in C(\mathbf{A})$ se e solo se $\mathbf{y} = \mathbf{A}\mathbf{x}$ per un vettore $\mathbf{x} \in \mathbb{C}^{n}$, e similmente $\mathbf{x} \in C(\mathbf{A}^{H})$ se e solo se $\mathbf{x} = \mathbf{A}^{H}\mathbf{y}$ per un vettore $\mathbf{y} \in \mathbb{C}^{m}$. Atteso ciò, risulta, per ogni vettore $\mathbf{y} \in C(\mathbf{A})$ e ogni vettore $\mathbf{x} \in C(\mathbf{A}^{H})$:

$$\begin{aligned} f_{\mathbf{A}}(f_{\mathbf{A}^{+}}(\mathbf{y})) &= \mathbf{A}\mathbf{A}^{+}\mathbf{A}\mathbf{x} = \mathbf{A}\mathbf{x} = \mathbf{y} \\ f_{\mathbf{A}^{+}}(f_{\mathbf{A}}(\mathbf{x})) &= \mathbf{A}^{+}\mathbf{A}\mathbf{A}^{H}\mathbf{y} = \mathbf{A}^{H}\mathbf{y} = \mathbf{x}. \end{aligned}$$

5. Eliminazione di Gauss per il calcolo delle matrici inverse

Si è visto nel Paragrafo 4 che, se si conosce una inversa destra $\mathbf{R}$ della matrice $\mathbf{A}$, si ricava subito una soluzione $\mathbf{v}$ del sistema lineare $\mathbf{A}\mathbf{x} = \mathbf{b}$: essa è data da $\mathbf{v} = \mathbf{R}\mathbf{b}$. In particolare, se la matrice $\mathbf{A}$ è quadrata e invertibile, l'unica soluzione del sistema è $\mathbf{A}^{-1}\mathbf{b}$. Pertanto, pur non essendo l'esistenza di una inversa destra di $\mathbf{A}$ condizione necessaria per la risolubilità del sistema, sembra che un modo per risolverlo, alternativo all'algoritmo della EG, sia quello di cercare una inversa destra della matrice dei coefficienti.

In realtà è vero il contrario, cioè la ricerca di una inversa destra (o bilatera, nel caso quadrato) di una matrice viene ricondotta alla soluzione di una serie di sistemi lineari; tramite l'*algoritmo di Gauss-Jordan*, che perfeziona la EG, questa serie di sistemi viene trattata in blocco e produce la inversa.

Vediamo dapprima su di un esempio come funziona tale algoritmo per una matrice quadrata, dopo di che cercheremo di capire perché esso produce la matrice inversa; successivamente lo estenderemo alla matrici rettangolari.

Esempio 5.1. Sia data la matrice 3×3:

$$\mathbf{A} = \begin{bmatrix} 1 & -1 & 2 \\ 0 & 2 & 1 \\ -1 & 0 & -2 \end{bmatrix}.$$

Si consideri la matrice a blocchi 3×6:

$$\begin{bmatrix}\mathbf{A} \mid \mathbf{I}_3\end{bmatrix} = \left[\begin{array}{ccc|ccc} 1 & -1 & 2 & 1 & 0 & 0 \\ 0 & 2 & 1 & 0 & 1 & 0 \\ -1 & 0 & -2 & 0 & 0 & 1 \end{array}\right]$$

ottenuta affiancando a destra alla matrice $\mathbf{A}$ la matrice identità $\mathbf{I}_3$. Lo scopo dell'algoritmo di Gauss-Jordan è di modificare con le operazioni elementari tale matrice a blocchi fino a ottenere una matrice del tipo

$$\begin{bmatrix}\mathbf{I}_3 \mid \mathbf{B}\end{bmatrix}.$$

La matrice $\mathbf{B}$ risulterà essere la matrice inversa della matrice $\mathbf{A}$.

Si esegue quindi la usuale EG sulla matrice $\begin{bmatrix}\mathbf{A} \mid \mathbf{I}_3\end{bmatrix}$ pervenendo alla matrice

$$\left[\begin{array}{ccc|ccc} 1 & -1 & 2 & 1 & 0 & 0 \\ 0 & 1 & \frac{1}{2} & 0 & \frac{1}{2} & 0 \\ 0 & 0 & 1 & 2 & 1 & 2 \end{array}\right].$$

Il blocco di sinistra è una forma ridotta di $\mathbf{A}$; ora inizia la parte nuova dell'algoritmo. Si procede quindi con quella che si chiama *eliminazione all'indietro* che, tramite le solite operazioni elementari, pone degli zeri *al di sopra* degli elementi diagonali, partendo dall'ultima riga e risalendo fino alla prima.

Usando come pivot il coefficiente di posto $(3,3)$, si sostituisce quindi alla seconda riga la sua somma con la terza moltiplicata per $-1/2$, e alla prima riga la sua somma con la terza moltiplicata per -2; si ottiene la matrice

$$\left[\begin{array}{ccc|ccc} 1 & -1 & 0 & -3 & -2 & -4 \\ 0 & 1 & 0 & -1 & 0 & -1 \\ 0 & 0 & 1 & 2 & 1 & 2 \end{array}\right].$$

Ora, usando il coefficiente di posto $(2,2)$, si sostituisce alla prima riga la sua somma con la seconda moltiplicata per 1, ottenendo la matrice

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 0 & -4 & -2 & -5 \\ 0 & 1 & 0 & -1 & 0 & -1 \\ 0 & 0 & 1 & 2 & 1 & 2 \end{array}\right].$$

La matrice ha assunto quindi la forma desiderata $[\mathbf{I}_3 \mid \mathbf{B}]$, con

$$\mathbf{B} = \begin{bmatrix} -4 & -2 & -5 \\ -1 & 0 & -1 \\ 2 & 1 & 2 \end{bmatrix}.$$

La matrice $\mathbf{B}$ così ottenuta coincide con l'inversa $\mathbf{A}^{-1}$: il lettore verifichi infatti che $\mathbf{AB} = \mathbf{I}_3$. □

Cerchiamo ora di capire, in tutta generalità, perché l'algoritmo di Gauss-Jordan produce la matrice inversa. La spiegazione è fornita nella dimostrazione della seguente proposizione.

Proposizione 5.2. *Sia* $\mathbf{A}$ *una matrice quadrata* $n \times n$*. Se* $\mathbf{A}$ *è invertibile, la sua inversa* $\mathbf{A}^{-1}$ *si ottiene a partire dalla matrice a blocchi* $[\mathbf{A} \mid \mathbf{I}_n]$*, operando su di essa con l'algoritmo di Gauss-Jordan fino a trasformarla nella forma* $[\mathbf{I}_n \mid \mathbf{B}]$*. Allora la matrice inversa* $\mathbf{A}^{-1}$ *coincide con la matrice* $\mathbf{B}$.

Dimostrazione. Mettiamo in evidenza le colonne della matrice $\mathbf{A}^{-1}$:

$$\mathbf{A}^{-1} = [\mathbf{v}_1\ \mathbf{v}_2\ \ldots\ \mathbf{v}_n].$$

L'uguaglianza $\mathbf{AA}^{-1} = \mathbf{I}_n$ si può scrivere come una serie di n uguaglianze

$$\mathbf{Av}_i = \mathbf{e}_i \qquad (i = 1, 2, \ldots, n)$$

giacché $\mathbf{Av}_i$ è la i-esima colonna della matrice prodotto $\mathbf{AA}^{-1}$ ed $\mathbf{e}_i$ è la i-esima colonna della matrice identità. Perciò trovare $\mathbf{A}^{-1}$ significa risolvere gli n sistemi lineari, ciascuno in n equazioni ed n incognite: $\mathbf{Ax} = \mathbf{e}_i$, $(i = 1, 2, \ldots, n)$.

Questi sistemi sono tra di loro "parenti stretti", poiché condividono la matrice dei coefficienti, mentre i loro termini noti sono gli n vettori coordinati $\mathbf{e}_1, \ldots, \mathbf{e}_n$. Le operazioni elementari che si eseguono sulle matrici aumentate degli n sistemi

$$[\mathbf{A} \mid \mathbf{e}_1], \quad [\mathbf{A} \mid \mathbf{e}_2], \quad \ldots, \quad [\mathbf{A} \mid \mathbf{e}_n]$$

sono sempre le stesse, per cui è conveniente considerare una unica matrice, detta *matrice pluri-aumentata* di $\mathbf{A}$

$$[\mathbf{A} \mid \mathbf{e}_1 \quad \mathbf{e}_2 \quad \ldots \quad \mathbf{e}_n]$$

Se si eseguono in un sol colpo su tale matrice le operazioni elementari che si eseguirebbero per gli n sistemi, quindi se si opera la EG cui si fanno seguire la eliminazione all'indietro, si ottiene la matrice

$$[\mathbf{I}_n \mid \mathbf{B}] = [\mathbf{I}_n \mid \mathbf{b}_1 \quad \ldots \quad \mathbf{b}_n]$$

dove i vettori $\mathbf{b}_i$ sono le colonne della matrice $\mathbf{B}$. Ciò significa che gli n sistemi $\mathbf{Ax} = \mathbf{e}_i$ sono stati trasformati negli n sistemi equivalenti

$$\mathbf{I}_n\mathbf{x} = \mathbf{b}_i \qquad (i = 1, 2, \ldots, n).$$

Evidentemente le soluzioni di questi sistemi sono proprio i vettori $\mathbf{b}_i$, perciò per ogni $i = 1, 2, \dots, n$ risulta $\mathbf{Ab}_i = \mathbf{e}_i$. Ne consegue che $\mathbf{v}_i = \mathbf{b}_i$ per ogni $i = 1, 2, \dots, n$, pertanto $\mathbf{A}^{-1} = \mathbf{B}$. □

Nel corso dell'algoritmo di Gauss-Jordan applicato a una matrice invertibile può accadere che necessitino scambi di righe; ciò non ha però alcun effetto negativo sull'algoritmo, perché le soluzioni non sono alterate dagli scambi di riga.

Se si applica l'algoritmo di Gauss-Jordan a una matrice non invertibile $n \times n$ $\mathbf{A}$, la prima parte dell'algoritmo consistente nella usuale EG modificherà la matrice pluri-aumentata $\left[\mathbf{A} \mid \mathbf{I}_n\right]$ in una matrice $\left[\mathbf{U} \mid \mathbf{C}\right]$, dove $\mathbf{U}$ non sarà più triangolare superiore con elementi diagonali non-nulli (come nell'Esempio 5.1), perché altrimenti completando l'algoritmo si otterrebbe l'inversa che non esiste. La matrice $\mathbf{U}$ sarà solo a scala per righe con almeno una riga nulla; perciò la successiva parte dell'algoritmo, cioè l'eliminazione all'indietro, non potrà in alcun modo trasformare $\mathbf{U}$ in $\mathbf{I}_n$.

Una volta acquisito l'algoritmo di Gauss-Jordan, si ha un metodo costruttivo per vedere se una matrice quadrata ha inversa e, qualora ciò accada, di calcolare effettivamente tale inversa. Questo metodo è di gran lunga più economico rispetto ad altri possibili metodi, quali quello del calcolo della matrice aggiunta che fa uso dei determinanti (si veda il Capitolo 4).

Il metodo che abbiamo a disposizione può essere modificato facilmente per calcolare le matrici inverse destre di una matrice $m \times n$ di rango $m < n$, qualora esse si presentino in una forma opportuna.

Proposizione 5.3. *Sia* $\mathbf{A} = \left[\mathbf{B} \mid \mathbf{C}\right]$ *una matrice* $m \times n$*, con* $m < n$*, decomposta in due blocchi: il blocco* $\mathbf{B}$ *quadrato* $m \times m$ *invertibile, e il blocco* $\mathbf{C}$ $m \times (n-m)$*. Allora le matrici inverse destre della matrice* $\mathbf{A}$ *sono tutte e sole le matrici* $\mathbf{R}(\mathbf{Y})$ *che si ottengono nel modo seguente: si sceglie una arbitraria matrice* $(n-m) \times m$ $\mathbf{Y}$ *e si pone*

$$\mathbf{R}(\mathbf{Y}) = \begin{bmatrix} \mathbf{B}^{-1} - \mathbf{B}^{-1}\mathbf{CY} \\ \mathbf{Y} \end{bmatrix}.$$

Dimostrazione. Il prodotto a blocchi di $\mathbf{A}$ con $\mathbf{R}(\mathbf{Y})$ porge

$$\begin{aligned} \mathbf{A} \cdot \mathbf{R}(\mathbf{Y}) &= \left[\mathbf{B} \mid \mathbf{C}\right] \begin{bmatrix} \mathbf{B}^{-1} - \mathbf{B}^{-1}\mathbf{CY} \\ \mathbf{Y} \end{bmatrix} \\ &= \mathbf{BB}^{-1} - \mathbf{BB}^{-1}\mathbf{CY} + \mathbf{CY} \\ &= \mathbf{I}_m - \mathbf{CY} + \mathbf{CY} \\ &= \mathbf{I}_m. \end{aligned}$$

Pertanto tutte le matrici $\mathbf{R}(\mathbf{Y})$ definite in questo modo sono inverse destre di $\mathbf{A}$. Viceversa, se $\mathbf{R}$ è inversa destra di $\mathbf{A}$, decomponendola a blocchi nella forma

$$\mathbf{R} = \begin{bmatrix} \mathbf{X} \\ \mathbf{Y} \end{bmatrix}$$

con $\mathbf{X}$ e $\mathbf{Y}$ blocchi di dimensioni $m \times m$ e $(n-m) \times m$, rispettivamente, si ha:

$$\mathbf{AR} = \mathbf{I}_m \implies \mathbf{BX} + \mathbf{CY} = \mathbf{I}_m \implies \mathbf{B}^{-1}\mathbf{BX} + \mathbf{B}^{-1}\mathbf{CY} = \mathbf{B}^{-1} \implies \mathbf{X} = \mathbf{B}^{-1} - \mathbf{B}^{-1}\mathbf{CY}$$

quindi $\mathbf{R} = \mathbf{R}(\mathbf{Y})$. □

Diamo un esempio del metodo descritto nella precedente proposizione.

Esempio 5.4. Si vogliono trovare tutte le inverse destre della matrice

$$\mathbf{A} = \begin{bmatrix} 2 & 3 & 1 \\ 3 & 5 & 2 \end{bmatrix}.$$

Decomponiamo $\mathbf{A}$ a blocchi:

$$\mathbf{A} = [\mathbf{B} \mid \mathbf{C}]$$

dove

$$\mathbf{B} = \begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix}, \quad \mathbf{C} = \begin{bmatrix} 1 \\ 2 \end{bmatrix}.$$

Poiché $\mathbf{B}$ è invertibile, si può applicare la Proposizione 5.3. Sia quindi $\mathbf{Y} = [a\ b]$ una qualunque matrice 1×2; tenuto conto che

$$\mathbf{B}^{-1} = \begin{bmatrix} 5 & -3 \\ -3 & 2 \end{bmatrix}$$

(si ricordi l'Esempio 4.17) le inverse destre della matrice $\mathbf{A}$ sono allora le matrici

$$\begin{bmatrix} \mathbf{B}^{-1} - \mathbf{B}^{-1}\mathbf{CY} \\ \mathbf{Y} \end{bmatrix}$$

dove

$$\mathbf{B}^{-1} - \mathbf{B}^{-1}\mathbf{CY} = \begin{bmatrix} 5 & -3 \\ -3 & 2 \end{bmatrix} - \begin{bmatrix} 5 & -3 \\ -3 & 2 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \end{bmatrix} [a\ b].$$

Pertanto tutte e sole le matrici inverse destre della matrice $\mathbf{A}$ sono della forma

$$\begin{bmatrix} 5+a & -3+b \\ -3-a & 2-b \\ a & b \end{bmatrix}$$

con a e b scalari arbitrari. □

Per risolvere completamente il problema del calcolo dell'inversa destra di una matrice $m \times n$ di rango $m < n$, basterà trovare un metodo per trasformarla in una matrice soddisfacente all'ipotesi della Proposizione 5.3 e, una volta trovata l'inversa destra di quest'ultima matrice, risalire all'inversa destra della matrice di partenza. Questo metodo richiede alcuni risultati sulle matrici di permutazione che saranno provati più avanti, perciò non lo svilupperemo qui (si veda l'Esercizio 1.35). Mostriamo invece su di un esempio un modo più semplice e diretto per il calcolo delle inverse destre, basato sulla soluzione di sistemi lineari.

Esempio 5.5. Si vogliono trovare tutte le inverse destre della matrice

$$\mathbf{A} = \begin{bmatrix} 1 & -2 & -1 & 0 & 2 \\ 0 & 0 & 2 & 2 & -1 \\ -1 & 2 & 0 & -1 & -2 \end{bmatrix}.$$

È facile verificare che il blocco di $\mathbf{A}$ formato dalle prime tre colonne non è invertibile, perciò la Proposizione 5.3 non è applicabile. Si tratta di trovare tutte le matrici 5×3 $\mathbf{R} = [\mathbf{r}_1\ \mathbf{r}_2\ \mathbf{r}_3]$ tali che $\mathbf{AR} = \mathbf{I}_3$ o, equivalentemente, si tratta di risolvere i tre sistemi lineari $\mathbf{Ax} = \mathbf{e}_j$ $(j = 1, 2, 3)$. Conviene a tal fine considerare la matrice pluri-aumentata

$$\left[\mathbf{A} \mid \mathbf{I}_3\right] = \left[\begin{array}{ccccc|ccc} 1 & -2 & -1 & 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 2 & 2 & -1 & 0 & 1 & 0 \\ -1 & 2 & 0 & -1 & -2 & 0 & 0 & 1 \end{array}\right].$$

La EG su tale matrice produce la forma ridotta

$$\left[\begin{array}{ccccc|ccc} 1 & -2 & -1 & 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & -\frac{1}{2} & 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 & 0 & 1 & -2 & -1 & -2 \end{array}\right].$$

Con facili calcoli si vede che il sistema $\mathbf{Ax} = \mathbf{e}_1$ ha le infinite soluzioni dipendenti dai parametri h_1, k_1:

$$x_5 = -2, \quad x_4 = h_1, \quad x_3 = -1 - h_1, \quad x_2 = k_1, \quad x_1 = 4 - h_1 + 2k_1.$$

Analogamente, il sistema $\mathbf{Ax} = \mathbf{e}_2$ ha le infinite soluzioni dipendenti dai parametri h_2, k_2:

$$x_5 = -1, \quad x_4 = h_2, \quad x_3 = -h_2, \quad x_2 = k_2, \quad x_1 = 2 - h_2 + 2k_2.$$

Infine, il sistema $\mathbf{Ax} = \mathbf{e}_3$ ha le infinite soluzioni dipendenti dai parametri h_3, k_3:

$$x_5 = -2, \quad x_4 = h_3, \quad x_3 = -1 - h_3, \quad x_2 = k_3, \quad x_1 = 3 - h_3 + 2k_3.$$

In definitiva, le infinite inverse destre della matrice $\mathbf{A}$ sono tutte e sole le matrici dipendenti da 6 parametri:

$$\begin{bmatrix} 4 - h_1 + 2k_1 & 2 - h_2 + 2k_2 & 3 - h_3 + 2k_3 \\ k_1 & k_2 & k_3 \\ -1 - h_1 & -h_2 & -1 - h_3 \\ h_1 & h_2 & h_3 \\ -2 & -1 & -2 \end{bmatrix}.$$

□

Resta infine da esaminare come si trovano le inverse sinistre di una matrice $m \times n$ $\mathbf{A}$ di rango n, con $n > m$. Basta per ciò osservare che una matrice $\mathbf{L}$ è inversa sinistra di $\mathbf{A}$ se e solo se la matrice $\mathbf{L}^T$, trasposta di $\mathbf{L}$, è inversa destra della matrice $\mathbf{A}^T$. Perciò si determinano le inverse destre di $\mathbf{A}^T$ col procedimento sopra descritto e poi le si traspone, ottenendo tutte e sole le inverse sinistre di $\mathbf{A}$.

6. Matrici elementari e decomposizione *LU*

Scopo di questo Paragrafo è mostrare come la EG su di una matrice $\mathbf{A}$ produce una fattorizzazione della matrice stessa del tipo $\mathbf{A} = \mathbf{LU}$, dove la matrice $\mathbf{U}$ è una forma ridotta di $\mathbf{A}$, mentre la matrice $\mathbf{L}$ è una matrice triangolare inferiore invertibile, qualora non siano intervenuti scambi di righe. In presenza di scambi di righe questa fattorizzazione si ricava non per $\mathbf{A}$, ma per $\mathbf{PA}$, dove $\mathbf{P}$ è una opportuna matrice di permutazione (la cui definizione sarà data tra poco). La fattorizzazione prodotta si chiama *decomposizione LU* della matrice $\mathbf{A}$ (o di $\mathbf{PA}$).

Tale decomposizione di $\mathbf{A}$ deriva dal fatto che ogni singola operazione elementare che si esegue nel corso della EG corrisponde alla pre-moltiplicazione per una opportuna matrice invertibile; queste matrici si chiamano appunto *matrici elementari*. Cominciamo pertanto col presentare queste matrici, che sono di tre tipi diversi.

Matrici elementari $\mathbf{E}_{ij}(\alpha)$

Queste matrici corrispondono all'operazione elementare più importante della EG, che consiste nel sommare una riga con un multiplo non nullo di una riga che le sta sopra; è questa operazione che permette di far diventare 0 i coefficienti sotto ai pivot. Esse sono matrici quadrate, definite a partire da uno scalare $\alpha \neq 0$ e da una coppia di indici distinti $i \neq j$. Una matrice elementare $m \times m$ $\mathbf{E}_{ij}(\alpha)$ differisce dalla matrice identità $\mathbf{I}_m$ solo nel coefficiente di posto (i, j), dove anziché 0 compare lo scalare α. Conviene scrivere la matrice $\mathbf{E}_{ij}(\alpha)$ a blocchi riga e blocchi colonna:

$$\mathbf{E}_{ij}(\alpha) = \begin{bmatrix} \mathbf{e}_1^T \\ \mathbf{e}_2^T \\ \vdots \\ \mathbf{e}_i^T + \alpha\mathbf{e}_j^T \\ \vdots \\ \mathbf{e}_m^T \end{bmatrix} = \begin{bmatrix} \mathbf{e}_1 & \mathbf{e}_2 & \dots & \mathbf{e}_j + \alpha\mathbf{e}_i & \dots & \mathbf{e}_m \end{bmatrix}$$

dove la riga $\mathbf{e}_i^T + \alpha\mathbf{e}_j^T$ compare all'i-esimo posto, mentre la colonna $\mathbf{e}_j + \alpha\mathbf{e}_i$ compare al posto j-esimo. Si noti che $\mathbf{E}_{ij}(\alpha)$ è uni-triangolare (inferiore, se $i > j$).

Matrici elementari $\mathbf{E}_{ij}$

Queste matrici corrispondono all'operazione di scambio di due righe nella EG e sono chiamate *matrici di trasposizione* (o *di scambio*). Sono matrici quadrate definite a partire da una coppia (i, j) di indici distinti, che indicano le due righe che vengono scambiate. Una matrice elementare $m \times m$ di questo tipo differisce dalla matrice identità $\mathbf{I}_m$ per il fatto che sono scambiate tra di loro in $\mathbf{I}_m$ la riga i-esima e la riga j-esima o, equivalentemente, la colonna i-esima e la colonna j-esima. Si noti che tali matrici non sono matrici triangolari.

Matrici elementari $\mathbf{E}_i(\alpha)$

Queste matrici corrispondono all'operazione elementare di moltiplicazione della riga i-esima per lo scalare non nullo α. Sono matrici diagonali (già incontrate nel Paragrafo 1), che hanno sulla diagonale tutti 1 tranne che nel posto i-esimo, dove compare il coefficiente $\alpha \neq 0$.

Esempio 6.1. Esempi di matrici elementari dei tre tipi descritti nel caso di dimensione 3 sono:

$$\mathbf{E}_{31}(-1) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 0 & 1 \end{bmatrix}, \qquad \mathbf{E}_{13} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \qquad \mathbf{E}_2(5) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 1 \end{bmatrix}. \qquad \square$$

Diamo di seguito alcune proprietà cui soddisfano le matrici elementari.

(I) Tutte le matrici elementari sono matrici invertibili e risulta

$$\mathbf{E}_{ij}(\alpha)^{-1} = \mathbf{E}_{ij}(-\alpha); \qquad \mathbf{E}_{ij}^{-1} = \mathbf{E}_{ij}; \qquad \mathbf{E}_i(\alpha)^{-1} = \mathbf{E}_i(\alpha^{-1}).$$

Verifichiamo la prima uguaglianza:

$$\mathbf{E}_{ij}(\alpha)\mathbf{E}_{ij}(-\alpha) = \begin{bmatrix} \mathbf{e}_1^T \\ \mathbf{e}_2^T \\ \dots \\ \mathbf{e}_i^T + \alpha\mathbf{e}_j^T \\ \dots \\ \mathbf{e}_m^T \end{bmatrix} [\mathbf{e}_1\ \mathbf{e}_2\ \dots\ \mathbf{e}_j - \alpha\mathbf{e}_i\ \dots\ \mathbf{e}_m]$$

dove la riga $\mathbf{e}_i^T + \alpha\mathbf{e}_j^T$ compare all'i-esimo posto, mentre la colonna $\mathbf{e}_j - \alpha\mathbf{e}_i$ compare al posto j-esimo. Vogliamo provare che questo prodotto coincide con $\mathbf{I}_m$. Tenuto conto che $\mathbf{e}_i^T\mathbf{e}_i = 1$ e $\mathbf{e}_i^T\mathbf{e}_j = 0$ se $i \neq j$, si vede che il coefficiente del prodotto di posto (i, j) risulta uguale a

$$(\mathbf{e}_i^T + \alpha\mathbf{e}_j^T)(\mathbf{e}_j - \alpha\mathbf{e}_i) = -\alpha + \alpha = 0.$$

La verifica per gli altri coefficienti è immediata.

Le verifiche della seconda e terza uguaglianza sono facili esercizi lasciati al lettore.

(II) Per le trasposte delle matrici elementari si ha:

$$\mathbf{E}_{ij}(\alpha)^T = \mathbf{E}_{ji}(\alpha); \quad \mathbf{E}_{ij}^T = \mathbf{E}_{ij}; \quad \mathbf{E}_i(\alpha)^T = \mathbf{E}_i(\alpha).$$

Le verifiche sono immediate.

(III) Un prodotto di matrici elementari del tipo $\mathbf{E}_{ij}(\alpha)$ con $i > j$ è una matrice uni-triangolare inferiore.

Segue dal fatto che, se $i > j$, ogni matrice $\mathbf{E}_{ij}(\alpha)$ è una matrice uni-triangolare inferiore, e dall'Esempio 1.7.

(IV) Un prodotto di matrici elementari del tipo $\mathbf{E}_{ij}$ è una matrice che si ottiene dalla matrice identità permutandone le righe (o le colonne) in modo opportuno.

La dimostrazione è immediata conseguenza della successiva Proposizione 6.3 (b) (o della Proposizione 6.5 (b)).

Le matrici considerate nel precedente punto (IV), cioè le matrici che si ottengono moltiplicando tra di loro un certo numero di matrici di trasposizione, sono chiamate *matrici di permutazione*. Esse sono invertibili (in quanto prodotto di matrici invertibili) e sono caratterizzate dalla proprietà di avere in ogni riga e in ogni colonna tutti gli elementi nulli, tranne uno che è uguale a 1.

Esempio 6.2. Le permutazioni di n oggetti sono $n!$. Perciò esistono $3! = 6$ matrici di permutazione 3×3 distinte, che sono

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

$$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}. \qquad \square$$

Vogliamo ora esaminare quale è il risultato della pre-moltiplicazione per una matrice elementare su di una arbitraria matrice. L'Esempio 1.8 ci dice cosa accade pre-moltiplicando la matrice $\mathbf{A}$ per una matrice del tipo $\mathbf{E}_i(\alpha)$: poiché $\mathbf{E}_i(\alpha)$ è una matrice diagonale, $\mathbf{E}_i(\alpha)\mathbf{A}$ coincide con $\mathbf{A}$ tranne che per la i-esima riga, che si ottiene dalla i-esima riga di $\mathbf{A}$ moltiplicandola per α. Se per esempio nella i-esima riga di $\mathbf{A}$ c'è un certo pivot $d_i \neq 0$, pre-moltiplicando $\mathbf{A}$ per $\mathbf{E}_i(d_i^{-1})$ si rende quel pivot uguale a 1. Ciò costituisce il punto (c) della seguente Proposizione 6.3; ciò che accade pre-moltiplicando per una matrice elementare degli altri due tipi è descritto nei punti (a) e (b).

Proposizione 6.3. *Sia* $\mathbf{A}$ *una matrice* $m \times n$.

(a) *La pre-moltiplicazione di* $\mathbf{A}$ *per la matrice* $m \times m$ $\mathbf{E}_{ij}(\alpha)$ *modifica la sola riga* i*-esima di* $\mathbf{A}$*, che diventa uguale alla somma della riga* i*-esima con la riga* j*-esima moltiplicata per* α.

(b) *La pre-moltiplicazione di* $\mathbf{A}$ *per la matrice* $m \times m$ $\mathbf{E}_{ij}$ *scambia tra di loro la riga* i*-esima e la riga* j*-esima di* $\mathbf{A}$ *e lascia invariate le altre righe.*

(c) *La pre-moltiplicazione di* $\mathbf{A}$ *per la matrice* $m \times m$ $\mathbf{E}_i(\alpha)$ *moltiplica la riga* i*-esima di* $\mathbf{A}$ *per* α *e lascia invariate le altre righe.*

Dimostrazione. (a) Eseguiamo il prodotto $\mathbf{E}_{ij}(\alpha)\mathbf{A}$ decomponendo $\mathbf{E}_{ij}(\alpha)$ in blocchi riga:

$$\mathbf{E}_{ij}(\alpha)\mathbf{A} = \begin{bmatrix} \mathbf{e}_1^T \\ \mathbf{e}_2^T \\ \vdots \\ \alpha\mathbf{e}_j^T + \mathbf{e}_i^T \\ \vdots \\ \mathbf{e}_m^T \end{bmatrix} \mathbf{A} = \begin{bmatrix} \mathbf{e}_1^T\mathbf{A} \\ \mathbf{e}_2^T\mathbf{A} \\ \vdots \\ (\alpha\mathbf{e}_j^T + \mathbf{e}_i^T)\mathbf{A} \\ \vdots \\ \mathbf{e}_m^T\mathbf{A} \end{bmatrix}.$$

L'asserto segue subito non appena si ricordi che nella Proposizione 2.13 (b) si è visto che $\mathbf{e}_i^T\mathbf{A}$ coincide con la i-esima riga di $\mathbf{A}$.

(b) Analoga alla precedente, tenendo conto che la i-esima riga di $\mathbf{E}_{ij}$ coincide con $\mathbf{e}_j^T$ e la j-esima riga coincide con $\mathbf{e}_i^T$.

(c) Visto sopra. □

Osservazione 6.4. Possiamo dare ora la dimostrazione del Lemma 4.5, cioè del fatto che, data una matrice $\mathbf{A}$, esiste una matrice invertibile $\mathbf{E}$ tale che

$$\mathbf{EA} = \begin{bmatrix} a & \mathbf{x}^T \\ \mathbf{0} & \mathbf{X} \end{bmatrix}.$$

Se la prima colonna di $\mathbf{A}$ è nulla, si ponga $\mathbf{E} = \mathbf{I}$, altrimenti $\mathbf{E}$ non è altro che il prodotto delle matrici elementari usate per mettere 0 sotto al primo pivot a.

Per quanto riguarda la post-moltiplicazione di una matrice $\mathbf{A}$ per matrici elementari, vale un risultato analogo alla Proposizione 6.3, che riguarda non più le righe, ma le colonne di $\mathbf{A}$. La sua dimostrazione è analoga a quella della Proposizione 6.3, usando la Proposizione 2.13 (a), oppure si può ricavare passando alle matrici trasposte, ed è lasciata come esercizio.

Proposizione 6.5. *Sia* $\mathbf{A}$ *una matrice* $m \times n$.

(a) *La post-moltiplicazione di* $\mathbf{A}$ *per la matrice* $n \times n$ $\mathbf{E}_{ij}(\alpha)$ *modifica la sola colonna* j*-esima di* $\mathbf{A}$*, che diventa uguale alla somma della colonna* j*-esima con la colonna* i*-esima moltiplicata per* α.

(b) *La post-moltiplicazione di* $\mathbf{A}$ *per la matrice* $n \times n$ $\mathbf{E}_{ij}$ *scambia tra di loro la colonna* i*-esima e la colonna* j*-esima di* $\mathbf{A}$ *e lascia invariate le altre colonne.*

(c) *La post-moltiplicazione di* $\mathbf{A}$ *per la matrice* $n \times n$ $\mathbf{E}_i(\alpha)$ *moltiplica la colonna* i*-esima di* $\mathbf{A}$ *per* α *e lascia invariate le altre colonne.* □

La Proposizione 6.3 consente di tradurre in fattorizzazione matriciale la EG eseguita su una matrice.

Teorema 6.6. *Sia* $\mathbf{A}$ *una matrice* $m \times n$*. La EG su* $\mathbf{A}$*, qualora non necessiti di scambi di righe, produce una decomposizione* $\mathbf{A} = \mathbf{LU}$*, dove* $\mathbf{U}$ *è una forma ridotta di* $\mathbf{A}$ *ed* $\mathbf{L}$ *è una matrice triangolare inferiore invertibile.*

Dimostrazione. La EG presentata nel Paragrafo 4, qualora non siano necessari scambi di righe, consiste nell'applicare successivamente un certo numero di operazioni elementari corrispondenti alla pre-moltiplicazione per matrici elementari di tipo $\mathbf{E}_{ij}(\alpha)$ e di tipo $\mathbf{E}_i(\alpha)$ per scalari $\alpha \neq 0$. Se denotiamo con $\mathbf{E}_1, \mathbf{E}_2, \dots, \mathbf{E}_r$ tali matrici elementari, nell'ordine con cui vengono applicate, risulterà

$$\mathbf{E}_r \cdot \dots \cdot \mathbf{E}_2 \cdot \mathbf{E}_1 \cdot \mathbf{A} = \mathbf{U}$$

dove **U** è una forma ridotta di **A**; si noti che, poiché le matrici elementari operano a sinistra di **A**, l'ordine di scrittura è inverso di quello con cui agiscono. Sia

$$\mathbf{E} = \mathbf{E}_r \cdot \dots \cdot \mathbf{E}_2 \cdot \mathbf{E}_1$$

il prodotto delle matrici elementari usate. La matrice **E**, in quanto prodotto di matrici triangolari inferiori invertibili, è triangolare inferiore invertibile. Poniamo $\mathbf{L} = \mathbf{E}^{-1}$; tale matrice è ancora triangolare inferiore, per l'Esempio 4.16, e risulta $\mathbf{A} = \mathbf{L}\mathbf{U}$, come si voleva provare. □

Vediamo su di un esempio già usato come avviene la fattorizzazione di una matrice tramite la EG.

Esempio 6.7. Riprendiamo il sistema lineare esaminato nell'Esempio 3.2, di cui consideriamo solo la matrice dei coefficienti (e non quella aumentata):

$$\mathbf{B} = \begin{bmatrix} 2 & 6 & 3 & 2 \\ 1 & -2 & 1/2 & 9/4 \\ -1 & 1 & -1/2 & -1 \end{bmatrix}.$$

Le operazioni elementari applicate in successione a partire dalla matrice **B** (si veda l'Esempio 3.1) consistevano nel:

- moltiplicare la prima riga per $1/2$;
- sommare alla seconda riga la prima moltiplicata per -1;
- sommare alla terza riga la prima moltiplicata per 1;
- moltiplicare la seconda riga per $-1/5$;
- sommare alla terza riga la seconda moltiplicata per -4;
- moltiplicare la terza riga per 5.

A tali operazioni corrispondono ordinatamente le pre-moltiplicazioni per le matrici elementari

$$\mathbf{E}_1 = \mathbf{E}_1(1/2), \quad \mathbf{E}_2 = \mathbf{E}_{21}(-1), \quad \mathbf{E}_3 = \mathbf{E}_{31}(1),$$
$$\mathbf{E}_4 = \mathbf{E}_2(-1/5), \quad \mathbf{E}_5 = \mathbf{E}_{32}(-4), \quad \mathbf{E}_6 = \mathbf{E}_3(5).$$

La forma ridotta cui si perviene al termine della EG nell'Esempio 3.2 (denotata con **V**) è la seguente:

$$\mathbf{V} = \begin{bmatrix} 1 & 3 & 3/2 & 1 \\ 0 & 1 & 1/5 & -1/4 \\ 0 & 0 & 1 & 5 \end{bmatrix}.$$

Un calcolo diretto mostra che

$$\begin{aligned}\mathbf{E} &= \mathbf{E}_6\mathbf{E}_5\mathbf{E}_4\mathbf{E}_3\mathbf{E}_2\mathbf{E}_1\\ &= \begin{bmatrix}1&0&0\\0&1&0\\0&0&5\end{bmatrix}\begin{bmatrix}1&0&0\\0&1&0\\0&-4&1\end{bmatrix}\begin{bmatrix}1&0&0\\0&-1/5&0\\0&0&1\end{bmatrix}\begin{bmatrix}1&0&0\\0&1&0\\1&0&1\end{bmatrix}\begin{bmatrix}1&0&0\\-1&1&0\\0&0&1\end{bmatrix}\begin{bmatrix}1/2&0&0\\0&1&0\\0&0&1\end{bmatrix}\\ &= \begin{bmatrix}1/2&0&0\\1/10&-1/5&0\\1/2&4&5\end{bmatrix}.\end{aligned}$$

Pertanto la matrice **E**, una volta invertita, dà la matrice triangolare inferiore **L** che fattorizza **A**; il calcolo con l'algoritmo di Gauss-Jordan della matrice $\mathbf{L} = \mathbf{E}^{-1}$ porge

$$\mathbf{L} = \begin{bmatrix}2&0&0\\1&-5&0\\-1&4&1/5\end{bmatrix}.$$

Si osservi che

$$\begin{aligned}\mathbf{L} &= \mathbf{E}_1^{-1}\mathbf{E}_2^{-1}\mathbf{E}_3^{-1}\mathbf{E}_4^{-1}\mathbf{E}_5^{-1}\mathbf{E}_6^{-1}\\ &= \mathbf{E}_1(2)\mathbf{E}_{21}(1)\mathbf{E}_{31}(-1)\mathbf{E}_2(-5)\mathbf{E}_{32}(4)\mathbf{E}_3(1/5),\end{aligned}$$

dove i coefficienti non nulli che compaiono ordinatamente dall'alto verso il basso nella prima colonna di **L**, poi nella seconda colonna e infine nella terza, coincidono con gli scalari che compaiono ordinatamente tra parentesi (da sinistra verso destra) nelle matrici elementari il cui prodotto dà appunto la matrice **L**. Il lettore verifichi che $\mathbf{A} = \mathbf{LU}$. □

A questo punto sorgono naturali due domande. Si possono descrivere facilmente gli elementi della matrice **L**, a partire dalle operazioni elementari eseguite? E cosa accade se nella EG necessitano permutazioni?

Cominciamo con l'esaminare la seconda domanda. Supponiamo che nel corso della EG sulla matrice **A** compaiano, alternate a operazioni elementari corrispondenti a matrici elementari del tipo $\mathbf{E}_{ij}(\alpha)$ ed $\mathbf{E}_i(\alpha)$, anche un certo numero di scambi di righe; supponiamo inoltre che a tali scambi di righe corrispondano ordinatamente le matrici di trasposizione $\mathbf{E}_{i_1 j_1}, \mathbf{E}_{i_2 j_2}, \dots, \mathbf{E}_{i_k j_k}$. Denotiamo con **P** la matrice di permutazione ottenuta facendo il prodotto di queste matrici di trasposizione nell'ordine con cui operano a sinistra su **A**, quindi

$$\mathbf{P} = \mathbf{E}_{i_k j_k} \cdot \ldots \mathbf{E}_{i_2 j_2} \cdot \mathbf{E}_{i_1 j_1}.$$

Osserviamo che una matrice di permutazione, in quanto prodotto di matrici invertibili, è invertibile. In queste notazioni vale la seguente proposizione.

Proposizione 6.8. *La EG sulla matrice* **PA** *non necessita di scambi di righe. Ovvero, se si eseguono subito su* **A** *ordinatamente tutti gli scambi di righe che si usano nel corso della EG e se si procede poi sulla matrice ottenuta con la EG, non sono più necessari scambi di righe.*

Dimostrazione. Siano $\mathbf{E}_{i_1 j_1}, \mathbf{E}_{i_2 j_2}, \dots, \mathbf{E}_{i_k j_k}$ le matrici di scambio che intervengono ordinatamente nella EG; possiamo supporre $i_h < j_h$ per ogni $h \le k$. Si rende necessario far operare $\mathbf{E}_{i_1 j_1}$ perché dopo avere sistemato le colonne fino alla $(i_1 - 1)$-esima inclusa, al posto (i_1, i_1) troviamo lo 0 e vogliamo sostituirlo con l'elemento di posto (i_1, j_1). Prima di $\mathbf{E}_{i_1 j_1}$ hanno operato matrici del tipo $\mathbf{E}_{rs}(\alpha)$ e $\mathbf{E}_r(\alpha)$ con indice di colonna $s < i_1$. È facile verificare (si veda l'Esercizio 1.50) che, se $s < i < j$, risulta

$$\mathbf{E}_{ij}\mathbf{E}_{is}(\alpha) = \mathbf{E}_{js}(\alpha)\mathbf{E}_{ij}, \qquad \mathbf{E}_{ij}\mathbf{E}_{js}(\alpha) = \mathbf{E}_{is}(\alpha)\mathbf{E}_{ij},$$
$$\mathbf{E}_{ij}\mathbf{E}_{i}(\alpha) = \mathbf{E}_{j}(\alpha)\mathbf{E}_{ij},$$

mentre se $r \neq i, j$, allora

$$\mathbf{E}_{ij}\mathbf{E}_{rs}(\alpha) = \mathbf{E}_{rs}(\alpha)\mathbf{E}_{ij}, \qquad \mathbf{E}_{ij}\mathbf{E}_{r}(\alpha) = \mathbf{E}_{r}(\alpha)\mathbf{E}_{ij}.$$

Pertanto si può permutare $\mathbf{E}_{i_1 j_1}$ con tutte le matrici elementari che hanno operato prima di essa, alterando possibilmente gli indici di riga di tali matrici ma non gli indici delle colonne, che restano sempre minori di i_1. Eseguiamo la stessa procedura sulla matrice $\mathbf{E}_{i_2 j_2}$. Permutiamola quindi con tutte le matrici di tipo $\mathbf{E}_{rs}(\alpha)$ e $\mathbf{E}_r(\alpha)$ che operano prima di essa, di cui quelle che precedevano $\mathbf{E}_{i_1 j_1}$ sono state modificate. Ma tutte tali matrici hanno indici di colonna minori di i_2 e tale proprietà si conserva dopo le permutazioni per le formule viste sopra. Continuando in questo modo, si portano a operare per prime sulla matrice $\mathbf{A}$ ordinatamente le matrici $\mathbf{E}_{i_1 j_1}, \mathbf{E}_{i_2 j_2}, \dots, \mathbf{E}_{i_k j_k}$, il cui prodotto nell'ordine rovesciato con cui sono pre-moltiplicate ad $\mathbf{A}$ è $\mathbf{P} = \mathbf{E}_{i_k j_k} \cdot \ldots \mathbf{E}_{i_2 j_2} \cdot \mathbf{E}_{i_1 j_1}$. Le matrici che ora pre-moltiplicano $\mathbf{PA}$, il cui risultato è la forma ridotta $\mathbf{U}$, sono matrici elementari del tipo $\mathbf{E}_{rs}(\alpha)$ con $r > s$ e $\mathbf{E}_r(\alpha)$, da cui l'asserto. □

Dalla Proposizione 6.8 si può trarre immediatamente il seguente risultato.

Teorema 6.9. *Sia* $\mathbf{A}$ *una matrice* $m \times n$. *Qualora la EG su* $\mathbf{A}$ *necessiti di scambi di righe, si possono eseguire subito tali scambi su* $\mathbf{A}$ *ottenendo la nuova matrice* $\mathbf{PA}$, *ove* $\mathbf{P}$ *denota una matrice di permutazione. La EG su* $\mathbf{PA}$ *produce una fattorizzazione* $\mathbf{PA} = \mathbf{LU}$, *dove* $\mathbf{U}$ *è una forma ridotta di* $\mathbf{A}$ *ed* $\mathbf{L}$ *è una matrice triangolare inferiore invertibile. Pertanto* $\mathbf{A} = \mathbf{P}^{-1}\mathbf{LU}$. □

Si noti che nel Teorema 6.9 la matrice $\mathbf{P}^{-1}\mathbf{L}$ è una matrice invertibile e che

$$\mathbf{P} = \mathbf{E}_{i_k j_k} \cdot \ldots \mathbf{E}_{i_2 j_2} \cdot \mathbf{E}_{i_1 j_1} \implies \mathbf{P}^{-1} = \mathbf{E}_{i_1 j_1}\mathbf{E}_{i_2 j_2} \cdot \ldots \cdot \mathbf{E}_{i_k j_k} = \mathbf{P}^T$$

in virtù del fatto che $\mathbf{E}_{ij}^{-1} = \mathbf{E}_{ij} = \mathbf{E}_{ij}^T$ per ogni matrice di scambio $\mathbf{E}_{ij}$ (si veda l'Esercizio 1.46). Il Teorema 6.9 fornisce inoltre la dimostrazione del Lemma 4.5, (ii).

Forniamo un esempio della situazione descritta nel Teorema 6.9.

Esempio 6.10. Consideriamo la matrice

$$\mathbf{A} = \begin{bmatrix} 1 & 2 & 2 & 1 & 1 \\ 1 & 2 & 2 & 2 & 2 \\ 2 & 5 & -1 & 3 & 4 \\ 1 & 2 & 5 & 1 & 2 \end{bmatrix}.$$

Sommando alla seconda riga l'opposto della prima, alla terza riga la prima moltiplicata per -2, e alla quarta riga l'opposto della prima, si ricava la matrice

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

Eseguiamo prima lo scambio di seconda e terza riga, poi nella matrice ottenuta lo scambio tra terza e quarta riga, ottenendo la matrice

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

dalla quale, moltiplicando la terza riga per $1/3$, si ottiene la forma ridotta

$$\mathbf{U} = \begin{bmatrix} 1 & 2 & 2 & 1 & 1 \\ 0 & 1 & -5 & 1 & 2 \\ 0 & 0 & 1 & 0 & 1/3 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

Le operazioni che sono state eseguite corrispondono alla pre-moltiplicazione di $\mathbf{A}$ per opportune matrici elementari; più precisamente, la matrice ottenuta alla fine è la matrice

$$\mathbf{E}_3(1/3)\mathbf{E}_{34}\mathbf{E}_{23}\mathbf{E}_{41}(-1)\mathbf{E}_{31}(-2)\mathbf{E}_{21}(-1)\mathbf{A}.$$

Il Teorema 6.9 ci dice che pre-moltiplicando $\mathbf{A}$ per la matrice di permutazione

$$\mathbf{P} = \mathbf{E}_{34}\mathbf{E}_{23} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

la nuova matrice

$$\mathbf{PA} = \begin{bmatrix} 1 & 2 & 2 & 1 & 1 \\ 2 & 5 & -1 & 3 & 4 \\ 1 & 2 & 5 & 1 & 2 \\ 1 & 2 & 2 & 2 & 2 \end{bmatrix}$$

non avrà bisogno, nell'eseguire la EG, di alcuno scambio di righe. In effetti, la EG su $\mathbf{PA}$ porge

$$\mathbf{E}_3(1/3)\mathbf{E}_{41}(-1)\mathbf{E}_{31}(-1)\mathbf{E}_{21}(-2)\mathbf{PA} = \mathbf{U}.$$

Quindi si ha la decomposizione

$$\mathbf{PA} = \mathbf{LU}$$

dove $\mathbf{L}$ è la matrice triangolare inferiore data da

$$\mathbf{L} = \mathbf{E}_{21}(2)\mathbf{E}_{31}(1)\mathbf{E}_{41}(1)\mathbf{E}_{3}(3) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 \\ 1 & 0 & 3 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}.$$

Ne consegue che per $\mathbf{A}$ si ha la seguente fattorizzazione:

$$\begin{aligned} \mathbf{A} &= \mathbf{P}^{-1}\mathbf{L}\mathbf{U} \\ &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 \\ 1 & 0 & 3 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 2 & 1 & 1 \\ 0 & 1 & -5 & 1 & 2 \\ 0 & 0 & 1 & 0 & 1/3 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 2 & 1 & 0 & 0 \\ 1 & 0 & 3 & 0 \end{bmatrix} \begin{bmatrix} 1 & 2 & 2 & 1 & 1 \\ 0 & 1 & -5 & 1 & 2 \\ 0 & 0 & 1 & 0 & 1/3 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}. \end{aligned}$$

Si noti che il primo fattore nell'ultimo prodotto non è una matrice triangolare inferiore; resta però una matrice invertibile. □

Ritorniamo ora alla prima domanda posta in precedenza: è possibile determinare facilmente i coefficienti della matrice triangolare inferiore $\mathbf{L}$ che fattorizza la matrice $\mathbf{A}$? In virtù del Teorema 6.9, ci limiteremo a considerare il caso in cui non necessitano scambi di righe; se infatti intervengono scambi, fattorizzeremo la matrice $\mathbf{PA}$ per la quale la EG non necessita di scambi di righe.

La risposta alla precedente domanda è positiva, come suggerisce l'osservazione alla fine dell'Esempio 6.7; essa dipende dal seguente lemma tecnico. Per renderne più scorrevole l'enunciato, conveniamo di denotare con $\mathbf{E}_{ii}(\alpha)$ la matrice elementare $\mathbf{E}_{i}(\alpha)$, per cui tra le matrici elementari $\mathbf{E}_{ij}(\alpha)$ considerate nel lemma potrà succedere, oltre che $i > j$, anche che $i = j$. Introduciamo inoltre la seguente definizione: diremo che la coppia ordinata di numeri interi positivi (i_1, j_1) è minore della coppia (i_2, j_2) nell'ordine *anti-lessicografico* se $j_1 < j_2$, oppure, nel caso in cui $j_1 = j_2$, se $i_1 < i_2$.

Lemma 6.11. *Se la matrice triangolare inferiore* $\mathbf{L} = [l_{ij}]$ *è prodotto di matrici elementari triangolari inferiori*

$$\mathbf{L} = \mathbf{E}_{i_1 j_1}(\alpha_1)\mathbf{E}_{i_2 j_2}(\alpha_2)\ldots\mathbf{E}_{i_r j_r}(\alpha_r)$$

con gli scalari $\alpha_h \neq 0$, *e le coppie ordinate di indici* (i_h, j_h) $(h \leq r)$ *si susseguono in modo crescente nell'ordine anti-lessicografico, allora* $l_{i_h j_h} = \alpha_h$ *per ogni* $h \leq r$*; i restanti coefficienti sulla diagonale di* $\mathbf{L}$ *sono uguali a* 1 *e i restanti coefficienti al di sotto della diagonale sono uguali a* 0.

Dimostrazione. Facciamo induzione su r. Per $r = 1$, la matrice $\mathbf{L} = \mathbf{E}_{i_1 j_1}(\alpha_1)$ ha l'elemento $l_{i_1 j_1}$ coincidente con α_1 e per il resto coincide con la matrice identica, come richiesto. Sia $r > 1$ e l'asserto vero per $s = r-1$. Allora $\mathbf{L}_s = \mathbf{E}_{i_1 j_1}(\alpha_1)\mathbf{E}_{i_2 j_2}(\alpha_2)\dots\mathbf{E}_{i_s j_s}(\alpha_s)$ soddisfa a quanto richiesto. Eseguendo il prodotto

$$\mathbf{L}_s\mathbf{E}_{i_r j_r}(\alpha_r)$$

si modifica $\mathbf{L}_s$ perché si somma alla sua colonna j_r-esima la colonna i_r-esima moltiplicata per α_r. Ma se $j_r < i_r$, ciò equivale a sostituire il coefficiente nullo di posto (i_r, j_r) di $\mathbf{L}_s$ con α_r; se invece $j_r = i_r$, ciò equivale a sostituire 1 al posto (i_r, i_r) di $\mathbf{L}_s$ con α_r, da cui l'asserto. □

Esempio 6.12. Applichiamo il Lemma 6.11 al seguente prodotto di matrici elementari 4×4, che si trovano nell'ordine anti-lessicografico crescente richiesto nel lemma:

$$\begin{aligned}
&\mathbf{E}_{21}(-3)\mathbf{E}_{41}(2)\mathbf{E}_{22}(7)\mathbf{E}_{32}(5)\mathbf{E}_{42}(-7)\mathbf{E}_{33}(3)\mathbf{E}_{43}(4)\mathbf{E}_{44}(5) = \\
&= \begin{bmatrix} 1 & 0 & 0 & 0 \\ -3 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 2 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 7 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 5 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \cdot \\
&\cdot \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -7 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 4 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 5 \end{bmatrix} \\
&= \begin{bmatrix} 1 & 0 & 0 & 0 \\ -3 & 7 & 0 & 0 \\ 0 & 5 & 3 & 0 \\ 2 & -7 & 4 & 5 \end{bmatrix}.
\end{aligned}$$

□

Dal Lemma 6.11 ricaviamo la seguente conseguenza.

Proposizione 6.13. *Sia* $\mathbf{A}$ *una matrice per cui la EG non necessita di scambi di righe. La matrice triangolare inferiore invertibile* $\mathbf{L}$ *ottenuta nel Teorema 6.6 ha come coefficiente di posto* (i, j)*:*

(a) *lo scalare* $-\alpha$ *se* $i > j$*, dove* $\mathbf{E}_{ij}(\alpha)$ *è la matrice elementare usata per porre* 0 *al posto* (i, j)*, oppure* 0 *se non si è eseguita alcuna operazione elementare;*

(b) *lo scalare* α^{-1} *se* $i = j$*, dove* $\mathbf{E}_i(\alpha)$ *è la matrice elementare usata per porre* 1 *al posto* (i, i)*, oppure* 1 *se non si è eseguita alcuna operazione elementare.*

Dimostrazione. Si osservi che l'ordine con cui si eseguono le operazioni elementari nella EG fa sì che le matrici elementari che pre-moltiplicano $\mathbf{A}$ si susseguono (da sinistra verso destra) in ordine inverso rispetto a quello considerato nel Lemma 6.11. Ma la matrice $\mathbf{E}$ prodotto di tali matrici elementari va invertita (si passa da $\mathbf{EA} = \mathbf{U}$ ad $\mathbf{A} = \mathbf{E}^{-1}\mathbf{U}$). Quindi l'ordine delle matrici elementari in $\mathbf{E}^{-1} = \mathbf{L}$ viene esso pure invertito e coincide con quello del Lemma 6.11, mentre nel passaggio all'inversa i coefficienti α delle matrici $\mathbf{E}_{ij}(\alpha)$ cambiano di segno e quelli delle matrici $\mathbf{E}_i(\alpha)$ vengono invertiti, per la proprietà (I). Il Lemma 6.11 assicura allora l'asserto. □

Il lettore può verificare nell'Esempio 6.10 come la matrice $\mathbf{L}$ nella decomposizione $\mathbf{PA} = \mathbf{LU}$ si ottenga proprio nel modo descritto nella Proposizione 6.13, a partire dalle quattro matrici elementari usate per ottenere tale decomposizione.

La decomposizione LU del Teorema 6.6 non è simmetrica, nel senso che, mentre i primi elementi non nulli di ogni riga di $\mathbf{U}$ sono uguali a 1, i coefficienti l_{ii} sulla diagonale di $\mathbf{L}$ non lo sono. La cosa si rimedia nel modo seguente: si divide ogni colonna di $\mathbf{L}$ per il suo coefficiente diagonale, ottenendo la nuova matrice $\mathbf{L}_0$ che ha i primi elementi non nulli di ogni colonna uguali a 1; per l'Esempio 1.9 risulta

$$\mathbf{L} = \mathbf{L}_0\mathbf{D}$$

dove $\mathbf{D} = \mathbf{Diag}(l_{11}, \dots, l_{nn})$. Allora la decomposizione $\mathbf{A} = \mathbf{LU}$ diviene $\mathbf{A} = \mathbf{L}_0\mathbf{DU}$ che è simmetrica nel senso sopra descritto.

Esempio 6.14. La decomposizione LU della matrice $\mathbf{B}$ dell'Esempio 6.7 è la seguente

$$\mathbf{B} = \begin{bmatrix} 2 & 0 & 0 \\ 1 & -5 & 0 \\ -1 & 4 & 1/5 \end{bmatrix} \cdot \begin{bmatrix} 1 & 3 & 3/2 & 1 \\ 0 & 1 & 1/5 & -1/4 \\ 0 & 0 & 1 & 5 \end{bmatrix}.$$

La decomposizione $\mathbf{B} = \mathbf{L}_0\mathbf{DU}$ sopra descritta è allora la seguente

$$\mathbf{B} = \begin{bmatrix} 1 & 0 & 0 \\ 1/2 & 1 & 0 \\ -1/2 & -4/5 & 1 \end{bmatrix} \cdot \begin{bmatrix} 2 & 0 & 0 \\ 0 & -5 & 0 \\ 0 & 0 & 1/5 \end{bmatrix} \cdot \begin{bmatrix} 1 & 3 & 3/2 & 1 \\ 0 & 1 & 1/5 & -1/4 \\ 0 & 0 & 1 & 5 \end{bmatrix}.$$ □

Decomposizioni a rango pieno

Nel Paragrafo 3 il numero k di righe non nulle di una forma ridotta $\mathbf{U}$ della matrice $m \times n$ $\mathbf{A}$ è stato chiamato rango di $\mathbf{A}$. Abbiamo inoltre anticipato che tale numero dipende solo da $\mathbf{A}$. Se la EG su $\mathbf{A}$ non richiede scambi di righe, otteniamo, tramite il Teorema 6.6, una decomposizione $\mathbf{A} = \mathbf{LU}$, dove $\mathbf{U}$ ha $m - k$ righe nulle. Queste righe vengono moltiplicate per le ultime $m - k$ colonne della matrice $\mathbf{L}$; infatti, decomposte $\mathbf{L}$ e $\mathbf{U}$ rispettivamente in blocchi colonna e blocchi riga, si ha:

$$\begin{aligned} \mathbf{A} = \mathbf{LU} &= [\mathbf{l}_1\ \mathbf{l}_2\ \dots\ \mathbf{l}_m] \begin{bmatrix} \mathbf{u}_1^T \\ \mathbf{u}_2^T \\ \dots \\ \mathbf{u}_m^T \end{bmatrix} \\ &= \mathbf{l}_1\mathbf{u}_1^T + \dots + \mathbf{l}_k\mathbf{u}_k^T + \mathbf{l}_{k+1}\mathbf{0}^T + \dots + \mathbf{l}_m\mathbf{0}^T. \end{aligned}$$

Quindi $\mathbf{A} = \mathbf{BC}$, dove

$$\mathbf{B} = [\mathbf{l}_1\ \mathbf{l}_2\ \dots\ \mathbf{l}_k], \qquad \mathbf{C} = \begin{bmatrix} \mathbf{u}_1^T \\ \mathbf{u}_2^T \\ \dots \\ \mathbf{u}_k^T \end{bmatrix}.$$

Se invece la EG su $\mathbf{A}$ richiede scambi di righe, allora si ha la decomposizione $\mathbf{PA} = \mathbf{LU}$, con $\mathbf{P}$ opportuna matrice di permutazione, quindi $\mathbf{A} = \mathbf{P}^{-1}\mathbf{LU}$. Si ha allora, analogamente a prima, una decomposizione $\mathbf{A} = \mathbf{BC}$, dove ora $\mathbf{B}$ è la sottomatrice di $\mathbf{P}^{-1}\mathbf{L}$ formata dalle prime k colonne. Tali decomposizioni di $\mathbf{A}$ si chiamano *decomposizioni a rango pieno*, e sono caratterizzate dal fatto che il numero di colonne del primo fattore, che coincide col numero di righe del secondo fattore, è uguale al rango di $\mathbf{A}$.

Osserviamo che la decomposizione ottenuta in questo modo mostra che ogni matrice $\mathbf{A}$ soddisfa alle ipotesi della Proposizione 4.19, che assicura l'esistenza della matrice pseudo-inversa: infatti è immediato verificare che $\mathbf{B}$ ha inversa sinistra, essendo formata dalle prime k colonne di una matrice invertibile (vedi l'Esercizio 1.27), e che $\mathbf{C}$ ha inversa destra, essendo matrice in forma ridotta senza righe nulle.

Esempio 6.15. Data la matrice

$$\mathbf{A} = \begin{bmatrix} 3 & -1 & 4 \\ 2 & -2/3 & 5/3 \\ -6 & 2 & -8 \end{bmatrix}$$

la EG, non essendo necessari scambi di righe, produce:

$$\mathbf{E}_2(-1)\mathbf{E}_{31}(6)\mathbf{E}_{21}(-2)\mathbf{E}_1(1/3)\mathbf{A} = \begin{bmatrix} 1 & -1/3 & 4/3 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} = \mathbf{U}.$$

Quindi si ha la decomposizione

$$\begin{aligned} \mathbf{A} = \mathbf{LU} &= \mathbf{E}_1(3)\mathbf{E}_{21}(2)\mathbf{E}_{31}(-6)\mathbf{E}_2(-1)\mathbf{U} \\ &= \begin{bmatrix} 3 & 0 & 0 \\ 2 & -1 & 0 \\ -6 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -1/3 & 4/3 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}. \end{aligned}$$

Ne consegue che una decomposizione a rango pieno di $\mathbf{A}$ è data da

$$\mathbf{A} = \begin{bmatrix} 3 & 0 \\ 2 & -1 \\ -6 & 0 \end{bmatrix} \begin{bmatrix} 1 & -1/3 & 4/3 \\ 0 & 0 & 1 \end{bmatrix}.$$

□

Esercizi

Paragrafo 1

1.1. Sia $\mathbf{A}$ una matrice $m \times n$ e $\mathbf{D} = \mathbf{Diag}(d, d, \dots, d)$ una matrice scalare $m \times m$. Allora $\mathbf{DA} = d\mathbf{A}$. Analogamente se si postmoltiplica $\mathbf{A}$ per una matrice scalare.

1.2. Provare quanto asserito nell'Esempio 1.7.

1.3. Si trovino tutte le matrici complesse 2×2 che commutano con tutte le matrici complesse 2×2 triangolari superiori.

1.4. Si trovino due matrici complesse 2×2 non nulle $\mathbf{X}$ e $\mathbf{Y}$ tali che $\mathbf{X}^2 + \mathbf{Y}^2 = \mathbb{O}$.

1.5. Si trovino tutte le matrici reali simmetriche 2×2 $\mathbf{A}$ tali che $\mathbf{A}^2 = \mathbf{I}_2$.

1.6. Si provi che non esiste alcuna matrice complessa 2×2 $\mathbf{A}$ tale che

$$\mathbf{A}^2 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}.$$

1.7. Si trovino tutte le matrici complesse 2×2 $\mathbf{A}$ tali che $\mathbf{A}^2 = -\mathbf{I}_2$.

1.8. Siano $\mathbf{A}$ una matrice con la i-esima riga nulla e $\mathbf{B}$ una matrice a essa conforme per il prodotto a destra. Si provi che $\mathbf{AB}$ ha la i-esima riga nulla.

1.9. Sia $\mathbf{B}$ una matrice con la i-esima colonna nulla e $\mathbf{A}$ una matrice a essa conforme per il prodotto a sinistra. Si provi che $\mathbf{AB}$ ha la i-esima colonna nulla.

Paragrafo 2

1.10. Si provi che, dato un qualunque vettore complesso non nullo $\mathbf{x}$, $\mathbf{x}^H\mathbf{x}$ è un numero reale positivo.

1.11. Una matrice complessa $n \times n$ $\mathbf{U}$ si dice *unitaria* se $\mathbf{U}^H\mathbf{U} = \mathbf{I}_n = \mathbf{U}\mathbf{U}^H$. Si provi che, se $\mathbf{U}$ è unitaria ed hermitiana, allora la matrice $\mathbf{P} = \frac{1}{2}(\mathbf{I}_n - \mathbf{U})$ soddisfa alle uguaglianze $\mathbf{P} = \mathbf{P}^H$ e $\mathbf{P}^2 = \mathbf{P}$.

1.12. Sia $\mathbf{P}$ una matrice che soddisfa alle uguaglianze $\mathbf{P} = \mathbf{P}^H$ e $\mathbf{P}^2 = \mathbf{P}$. Si provi che la matrice $\mathbf{U} = \mathbf{I}_n - 2\mathbf{P}$ è unitaria ed hermitiana.

1.13. Si verifichino le proprietà (a)–(f) enunciate dopo l'Esempio 2.7.

1.14. Si verifichi che le matrici hermitiane, quelle anti-hermitiane e quelle unitarie sono matrici normali.

1.15. Trovare una matrice normale 2×2 che non è né hermitiana, né anti-hermitiana, né unitaria.

1.16. Quante sono le matrici diagonali $n \times n$ che sono contemporaneamente hermitiane e unitarie?

1.17. Data una matrice $n \times n$ $\mathbf{A} = [a_{ij}]$, si chiama *traccia* di $\mathbf{A}$ la somma dei suoi coefficienti diagonali, cioè lo scalare $\mathrm{Tr}(\mathbf{A}) = \sum_{1 \le i \le n} a_{ii}$. Si provi che, se $\mathbf{A}$ e $\mathbf{B}$ sono matrici conformi per la somma e α è uno scalare, si ha $\mathrm{Tr}(\mathbf{A}+\mathbf{B}) = \mathrm{Tr}(\mathbf{A}) + \mathrm{Tr}(\mathbf{B})$ e $\mathrm{Tr}(\alpha\mathbf{A}) = \alpha\,\mathrm{Tr}(\mathbf{A}$; se invece $\mathbf{A}$ e $\mathbf{B}$ sono matrici conformi per il prodotto, si ha $\mathrm{Tr}(\mathbf{AB}) = \mathrm{Tr}(\mathbf{BA})$.

Paragrafo 3

1.18. Sia $\mathbf{A}$ una matrice $m \times n$ di rango 1. Si provi che $\mathbf{A} = \mathbf{v}\mathbf{u}^T$, dove $\mathbf{v} \in \mathbb{C}^m$ e $\mathbf{u}^T \in \mathbb{C}_n$.

1.19. Si spieghi perché un sistema lineare con una matrice dei coefficienti $\mathbf{A}$ $m \times n$ con $m < n$ non può avere esattamente una soluzione.

1.20. Una matrice $\mathbf{A}$ si dice *equivalente per righe* alla matrice $\mathbf{B}$, e si scrive $\mathbf{A} \sim \mathbf{B}$, se $\mathbf{B}$ si ottiene da $\mathbf{A}$ con un numero finito di operazioni elementari. Si provi che

(i) $\mathbf{A} \sim \mathbf{A}$;

(ii) se $\mathbf{A} \sim \mathbf{B}$, allora $\mathbf{B} \sim \mathbf{A}$;

(iii) se $\mathbf{A} \sim \mathbf{B}$ e $\mathbf{B} \sim \mathbf{C}$, allora $\mathbf{A} \sim \mathbf{C}$.

1.21. Siano $\mathbf{A}$ una matrice $m \times n$ e $\mathbf{B}$ una matrice $n \times p$. Si considerino i due sistemi lineari

(i) $\mathbf{ABx} = \mathbf{Av}$

(ii) $\mathbf{Bx} = \mathbf{v}$.

Si provi che: ogni soluzione di (ii) è anche soluzione di (i) e che $\mathbf{x}_0$ è soluzione di (i) se e solo se $\mathbf{Bx}_0 = \mathbf{v} + \mathbf{n}$, dove $\mathbf{An} = \mathbf{0}$.

1.22. Impiegando la definizione di rango data nel Paragrafo 3, si provi che il rango di una matrice triangolare a blocchi coincide con la somma dei ranghi dei blocchi diagonali.

1.23. Caratterizzare le matrici non nulle $\mathbf{A}$ che sono divisori di zero, tali cioè che premoltiplicate o post-moltiplicate per opportune matrici non nulle danno la matrice nulla.

Paragrafo 4

1.24. Si verifichino le proprietà (a)–(c) delle matrici invertibili enunciate prima dell'Esempio 4.16.

1.25. Dimostrare quanto enunciato nell'Esempio 4.16 sulle matrici triangolari invertibili (si faccia induzione sull'ordine).

1.26. Si provi direttamente che, se la matrice $\mathbf{R}$ è una inversa destra della matrice $\mathbf{A}$ tale che $\mathbf{RA}$ è hermitiana, allora $\mathbf{R} = \mathbf{A}^H(\mathbf{AA}^H)^{-1}$ (usare il prodotto $\mathbf{RAA}^H$).

1.27. Sia $\mathbf{B}$ una sottomatrice di una matrice invertibile $n \times n$ $\mathbf{A}$, formata dalle prime k colonne di $\mathbf{A}$. Si provi che $\mathbf{B}$ ha inversa sinistra.

1.28. Si provi che una matrice $\mathbf{A}$ che ha una inversa destra simmetrica $\mathbf{R}$ è invertibile (provare che $\mathbf{RA}^T = \mathbf{I}$).

1.29. Si provi direttamente che una matrice quadrata $\mathbf{A}$ che ha una unica inversa destra $\mathbf{R}$ è invertibile (si consideri la matrice $\mathbf{RA} - \mathbf{I} + \mathbf{R}$).

1.30. Si trovino una matrice 2×2 $\mathbf{A}$ e una sua fattorizzazione $\mathbf{A} = \mathbf{BC}$ tali che $\mathbf{A}^+ \neq \mathbf{C}^+\mathbf{B}^+$.

1.31. Si verifichino le proprietà (pi$_1$)–(pi$_6$) della matrice pseudo-inversa.

1.32. Sia $\mathbf{A}$ una matrice $m \times n$ di rango n. Si provi che $\mathbf{A}^+ = \mathbf{A}^H$ se e solo se $\mathbf{AA}^H$ è una matrice idempotente, cioè coincide col suo quadrato.

1.33. Sia $\mathbf{A}$ una matrice di rango 1. Si provi che $\mathbf{A}^+ = (\mathbf{u}^H\mathbf{u})^{-1}(\mathbf{v}^H\mathbf{v})^{-1}\mathbf{A}^H$ per opportuni vettori $\mathbf{u}$ e $\mathbf{v}$.

1.34. Si provi che le due matrici $\mathbf{AA}^+$ e $\mathbf{A}^+\mathbf{A}$ sono idempotenti e che $(\mathbf{AA}^H)^+ = (\mathbf{A}^+)^H\mathbf{A}^+$.

Paragrafo 5

1.35. Trovare tutte le inverse destre $\mathbf{R}$ di una matrice $m \times n$ $\mathbf{A}$ di rango $m < n$, postmoltiplicando $\mathbf{A}$ per una matrice di permutazione $\mathbf{P}$ in modo che $\mathbf{AP}$ soddisfi alle ipotesi della Proposizione 5.3 e ricavando $\mathbf{R}$ dalle inverse destre di $\mathbf{AP}$ (si veda il Paragrafo 6 per le matrici di permutazione).

1.36. Si applichi il procedimento descritto nell'Esercizio 1.35 all'Esempio 5.5.

1.37. Calcolare con l'algoritmo di inversione di Gauss-Jordan la inversa della matrice

$$\mathbf{A} = \begin{bmatrix} a & 1 & 0 \\ 0 & b & 1 \\ 0 & 0 & c \end{bmatrix}$$

dove a, b e c sono scalari non nulli.

1.38. Si provi che una matrice con una riga o una colonna nulla non è invertibile.

1.39. Siano $\mathbf{A}$ e $\mathbf{B}$ matrici $n \times n$ e sia $\mathbf{A}$ invertibile. Si provi che applicando l'algoritmo di Gauss-Jordan alla matrice a blocchi $[\mathbf{A} \mid \mathbf{B}]$ si perviene alla matrice a blocchi $[\mathbf{I}_n \mid \mathbf{A}^{-1}\mathbf{B}]$.

Paragrafo 6

1.40. Una matrice in forma ridotta $\mathbf{S}$ di rango k si dice *in forma a scala per righe ridotta* se le k colonne dominanti coincidono con i vettori cooordinati $\mathbf{e}_1, \dots, \mathbf{e}_k$. Si provi che ogni matrice $\mathbf{A}$ si trasforma con operazioni elementari in una matrice in forma a scala per righe ridotta $\mathbf{S}$ e che $\mathbf{S} = \mathbf{EA}$, dove $\mathbf{E}$ è una matrice invertibile.

1.41. Siano $\mathbf{S}$ ed $\mathbf{S}'$ due forme a scala per righe ridotte della stessa matrice $\mathbf{A}$. Si provi che $\mathbf{S} = \mathbf{S}'$ (si provi che $\mathbf{VS} = \mathbf{S}'$, dove $\mathbf{V}$ è una matrice invertibile, e si sfrutti la forma speciale di $\mathbf{S}$ ed $\mathbf{S}'$ per provare che $\mathbf{Ve}_i = \mathbf{e}_i$ per ogni i).

1.42. Una matrice $\mathbf{A}$ è invertibile se e solo se è prodotto di matrici elementari.

1.43. Data una matrice $m \times n$ $\mathbf{A}$ di rango k, esistono matrici invertibili $\mathbf{U}$ e $\mathbf{V}$ di dimensioni rispettivamente m ed n, tali che

$$\mathbf{UAV} = \begin{bmatrix} \mathbf{I}_k & \mathbb{O} \\ \mathbb{O} & \mathbb{O} \end{bmatrix}.$$

1.44. Si verifichi che $\mathbf{E}_{ij}^{-1} = \mathbf{E}_{ij} = \mathbf{E}_{ij}^T$ e $\mathbf{E}_i(\alpha)^{-1} = \mathbf{E}_i(\alpha^{-1})$ $(\alpha \neq 0)$.

1.45. Provare la Proposizione 6.5 usando la Proposizione 6.3 e passando alle matrici trasposte.

1.46. Si provi che, se $\mathbf{P}$ è una matrice di permutazione, allora $\mathbf{P}^{-1} = \mathbf{P}^T$.

1.47. La permutazione π dell'insieme $\{1, 2, \dots, n\}$ che manda 1 in i_1, 2 in i_2, ..., n in i_n, si può denotare con il simbolo

$$\pi = \begin{bmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{bmatrix}.$$

Sia $\mathbf{P}$ la matrice di permutazione ottenuta dalla matrice identica $\mathbf{I}_n$ permutandone le righe tramite la permutazione π. Si provi che $\mathbf{P}^T$ si ottiene da $\mathbf{I}_n$ permutandone le colonne con la permutazione π (si scriva $\mathbf{P}$ come prodotto di matrici di trasposizione).

1.48. Sia $\mathbf{A}$ una matrice $n \times n$ e sia $\mathbf{P}$ una matrice di permutazione dello stesso ordine ottenuta dalla matrice identica permutandone le righe con la permutazione π. Si provi che $\mathbf{PA}$ si ottiene da $\mathbf{A}$ permutandone le righe con la permutazione π, mentre $\mathbf{AP}^T$ si ottiene da $\mathbf{A}$ permutandone le colonne con la permutazione π.

1.49. Nelle notazioni dell'Esercizio 1.48, si provi che la matrice $\mathbf{B} = \mathbf{PAP}^T$ (che si dice *cogrediente* alla matrice $\mathbf{A}$) si ottiene da $\mathbf{A}$ permutandone le righe e le colonne con la permutazione π. Si provi inoltre che la diagonale di $\mathbf{B}$ si ottiene da quella di $\mathbf{A}$ tramite la medesima permutazione.

1.50. Si provi che, se $s < i < j$, risulta $\mathbf{E}_{ij}\mathbf{E}_{is}(\alpha) = \mathbf{E}_{js}(\alpha)\mathbf{E}_{ij}$, $\mathbf{E}_{ij}\mathbf{E}_{js}(\alpha) = \mathbf{E}_{is}(\alpha)\mathbf{E}_{ij}$, e se $r \neq i, j$, allora $\mathbf{E}_{ij}\mathbf{E}_{rs}(\alpha) = \mathbf{E}_{rs}(\alpha)\mathbf{E}_{ij}$.

Capitolo 2

Spazi vettoriali

Molto spesso in matematica si scoprono analogie in questioni diverse che, viste più astrattamente, ammettono di essere trattate allo stesso modo.

Dovrebbe ormai essere chiaro, per esempio, che ci sono somiglianze molto strette fra gli insiemi dei vettori colonna con due, tre o un qualunque numero di righe. Il concetto di spazio vettoriale permette di vederli dallo stesso punto di osservazione, cogliendo allo stesso tempo ciò che li distingue fra loro.

Lo sviluppo storico di un concetto matematico astratto è lungo e non lo seguiremo. Non si possono comunque tacere i nomi di Cayley, Sylvester e Steinitz che hanno contribuito a creare quello di spazio vettoriale.

L'idea di fondo nelle astrazioni è di cercare di isolare alcuni aspetti di una teoria, ignorandone altri. Nel nostro caso quelli che terremo sono:

- due vettori colonna con lo stesso numero di righe possono essere sommati;
- un vettore colonna può essere moltiplicato per uno scalare.

Naturalmente le operazioni che possiamo eseguire sui vettori hanno certe proprietà; anche fra queste ne isoleremo alcune che serviranno come definizione della nozione di spazio vettoriale.

Esamineremo i concetti fondamentali di insiemi di generatori, di insiemi linearmente dipendenti e indipendenti, per arrivare a quelli di base e dimensione.

Le funzioni tra spazi vettoriali che rispettano le operazioni, dette applicazioni lineari e oggetto della seconda parte di questo Capitolo, ci forniranno gli strumenti utili per considerare quattro sottospazi associati in modo naturale a una generica matrice complessa e saranno chiamati "sottospazi fondamentali".

1. Spazi vettoriali e sottospazi

Uno *spazio vettoriale* (*complesso*) V è un insieme sul quale siano definite due operazioni:

$$\begin{aligned} V \times V &\to V \\ (\mathbf{u}, \mathbf{v}) &\mapsto \mathbf{u} + \mathbf{v} \end{aligned} \qquad\qquad \begin{aligned} \mathbb{C} \times V& \\ (\alpha, \mathbf{v}) &\mapsto \alpha\mathbf{v} \end{aligned}$$

La prima si chiama *addizione*, la seconda *moltiplicazione per scalari*. Gli elementi di V saranno chiamati *vettori*. Richiediamo anche che le operazioni abbiano le seguenti proprietà:

(A_1) per ogni $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$,
$$\mathbf{u} + (\mathbf{v} + \mathbf{w}) = (\mathbf{u} + \mathbf{v}) + \mathbf{w};$$

(A_2) esiste un elemento $\mathbf{0} \in V$ tale che, per ogni $\mathbf{v} \in V$,
$$\mathbf{0} + \mathbf{v} = \mathbf{v}, \qquad \mathbf{v} + \mathbf{0} = \mathbf{v};$$

(A_3) per ogni $\mathbf{v} \in V$ esiste $\mathbf{w} \in V$ tale che
$$\mathbf{v} + \mathbf{w} = \mathbf{0}, \qquad \mathbf{w} + \mathbf{v} = \mathbf{0}.$$

(M_1) per ogni $\alpha, \beta \in \mathbb{C}$ e ogni $\mathbf{v} \in V$,
$$\alpha(\beta\mathbf{v}) = (\alpha\beta)\mathbf{v};$$

(M_2) per ogni $\alpha, \beta \in \mathbb{C}$ e ogni $\mathbf{v} \in V$,
$$(\alpha + \beta)\mathbf{v} = \alpha\mathbf{v} + \beta\mathbf{v};$$

(M_3) per ogni $\alpha \in \mathbb{C}$ e ogni $\mathbf{u}, \mathbf{v} \in V$,
$$\alpha(\mathbf{u} + \mathbf{v}) = \alpha\mathbf{u} + \alpha\mathbf{v};$$

(M_4) per ogni $\mathbf{v} \in V$,
$$1\mathbf{v} = \mathbf{v}.$$

È bene fare qualche commento sulle condizioni appena enunciate, che chiameremo *regole di calcolo* negli spazi vettoriali.

Nella (A_1) stiamo imponendo che l'addizione sia *associativa*. Quindi, come si fa con le espressioni numeriche, potremo omettere le parentesi quando si sommano più elementi di uno spazio vettoriale.

Nella (A_2) chiediamo l'esistenza di un elemento speciale, che denoteremo sempre con $\mathbf{0}$; come vedremo non c'è pericolo di confusione, perché questo elemento è unico (in ogni spazio vettoriale) e sarà chiamato anche *vettore nullo*.

Nella (A_3) va notato l'ordine diverso delle parole 'per ogni' e 'esiste' rispetto alla precedente: l'elemento $\mathbf{w}$ dipende da $\mathbf{v}$ e si chiamerà *opposto* di $\mathbf{v}$, perché vedremo che è unico.

Nelle condizioni successive abbiamo implicitamente usato una convenzione: che la moltiplicazione per scalari abbia la precedenza sull'addizione.

La (M_1) è una specie di proprietà associativa, la (M_2) e la (M_3) si chiamano proprietà *distributive*. Insieme alle altre dicono che le espressioni algebriche negli spazi vettoriali si trattano allo stesso modo in cui si è abituati con quelle numeriche.

Per finire, la (M_4) impone una proprietà che sappiamo valere per i vettori colonna. Pur venendo per ultima è molto importante, come vedremo.

Elenchiamo ora alcuni risultati che dimostreremo solo usando le regole di calcolo appena esposte.

Proposizione 1.1. *Sia V uno spazio vettoriale complesso.*

(1) *L'elemento neutro dell'addizione è unico.*

(2) *L'opposto di un elemento $\mathbf{v} \in V$ è unico.*

(3) *Per ogni $\mathbf{u}, \mathbf{v} \in V$, si ha*

$$\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}.$$

Dimostrazione. (1) Supponiamo esista un elemento $\mathbf{z} \in V$ tale che, per ogni $\mathbf{v} \in V$,

$$\mathbf{z} + \mathbf{v} = \mathbf{v}, \qquad \mathbf{v} + \mathbf{z} = \mathbf{v},$$

cioè un altro elemento neutro. La proprietà vale anche quando al posto di $\mathbf{v}$ scriviamo $\mathbf{0}$:

$$\mathbf{z} + \mathbf{0} = \mathbf{0}, \qquad \mathbf{0} + \mathbf{z} = \mathbf{0}.$$

Ma la proprietà (A_2) dice che $\mathbf{z} + \mathbf{0} = \mathbf{z}$, perché $\mathbf{z} \in V$. Dunque $\mathbf{z} = \mathbf{0}$.

(2) Supponiamo che esistano due elementi $\mathbf{w}$ e $\mathbf{w}'$ che si comportino da opposto di $\mathbf{v}$, cioè:

$$\begin{aligned} \mathbf{v} + \mathbf{w} &= \mathbf{0}, & \mathbf{w} + \mathbf{v} &= \mathbf{0}, \\ \mathbf{v} + \mathbf{w}' &= \mathbf{0}, & \mathbf{w}' + \mathbf{v} &= \mathbf{0}. \end{aligned}$$

Consideriamo allora l'elemento

$$\mathbf{u} = (\mathbf{w} + \mathbf{v}) + \mathbf{w}' = \mathbf{w} + (\mathbf{v} + \mathbf{w}'),$$

dove la seconda uguaglianza segue dalla (A_1). Applichiamo allora ciò che sappiamo: dalla (A_3) e dalla (A_2) segue

$$\mathbf{u} = (\mathbf{w} + \mathbf{v}) + \mathbf{w}' = \mathbf{0} + \mathbf{w}' = \mathbf{w}'.$$

Dall'ipotesi su $\mathbf{w}'$ e dalla (A_2) segue

$$\mathbf{u} = \mathbf{w} + (\mathbf{v} + \mathbf{w}') = \mathbf{w} + \mathbf{0} = \mathbf{w}.$$

Dunque $\mathbf{w} = \mathbf{w}'$.

(3) Useremo tutte le proprietà tranne la (M_1). Poniamo

$$\mathbf{w} = (1+1)(\mathbf{u} + \mathbf{v}).$$

Allora

$$\begin{aligned} \mathbf{w} &= 1(\mathbf{u} + \mathbf{v}) + 1(\mathbf{u} + \mathbf{v}) && (M_2) \\ &= (\mathbf{u} + \mathbf{v}) + (\mathbf{u} + \mathbf{v}) && (M_4) \\ &= \mathbf{u} + \mathbf{v} + \mathbf{u} + \mathbf{v} && (A_1) \\ \mathbf{w} &= (1+1)\mathbf{u} + (1+1)\mathbf{v} && (M_3) \\ &= (1\mathbf{u} + 1\mathbf{u}) + (1\mathbf{v} + 1\mathbf{v}) && (M_2) \\ &= (\mathbf{u} + \mathbf{u}) + (\mathbf{v} + \mathbf{v}) && (M_4) \\ &= \mathbf{u} + \mathbf{u} + \mathbf{v} + \mathbf{v} && (A_1). \end{aligned}$$

Possiamo allora calcolare $(-\mathbf{u})+\mathbf{w}+(-\mathbf{v})$ in due modi:

$$\begin{aligned}(-\mathbf{u})+\mathbf{w}+(-\mathbf{v}) &= (-\mathbf{u})+\mathbf{u}+\mathbf{v}+\mathbf{u}+\mathbf{v}+(-\mathbf{v})\\ &= \mathbf{0}+\mathbf{v}+\mathbf{u}+\mathbf{0}\\ &= \mathbf{v}+\mathbf{u}\\ (-\mathbf{u})+\mathbf{w}+(-\mathbf{v}) &= (-\mathbf{u})+\mathbf{u}+\mathbf{u}+\mathbf{v}+\mathbf{v}+(-\mathbf{v})\\ &= \mathbf{0}+\mathbf{u}+\mathbf{v}+\mathbf{0}\\ &= \mathbf{u}+\mathbf{v}\end{aligned}$$

dove abbiamo usato la (A_3) e la (A_2), oltre alla (A_1). □

Useremo una notazione speciale per l'opposto, giustificata dal fatto che esso esiste, per la regola (A_3), ed è unico per quanto visto in (2):

l'opposto di $\mathbf{v}$ si denota con $-\mathbf{v}$.

Il risultato (3) dice che l'addizione in uno spazio vettoriale è *commutativa*.

Ci sono altre proprietà che sono quasi ovvie negli spazi vettoriali già noti, ma che discendono dalle regole di calcolo. Invitiamo il lettore a esplicitare quali regole vengono usate in ogni passaggio. Notiamo anche la differenza fra 0 e $\mathbf{0}$: con il primo indichiamo il numero complesso zero, con il secondo il vettore nullo.

Proposizione 1.2. *Sia V uno spazio vettoriale.*

(i) *Per ogni* $\mathbf{v}\in V$*, si ha*
$$0\mathbf{v}=\mathbf{0}.$$

(ii) *Se* $\alpha\in\mathbb{C}$, $\mathbf{v}\in V$ *e* $\alpha\mathbf{v}=\mathbf{0}$ *si ha* $\alpha=0$ *oppure* $\mathbf{v}=\mathbf{0}$.

(iii) *Per ogni* $\alpha\in\mathbb{C}$*, si ha*
$$\alpha\mathbf{0}=\mathbf{0}.$$

(iv) *Se* $\mathbf{v},\mathbf{w}\in V$*, allora* $\mathbf{w}=-\mathbf{v}$ *se e solo se* $\mathbf{v}+\mathbf{w}=\mathbf{0}$.

(v) *Per ogni* $\mathbf{v}\in V$ *e ogni* $\alpha\in\mathbb{C}$*, si ha*
$$-(\alpha\mathbf{v})=(-\alpha)\mathbf{v}=\alpha(-\mathbf{v}).$$

Dimostrazione. (1) Poniamo $\mathbf{u}=0\mathbf{v}$; la proprietà fondamentale di 0 è che $0+0=0$; allora
$$\mathbf{u}=0\mathbf{v}=(0+0)\mathbf{v}=0\mathbf{v}+0\mathbf{v}=\mathbf{u}+\mathbf{u}.$$

Perciò possiamo scrivere
$$\mathbf{0}=\mathbf{u}+(-\mathbf{u})=(\mathbf{u}+\mathbf{u})+(-\mathbf{u})=\mathbf{u}+(\mathbf{u}+(-\mathbf{u}))=\mathbf{u}+\mathbf{0}=\mathbf{u},$$

e quindi $\mathbf{u}=\mathbf{0}$.

(2) Se $\alpha=0$ non c'è nulla da dimostrare. Supponiamo allora $\alpha\neq 0$; allora
$$\mathbf{0}=\alpha^{-1}\mathbf{0}=\alpha^{-1}(\alpha\mathbf{v})=(\alpha^{-1}\alpha)\mathbf{v}=1\mathbf{v}=\mathbf{v}.$$

Lasciamo al lettore la giustificazione di ogni passaggio.

(3) Poniamo $\mathbf{u} = \alpha\mathbf{0}$; per la proprietà fondamentale di $\mathbf{0}$ che $\mathbf{0}+\mathbf{0}=\mathbf{0}$, abbiamo

$$\mathbf{u} = \alpha\mathbf{0} = \alpha(\mathbf{0}+\mathbf{0}) = \alpha\mathbf{0}+\alpha\mathbf{0} = \mathbf{u}+\mathbf{u}.$$

Come prima possiamo concludere che $\mathbf{u} = \mathbf{0}$.

(4) Se $\mathbf{w} = -\mathbf{v}$, che $\mathbf{v}+\mathbf{w} = \mathbf{0}$ fa parte della definizione. Se, viceversa, $\mathbf{0} = \mathbf{v}+\mathbf{w}$, possiamo sommare ad ambo i membri $-\mathbf{v}$; allora

$$-\mathbf{v} = -\mathbf{v}+\mathbf{0} = -\mathbf{v}+(\mathbf{v}+\mathbf{w}) = (-\mathbf{v}+\mathbf{v})+\mathbf{w} = \mathbf{0}+\mathbf{w} = \mathbf{w}$$

e la tesi è provata.

(5) Dimostreremo dapprima che $-(\alpha\mathbf{v}) = (-\alpha)\mathbf{v}$. Alla luce di (4) ci basta calcolare

$$\alpha\mathbf{v}+(-\alpha)\mathbf{v} = (\alpha+(-\alpha))\mathbf{v} = 0\mathbf{v} = \mathbf{0}$$

e abbiamo la tesi. Analogamente,

$$\alpha\mathbf{v}+\alpha(-\mathbf{v}) = \alpha(\mathbf{v}+(-\mathbf{v})) = \alpha\mathbf{0} = \mathbf{0},$$

così la dimostrazione è completa. □

Lo scopo di queste proposizioni è di mostrare come dalle poche regole di calcolo che abbiamo imposto, ne seguano molte altre.

Spazi vettoriali reali

In alcuni casi la moltiplicazione di un vettore per un numero complesso non ha senso; ne ha invece quella per un numero reale. Si pensi, per esempio, ai vettori della fisica. Questi non formano uno spazio vettoriale nel senso specificato finora, ma solo perché le regole di calcolo (M_1)–(M_4) si applicano solo a numeri reali.

Tuttavia è facile verificare che ogni enunciato finora dimostrato è valido anche in questo contesto. Parleremo in questo caso di *spazi vettoriali reali*. Dunque uno spazio vettoriale reale è un insieme V con l'operazione di addizione e quella di moltiplicazione per numeri reali, nel quale valgano le regole (A_1)–(A_3) e (M_1)–(M_4) ristrette ai numeri reali.

Di fatto è possibile anche una maggiore astrazione, definendo spazi vettoriali con moltiplicazione per *scalari* che siano elementi di quelli che in algebra si chiamano *campi*: esempi di campi noti allo studente dovrebbero essere i numeri razionali, i numeri reali e i numeri complessi, ma ne esistono altri. In essi le proprietà rilevanti sono di poter eseguire operazioni di addizione e moltiplicazione con regole analoghe a quelle in $\mathbb{C}$, fra cui l'esistenza dell'inverso rispetto alla moltiplicazione di ogni elemento diverso da 0. Un esempio molto importante è quello degli interi modulo p, dove p è un numero primo. Non seguiremo questo tipo di astrazione; quello che è rilevante notare è che i risultati che esporremo in questo Capitolo valgono per spazi vettoriali su campi qualunque.

Per parlare di spazi vettoriali in modo generico, chiameremo *scalari* i numeri per i quali è ammessa la moltiplicazione.

Esempi di spazi vettoriali

Vettori colonna e matrici. Per ogni $m \geq 1$, l'insieme delle matrici $\mathrm{M}_{m\times 1}(\mathbb{C})$ è uno spazio vettoriale, prendendo come addizione quella fra matrici e come moltiplicazione per scalari quella già definita. Questi spazi vettoriali sono i più importanti, quindi useremo per essi la notazione speciale $\mathbb{C}^m$.

Più in generale, per ogni $m, n \geq 1$, l'insieme delle matrici $\mathrm{M}_{m\times n}(\mathbb{C})$ di dimensioni $m \times n$ è uno spazio vettoriale, con le operazioni definite nel Capitolo 1 di addizione fra matrici e prodotto per numeri complessi.

Analogamente, $\mathrm{M}_{m\times n}(\mathbb{R})$ (cioè le matrici $m \times n$ a coefficienti reali) è uno spazio vettoriale reale. Porremo $\mathbb{R}^m = \mathrm{M}_{m\times 1}(\mathbb{R})$, come visto in precedenza.

Spazi di funzioni. Consideriamo l'insieme $\mathscr{C}([a,b])$ delle funzioni reali continue sull'intervallo $[a,b]$. Possiamo renderlo uno spazio vettoriale reale definendo, per $f, g \in \mathscr{C}([a,b])$ e $\alpha \in \mathbb{R}$,

$$(f+g)(t) = f(t) + g(t), \qquad (\alpha f)(t) = \alpha f(t), \quad t \in [a,b]$$

cioè definendo la funzione $f+g$ e la funzione αf sull'intervallo $[a,b]$. Verifiche note dimostrano che sia $f+g$ che αf sono ancora funzioni continue. Si lascia come esercizio al lettore la verifica che le regole di calcolo sono valide. Per esempio, il vettore nullo è la funzione che vale costantemente zero.

Polinomi. Un *polinomio reale a coefficienti reali* è un'espressione della forma

$$a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$$

per opportuni $a_0, a_1, \ldots, a_n \in \mathbb{R}$ detti *coefficienti*. La X non indica un numero, ma è solo un simbolo che obbedisce alle regole $X^a X^b = X^{a+b}$. Anche queste espressioni formano uno spazio vettoriale reale con l'usuale addizione e la moltiplicazione per scalari definita come al solito (una costante è un particolare polinomio). Notiamo che in questo contesto non ci interessa la moltiplicazione generale fra polinomi, solo quella per le costanti.

Questo spazio vettoriale sarà indicato con $\mathscr{P}(\mathbb{R})$.

Il *grado* di un polinomio è l'esponente massimo che compare effettivamente; così il grado di $2 - X + X^2$ è due, quello di $3X + 2X^4$ è quattro. Il polinomio nullo ha, per convenzione, grado $-\infty$.

Possiamo notare che, dati i polinomi f e g, il grado di $f+g$ è non maggiore del grado di f e di g. Analogamente, il grado di αf è non maggiore del grado di f, se α è uno scalare.

Di conseguenza l'insieme $\mathscr{P}_n(\mathbb{R})$ dei polinomi di grado $< n$ è esso stesso uno spazio vettoriale. In particolare $\mathscr{P}_0(\mathbb{R}) = \{0\}$ contiene solo il polinomio nullo, mentre possiamo considerare $\mathscr{P}_1(\mathbb{R}) = \mathbb{R}$.

Polinomi a coefficienti complessi. Tutto quanto detto per i polinomi a coefficienti reali vale ancora per polinomi a coefficienti complessi; useremo le notazioni $\mathscr{P}(\mathbb{C})$ e $\mathscr{P}_n(\mathbb{C})$.

Lo spazio vettoriale nullo. Un insieme con un solo elemento diventa in modo ovvio uno spazio vettoriale. Quell'unico elemento sarà $\mathbf{0}$, con l'unica possibile addizione e l'unica moltiplicazione per scalari, cioè $\mathbf{0}+\mathbf{0}=\mathbf{0}$ e $\alpha\mathbf{0}=\mathbf{0}$.

Sottospazi e combinazioni lineari

Consideriamo una matrice $\mathbf{A} \in \mathrm{M}_{m\times n}(\mathbb{C})$ e poniamo

$$\mathrm{N}(\mathbf{A}) = \{\mathbf{v} \in \mathbb{C}^n \mid \mathbf{A}\mathbf{v} = \mathbf{0}\}.$$

È ovvio che $\mathbf{0} \in \mathrm{N}(\mathbf{A})$. Se prendiamo due elementi $\mathbf{u}$ e $\mathbf{v}$ di $\mathrm{N}(\mathbf{A})$ e li sommiamo, otteniamo ancora un elemento di $\mathrm{N}(\mathbf{A})$: infatti

$$\mathbf{A}(\mathbf{u}+\mathbf{v}) = \mathbf{A}\mathbf{u}+\mathbf{A}\mathbf{v} = \mathbf{0}+\mathbf{0} = \mathbf{0}.$$

Analogamente, se $\alpha \in \mathbb{C}$,

$$\mathbf{A}(\alpha\mathbf{v}) = \alpha\mathbf{A}\mathbf{v} = \alpha\mathbf{0} = \mathbf{0},$$

quindi $\alpha\mathbf{v} \in \mathrm{N}(\mathbf{A})$. Non è difficile verificare allora che le regole di calcolo in $\mathrm{N}(\mathbf{A})$ valgono, dal momento che valgono in $\mathbb{C}^n$.

Questo esempio può essere generalizzato, notando che gli unici fatti usati sono che $\mathbf{0} \in \mathrm{N}(\mathbf{A})$, che dati $\mathbf{u},\mathbf{v} \in \mathrm{N}(\mathbf{A})$ anche $\mathbf{u}+\mathbf{v} \in \mathrm{N}(\mathbf{A})$ e che dato $\mathbf{v} \in \mathrm{N}(\mathbf{A})$ e $\alpha \in \mathbb{C}$ anche $\alpha\mathbf{v} \in \mathrm{N}(\mathbf{A})$.

Definizione. Un sottoinsieme U dello spazio vettoriale V si dice un *sottospazio vettoriale* (o semplicemente un sottospazio) se

(S_1) $\mathbf{0} \in U$;

(S_2) per ogni $\mathbf{v}_1,\mathbf{v}_2 \in U$, si ha $\mathbf{v}_1+\mathbf{v}_2 \in U$;

(S_3) per ogni $\mathbf{v} \in U$ e ogni $\alpha \in \mathbb{C}$, $\alpha\mathbf{v} \in U$.

Se U è un sottospazio vettoriale di V, le operazioni di V rendono U esso stesso uno spazio vettoriale. L'unica cosa non ovvia è l'esistenza degli opposti. Ma essa segue subito dal fatto che $-\mathbf{v} = (-1)\mathbf{v}$, per quanto visto prima.

Esempi 1.3. (1) Per ogni $n \geq 0$, $\mathscr{P}_n(\mathbb{C})$ è un sottospazio vettoriale di $\mathscr{P}(\mathbb{C})$.

(2) Se U è un sottospazio vettoriale di V e W è un sottospazio vettoriale di U, allora W è un sottospazio vettoriale di V.

(3) Se V è un qualunque spazio vettoriale, $\{\mathbf{0}\}$ e V sono sottospazi vettoriali di V. Un sottospazio U di V si dice *proprio* se $U \neq V$, cioè se esiste un elemento $\mathbf{v} \in V$ tale che $\mathbf{v} \notin U$.

(4) Sia V uno spazio vettoriale e sia $\mathbf{v} \in V$. Consideriamo

$$\langle\mathbf{v}\rangle = \{\,\alpha\mathbf{v} \mid \alpha \in \mathbb{C}\,\}$$

cioè l'insieme di tutti i *multipli scalari* di $\mathbf{v}$. Dimostriamo che $\langle\mathbf{v}\rangle$ è un sottospazio di V. Infatti $\mathbf{0} = 0\mathbf{v} \in \langle\mathbf{v}\rangle$. Se $\mathbf{v}_1,\mathbf{v}_2 \in \langle\mathbf{v}\rangle$, allora è $\mathbf{v}_1 = \alpha_1\mathbf{v}$ e $\mathbf{v}_2 = \alpha_2\mathbf{v}$, per opportuni scalari α_1 e α_2. Allora

$$\mathbf{v}_1+\mathbf{v}_2 = \alpha_1\mathbf{v}+\alpha_2\mathbf{v} = (\alpha_1+\alpha_2)\mathbf{v} \in \langle\mathbf{v}\rangle.$$

Se poi $\alpha \in \mathbb{C}$ e $\mathbf{v}_1 \in \langle \mathbf{v} \rangle$, possiamo scrivere $\mathbf{v}_1 = \alpha_1 \mathbf{v}$ e quindi

$$\alpha \mathbf{v}_1 = \alpha(\alpha_1 \mathbf{v}) = (\alpha\alpha_1)\mathbf{v} \in \langle \mathbf{v} \rangle. \qquad \square$$

Diamo un modo diverso di verificare se un certo sottoinsieme U dello spazio vettoriale V è un sottospazio.

Proposizione 1.4. *Sia V uno spazio vettoriale e sia U un sottoinsieme di V. Allora U è un sottospazio di V se e solo se*

(V_1) *$U \neq \emptyset$;*

(V_2) *per ogni $\mathbf{u}_1, \mathbf{u}_2 \in U$ e ogni $\beta_1, \beta_2 \in \mathbb{C}$, $\beta_1 \mathbf{u}_1 + \beta \mathbf{u}_2 \in U$.*

Dimostrazione. Verifichiamo che da (V_1) e (V_2) seguono (S_1), (S_2) e (S_3). Poiché $U \neq \emptyset$, esiste $\mathbf{u}_0 \in U$. Allora possiamo applicare (V_2) con $\beta_1 = 1$, $\beta_2 = -1$, $\mathbf{u}_1 = \mathbf{u}_2 = \mathbf{u}_0$, ottenendo che

$$\beta_1 \mathbf{u}_1 + \beta \mathbf{u}_2 = 1\mathbf{u}_0 + (-1)\mathbf{u}_0 = (1-1)\mathbf{u}_0 = \mathbf{0} \in U.$$

Dunque abbiamo provato che vale (S_1). La (S_2) si prova scegliendo $\beta_1 = \beta_2 = 1$. La (S_3) segue prendendo $\beta_1 = \alpha$, $\beta_2 = 0$, $\mathbf{u}_1 = \mathbf{v}$ e $\mathbf{u}_2 = \mathbf{u}_0$.

Verifichiamo ora che da (S_1), (S_2) e (S_3) seguono (V_1) e (V_2). Il fatto che $U \neq \emptyset$ è evidente. Per (S_3), $\beta_1 \mathbf{u}_1$ e $\beta_2 \mathbf{u}_2$ sono elementi di U, quindi anche $\beta_1 \mathbf{u}_1 + \beta_2 \mathbf{u}_2 \in U$, per ($S_2$). $\square$

Definizione. Un *insieme finito di vettori* dello spazio vettoriale V è una lista finita di elementi di V che denoteremo con lettere come $\mathscr{A}$, $\mathscr{B}$, eccetera. Scriveremo, per esempio

$$\mathscr{A} = \{\mathbf{v}_1; \mathbf{v}_2; \dots; \mathbf{v}_n\}.$$

La notazione non usuale vuole ricordare che stiamo usando un artificio, rispetto al solito concetto di insieme finito; infatti ammetteremo che fra i vettori che compaiono nell'elenco ci possano essere ripetizioni.

Quando nel seguito useremo la locuzione "insieme di vettori" sarà sempre in questo significato, sottintendendo "finito", a meno che non si dica esplicitamente il contrario.

Non è escluso il caso di $n = 0$, nel qual caso parleremo di *insieme vuoto*, indicato anche con $\{\}$.

Esempio 1.5. Una matrice $\mathbf{A} \in \mathrm{M}_{m\times n}(\mathbb{C})$ definisce un insieme di vettori in $\mathbb{C}^m$; scrivendo infatti $\mathbf{A} = [\mathbf{a}_1\ \mathbf{a}_2\ \dots\ \mathbf{a}_n]$, possiamo associare ad $\mathbf{A}$ l'insieme di n vettori

$$\{\mathbf{a}_1; \mathbf{a}_2; \dots; \mathbf{a}_n\}.$$

Questo è proprio un caso nel quale si possono avere ripetizioni, come accade considerando la matrice

$$\mathbf{A} = \begin{bmatrix} 1 & 2 & 0 & 1 & 0 \\ 2 & 3 & 0 & 2 & 0 \\ 1 & -1 & 0 & 1 & 0 \\ 2 & 2 & 0 & 2 & 0 \end{bmatrix}. \qquad \square$$

A ogni insieme di vettori di V possiamo associare un sottospazio di V. Supponiamo per esempio di avere un insieme formato da un solo vettore, cioè $\mathscr{A} = \{\mathbf{v}\}$. A questo insieme possiamo associare allora il sottospazio $\langle\mathbf{v}\rangle$ definito prima.

Più in generale, dato un insieme di vettori $\mathscr{A} = \{\mathbf{v}_1;\mathbf{v}_2;\dots;\mathbf{v}_n\}$, siano $\alpha_1,\alpha_2,\dots,\alpha_n \in \mathbb{C}$. Possiamo allora considerare l'elemento

$$\alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2 + \dots + \alpha_n\mathbf{v}_n \in V$$

che chiameremo *combinazione lineare* dei vettori dell'insieme $\mathscr{A}$, o semplicemente *combinazione lineare di* $\mathscr{A}$, con coefficienti $\alpha_1,\alpha_2,\dots,\alpha_n$.

Definizione. Dato l'insieme di vettori $\mathscr{A} = \{\mathbf{v}_1;\mathbf{v}_2;\dots;\mathbf{v}_n\}$ dello spazio vettoriale V, il *sottospazio generato* da $\mathscr{A}$ è l'insieme di tutte le combinazioni lineari dei vettori dell'insieme, che sarà indicato con

$$\langle\mathscr{A}\rangle \qquad \text{oppure con} \qquad \langle\mathbf{v}_1;\mathbf{v}_2;\dots;\mathbf{v}_n\rangle.$$

Per convenzione, nel caso dell'insieme vuoto, si pone

$$\langle\{\}\rangle = \{\mathbf{0}\}.$$

Il nome dato all'insieme delle combinazioni lineari è giustificato.

Proposizione 1.6. *Dato l'insieme di vettori $\mathscr{A}$ dello spazio vettoriale V, $\langle\mathscr{A}\rangle$ è un sottospazio di V.*

Dimostrazione. Il fatto è evidente, per definizione, se $\mathscr{A}$ è l'insieme vuoto. Supponiamo allora che $\mathscr{A} = \{\mathbf{v}_1;\mathbf{v}_2;\dots;\mathbf{v}_n\}$ e verifichiamo che $\langle\mathscr{A}\rangle$ è un sottospazio.

Possiamo scrivere $\mathbf{0}$ come combinazione lineare di questi vettori con coefficienti tutti nulli:

$$0\mathbf{v}_1 + 0\mathbf{v}_2 + \dots + 0\mathbf{v}_n = \mathbf{0}.$$

Se $\mathbf{u}_1,\mathbf{u}_2 \in \langle\mathscr{A}\rangle$, possiamo scrivere

$$\mathbf{u}_1 = \sum_{i=1}^{n} \alpha_i\mathbf{v}_i, \quad \mathbf{u}_2 = \sum_{i=1}^{n} \alpha'_i\mathbf{v}_i,$$

e, per $\beta_1,\beta_2 \in \mathbb{C}$, abbiamo

$$\beta_1\mathbf{u}_1 + \beta_2\mathbf{u}_2 = \beta_1\sum_{i=1}^{n} \alpha_i\mathbf{v}_i + \beta_2\sum_{i=1}^{n} \alpha'_i\mathbf{v}_i = \sum_{i=1}^{n} (\beta_1\alpha_i + \beta_2\alpha'_i)\mathbf{v}_i$$

e la verifica è completa. □

Il lettore esegua lo sviluppo della formula finale della dimostrazione, per esempio nel caso di $n = 3$, per rendersi conto delle regole di calcolo usate.

Esempio 1.7. Consideriamo l'insieme di vettori in $\mathbb{C}^3$

$$\mathscr{A} = \left\{ \mathbf{v}_1 = \begin{bmatrix} 1 \\ -1 \\ 0 \end{bmatrix}; \mathbf{v}_2 = \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix}; \mathbf{v}_3 = \begin{bmatrix} -1 \\ 4 \\ 0 \end{bmatrix} \right\}.$$

Una combinazione lineare dei vettori di $\mathscr{A}$ sarà un vettore della forma

$$\mathbf{v} = \alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2 + \alpha_3\mathbf{v}_3 = \begin{bmatrix} \alpha_1 + 2\alpha_2 - \alpha_3 \\ -\alpha_1 + \alpha_2 + 4\alpha_3 \\ 0 \end{bmatrix}$$

e, come si può dimostrare per esercizio, ogni vettore della forma

$$\begin{bmatrix} \beta_1 \\ \beta_2 \\ 0 \end{bmatrix}$$

può essere scritto come combinazione lineare dei vettori di $\mathscr{A}$. Svolgendo i calcoli si può comprendere come il concetto di combinazione lineare e quello di sistema lineare siano strettamente legati. □

Un insieme finito, nel senso usuale, non dipende dall'ordine con cui si elencano i suoi elementi. Lo stesso non accade nella nostra particolare accezione del termine; ma, per esempio, il sottospazio generato dall'insieme $\{\mathbf{u}; \mathbf{v}\}$ è lo stesso del sottospazio generato da $\{\mathbf{v}; \mathbf{u}\}$ a causa del fatto che l'addizione di vettori è commutativa. Ovviamente questo accade per qualunque numero di vettori nell'insieme.

Quando parleremo di *sottoinsieme* di un insieme finito di vettori, intenderemo che ogni vettore del sottoinsieme deve appartenere nell'insieme; inoltre supporremo sempre che, se un certo vettore compare k volte nel sottoinsieme, esso dovrà comparire *almeno* k volte nell'insieme.

Proposizione 1.8. *Se $\mathscr{A}$ è un sottoinsieme di $\mathscr{B}$, allora $\langle\mathscr{A}\rangle$ è un sottospazio di $\langle\mathscr{B}\rangle$.*

Dimostrazione. Di nuovo questo è ovvio nel caso in cui $\mathscr{A}$ sia l'insieme vuoto. Supponiamo perciò che $\mathscr{A}$ abbia m elementi, con $m > 0$. È allora evidente che possiamo scrivere $\mathscr{B}$ in modo che sia

$$\begin{aligned} \mathscr{A} &= \{\mathbf{v}_1; \mathbf{v}_2; \dots; \mathbf{v}_m\}, \\ \mathscr{B} &= \{\mathbf{v}_1; \mathbf{v}_2; \dots; \mathbf{v}_m; \mathbf{v}_{m+1}; \dots; \mathbf{v}_n\}. \end{aligned}$$

Ci basta verificare che ogni vettore che sia combinazione lineare dei vettori di $\mathscr{A}$ è combinazione lineare dei vettori di $\mathscr{B}$. Ora,

$$\alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2 + \dots + \alpha_m\mathbf{v}_m = \alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2 + \dots + \alpha_m\mathbf{v}_m + 0\mathbf{v}_{m+1} + \dots + 0\mathbf{v}_n$$

e la tesi è provata. □

Osserviamo che questa proposizione giustifica il fatto che si ponga $\langle\{\}\rangle = \{\mathbf{0}\}$, proprio perché l'insieme vuoto è sottoinsieme di ogni altro.

Possiamo anche mettere insieme due insiemi $\mathscr{A}$ e $\mathscr{B}$, semplicemente mettendo il secondo di seguito al primo. Indicheremo l'insieme così ottenuto con $\mathscr{A} \sqcup \mathscr{B}$. È ovvio che $\mathscr{A}$ e $\mathscr{B}$ sono entrambi sottoinsiemi di $\mathscr{A} \sqcup \mathscr{B}$. Si tratta della solita *unione* di insiemi, tenendo però conto delle eventuali ripetizioni di elementi; per questo useremo un simbolo diverso.

2. Insiemi di generatori e indipendenza lineare

Consideriamo lo spazio vettoriale $\mathbb{C}^n$ e, in esso, un insieme finito di vettori particolare: quello ottenuta dalla matrice identità $\mathbf{I}_n$. Porremo

$$\mathbf{I}_n = [\mathbf{e}_1\ \mathbf{e}_2\ \dots\ \mathbf{e}_n].$$

L'insieme $\mathscr{E} = \{\mathbf{e}_1; \mathbf{e}_2; \dots; \mathbf{e}_n\}$ ha una proprietà importante. Se infatti prendiamo $\mathbf{v} \in \mathbb{C}^n$, avremo

$$\mathbf{v} = \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix}$$

e, di conseguenza, come si può facilmente verificare,

$$\mathbf{v} = \alpha_1\mathbf{e}_1 + \alpha_2\mathbf{e}_2 + \dots + \alpha_n\mathbf{e}_n$$

e quindi

$$\langle \mathbf{e}_1; \mathbf{e}_2; \dots; \mathbf{e}_n \rangle = \mathbb{C}^n.$$

dal momento che ogni vettore di $\mathbb{C}^n$ si può scrivere come combinazione lineare dei vettori dell'insieme $\mathscr{E}$.

Definizione. Un insieme finito di vettori $\mathscr{A}$ nello spazio vettoriale V si dice un *insieme di generatori* di V se $\langle \mathscr{A} \rangle = V$, cioè ogni vettore di V si può scrivere come combinazione lineare dei vettori dell'insieme $\mathscr{A}$.

Esempi 2.1. Lo spazio vettoriale nullo $\{\mathbf{0}\}$ ammette come insieme di generatori sia l'insieme vuoto che l'insieme $\{\mathbf{0}\}$.

Se $n > 0$, l'insieme $\{1; X; X^2; \dots; X^{n-1}\}$ è un insieme di generatori di $\mathscr{P}_n(\mathbb{C})$.

Viceversa, non esistono insiemi finiti di generatori di $\mathscr{P}(\mathbb{C})$. Sia infatti $\mathscr{A}$ un insieme finito in $\mathscr{P}(\mathbb{C})$; se l'unico elemento di $\mathscr{A}$ è il polinomio nullo, il sottospazio generato è $\{0\}$. Altrimenti fra gli elementi di $\mathscr{A}$ ce ne sarà uno avente grado massimo, diciamo $k \geq 0$. Una combinazione lineare degli elementi di $\mathscr{A}$ non può allora avere grado maggiore di k e, in particolare, $X^{k+1} \notin \langle \mathscr{A} \rangle$. □

L'esempio seguente mostra che esiste una connessione fra insiemi di generatori e sistemi lineari.

Esempio 2.2. Consideriamo i seguenti vettori di $\mathbb{C}^2$:

$$\mathbf{v}_1 = \begin{bmatrix} 2 \\ 1 \end{bmatrix}, \quad \mathbf{v}_2 = \begin{bmatrix} -1 \\ 3 \end{bmatrix}, \quad \mathbf{v}_3 = \begin{bmatrix} 1 \\ -2 \end{bmatrix}$$

e dimostriamo che $\mathscr{A} = \{\mathbf{v}_1; \mathbf{v}_2; \mathbf{v}_3\}$ è un insieme di generatori di $\mathbb{C}^2$. Preso un qualunque vettore $\mathbf{v} = [r\ s]^T \in \mathbb{C}^2$, dobbiamo poterlo scrivere come combinazione lineare dei tre vettori dati, cioè trovare numeri complessi α_1, α_2 e α_3 in modo che

$$\mathbf{v} = \alpha_1 \mathbf{v}_1 + \alpha_2 \mathbf{v}_2 + \alpha_3 \mathbf{v}_3$$

o, esplicitamente

$$\begin{cases} 2\alpha_1 - \alpha_2 + \alpha_3 = r \\ \alpha_1 + 3\alpha_2 - 2\alpha_3 = s \end{cases}$$

e si verifica facilmente che tale sistema ha soluzione per ogni $r, s \in \mathbb{C}$.

Il lettore può osservare che anche l'insieme $\{\mathbf{v}_1; \mathbf{v}_2\}$ è un insieme di generatori di $\mathbb{C}^2$, mentre nessun insieme con un solo elemento può essere un insieme di generatori. □

Definizione. Diremo che lo spazio vettoriale V è *finitamente generato* se ammette un insieme finito di generatori.

Nel seguito, tranne esplicito avviso in contrario, considereremo solo spazi finitamente generati. Lo spazio vettoriale $\mathscr{P}(\mathbb{C})$ non è finitamente generato. La teoria si può generalizzare anche per spazi vettoriali non finitamente generati, che sono fra l'altro molto utili soprattutto in relazione al concetto di prodotto scalare che si vedrà nel Capitolo 3 e per applicazioni alla fisica. Per i nostri scopi, che sono quelli legati ai sistemi lineari, gli spazi finitamente generati saranno sufficienti.

Per definizione, dato un insieme finito di vettori $\mathscr{A}$ in V, il sottospazio $\langle \mathscr{A} \rangle$ è finitamente generato e $\mathscr{A}$ ne è un insieme di generatori.

Proposizione 2.3. *Lo spazio vettoriale delle matrici* $\mathrm{M}_{m\times n}(\mathbb{C})$ *è finitamente generato.*

Dimostrazione. Esercizio: si considerino le matrici che hanno un solo coefficiente uguale a 1 e tutti gli altri 0; esse sono mn. Si può scrivere ogni matrice come combinazione lineare di queste? □

Proposizione 2.4. *Se* $\mathscr{A}$ *e* $\mathscr{B}$ *sono insiemi di vettori nello spazio vettoriale* V *tali che*

(i) $\mathscr{A}$ *è un sottoinsieme di* $\mathscr{B}$,

(ii) $\mathscr{A}$ *è un insieme di generatori di* V,

allora anche $\mathscr{B}$ *è un insieme di generatori.*

Dimostrazione. Dalle ipotesi segue che

$$V = \langle \mathscr{A} \rangle \subseteq \langle \mathscr{B} \rangle \subseteq V$$

e quindi la tesi. □

In certi casi è possibile anche eseguire un'operazione inversa.

Proposizione 2.5. *Se* $\{\mathbf{v}_1; \mathbf{v}_2; \dots; \mathbf{v}_n\}$ *è un insieme di generatori dello spazio vettoriale* V *e* $\mathbf{v}_n \in \langle \mathbf{v}_1; \mathbf{v}_2; \dots; \mathbf{v}_{n-1} \rangle$, *allora anche* $\{\mathbf{v}_1; \mathbf{v}_2; \dots; \mathbf{v}_{n-1}\}$ *è un insieme di generatori di* V.

Dimostrazione. Sia $\mathbf{v} \in V$; sappiamo scrivere

$$\mathbf{v} = \sum_{i=1}^{n} \alpha_i \mathbf{v}_i$$

per opportuni coefficienti. Per ipotesi,

$$\mathbf{v}_n = \sum_{i=1}^{n-1} \beta_i \mathbf{v}_i$$

per opportuni coefficienti. Ci basta allora sostituire nella prima uguaglianza e ottenere

$$\mathbf{v} = \sum_{i=1}^{n-1} \alpha_i \mathbf{v}_i + \sum_{i=1}^{n-1} \alpha_n \beta_i \mathbf{v}_i = \sum_{i=1}^{n-1} (\alpha_i + \alpha_n \beta_i) \mathbf{v}_i$$

come richiesto. □

La proposizione precedente dice che, ogni volta che un vettore di un insieme è combinazione lineare degli altri, lo possiamo togliere dall'insieme senza cambiare lo spazio generato. Il fatto che nella proposizione abbiamo parlato dell'ultimo vettore è ovviamente non rilevante, perché il sottospazio generato da un insieme di vettori non dipende dall'ordine.

Esempio 2.6. Consideriamo la matrice

$$\mathbf{U} = [\mathbf{u}_1\ \mathbf{u}_2\ \mathbf{u}_3\ \mathbf{u}_4\ \mathbf{u}_5] = \begin{bmatrix} 1 & -2 & 2 & 1 & 3 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

che è in forma ridotta. Possiamo scrivere

$$\mathbf{u}_4 = 3\mathbf{u}_1 + 0\mathbf{u}_2 - \mathbf{u}_3 + 0\mathbf{u}_5.$$

e, se un vettore $\mathbf{v} \in \mathbb{C}^3$ è combinazione lineare di $\{\mathbf{u}_1; \mathbf{u}_2; \mathbf{u}_3; \mathbf{u}_4; \mathbf{u}_5\}$, per esempio

$$\mathbf{v} = \alpha_1 \mathbf{u}_1 + \alpha_2 \mathbf{u}_2 + \alpha_3 \mathbf{u}_3 + \alpha_4 \mathbf{u}_4 + \alpha_5 \mathbf{u}_5,$$

abbiamo anche

$$\begin{aligned}\mathbf{v} &= \alpha_1\mathbf{u}_1 + \alpha_2\mathbf{u}_2 + \alpha_3\mathbf{u}_3 + \alpha_4(3\mathbf{u}_1 + 0\mathbf{u}_2 - \mathbf{u}_3 + 0\mathbf{u}_5) + \alpha_5\mathbf{u}_5 \\ &= (\alpha_1 + 3\alpha_4)\mathbf{u}_1 + \alpha_2\mathbf{u}_2 + (\alpha_3 - \alpha_4)\mathbf{u}_3 + \alpha_5\mathbf{u}_5.\end{aligned}$$

Abbiamo quindi che

$$V = \langle \mathbf{u}_1; \mathbf{u}_2; \mathbf{u}_3; \mathbf{u}_4; \mathbf{u}_5 \rangle = \langle \mathbf{u}_1; \mathbf{u}_2; \mathbf{u}_3; \mathbf{u}_5 \rangle.$$

Il lettore verifichi anche che

$$V = \langle \mathbf{u}_1; \mathbf{u}_3; \mathbf{u}_5 \rangle$$

ma che non è più possibile eliminare altri vettori dall'insieme senza cambiare il sottospazio generato (per esempio, $\mathbf{u}_5$ non è combinazione lineare di $\mathbf{u}_1$ e di $\mathbf{u}_3$). □

La nozione di insieme di generatori corrisponde, come ora vedremo, a quella di sistema lineare risolubile. Il concetto collegato di sistema con al più una soluzione corrisponde, come vedremo in seguito, a quello di insieme linearmente indipendente.

Consideriamo il sistema lineare di m equazioni in n incognite $\mathbf{A}\mathbf{x} = \mathbf{b}$ e supponiamo che $[\alpha_1\ \alpha_2\ \dots\ \alpha_n]^T$ e $[\beta_1\ \beta_2\ \dots\ \beta_n]^T$ siano soluzioni distinte del sistema. Se scriviamo $\mathbf{A} = [\mathbf{a}_1\ \mathbf{a}_2\ \dots\ \mathbf{a}_n]$, questo si esprime con le relazioni

$$\begin{aligned}\mathbf{b} &= \alpha_1\mathbf{a}_1 + \alpha_2\mathbf{a}_2 + \dots + \alpha_n\mathbf{a}_n \\ &= \beta_1\mathbf{a}_1 + \beta_2\mathbf{a}_2 + \dots + \beta_n\mathbf{a}_n\end{aligned}$$

e dunque il vettore $\mathbf{b}$ si può scrivere in almeno due modi come combinazione lineare dell'insieme delle colonne di $\mathbf{A}$. In effetti il sistema ha infinite soluzioni.

Se poniamo $\gamma_i = \alpha_i - \beta_i$ ($i = 1, 2, \dots, n$), abbiamo che

$$\gamma_1\mathbf{a}_1 + \gamma_2\mathbf{a}_2 + \dots + \gamma_n\mathbf{a}_n = \mathbf{0}$$

e almeno uno fra i coefficienti γ_i è diverso da 0 (altrimenti le due soluzioni da cui siamo partiti non sarebbero distinte).

Definizione. Un insieme di vettori $\mathscr{A} = \{\mathbf{v}_1; \mathbf{v}_2; \dots; \mathbf{v}_n\}$ si dice *linearmente dipendente* se esistono scalari $\alpha_1, \alpha_2, \dots, \alpha_n$ *non tutti nulli* tali che

$$\alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2 + \alpha_n\mathbf{v}_n = \mathbf{0}.$$

Attenzione: nella condizione precedente basta che *anche uno solo* dei coefficienti sia diverso da 0. Per esempio, ogni insieme in cui compaia il vettore nullo è linearmente dipendente. Infatti, se $\mathscr{A} = \{\mathbf{v}_1 = \mathbf{0}; \mathbf{v}_2; \dots; \mathbf{v}_n\}$, possiamo prendere $\alpha_1 = 1$ e $\alpha_i = 0$, per $i = 2, \dots, n$. Evidentemente

$$\sum_{i=1}^{n} \alpha_i\mathbf{v}_i = \mathbf{0}.$$

Esempio 2.7. Consideriamo l'insieme di vettori in $\mathbb{C}^3$ già visto nell'esempio 1.7:

$$\mathscr{A} = \left\{ \mathbf{v}_1 = \begin{bmatrix} 1 \\ -1 \\ 0 \end{bmatrix}; \mathbf{v}_2 = \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix}; \mathbf{v}_3 = \begin{bmatrix} -1 \\ 4 \\ 0 \end{bmatrix} \right\}.$$

Una combinazione lineare dei vettori di $\mathscr{A}$ sarà un vettore della forma

$$\mathbf{v} = \alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2 + \alpha_3\mathbf{v}_3 = \begin{bmatrix} \alpha_1 + 2\alpha_2 - \alpha_3 \\ -\alpha_1 + \alpha_2 + 4\alpha_3 \\ 0 \end{bmatrix}$$

ed è facile verificare che, per $\alpha_1 = 3$, $\alpha_2 = -1$ e $\alpha_3 = 1$, la combinazione lineare corrispondente è il vettore nullo. □

Proposizione 2.8. *Se $\mathscr{A}$ è un sottoinsieme non vuoto dell'insieme di vettori $\mathscr{B}$ e $\mathscr{A}$ è linearmente dipendente, allora anche $\mathscr{B}$ è linearmente dipendente.*

Dimostrazione. Possiamo supporre che

$$\mathscr{A} = \{\mathbf{v}_1; \dots; \mathbf{v}_m\}$$
$$\mathscr{B} = \{\mathbf{v}_1; \dots; \mathbf{v}_m; \mathbf{v}_{m+1}; \dots; \mathbf{v}_n\}$$

e che

$$\sum_{i=1}^{m} \alpha_i \mathbf{v}_i = \mathbf{0},$$

dove i coefficienti α_i $(i = 1, \dots, m)$ non sono tutti nulli. Poniamo $\alpha_{m+1} = \dots = \alpha_n = 0$ e abbiamo

$$\sum_{i=1}^{n} \alpha_i \mathbf{v}_i = \sum_{i=1}^{m} \alpha_i \mathbf{v}_i + \sum_{i=m+1}^{n} \alpha_i \mathbf{v}_i = \mathbf{0},$$

e quindi la tesi. □

Esempio 2.9. Se nell'insieme $\mathscr{A}$ ci sono due vettori uguali, esso è linearmente dipendente. Vista la Proposizione 2.8, basta dimostrare che l'insieme $\{\mathbf{v}; \mathbf{v}\}$ è linearmente dipendente. In effetti

$$1\mathbf{v} + (-1)\mathbf{v} = \mathbf{0}$$

e abbiamo la tesi. □

Di fatto la nozione più importante è il contrario della dipendenza lineare.

Definizione. Un insieme di vettori $\mathscr{A}$ è *linearmente indipendente* se non è linearmente dipendente. Per convenzione, anche l'insieme vuoto è linearmente indipendente.

Come possiamo allora verificare se un insieme di vettori è linearmente indipendente? La cosa è ovvia per l'insieme vuoto: un insieme linearmente dipendente ha, per definizione, almeno un elemento.

Proposizione 2.10. *L'insieme* $\mathscr{A} = \{\mathbf{v}_1; \mathbf{v}_2; \dots; \mathbf{v}_n\}$ *è linearmente indipendente se e solo se, per* $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{C}$*, da*

$$\alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2 + \dots + \alpha_n\mathbf{v}_n = \mathbf{0}$$

segue che $\alpha_1 = 0$, $\alpha_2 = 0, \dots, \alpha_n = 0$.

Dimostrazione. Si tratta semplicemente di applicare la definizione di insieme linearmente dipendente. □

Esempio 2.11. L'insieme $\mathscr{E}$ delle colonne dell'identità $\mathbf{I}_n$ è un insieme linearmente indipendente di vettori di $\mathbb{C}^n$. Infatti, da

$$\alpha_1\mathbf{e}_1 + \alpha_2\mathbf{e}_2 + \dots + \alpha_n\mathbf{e}_n = \mathbf{0}$$

segue che $\alpha_1 = 0$, $\alpha_2 = 0, \dots, \alpha_n = 0$. Il lettore scriva esplicitamente i calcoli per $n = 4$.

L'insieme di vettori in $\mathbb{C}^4$

$$\left\{ \mathbf{v}_1 = \begin{bmatrix} 1 \\ -1 \\ 2 \\ 0 \end{bmatrix}; \mathbf{v}_2 = \begin{bmatrix} 2 \\ 1 \\ 2 \\ 0 \end{bmatrix}; \mathbf{v}_3 = \begin{bmatrix} 0 \\ 3 \\ 2 \\ 0 \end{bmatrix} \right\}$$

è linearmente indipendente. Infatti, scrivere

$$\alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2 + \alpha_3\mathbf{v}_3 = \mathbf{0}$$

equivale a scrivere il sistema lineare

$$\begin{cases} \alpha_1 + 2\alpha_2 = 0 \\ -\alpha_1 + \alpha_2 + 3\alpha_3 = 0 \\ 2\alpha_1 + 2\alpha_2 + 2\alpha_3 = 0 \end{cases}$$

il quale ammette solo la soluzione $\alpha_1 = 0$, $\alpha_2 = 0$, $\alpha_3 = 0$. □

Vediamo subito alcune conseguenze della definizione.

Proposizione 2.12. *Se* $\mathscr{A}$ *è un insieme linearmente indipendente, ogni suo sottoinsieme è ancora linearmente indipendente.*

Dimostrazione. Se un sottoinsieme di $\mathscr{A}$ fosse linearmente dipendente, anche $\mathscr{A}$ lo sarebbe. □

Proposizione 2.13. *Se* $\mathscr{A}$ *è un insieme linearmente indipendente, esso consiste di vettori a due a due distinti e non nulli.* □

Esempio 2.14. Se $\mathbf{v} \in V$ e $\mathbf{v} \neq \mathbf{0}$, allora $\{\mathbf{v}\}$ è linearmente indipendente. Infatti, se $\alpha\mathbf{v} = \mathbf{0}$, sappiamo che o $\alpha = 0$ oppure $\mathbf{v} = \mathbf{0}$. □

Sotto certe condizioni possiamo aggiungere vettori a un insieme linearmente indipendente ottenendo ancora un insieme linearmente indipendente. La dimostrazione che segue è un buon esempio per capire la tecnica che si usa per verificare l'indipendenza lineare.

Teorema 2.15. *Sia $\mathscr{A}$ un insieme linearmente indipendente nello spazio vettoriale V e sia $\mathbf{v} \in V$ tale che $\mathbf{v} \notin \langle \mathscr{A} \rangle$. Allora l'insieme $\mathscr{B} = \mathscr{A} \sqcup \{\mathbf{v}\}$ è linearmente indipendente.*

Dimostrazione. La cosa è ovvia se $\mathscr{A}$ è l'insieme vuoto, per l'Esempio precedente. Supponiamo allora $\mathscr{A} = \{\mathbf{v}_1; \dots; \mathbf{v}_n\}$. Prendiamo scalari $\alpha_1, \dots, \alpha_n$ e α tali che

$$\alpha_1 \mathbf{v}_1 + \dots + \alpha_n \mathbf{v}_n + \alpha \mathbf{v} = \mathbf{0}.$$

Supponiamo, per assurdo, che $\alpha \neq 0$. Allora

$$-\alpha \mathbf{v} = \sum_{i=1}^{n} \alpha_i \mathbf{v}_i$$

e, ponendo $\beta_i = -\alpha^{-1} \alpha_i$, otteniamo

$$\mathbf{v} = \sum_{i=1}^{n} \beta_i \mathbf{v}_i$$

da cui seguirebbe $\mathbf{v} \in \langle \mathscr{A} \rangle$, contraddizione.

Dunque $\alpha = 0$ e quindi anche

$$\sum_{i=1}^{n} \alpha_i \mathbf{v}_i = \mathbf{0}.$$

Per ipotesi l'insieme $\mathscr{A}$ è linearmente indipendente, quindi anche $\alpha_1 = 0$, $\alpha_2 = 0$, ..., $\alpha_n = 0$, e, come si voleva, tutti gli scalari sono nulli. □

Esempio 2.16. Sia $\mathbf{U}$ una matrice $n \times p$ in forma ridotta e siano $\mathbf{v}_1$, $\mathbf{v}_2$, ..., $\mathbf{v}_k$ le sue colonne dominanti. Allora l'insieme di vettori $\{\mathbf{v}_1; \mathbf{v}_2; \dots; \mathbf{v}_k\}$ in $\mathbb{C}^n$ è linearmente indipendente.

Se infatti ricordiamo come risultano le colonne dominanti dopo la EG, possiamo scrivere

$$\mathbf{v}_i = \begin{bmatrix} * \\ \vdots \\ * \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \begin{array}{l} \\ \\ \\ \leftarrow i \\ \\ \\ \\ \end{array}$$

dove gli asterischi indicano i coefficienti che effettivamente compaiono. Completeremo la dimostrazione per induzione.

Se c'è una sola colonna dominante, l'insieme è formato da un solo vettore non nullo e quindi è linearmente indipendente per l'Esempio 2.14. Supponiamo allora che $k > 1$; la matrice $\mathbf{U}'$ che ha come colonne quelle precedenti l'ultima colonna dominante di $\mathbf{U}$ è ancora in forma ridotta e ha esattamente come colonne dominanti le prime $k-1$ colonne dominanti di $\mathbf{U}$. Per ipotesi induttiva l'insieme di queste colonne è linearmente indipendente. Ci basta allora verificare che $\mathbf{v}_k \notin \langle \mathbf{v}_1; \dots; \mathbf{v}_{k-1} \rangle$ e applicare il Teorema 2.15.

Ma una combinazione lineare delle prime $k-1$ colonne dominanti ha tutti i coefficienti dalla k-esima riga in poi nulli, e quindi non può essere uguale a $\mathbf{v}_k$ che sulla k-esima riga ha 1.

Per via della proposizione 2.12 ogni insieme formato da colonne dominanti (distinte) di una matrice in forma ridotta è linearmente indipendente. □

Esempio 2.17. Consideriamo una matrice reale $\mathbf{U}$ di dimensioni $m \times n$ che sia in forma ridotta. Allora l'insieme delle righe non nulle di $\mathbf{U}$ è linearmente indipendente in $\mathbb{R}_n$ (esercizio). Lo stesso naturalmente vale per matrici complesse.

Per esempio, si consideri la matrice

$$\mathbf{U} = \begin{bmatrix} 1 & -1 & 2 & 3 & 5 & 4 \\ 0 & 0 & 1 & 1 & 2 & -2 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Chiamando $\mathbf{r}_1$, $\mathbf{r}_2$, $\mathbf{r}_3$ e $\mathbf{r}_4$ le righe di $\mathbf{U}$, abbiamo che

$$\mathbf{0} = \alpha_1 \mathbf{r}_1 + \alpha_2 \mathbf{r}_2 + \alpha_3 \mathbf{r}_3$$

equivale al sistema lineare

$$\begin{cases} \alpha_1 = 0 \\ -\alpha_1 = 0 \\ 2\alpha_1 + \alpha_2 = 0 \\ 3\alpha_1 + \alpha_2 = 0 \\ 5\alpha_1 + 2\alpha_2 + \alpha_3 = 0 \\ 4\alpha_1 - 2\alpha_2 = 0 \end{cases}$$

il quale ha come unica soluzione $\alpha_1 = 0$, $\alpha_2 = 0$, $\alpha_3 = 0$. □

3. Basi e dimensione

Ora metteremo insieme i due concetti di insieme di generatori e di insieme linearmente indipendente. Osserviamo che la procedura esposta nella Proposizione 2.5 permette di eliminare da un insieme di generatori vettori che siano combinazione lineare degli altri; quando questa non può più essere eseguita, rimaniamo con un insieme linearmente indipendente.

Proposizione 3.1. *Un insieme di vettori $\mathscr{A}$ è linearmente indipendente se e solo se nessuno dei vettori di $\mathscr{A}$ è combinazione lineare degli altri.*

Dimostrazione. Supponiamo che $\mathscr{A}$ sia linearmente indipendente; se è l'insieme vuoto, evidentemente non ci sono vettori che possano essere combinazione lineare degli altri (perché non ce ne sono). Sia allora $\mathscr{A} = \{\mathbf{v}_1;\dots;\mathbf{v}_n\}$ e supponiamo per assurdo che $\mathbf{v}_n$ sia combinazione lineare dei rimanenti (non è restrittivo, cambiando eventualmente l'ordine dell'elenco). Dunque possiamo scrivere

$$\mathbf{v}_n = \sum_{i=1}^{n-1} \alpha_i \mathbf{v}_i,$$

da cui, ponendo $\alpha_n = -1$, otteniamo

$$\sum_{i=1}^{n} \alpha_i \mathbf{v}_i = \mathbf{0}$$

che, essendo l'insieme linearmente indipendente, implica in particolare $\alpha_n = 0$, che è assurdo.

Supponiamo viceversa che nessuno dei vettori di $\mathscr{A}$ sia combinazione lineare dei rimanenti e dimostriamo che $\mathscr{A}$ è linearmente indipendente. Se $\alpha_i \in \mathbb{C}$ $(i = 1,\dots,n)$ e

$$\sum_{i=1}^{n} \alpha_i \mathbf{v}_i = \mathbf{0}$$

con $\alpha_n \neq 0$, possiamo scrivere anche

$$\mathbf{v}_n = \sum_{i=1}^{n-1} \beta_i \mathbf{v}_i$$

dove $\beta_i = -\alpha_n^{-1}\alpha_i$. Questo non è possibile, per ipotesi e dunque $\alpha_n = 0$. Allo stesso modo possiamo dimostrare che $\alpha_i = 0$ $(i = 1,\dots,n-1)$. □

Da questa proposizione discende dunque che la procedura della Proposizione 2.5 a un certo punto termina e precisamente quando l'insieme ottenuto è linearmente indipendente. Ricordiamo che uno spazio vettoriale V si dice finitamente generato quando ha un insieme (finito) di generatori.

Definizione. Un insieme $\mathscr{A}$ di vettori di V si dice una *base* di V se è un insieme di generatori ed è linearmente indipendente.

Teorema 3.2. *Sia V uno spazio vettoriale finitamente generato. Allora V ha una base.*

Dimostrazione. Sia $\mathscr{A}$ un insieme di generatori di V. Applichiamo la procedura della Proposizione 2.5 fino a che è possibile, ottenendo un insieme $\mathscr{B}$ che è ancora un insieme di generatori ed è anche linearmente indipendente. □

Esempio 3.3. Lo spazio vettoriale $\mathbb{C}^n$ ha come base l'insieme $\mathscr{E}$ dei vettori coordinati

$$\mathscr{E} = \{\mathbf{e}_1; \mathbf{e}_2; \dots; \mathbf{e}_n\}.$$

La verifica è già stata fatta in esempi precedenti, ma la ripetiamo. Ogni elemento di $\mathbb{C}^n$ è combinazione lineare di questi vettori: se $\mathbf{v} = [\alpha_1\ \alpha_2\ \dots\ \alpha_n]^T$, possiamo scrivere

$$\mathbf{v} = \sum_{i=1}^{n} \alpha_i \mathbf{e}_i$$

e dunque $\mathscr{E}$ è un insieme di generatori.

Inoltre,

$$\sum_{i=1}^{n} \alpha_i \mathbf{e}_i = [\alpha_1\ \alpha_2\ \dots\ \alpha_n]^T$$

e perciò, da $\sum_{i=1}^{n} \alpha_i \mathbf{e}_i = \mathbf{0}$ segue che $\alpha_1 = 0$, $\alpha_2 = 0$, ..., $\alpha_n = 0$, cioè che $\mathscr{E}$ è anche linearmente indipendente. Chiameremo $\mathscr{E}$ la *base canonica* di $\mathbb{C}^n$. □

Esempio 3.4. Lo spazio vettoriale nullo $\{\mathbf{0}\}$ ha come base l'insieme vuoto. Infatti l'insieme vuoto è un insieme di generatori di $\{\mathbf{0}\}$, per definizione, ed è linearmente indipendente. □

Esempio 3.5. L'insieme $\{p_1 = 1 - X; p_2 = 1 + X; p_3 = 1 - X^2\}$ è una base di $\mathscr{P}_3(\mathbb{C})$. Per verificarlo dimostriamo che è sia un insieme di generatori che un insieme linearmente indipendente. Come vedremo, si tratta di analizzare sistemi lineari. Cerchiamo di capire quello che occorre vedere: intanto che ogni polinomio $a_0 + a_1X + a_2X^2$ è combinazione lineare di $\{p_1; p_2; p_3\}$, cioè che esistono α_1, α_2 e α_3 tali che

$$a_0 + a_1X + a_2X^2 = \alpha_1 p_1 + \alpha_2 p_2 + \alpha_3 p_3.$$

Questo si traduce nel sistema lineare

$$\begin{cases} \alpha_1 + \alpha_2 + \alpha_3 = a_0 \\ -\alpha_1 + \alpha_2 = a_1 \\ -\alpha_3 = a_2 \end{cases}$$

che ha come matrice

$$\left[\begin{array}{ccc|c} 1 & 1 & 1 & a_0 \\ -1 & 1 & 0 & a_1 \\ 0 & 0 & -1 & a_2 \end{array}\right]$$

e una semplice EG porta alla forma ridotta

$$\left[\begin{array}{ccc|c} 1 & 1 & 1 & a_0 \\ 0 & 1 & 1/2 & (a_0 + a_1)/2 \\ 0 & 0 & 1 & -a_2 \end{array}\right]$$

da cui si vede che ogni sistema del genere, al variare di a_0, a_1 e a_2 ha un'unica soluzione. Dunque la soluzione esiste e l'insieme è di generatori; inoltre, quando $a_0 = 0$, $a_1 = 0$ e $a_2 = 0$, cioè il sistema è omogeneo, anch'esso ha un'unica soluzione, quella con $\alpha_1 = 0$, $\alpha_2 = 0$ e $\alpha_3 = 0$, perciò l'insieme dato è anche linearmente indipendente. □

Ovviamente anche l'insieme $\{1; X; X^2\}$ è una base di $\mathscr{P}_3(\mathbb{C})$, come si verifica immediatamente: il sistema lineare costruito come il precedente ha come matrice dei coefficienti l'identità. Di fatto ogni spazio vettoriale di dimensione finita ha infinite basi, con l'eccezione dello spazio vettoriale nullo che ha come unica base l'insieme vuoto.

Esempio 3.6. Se $\mathscr{B} = \{\mathbf{v}_1; \mathbf{v}_2; \dots; \mathbf{v}_n\}$ è una base di V, per ogni scalare $\gamma \neq 0$ anche

$$\mathscr{B}' = \{\mathbf{v}_1' = \gamma\mathbf{v}_1; \mathbf{v}_2; \dots; \mathbf{v}_n\}$$

è una base di V.

Dimostriamo infatti che $\mathscr{B}'$ è un insieme di generatori. Se $\mathbf{v} \in V$, sappiamo che esistono scalari $\alpha_1, \alpha_2, \dots, \alpha_n$ tali che

$$\mathbf{v} = \alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2 + \dots + \alpha_n\mathbf{v}_n$$

e quindi

$$\mathbf{v} = (\alpha_1\gamma^{-1})\mathbf{v}_1' + \alpha_2\mathbf{v}_2 + \dots + \alpha_n\mathbf{v}_n$$

cioè $\mathbf{v} \in \langle\mathscr{B}'\rangle$.

Lasciamo come esercizio la dimostrazione che $\mathscr{B}'$ è linearmente indipendente. □

Negli esempi che abbiamo illustrato abbiamo visto che basi diverse dello stesso spazio vettoriale hanno qualcosa in comune: il numero di elementi. Questo non è casuale, anzi è un fatto fondamentale della teoria degli spazi vettoriali. Il teorema che segue è dovuto a Steinitz, un suo corollario è appunto che due basi di uno stesso spazio vettoriale hanno lo stesso numero di elementi.

La dimostrazione di questo teorema è importantissima, perché usa una tecnica ingegnosa: se $\mathscr{B}$ è un insieme linearmente indipendente e $\mathscr{A}$ un insieme di generatori, entrambi nello spazio vettoriale V, allora possiamo mettere ogni vettore di $\mathscr{B}$ al posto di uno di $\mathscr{A}$ ottenendo ancora un insieme di generatori.

Ricordiamo prima due fatti. Primo: quando diciamo che un insieme finito di vettori ha n elementi, intendiamo contare anche gli elementi eventualmente ripetuti. Secondo: in un insieme linearmente indipendente non ci sono ripetizioni.

Teorema 3.7. *Sia V uno spazio vettoriale finitamente generato. Siano $\mathscr{A}$ un insieme di generatori di V e $\mathscr{B}$ un insieme linearmente indipendente di vettori di V. Se $\mathscr{A}$ ha n elementi e $\mathscr{B}$ ha m elementi, allora $m \leq n$.*

Dimostrazione. Se $\mathscr{B}$ è l'insieme vuoto, non c'è niente da dimostrare; quindi assumiamo che $m > 0$. Allora, necessariamente, $n \geq 1$: altrimenti $\mathscr{A}$ sarebbe l'insieme vuoto che genera lo spazio vettoriale nullo, nel quale non potrebbero esistere m vettori non nulli distinti (si veda 2.13).

Supponiamo perciò

$$\mathscr{B} = \{\mathbf{w}_1; \dots; \mathbf{w}_m\}, \qquad \mathscr{A} = \{\mathbf{v}_1; \dots; \mathbf{v}_n\}.$$

Procederemo per induzione, dimostrando la seguente affermazione: *Se* $0 \le k \le m$, *esiste un insieme di generatori* $\mathscr{C}_k$ *formato da* k *vettori dell'insieme* $\mathscr{B}$ *e da* $n-k$ *vettori dell'insieme* $\mathscr{A}$.

Chiaramente questo prova che $m \le n$, altrimenti non potremmo costruire l'insieme $\mathscr{C}_m$.

Il passo base, $k=0$, è ovvio: basta prendere $\mathscr{C}_0 = \mathscr{A}$. Supponiamo allora di avere a disposizione l'insieme $\mathscr{C}_k$ e che $k+1 \le m$. Non è restrittivo supporre che

$$\mathscr{C}_k = \{\mathbf{w}_1; \dots; \mathbf{w}_k; \mathbf{v}_{k+1}; \dots; \mathbf{v}_n\}$$

eventualmente riordinando gli insiemi da cui siamo partiti. Per ipotesi induttiva, $\mathscr{C}_k$ è un insieme di generatori, quindi possiamo scrivere

$$\mathbf{w}_{k+1} = \sum_{i=1}^{k} \alpha_i \mathbf{w}_i + \sum_{j=k+1}^{n} \beta_j \mathbf{v}_j. \tag{*}$$

Non è possibile che $\beta_{k+1} = \cdots = \beta_n = 0$, perché in tal caso

$$\mathbf{w}_{k+1} = \sum_{i=1}^{k} \alpha_i \mathbf{w}_i$$

e l'insieme $\mathscr{B}$ non sarebbe linearmente indipendente. Dunque possiamo supporre che $\beta_{k+1} \ne 0$, eventualmente riordinando $\mathscr{A}$. Consideriamo l'insieme

$$\mathscr{C}'_k = \{\mathbf{w}_1; \dots; \mathbf{w}_k; \mathbf{w}_{k+1}; \mathbf{v}_{k+1}; \dots; \mathbf{v}_n\}.$$

Poiché esso contiene un insieme di generatori, anche $\mathscr{C}'_k$ è un insieme di generatori. La relazione (*) si può anche scrivere

$$\mathbf{v}_{k+1} = \sum_{i=1}^{k+1} \gamma_i \mathbf{w}_i + \sum_{j=k+2}^{n} \delta_j \mathbf{v}_j$$

(si calcolino i coefficienti γ_i per esercizio) e quindi l'insieme che si ottiene eliminando da $\mathscr{C}'_k$ il vettore $\mathbf{v}_{k+1}$ è ancora un insieme di generatori (per 2.5). Chiamiamo $\mathscr{C}_{k+1}$ questo insieme, perché ha le proprietà richieste. □

La tecnica della dimostrazione è importante di per sé e quindi la isoliamo in un risultato a parte.

Teorema 3.8. *Siano* $\mathscr{A}$ *un insieme di generatori dello spazio vettoriale* V *e* $\mathscr{B}$ *un insieme linearmente indipendente di vettori di* V. *Supponiamo che* $\mathscr{A}$ *abbia* n *elementi e che* $\mathscr{B}$ *abbia* m *elementi. Allora esiste un insieme di generatori* $\mathscr{C}$ *formato da tutti i vettori di* $\mathscr{B}$ *e da* $n-m$ *vettori di* $\mathscr{A}$.

Siccome ogni spazio che consideriamo ha un insieme di generatori, possiamo usare questo per ottenere che *ogni insieme linearmente indipendente può essere completato a una base.*

Esempio 3.9. Per illustrare il risultato precedente, applichiamo la tecnica della dimostrazione del Teorema 3.7 agli insiemi $\mathscr{A} = \{\mathbf{e}_1; \mathbf{e}_2; \mathbf{e}_3; \mathbf{e}_4\}$ e $\mathscr{B} = \{\mathbf{u}; \mathbf{v}\}$ in $\mathbb{C}^4$, dove

$$\mathbf{u} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 2 \end{bmatrix}, \qquad \mathbf{v} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}.$$

Si esegue l'EG sulla matrice $[\mathbf{u}\ \mathbf{v}\ \mathbf{e}_1\ \mathbf{e}_2\ \mathbf{e}_3\ \mathbf{e}_4]$:

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 2 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & -2 & 0 & 0 & 1 \end{bmatrix}$$
$$\to \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 \\ 0 & 0 & -2 & 0 & 0 & 1 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & -1/2 \\ 0 & 0 & 0 & 1 & -1 & 0 \end{bmatrix}.$$

Le colonne dominanti sono le prime quattro e quindi l'insieme $\{\mathbf{u}; \mathbf{v}; \mathbf{e}_1; \mathbf{e}_2\}$ è linearmente indipendente, quindi una base di $\mathbb{C}^4$. Per maggiori dettagli, si veda il Teorema 5.5 a pagina 100. □

Il teorema appena dimostrato ha una conseguenza importantissima.

Teorema 3.10. *Sia V uno spazio vettoriale finitamente generato; siano $\mathscr{A}$ e $\mathscr{B}$ basi di V. Allora $\mathscr{A}$ e $\mathscr{B}$ hanno lo stesso numero di elementi.*

Dimostrazione. Sia n il numero di elementi di $\mathscr{A}$ e sia m il numero di elementi di $\mathscr{B}$.

- Siccome $\mathscr{A}$ è un insieme di generatori e $\mathscr{B}$ è linearmente indipendente, il Teorema 3.7 dice che $m \le n$.
- Siccome $\mathscr{B}$ è un insieme di generatori e $\mathscr{A}$ è linearmente indipendente, il Teorema 3.7 dice che $n \le m$.

Dunque deve essere $m = n$. □

Abbiamo già visto che ogni spazio vettoriale V finitamente generato ha una base. Ciò che abbiamo dimostrato è che due basi di V devono avere lo stesso numero di elementi. Si noti che V può avere molte basi (di fatto ne ha infinite, se non è lo spazio nullo); tuttavia due basi diverse hanno in comune il numero di elementi.

Definizione. Se V è uno spazio vettoriale finitamente generato, il numero di elementi di una sua base si indica con $\dim V$ e si chiama *dimensione* di V.

Esempi 3.11. (1) Lo spazio $\mathbb{C}^n$ ha dimensione n, perché la base canonica $\mathscr{E}$ ha n elementi.

(2) Sia $\mathbf{U}$ una matrice $m \times n$ in forma ridotta. Scriviamola come

$$\mathbf{U} = [\mathbf{u}_1 \ \mathbf{u}_2 \ \dots \ \mathbf{u}_n]$$

e consideriamo $V = \langle \mathbf{u}_1; \mathbf{u}_2; \dots; \mathbf{u}_n \rangle$, che è un sottospazio di $\mathbb{C}^n$. Per quanto visto nell'Esempio 2.16, l'insieme delle colonne dominanti è linearmente indipendente. Ogni altra colonna è combinazione lineare delle colonne dominanti che la precedono, come indica l'Esempio 2.6 (si veda anche l'Esercizio 2.10) e pertanto le colonne dominanti formano una base di V. Quindi, se k è il numero delle colonne dominanti (che è uguale al numero di righe non nulle), $\dim V = k$.

(3) Lo spazio $\{\mathbf{0}\}$ ha dimensione 0; una sua base è l'insieme vuoto. □

Per calcolare la dimensione di uno spazio vettoriale dobbiamo contare gli elementi di una sua base. In certe situazioni non è facile determinare una base, perciò ci si accontenta di maggiorare o minorare la dimensione tramite il numero di elementi di un insieme di generatori (Teorema 3.13) o di un insieme linearmente indipendente (Teorema 3.14) rispettivamente.

Cominciamo con un lemma che dimostra un fatto intuitivamente chiaro, ma che non è del tutto ovvio, come si vedrà.

Lemma 3.12. *Se V è uno spazio vettoriale finitamente generato e U è un sottospazio di V, allora U è finitamente generato e* $\dim U \le \dim V$.

Dimostrazione. Procederemo per assurdo, assumendo quindi che U non sia finitamente generato: ciò significa che nessun insieme di vettori di U è un insieme di generatori. In particolare $U \neq \{\mathbf{0}\}$, perché altrimenti l'insieme vuoto sarebbe un insieme di generatori. Dunque esiste $\mathbf{u}_1 \in U$, $\mathbf{u}_1 \neq \mathbf{0}$.

L'insieme $\mathscr{A}_1 = \{\mathbf{u}_1\}$ non genera U, quindi esiste un vettore $\mathbf{u}_2 \in U$ tale che $\mathbf{u}_2 \notin \langle \mathscr{A}_1 \rangle$. Ma allora (si veda 2.15) l'insieme $\mathscr{A}_2 = \{\mathbf{u}_1; \mathbf{u}_2\}$ è linearmente indipendente.

Possiamo andare avanti per induzione allo stesso modo: se abbiamo ottenuto l'insieme linearmente indipendente $\mathscr{A}_k$ in U, questo non genera e quindi, prendendo

$$\mathbf{u}_{k+1} \in U \setminus \langle \mathscr{A}_k \rangle$$

l'insieme $\mathscr{A}_{k+1} = \mathscr{A}_k \sqcup \{\mathbf{u}_{k+1}\}$ è linearmente indipendente.

Lo spazio V abbia dimensione n: allora esiste un insieme di generatori di lunghezza n. Ma abbiamo costruito con il procedimento induttivo l'insieme $\mathscr{A}_{n+1}$ che è linearmente indipendente in U, quindi anche in V. Questo contraddice il Teorema 3.7.

Dunque U è finitamente generato e perciò ha una base che avrà m elementi, con $m \le \dim V$, sempre per il Teorema 3.7. □

Teorema 3.13. *Sia V uno spazio vettoriale finitamente generato. Allora* $\dim V$ *è il numero minimo di elementi di un insieme di generatori di V.*

Dimostrazione. Sia $\mathscr{A}$ un insieme di generatori con numero minimo n di elementi. Ciò significa che ogni altro insieme di generatori ha numero di elementi $\ge n$. Se $\mathscr{A}$ non è linearmente indipendente, possiamo ottenerne un insieme di generatori togliendo un vettore (Proposizione 2.5). Assurdo. □

Teorema 3.14. *Sia V uno spazio vettoriale finitamente generato. Allora* $\dim V$ *è il numero massimo di elementi di un insieme linearmente indipendente in V.*

Dimostrazione. Il numero massimo di elementi esiste, perché un insieme linearmente indipendente ha al più tanti elementi quanti un insieme di generatori (Teorema 3.7). Se $\mathscr{A}$ è un insieme linearmente indipendente con numero massimo di vettori e $\langle\mathscr{A}\rangle \neq V$, potremmo aggiungere ad $\mathscr{A}$ un vettore ottenendo ancora un insieme linearmente indipendente (si veda il Teorema 2.15). Assurdo. □

Teorema 3.15. *Se* $\dim V = n$ *e* $\mathscr{A}$ *è un insieme linearmente indipendente di vettori di V con n elementi, allora $\mathscr{A}$ è una base di V.*

Dimostrazione. Se $\mathscr{A}$ non fosse una base di V, il Teorema 3.8 ci permetterebbe di completarla a una base che avrebbe $m > n$ elementi. Assurdo. □

Come conseguenza di questo fatto otteniamo una tecnica per dimostrare che un sottospazio U di V coincide con V: infatti $U = V$ se e solo se $\dim U = \dim V$. Infatti un'implicazione è ovvia. Se invece $\dim U = \dim V$, troviamo in U una base il cui numero di elementi è uguale al numero massimo di elementi di un insieme linearmente indipendente in V. Essa perciò è una base di V e ogni vettore di V è combinazione lineare di vettori di U, quindi appartiene a U.

Introduciamo ora uno spazio vettoriale che viene associato a una generica matrice complessa; tale spazio è uno dei quattro cosiddetti “sottospazi fondamentali” della matrice, che saranno esaminati più in dettaglio nel Paragrafo 5.

Sia $\mathbf{A}$ una matrice $m \times n$, $\mathbf{A} = [\mathbf{v}_1 \ \dots \ \mathbf{v}_n]$. Definiamo

$$\mathrm{C}(\mathbf{A}) = \langle \mathbf{v}_1; \mathbf{v}_2; \dots; \mathbf{v}_n \rangle$$

che chiameremo *spazio delle colonne* di $\mathbf{A}$; è un sottospazio di $\mathbb{C}^m$ e quindi $\dim \mathrm{C}(\mathbf{A}) \leq m$. Inoltre $\mathrm{C}(\mathbf{A})$ ha un insieme di generatori con n elementi, quindi $\dim \mathrm{C}(\mathbf{A}) \leq n$.

Esempio 3.16. Applichiamo i due Teoremi appena visti per vedere se i tre vettori di $\mathbb{C}^3$

$$\mathbf{v}_1 = \begin{bmatrix} 2 \\ 1 \\ 5 \end{bmatrix}, \quad \mathbf{v}_2 = \begin{bmatrix} 1 \\ -2 \\ 0 \end{bmatrix}, \quad \mathbf{v}_3 = \begin{bmatrix} 3 \\ 0 \\ 2 \end{bmatrix}$$

formano una base di $\mathbb{C}^3$.

Impiegando il Teorema 3.13, si tratta di vedere se l'insieme $\{\mathbf{v}_1; \mathbf{v}_2; \mathbf{v}_3\}$ genera $\mathbb{C}^3$; in altre parole, preso un generico vettore $\mathbf{v} = [a \ b \ c]^T \in \mathbb{C}^3$, bisogna trovare tre scalari $x_1, x_2, x_3 \in \mathbb{C}$ tali che

$$x_1\mathbf{v}_1 + x_2\mathbf{v}_2 + x_3\mathbf{v}_3 = \mathbf{v};$$

in definitiva, bisogna vedere se ha soluzioni il sistema $\mathbf{Ax} = \mathbf{v}$, dove $\mathbf{x} = [x_1 \ x_2 \ x_3]^T$ e $\mathbf{A} = [\mathbf{v}_1 \ \mathbf{v}_2 \ \mathbf{v}_3]$.

Impiegando il Teorema 3.14 occorre invece vedere se l'insieme $\{\mathbf{v}_1; \mathbf{v}_2; \mathbf{v}_3\}$ è linearmente indipendente, il che equivale al fatto che il sistema $\mathbf{Ax} = \mathbf{0}$ abbia unicamente la soluzione nulla.

Il Teorema 4.15 del Capitolo 1 dice che ciascuno dei fatti precedenti è equivalente all'invertibilità della matrice **A**. □

Nel caso **A** sia in forma ridotta, sappiamo calcolare la dimensione di C(**A**) (si veda l'Esempio 3.11 (2)): è precisamente il numero di colonne dominanti. Per il caso generale avremo bisogno di un concetto più astratto, che è quello di applicazione lineare che vedremo nel Paragrafo seguente.

Esiste anche un concetto leggermente più generale di indipendenza lineare che ci sarà utile in futuro e che riguarda non già gli insiemi di elementi, bensì i sottospazi.

Supponiamo che U_1 e U_2 siano sottospazi di V. Possiamo definire altri due sottospazi: il primo è $U_1 \cap U_2$, il secondo è

$$U_1 + U_2 = \{\mathbf{u}_1 + \mathbf{u}_2 \mid \mathbf{u}_1 \in U_1, \mathbf{u}_2 \in U_2\}.$$

Si verifichi, per esercizio, che $U_1 + U_2$ è un sottospazio. È chiaro che si tratta del più piccolo sottospazio di V che contiene sia U_1 che U_2, così come $U_1 \cap U_2$ è il più grande sottospazio contenuto in entrambi.

Proposizione 3.17. *Se U_1 e U_2 sono sottospazi di V, allora*

$$\dim(U_1 + U_2) = \dim U_1 + \dim U_2 - \dim(U_1 \cap U_2).$$

Dimostrazione. Sia $\mathscr{B} = \{\mathbf{u}_1; \dots; \mathbf{u}_k\}$ una base di $U_1 \cap U_2$. Possiamo estendere $\mathscr{B}$ a una base

$$\mathscr{B}' = \{\mathbf{u}_1; \dots; \mathbf{u}_k; \mathbf{v}_{k+1}; \dots; \mathbf{v}_m\}$$

di U_1 e a una base

$$\mathscr{B}'' = \{\mathbf{u}_1; \dots; \mathbf{u}_k; \mathbf{w}_{k+1}; \dots; \mathbf{w}_n\}$$

di U_2. Consideriamo allora

$$\mathscr{C} = \{\mathbf{u}_1; \dots; \mathbf{u}_k; \mathbf{v}_{k+1}; \dots; \mathbf{v}_m; \mathbf{w}_{k+1}; \dots; \mathbf{w}_n\}$$

e verifichiamo che $\mathscr{C}$ è una base di $U_1 + U_2$.

Se $\mathbf{x} \in U_1$, abbiamo

$$\mathbf{x} = \alpha_1 \mathbf{u}_1 + \dots + \alpha_k \mathbf{u}_k + \gamma_{k+1} \mathbf{v}_{k+1} + \dots + \gamma_m \mathbf{v}_m.$$

Se $\mathbf{y} \in U_2$, abbiamo

$$\mathbf{y} = \beta_1 \mathbf{u}_1 + \dots + \beta_k \mathbf{u}_k + \delta_{k+1} \mathbf{w}_{k+1} + \dots + \delta_n \mathbf{w}_n.$$

Allora

$$\mathbf{x} + \mathbf{y} = (\alpha_1 + \beta_1)\mathbf{u}_1 + \dots + (\alpha_k + \beta_k)\mathbf{u}_k + \gamma_{k+1}\mathbf{v}_{k+1} + \dots + \gamma_m \mathbf{v}_m + \delta_{k+1}\mathbf{w}_{k+1} + \dots + \delta_n \mathbf{w}_n$$

e quindi $\mathscr{C}$ è un insieme di generatori di $U_1 + U_2$.

Supponiamo ora che

$$\alpha_1\mathbf{u}_1+\cdots+\alpha_k\mathbf{u}_k+\gamma_{k+1}\mathbf{v}_{k+1}+\cdots+\gamma_m\mathbf{v}_m+\delta_{k+1}\mathbf{w}_{k+1}+\cdots+\delta_n\mathbf{w}_n=\mathbf{0}.$$

Allora

$$\mathbf{x}=\alpha_1\mathbf{u}_1+\cdots+\alpha_k\mathbf{u}_k+\gamma_{k+1}\mathbf{v}_{k+1}+\cdots+\gamma_m\mathbf{v}_m=-(\delta_{k+1}\mathbf{w}_{k+1}+\cdots+\delta_n\mathbf{w}_n)\in U_1\cap U_2.$$

Perciò $\mathbf{x}=\beta_1\mathbf{u}_1+\cdots+\beta_k\mathbf{u}_k$ e quindi

$$(\alpha_1-\beta_1)\mathbf{u}_1+\cdots+(\alpha_k-\beta_k)\mathbf{u}_k+\gamma_{k+1}\mathbf{v}_{k+1}+\cdots+\gamma_m\mathbf{v}_m=\mathbf{0}$$

da cui $\gamma_{k+1}=\cdots=\gamma_m=0$ perché $\mathscr{B}'$ è linearmente indipendente. Analogamente $\delta_{k+1}=\cdots=\delta_n=0$. Ma allora

$$\alpha_1\mathbf{u}_1+\cdots+\alpha_k\mathbf{u}_k=\mathbf{0}$$

e $\alpha_1=\cdots=\alpha_k=0$. □

Nel caso particolare in cui $U_1\cap U_2=\{\mathbf{0}\}$, scriveremo $U_1+U_2=U_1\oplus U_2$ e parleremo di *somma diretta di sottospazi.*

Proposizione 3.18. *Siano U_1 e U_2 sottospazi di V. Le seguenti affermazioni sono equivalenti:*

(1) $U_1+U_2=U_1\oplus U_2$*;*

(2) *ogni elemento di U_1+U_2 si scrive in modo unico come somma di un elemento di U_1 e un elemento di U_2;*

(3) *se $\mathbf{u}_1\in U_1$, $\mathbf{u}_2\in U_2$ e $\mathbf{u}_1+\mathbf{u}_2=\mathbf{0}$, allora $\mathbf{u}_1=\mathbf{0}$ e $\mathbf{u}_2=\mathbf{0}$.*

Dimostrazione. (1) $\Longrightarrow$ (2) Se $\mathbf{x}+\mathbf{y}=\mathbf{x}'+\mathbf{y}'$, con $\mathbf{x},\mathbf{x}'\in U_1$ e $\mathbf{y},\mathbf{y}'\in U_2$, allora

$$\mathbf{x}-\mathbf{x}'=\mathbf{y}'-\mathbf{y}\in U_1\cap U_2.$$

Per ipotesi $U_1\cap U_2=\{\mathbf{0}\}$, quindi $\mathbf{x}=\mathbf{x}'$ e $\mathbf{y}=\mathbf{y}'$.

(2) $\Longrightarrow$ (3) Evidente, perché $\mathbf{0}=\mathbf{u}_1+\mathbf{u}_2=\mathbf{0}+\mathbf{0}$.

(3) $\Longrightarrow$ (1) Se $\mathbf{v}\in U_1\cap U_2$, allora $\mathbf{0}=\mathbf{v}+(-\mathbf{v})$. Ma $\mathbf{v}\in U_1$ e $-\mathbf{v}\in U_2$, quindi $\mathbf{v}=-\mathbf{v}=\mathbf{0}$. □

Più in generale diremo che i sottospazi U_1, U_2, …, U_k di V sono *indipendenti* se, da $\mathbf{u}_i\in U_i$ $(i=1,2,\dots,k)$ e $\mathbf{u}_1+\mathbf{u}_2+\cdots+\mathbf{u}_k=\mathbf{0}$ segue $\mathbf{u}_1=\mathbf{u}_2=\cdots=\mathbf{u}_k=\mathbf{0}$.

Per esempio, se $\mathscr{B}=\{\mathbf{v}_1;\dots;\mathbf{v}_k\}$ è un insieme linearmente indipendente, allora i sottospazi $\langle\mathbf{v}_1\rangle$, …, $\langle\mathbf{v}_k\rangle$ sono indipendenti.

Enunciamo, lasciando la dimostrazione per esercizio, il seguente risultato. Prima però osserviamo che la definizione di somma di due sottospazi si estende facilmente a un numero qualunque di essi.

Proposizione 3.19. *Se i sottospazi U_1, U_2, …, U_k di V sono indipendenti, allora*

$$\dim(U_1+U_2+\cdots+U_k)=\dim U_1+\dim U_2+\cdots+\dim U_k.$$

In tal caso, se $\mathscr{B}_1$, $\mathscr{B}_2$, …, $\mathscr{B}_k$ sono basi di U_1, U_2, …, U_k rispettivamente, allora $\mathscr{B}_1\sqcup\mathscr{B}_2\sqcup\cdots\sqcup\mathscr{B}_k$ è una base di $U_1+U_2+\cdots+U_k$. □

4. Applicazioni lineari

Una tecnica fondamentale in algebra è di confrontare fra loro due strutture diverse: nel nostro caso trattiamo di spazi vettoriali. Per il confronto si impiegano applicazioni; "applicazione" è praticamente sinonimo di funzione, ma per evitare equivoci useremo questo termine.

Definizione. Siano V e W spazi vettoriali e sia $f\colon V \to W$ un'applicazione di dominio V e codominio W. Diremo che f è un'*applicazione lineare* se

(L_1) per ogni $\mathbf{v}_1, \mathbf{v}_2 \in V$,
$$f(\mathbf{v}_1 + \mathbf{v}_2) = f(\mathbf{v}_1) + f(\mathbf{v}_2);$$
(L_2) per ogni $\mathbf{v} \in V$ e ogni scalare α,
$$f(\alpha\mathbf{v}) = \alpha f(\mathbf{v}).$$

Notiamo che nelle formule della definizione si usano, a sinistra del segno di uguaglianza, le operazioni in V e, a destra, le operazioni di W.

Esempi 4.1. (1) Se λ è uno scalare, l'applicazione $V \to V$ definita da $\mathbf{v} \mapsto \lambda\mathbf{v}$ è lineare.

(2) Se $f\colon V \to W$ è un'applicazione lineare e U è un sottospazio di V, allora l'applicazione $f|U\colon U \to W$ definita tramite $\mathbf{u} \mapsto f(\mathbf{u})$ è lineare. Si chiama *restrizione* di f al sottospazio U.

(3) Scegliamo $1 \le i_1 < i_2 < \dots < i_d \le n$ e per un vettore $\mathbf{v} = [\alpha_1\ \alpha_2\ \dots\ \alpha_n]^T \in \mathbb{C}^n$ poniamo
$$f(\mathbf{v}) = \begin{bmatrix} \alpha_{i_1} \\ \alpha_{i_2} \\ \vdots \\ \alpha_{i_d} \end{bmatrix}.$$
L'applicazione $f\colon \mathbb{C}^n \to \mathbb{C}^d$ così ottenuta è lineare. Possiamo chiamarla *scelta delle componenti* $i_1, i_2, \dots, i_d$.

(4) L'applicazione $f\colon V \to W$ definita ponendo $f(\mathbf{v}) = \mathbf{0}$, per ogni $\mathbf{v} \in V$ è lineare e si chiama *applicazione nulla.* □

Elenchiamo alcune semplici conseguenze della definizione.

Proposizione 4.2. *Se $f\colon V \to W$ è un'applicazione lineare, allora $f(\mathbf{0}) = \mathbf{0}$.*

Dimostrazione. Poniamo $\mathbf{w} = f(\mathbf{0})$. Siccome $\mathbf{0} = \mathbf{0} + \mathbf{0}$ (stiamo usando il vettore nullo di V), abbiamo per la (L1)
$$\mathbf{w} = f(\mathbf{0}) = f(\mathbf{0} + \mathbf{0}) = f(\mathbf{0}) + f(\mathbf{0}) = \mathbf{w} + \mathbf{w}$$
da cui $\mathbf{w} = \mathbf{0}$ (il vettore nullo di W). □

Come per i sottospazi, esiste un modo "breve" per verificare che un'applicazione è lineare.

Proposizione 4.3. *Siano V e W spazi vettoriali e sia $f\colon V \to W$ un'applicazione di dominio V e codominio W. Allora f è lineare se e solo se, per ogni $\mathbf{v}_1, \mathbf{v}_2 \in V$ e per gli scalari α_1, α_2,*

$$f(\alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2) = \alpha_1 f(\mathbf{v}_1) + \alpha_2 f(\mathbf{v}_2).$$

Dimostrazione. Se f è lineare, basta applicare le condizioni (L_1) e (L_2). Supponiamo che per f valga la condizione data. Se prendiamo $\alpha_1 = \alpha_2 = 1$, abbiamo

$$f(\mathbf{v}_1 + \mathbf{v}_2) = f(1\mathbf{v}_1 + 1\mathbf{v}_2) = 1f(\mathbf{v}_1) + 1f(\mathbf{v}_2) = f(\mathbf{v}_1) + f(\mathbf{v}_2)$$

che è la (L_1). Se prendiamo $\mathbf{v}_1 = \mathbf{v}$, $\mathbf{v}_2 = \mathbf{0}$, $\alpha_1 = \alpha$ e $\alpha_2 = 0$, abbiamo

$$f(\alpha\mathbf{v}) = f(\alpha\mathbf{v} + 0\mathbf{0}) = \alpha f(\mathbf{v}) + 0f(\mathbf{0}) = \alpha f(\mathbf{v})$$

che è la (L_2). □

Con una semplice induzione si dimostra il corollario seguente che useremo spesso in futuro.

Corollario 4.4. *Sia $f\colon V \to W$ un'applicazione lineare tra spazi vettoriali; siano $\mathbf{v}_i \in V$ e α_i scalari ($i = 1, \dots, n$). Allora*

$$f(\alpha_1\mathbf{v}_1 + \dots + \alpha_n\mathbf{v}_n) = \alpha_1 f(\mathbf{v}_1) + \dots + \alpha_n f(\mathbf{v}_n).$$

Esempio 4.5. Sia $\mathbf{A}$ una matrice $m \times n$. Dato $\mathbf{v} \in \mathbb{C}^n$ possiamo considerare $\mathbf{A}\mathbf{v} \in \mathbb{C}^m$; quindi possiamo definire un'applicazione

$$\begin{aligned} f_{\mathbf{A}}\colon \mathbb{C}^n &\to \mathbb{C}^m \\ \mathbf{v} &\mapsto \mathbf{A}\mathbf{v} \end{aligned}$$

che è lineare. Questo segue facilmente dalle proprietà del prodotto di matrici. L'applicazione $f_{\mathbf{A}}$ si dice *indotta da* $\mathbf{A}$. □

Questo esempio è fondamentale. Vedremo più avanti che, in un certo senso, ogni applicazione lineare tra spazi vettoriali di dimensione finita è di questo tipo. Renderemo precisa questa affermazione quando parleremo di coordinate.

Possiamo naturalmente considerare applicazioni lineari anche fra spazi vettoriali reali, con le analoghe definizioni. Ne diamo due esempi.

Esempi 4.6. (1) Se $\mathbf{A}$ è la matrice

$$\mathbf{A} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

allora $f_{\mathbf{A}}\colon \mathbb{R}^2 \to \mathbb{R}^2$ è l'applicazione lineare

$$\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \mapsto f_{\mathbf{A}}(\mathbf{x}) = \mathbf{A}\mathbf{x} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} x_2 \\ x_1 \end{bmatrix}.$$

(2) Se $\mathbf{B}$ è la matrice
$$\mathbf{B} = \begin{bmatrix} \cos\alpha & -\operatorname{sen}\alpha \\ \operatorname{sen}\alpha & \cos\alpha \end{bmatrix}$$
allora
$$f_{\mathbf{B}}\left(\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}\right) = \begin{bmatrix} x_1\cos\alpha - x_2\operatorname{sen}\alpha \\ x_1\operatorname{sen}\alpha + x_2\cos\alpha \end{bmatrix}. \qquad \square$$

Talvolta è utile considerare più applicazioni lineari; la composizione di due, qualora sia definita, è ancora lineare.

Proposizione 4.7. *Siano U, V e W spazi vettoriali; siano $f\colon U \to V$ e $g\colon V \to W$ applicazioni lineari. Allora $g \circ f\colon U \to W$ è un'applicazione lineare.*

Dimostrazione. Basta eseguire le verifiche. Abbiamo
$$\begin{aligned} g \circ f(\mathbf{u}_1 + \mathbf{u}_2) &= g(f(\mathbf{u}_1 + \mathbf{u}_2)) = g(f(\mathbf{u}_1) + f(\mathbf{u}_2)) \\ &= g(f(\mathbf{u}_1)) + g(f(\mathbf{u}_2)) = g \circ f(\mathbf{u}_1) + g \circ f(\mathbf{u}_2) \end{aligned}$$
e questo prova la (L_1). Analogamente
$$g \circ f(\alpha\mathbf{u}) = g(f(\alpha\mathbf{u})) = g(\alpha f(\mathbf{u})) = \alpha(g(f(\mathbf{u}))) = \alpha(g \circ f(\mathbf{u}))$$
prova la (L_2). $\square$

Esempio 4.8. Per essere in questa situazione quando si hanno applicazioni indotte da matrici, consideriamo una matrice $\mathbf{A}$ che sia $m \times n$ e una matrice $\mathbf{B}$ che sia $n \times p$. Le applicazioni indotte sono
$$f_{\mathbf{A}}\colon \mathbb{C}^n \to \mathbb{C}^m, \qquad f_{\mathbf{B}}\colon \mathbb{C}^p \to \mathbb{C}^n.$$
La composizione $f_{\mathbf{A}} \circ f_{\mathbf{B}}$ ha senso ed è lineare. Questo si vede anche direttamente perché, per $\mathbf{v} \in \mathbb{C}^p$,
$$f_{\mathbf{A}} \circ f_{\mathbf{B}}(\mathbf{v}) = f_{\mathbf{A}}(f_{\mathbf{B}}(\mathbf{v})) = f_{\mathbf{A}}(\mathbf{B}\mathbf{v}) = \mathbf{A}(\mathbf{B}\mathbf{v}) = (\mathbf{A}\mathbf{B})\mathbf{v} = f_{\mathbf{A}\mathbf{B}}(\mathbf{v}).$$
Dunque, nel caso di applicazioni lineari indotte da matrici, la composizione corrisponde al prodotto di matrici. Questo è la motivazione profonda della definizione di prodotto di matrici che abbiamo usato. $\square$

Ogni applicazione lineare definisce un sottospazio del dominio e un sottospazio del codominio.

Definizione. Se $f\colon V \to W$ è un'applicazione lineare tra spazi vettoriali, allora
$$\mathrm{N}(f) = \{\mathbf{v} \in V \mid f(\mathbf{v}) = \mathbf{0}\}$$
è un sottospazio di V, detto *spazio nullo di f*. Analogamente
$$\mathrm{Im}(f) = \{f(\mathbf{v}) \mid \mathbf{v} \in V\}$$
è un sottospazio di W, detto *immagine di f*.

Esempi 4.9. (1) Consideriamo l'applicazione lineare definita nell'esempio 4.1 (3) di scelta delle componenti. Per fissare le idee, consideriamo la scelta della seconda, terza e quinta componente in $\mathbb{C}^5$, quindi l'applicazione lineare $f\colon \mathbb{C}^5 \to \mathbb{C}^3$ definita da

$$f\left(\begin{bmatrix}\alpha_1\\ \alpha_2\\ \alpha_3\\ \alpha_4\\ \alpha_5\end{bmatrix}\right) = \begin{bmatrix}\alpha_2\\ \alpha_3\\ \alpha_5\end{bmatrix}.$$

Lo spazio nullo $\mathrm{N}(f)$ è:

$$\mathrm{N}(f) = \{\,[\alpha_1\ 0\ 0\ \alpha_4\ 0]^T \mid \alpha_1, \alpha_4 \in \mathbb{C}\} = \langle \mathbf{e}_1; \mathbf{e}_4 \rangle.$$

L'immagine, come si verifica facilmente, è: $\mathrm{Im}(f) = \mathbb{C}^3$.

(2) Sia $f\colon \mathbb{R}^3 \to \mathbb{R}^2$ l'applicazione lineare definita da:

$$f\left(\begin{bmatrix}x_1\\ x_2\\ x_3\end{bmatrix}\right) = \begin{bmatrix}x_1 + 2x_2 - x_3\\ -2x_1 - 4x_2 + 2x_3\end{bmatrix}.$$

Poniamo $\mathbf{w} = [1\ {-2}]^T$: allora ogni elemento di $\mathrm{Im}(f)$ è un multiplo scalare di $\mathbf{w}$, perché

$$\begin{bmatrix}x_1 + 2x_2 - x_3\\ -2x_1 - 4x_2 + 2x_3\end{bmatrix} = (x_1 + 2x_2 - x_3)\begin{bmatrix}1\\ -2\end{bmatrix}.$$

Inoltre $\mathbf{w} = f(\mathbf{e}_1)$, quindi $\mathrm{Im}(f) = \langle \mathbf{w} \rangle$.

Un vettore $\mathbf{v} = [\alpha_1\ \alpha_2\ \alpha_3]^T$ appartiene a $\mathrm{N}(f)$ se e solo se $\alpha_1 + 2\alpha_2 - \alpha_3 = 0$. □

Ovviamente va dimostrato che $\mathrm{N}(f)$ è un sottospazio di V e che $\mathrm{Im}(f)$ è un sottospazio di W.

Siano $\mathbf{v}_1, \mathbf{v}_2 \in \mathrm{N}(f)$ e siano α_1 e α_2 scalari. Allora

$$f(\alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2) = \alpha_1 f(\mathbf{v}_1) + \alpha_2 f(\mathbf{v}_2) = \alpha_1\mathbf{0} + \alpha_2\mathbf{0} = \mathbf{0},$$

dunque $\alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2 \in \mathrm{N}(f)$. Abbiamo già mostrato che $\mathbf{0} \in \mathrm{N}(f)$, infatti $f(\mathbf{0}) = \mathbf{0}$.

È poi ovvio che $\mathrm{Im}(f)$ non sia vuota; siano $\mathbf{w}_1, \mathbf{w}_2 \in \mathrm{Im}(f)$ e siano α_1 e α_2 scalari. Allora, per definizione, possiamo scrivere $\mathbf{w}_1 = f(\mathbf{v}_1)$ e $\mathbf{w}_2 = f(\mathbf{v}_2)$ per opportuni $\mathbf{v}_1, \mathbf{v}_2 \in V$. Dunque

$$\alpha_1\mathbf{w}_1 + \alpha_2\mathbf{w}_2 = \alpha_1 f(\mathbf{v}_1) + \alpha_2 f(\mathbf{v}_2) = f(\alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2) \in \mathrm{Im}(f).$$

Notiamo che, per dimostrare che $\mathbf{w} \in \mathrm{Im}(f)$, basta riuscire a scrivere $\mathbf{w} = f(\mathbf{v})$ per un $\mathbf{v} \in V$.

È particolarmente importante il caso in cui $\mathrm{N}(f) = \{\mathbf{0}\}$.

Proposizione 4.10. *Un'applicazione lineare $f\colon V \to W$ è iniettiva se e solo se* $\mathrm{N}(f) = \{\mathbf{0}\}$.

Dimostrazione. Supponiamo che f sia iniettiva e sia $\mathbf{v} \in \mathrm{N}(f)$. Allora $f(\mathbf{v}) = \mathbf{0} = f(\mathbf{0})$ e quindi $\mathbf{v} = \mathbf{0}$, cioè l'unico elemento di $\mathrm{N}(f)$ è il vettore nullo.

Viceversa, supponiamo che $\mathrm{N}(f) = \{\mathbf{0}\}$ e supponiamo che $f(\mathbf{v}_1) = f(\mathbf{v}_2)$. Allora

$$\mathbf{0} = f(\mathbf{v}_1) - f(\mathbf{v}_2) = f(\mathbf{v}_1 - \mathbf{v}_2)$$

cioè $\mathbf{v}_1 - \mathbf{v}_2 \in \mathrm{N}(f)$. Per ipotesi, allora, $\mathbf{v}_1 - \mathbf{v}_2 = \mathbf{0}$, quindi $\mathbf{v}_1 = \mathbf{v}_2$ e f è iniettiva. □

Data un'applicazione lineare $f : V \to W$ e un insieme finito $\mathscr{A}$ di vettori in V possiamo considerare l'insieme $f[\mathscr{A}]$ ottenuto valutando f nei vettori di $\mathscr{A}$. Più esplicitamente, se $\mathscr{A} = \{\mathbf{v}_1; \mathbf{v}_2; \dots; \mathbf{v}_n\}$, poniamo

$$f[\mathscr{A}] = \{f(\mathbf{v}_1); f(\mathbf{v}_2); \dots; f(\mathbf{v}_n)\}.$$

Per convenzione associamo all'insieme vuoto l'insieme vuoto: $f[\{\}] = \{\}$.

Proposizione 4.11. *Sia $f : V \to W$ un'applicazione lineare e sia $\mathscr{A}$ un insieme finito di vettori di V.*

(1) *Se $f[\mathscr{A}]$ è linearmente indipendente, allora $\mathscr{A}$ è linearmente indipendente.*
(2) *Se f è iniettiva e $\mathscr{A}$ è linearmente indipendente, allora $f[\mathscr{A}]$ è linearmente indipendente.*

Dimostrazione. Entrambi i casi sono ovvi se $\mathscr{A}$ è vuoto. Se non è vuoto, scriviamo $\mathscr{A} = \{\mathbf{v}_1; \dots; \mathbf{v}_n\}$.

(1) Supponiamo che $f[\mathscr{A}]$ sia linearmente indipendente e sia

$$\sum_{i=1}^{n} \alpha_i \mathbf{v}_i = \mathbf{0};$$

abbiamo, in W,

$$\mathbf{0} = f(\mathbf{0}) = f\Big(\sum_{i=1}^{n} \alpha_i \mathbf{v}_i\Big) = \sum_{i=1}^{n} \alpha_i f(\mathbf{v}_i)$$

e, per l'ipotesi che $f[\mathscr{A}]$ è linearmente indipendente, $\alpha_1 = \dots = \alpha_n = 0$.

(2) Supponiamo di avere

$$\mathbf{0} = \sum_{i=1}^{n} \alpha_i f(\mathbf{v}_i).$$

Allora

$$\mathbf{0} = \sum_{i=1}^{n} \alpha_i f(\mathbf{v}_i) = f\Big(\sum_{i=1}^{n} \alpha_i \mathbf{v}_i\Big)$$

e quindi $\sum_{i=1}^{n} \alpha_i \mathbf{v}_i \in \mathrm{N}(f)$. Per ipotesi allora $\sum_{i=1}^{n} \alpha_i \mathbf{v}_i = \mathbf{0}$ e dunque $\alpha_1 = \dots = \alpha_n = 0$. □

Ci riferiremo al teorema seguente con il nome di *nullità + rango*. Se $f : V \to W$ è lineare e V ha dimensione finita, diremo *nullità di f* la dimensione di $\mathrm{N}(f)$ e *rango di f* la dimensione di $\mathrm{Im}(f)$.

Teorema 4.12 (Nullità + rango)**.** *Sia $f\colon V \to W$ un'applicazione lineare tra spazi vettoriali e supponiamo che V sia finitamente generato. Allora* $\mathrm{Im}(f)$ *è finitamente generato e*

$$\dim V = \dim \mathrm{N}(f) + \dim \mathrm{Im}(f).$$

Dimostrazione. Sia $\mathscr{A} = \{\mathbf{v}_1;\dots;\mathbf{v}_n\}$ un insieme di generatori di V (nel caso in cui $\mathscr{A}$ sia l'insieme vuoto il teorema è di facile verifica). Poniamo $\mathbf{w}_i = f(\mathbf{v}_i)$ $(i = 1,\dots,n)$. Se $\mathbf{w} \in \mathrm{Im}(f)$, esiste $\mathbf{v} \in V$ tale che $\mathbf{w} = f(\mathbf{v})$. Ora $\mathbf{v}$ si può scrivere come combinazione lineare dei vettori di $\mathscr{A}$:

$$\mathbf{v} = \sum_{i=1}^{n} \alpha_i \mathbf{v}_i.$$

Per il Corollario 4.4, abbiamo:

$$\mathbf{w} = f(\mathbf{v}) = f\Bigl(\sum_{i=1}^{n} \alpha_i \mathbf{v}_i\Bigr) = \sum_{i=1}^{n} \alpha_i f(\mathbf{v}_i) = \sum_{i=1}^{n} \alpha_i \mathbf{w}_i$$

e dunque $f[\mathscr{A}] = \{\mathbf{w}_1;\dots;\mathbf{w}_n\}$ è un insieme di generatori di $\mathrm{Im}(f)$ che quindi è finitamente generato.

Completiamo la dimostrazione facendo vedere che, se $\dim \mathrm{N}(f) = n$ e $\dim \mathrm{Im}(f) = k$, allora V ha una base con $n+k$ elementi. Le notazioni del seguito non hanno nessuna relazione con le precedenti.

Se $\dim \mathrm{Im}(f) = 0$, allora $\mathrm{Im}(f) = \{\mathbf{0}\}$ e quindi $\mathrm{N}(f) = V$. La relazione da dimostrare è, in questo caso, valida.

Sia $\{\mathbf{w}_1;\dots;\mathbf{w}_k\}$ una base di $\mathrm{Im}(f)$. Possiamo allora scrivere $\mathbf{w}_i = f(\mathbf{v}_i)$ $(i = 1,\dots,k)$ per opportuni vettori di V e poniamo $\mathscr{B} = \{\mathbf{v}_1;\dots;\mathbf{v}_k\}$. Fissiamo anche una base $\mathscr{A}$ di $\mathrm{N}(f)$.

Sistemiamo il caso in cui $\mathscr{A}$ è vuota, cioè $\mathrm{N}(f) = \{\mathbf{0}\}$, quindi f è iniettiva. Per 4.10, $\dim V \le k$ perché insiemi linearmente indipendenti vanno in insiemi linearmente indipendenti. Ora l'insieme $\mathscr{B}$ è linearmente indipendente, per 4.4, perciò $k \le \dim V$. In definitiva $\dim V = k$.

Possiamo perciò supporre che $\mathscr{A}$ non sia vuoto: $\mathscr{A} = \{\mathbf{u}_1;\dots;\mathbf{u}_n\}$. Dimostreremo che $\mathscr{C} = \mathscr{A} \sqcup \mathscr{B}$ è una base di V.

L'insieme $\mathscr{C}$ è un insieme di generatori di V. Sia $\mathbf{v} \in V$. Siccome $f(\mathbf{v}) \in \mathrm{Im}(f)$, abbiamo

$$f(\mathbf{v}) = \sum_{j=1}^{k} \beta_j \mathbf{w}_j.$$

Consideriamo il vettore

$$\mathbf{v}' = \sum_{j=1}^{k} \beta_j \mathbf{v}_j.$$

In generale non potremo aspettarci che $\mathbf{v}' = \mathbf{v}$. Tuttavia

$$f(\mathbf{v} - \mathbf{v}') = f(\mathbf{v}) - f(\mathbf{v}') = \sum_{j=1}^{k} \beta_j \mathbf{w}_j - f\Bigl(\sum_{j=1}^{k} \beta_j \mathbf{v}_j\Bigr) = \sum_{j=1}^{k} \beta_j \mathbf{w}_j - \sum_{j=1}^{k} \beta_j f(\mathbf{v}_j) = \mathbf{0}.$$

Dunque $\mathbf{v}-\mathbf{v}' \in \mathrm{N}(f)$ e possiamo scrivere

$$\mathbf{v}-\mathbf{v}' = \sum_{i=1}^{n} \alpha_i \mathbf{u}_i,$$

da cui

$$\mathbf{v} = \sum_{i=1}^{n} \alpha_i \mathbf{u}_i + \mathbf{v}' = \sum_{i=1}^{n} \alpha_i \mathbf{u}_i + \sum_{j=1}^{k} \beta_j \mathbf{v}_j$$

e quindi $\mathbf{v} \in \langle \mathscr{C} \rangle$.

L'insieme $\mathscr{C}$ è linearmente indipendente. Supponiamo di avere

$$\mathbf{0} = \sum_{i=1}^{n} \alpha_i \mathbf{u}_i + \sum_{j=1}^{k} \beta_j \mathbf{v}_j.$$

Allora

$$\mathbf{0} = f(\mathbf{0}) = f\Bigl(\sum_{i=1}^{n} \alpha_i \mathbf{u}_i + \sum_{j=1}^{k} \beta_j \mathbf{v}_j\Bigr) = \sum_{i=1}^{n} \alpha_i f(\mathbf{u}_i) + \sum_{j=1}^{k} \beta_j f(\mathbf{v}_j) = \sum_{j=1}^{k} \beta_j \mathbf{w}_j$$

in quanto $\mathbf{u}_i \in \mathrm{N}(f)$ $(i = 1, \dots, n)$. Per l'indipendenza lineare di $f[\mathscr{B}]$ possiamo concludere che $\beta_1 = \dots = \beta_k = 0$. Ma allora

$$\mathbf{0} = \sum_{i=1}^{n} \alpha_i \mathbf{u}_i$$

e, per l'indipendenza lineare di $\mathscr{A}$, abbiamo che $\alpha_1 = \dots = \alpha_n = 0$. □

Diamo subito una conseguenza rilevante di questo teorema. Ricordiamo che l'applicazione $f\colon V \to W$ è *suriettiva* se $\mathrm{Im}(f) = W$.

Corollario 4.13. *Se V è uno spazio vettoriale finitamente generato e $f\colon V \to V$ è lineare, allora f è iniettiva se e solo se f è suriettiva.*

Dimostrazione. Dire che f è iniettiva equivale a dire che $\dim \mathrm{N}(f) = 0$. Il teorema nullità + rango dice allora che $\dim V = 0 + \dim \mathrm{Im}(f)$, cioè che $\dim \mathrm{Im}(f) = \dim V$. L'osservazione dopo 3.15 dice che $\mathrm{Im}(f) = V$.

Viceversa, se f è suriettiva abbiamo $\mathrm{Im}(f) = V$ e quindi $\dim \mathrm{Im}(f) = \dim V$. Per il teorema nullità + rango, $\dim V = \dim \mathrm{N}(f) + \dim \mathrm{Im}(f)$ e quindi $\dim \mathrm{N}(f) = 0$. □

Attenzione: il corollario vale solo quando dominio e codominio di f *coincidono* (in tal caso l'applicazione lineare viene chiamata spesso *endomorfismo*) o, più in generale, quando hanno la stessa dimensione (esercizio). Non vale se dominio e codominio hanno dimensioni diverse perché in tal caso nessuna applicazione lineare iniettiva può essere suriettiva e nessuna applicazione lineare suriettiva può essere iniettiva.

Non vale nemmeno se V non è finitamente generato. Per esempio, l'applicazione $f\colon \mathscr{P}(\mathbb{C}) \to \mathscr{P}(\mathbb{C})$ definita da

$$f(p) = pq,$$

dove q è un fissato polinomio di grado > 0, è iniettiva ma non suriettiva. Ne lasciamo la verifica per esercizio: il polinomio costante 1 non può appartenere a $\operatorname{Im}(f)$.

Come già accennato, il caso di applicazioni lineari indotte da matrici è molto importante. Calcoliamo anzitutto $\operatorname{Im}(f_{\mathbf{A}})$, dove $\mathbf{A}$ è una matrice $m \times n$. Se scriviamo $\mathbf{A} = [\mathbf{a}_1\ \mathbf{a}_2\ \dots\ \mathbf{a}_n]$ e prendiamo $\mathbf{v} = [\alpha_1\ \alpha_2\ \dots\ \alpha_n]^T \in \mathbb{C}^n$, abbiamo

$$f_{\mathbf{A}}(\mathbf{v}) = \mathbf{A}\mathbf{v} = \alpha_1\mathbf{a}_1 + \dots + \alpha_n\mathbf{a}_n$$

e dunque $f_{\mathbf{A}}(\mathbf{v}) \in C(\mathbf{A})$. Ricordiamo che lo spazio delle colonne $C(\mathbf{A})$ della matrice $\mathbf{A}$ è il sottospazio di $\mathbb{C}^m$ generato dall'insieme delle colonne di $\mathbf{A}$. Viceversa, se un vettore appartiene a $C(\mathbf{A})$, esso si può scrivere come combinazione lineare dell'insieme delle colonne di $\mathbf{A}$, $\mathbf{w} = \alpha_1\mathbf{a}_1 + \dots + \alpha_n\mathbf{a}_n$, ed è evidente che $\mathbf{w} = \mathbf{A}\mathbf{v} = f_{\mathbf{A}}(\mathbf{v})$, dove $\mathbf{v} = [\alpha_1\ \alpha_2\ \dots\ \alpha_n]^T \in \mathbb{C}^n$. Quindi $C(\mathbf{A}) \subseteq \operatorname{Im}(f_{\mathbf{A}})$.

In definitiva $C(\mathbf{A})$ coincide con l'immagine di $f_{\mathbf{A}}$. Se ne può anche dare un'altra descrizione:

$C(\mathbf{A})$ è l'insieme dei vettori $\mathbf{b} \in \mathbb{C}^m$ per i quali il sistema lineare $\mathbf{A}\mathbf{x} = \mathbf{b}$ ha soluzione.

Lo *spazio nullo* di $f_{\mathbf{A}}$ è invece l'insieme dei vettori $\mathbf{v} \in \mathbb{C}^n$ tali che $\mathbf{A}\mathbf{v} = \mathbf{0}$. In questo caso si chiama anche *spazio nullo di* $\mathbf{A}$ e si indica con $N(\mathbf{A})$.

Avendo definito rango di un'applicazione lineare f la dimensione di $\operatorname{Im}(f)$ e visto che per una matrice $\mathbf{A}$ risulta $\operatorname{Im}(f_{\mathbf{A}}) = C(\mathbf{A})$, possiamo dare una nuova definizione.

Definizione. La dimensione dello spazio delle colonne di una matrice $\mathbf{A}$ si chiama *rango* di $\mathbf{A}$ e si denota con $\operatorname{rk}\mathbf{A}$.

Vedremo in seguito che questa nozione di rango di una matrice coincide con quella data nel Capitolo 1.

Vediamo come si comporta il rango delle applicazioni lineari rispetto alla composizione di applicazioni. Siano $f\colon U \to V$ e $g\colon V \to W$ lineari. Possiamo applicare il teorema nullità + rango a $g \circ f$:

$$\dim U = \dim N(g \circ f) + \dim \operatorname{Im}(g \circ f).$$

È facile vedere che $N(f) \subseteq N(g \circ f)$: infatti, se $f(\mathbf{u}) = \mathbf{0}$, è anche $g \circ f(\mathbf{u}) = g(\mathbf{0}) = \mathbf{0}$. Dunque $\dim N(f) \le \dim N(g \circ f)$. Sappiamo anche che

$$\dim U = \dim N(f) + \dim \operatorname{Im}(f);$$

mettendo assieme con la disuguaglianza precedente, otteniamo che

$$\dim \operatorname{Im}(g \circ f) \le \dim \operatorname{Im}(f)$$

e quindi il rango di $g \circ f$ non supera il rango di f. È anche evidente che $\operatorname{Im}(g \circ f) \subseteq \operatorname{Im}(g)$, quindi

$$\dim \operatorname{Im}(g \circ f) \le \dim \operatorname{Im}(g)$$

e quindi il rango di $g \circ f$ non supera nemmeno il rango di g.

Nel caso in cui le applicazioni lineari siano indotte da matrici, sappiamo che $f_{\mathbf{B}} \circ f_{\mathbf{A}} = f_{\mathbf{BA}}$, quindi ne ricaviamo

$$\operatorname{rk}\mathbf{BA} \le \operatorname{rk}\mathbf{A}, \qquad \operatorname{rk}\mathbf{BA} \le \operatorname{rk}\mathbf{B}.$$

Un ultimo fatto importante sulle applicazioni lineari.

Teorema 4.14. *Se $\mathscr{B} = \{\mathbf{v}_1;\dots;\mathbf{v}_n\}$ è una base dello spazio vettoriale V e $\{\mathbf{w}_1;\dots;\mathbf{w}_n\}$ è un insieme di vettori nello spazio vettoriale W, allora esiste una e una sola applicazione lineare $f\colon V \to W$ tale che $f(\mathbf{v}_i) = \mathbf{w}_i$ $(i = 1,2,\dots,n)$.*

Dimostrazione. Diamo solamente un'idea, tralasciando i dettagli. Se un'applicazione lineare f del tipo voluto esiste, essa è unica. Infatti, supponiamo che anche $g\colon V \to W$ abbia la proprietà richiesta, cioè che $g(\mathbf{v}_i) = \mathbf{w}_i$ $(i = 1,2,\dots,n)$. Se $\mathbf{v} \in V$, possiamo scrivere $\mathbf{v} = \sum_{i=1}^{n} \alpha_i \mathbf{v}_i$ e dunque

$$g(\mathbf{v}) = \sum_{i=1}^{n} \alpha_i g(\mathbf{v}_i) = \sum_{i=1}^{n} \alpha_i \mathbf{w}_i = \sum_{i=1}^{n} \alpha_i f(\mathbf{v}_i) = f(\mathbf{v}).$$

Come si definisce allora f? Proprio scrivendo

$$f(\mathbf{v}) = \sum_{i=1}^{n} \alpha_i \mathbf{w}_i$$

e l'aspetto complicato della verifica è appunto di controllare che questa posizione definisce un'applicazione lineare. Si tratta di un noioso controllo dei dettagli e lo omettiamo. □

5. I quattro sottospazi fondamentali di una matrice

Data una qualunque matrice $\mathbf{A}$ di dimensioni $m \times n$, si possono associare a essa quattro spazi vettoriali detti i quattro *sottospazi fondamentali* di $\mathbf{A}$. I primi due sottospazi li abbiamo già incontrati; sono

$\mathrm{C}(\mathbf{A})$ = *spazio delle colonne di* $\mathbf{A}$ (già introdotto nel Paragrafo 3), definito come il sottospazio di $\mathbb{C}^m$ generato dai vettori colonna di $\mathbf{A}$;

$\mathrm{N}(\mathbf{A})$ = *spazio nullo di* $\mathbf{A}$ (già incontrato nel Paragrafo 1), sottospazio di $\mathbb{C}^n$ formato dalle soluzioni del sistema omogeneo $\mathbf{Ax} = \mathbf{0}$.

Gli altri due sottospazi stanno, come i precedenti, uno in $\mathbb{C}^n$ e uno in $\mathbb{C}^m$; sono

$\mathrm{C}(\mathbf{A}^H)$ = spazio delle colonne della H-trasposta $\mathbf{A}^H$ di $\mathbf{A}$, sottospazio di $\mathbb{C}^n$, detto *spazio delle righe di* $\mathbf{A}$;

$\mathrm{N}(\mathbf{A}^H)$ = spazio nullo di $\mathbf{A}^H$, sottospazio di $\mathbb{C}^m$, detto *spazio nullo sinistro di* $\mathbf{A}$.

In questo Paragrafo esamineremo più in dettaglio questi quattro sottospazi; daremo spiegazione dopo il Teorema 5.6 del perché $C(\mathbf{A}^H)$ venga chiamato spazio delle righe di $\mathbf{A}$.

Abbiamo legato lo spazio delle colonne di una matrice $\mathbf{A}$ alla soluzione di sistemi lineari. Vediamo allora come caratterizzare, attraverso il rango, che abbiamo definito nel Paragrafo 4 come la dimensione dello spazio delle colonne, l'esistenza di inverse di $\mathbf{A}$; riotterremo risultati già visti nel Capitolo 1 in altro modo. Diamo qui per buono quanto vedremo più avanti, cioè che le definizioni di rango di una matrice date nel Capitolo 1 e nel Paragrafo precedente coincidono.

L'esistenza di un'inversa destra della matrice $\mathbf{A}$, di dimensioni $m \times n$, equivale alla risolubilità dei sistemi lineari $\mathbf{Ax} = \mathbf{e}_i$ $(i = 1, 2, \dots, m)$. Questo a sua volta significa che i vettori $\mathbf{e}_i$ appartengono allo spazio delle colonne di $\mathbf{A}$, quindi che $C(\mathbf{A})$ contiene una base di $\mathbb{C}^m$: ciò accade se e solo se $C(\mathbf{A}) = \mathbb{C}^m$. Questa uguaglianza si può anche scrivere $\operatorname{rk}\mathbf{A} = m$.

Abbiamo però visto che $\operatorname{rk}\mathbf{A} \le m$ e $\operatorname{rk}\mathbf{A} \le n$. Se $m > n$, l'uguaglianza $\operatorname{rk}\mathbf{A} = m$ non può verificarsi. Perciò abbiamo dimostrato i risultati che seguono; per il secondo basta ricordare che $\mathbf{A}$ ha un'inversa sinistra se e solo se $\mathbf{A}^H$ ha un'inversa destra.

Proposizione 5.1. *Sia* $\mathbf{A}$ *una matrice* $m \times n$.

(1) $\mathbf{A}$ *ha un'inversa destra se e solo se* $\operatorname{rk}\mathbf{A} = m \le n$.

(2) $\mathbf{A}$ *ha un'inversa sinistra se e solo se* $\operatorname{rk}\mathbf{A}^H = n \le m$. □

Si vedrà nel Teorema 5.8 che $\operatorname{rk}\mathbf{A} = \operatorname{rk}\mathbf{A}^H$. Da questi due fatti discende che una matrice non quadrata non può avere inversa destra *e* inversa sinistra e giustifica la definizione di matrice invertibile per le sole matrici quadrate, come già abbiamo osservato nel Capitolo 1.

Corollario 5.2. *Una matrice quadrata* $\mathbf{A}$ *di ordine* n *è invertibile se e solo se* $\operatorname{rk}\mathbf{A} = n$. □

Rimane il problema di calcolare il rango di una matrice; già nel Capitolo 1 questo era stato definito come il numero di colonne dominanti (in una forma ridotta); quello che mancava allora era la dimostrazione che questo numero è lo stesso, qualunque sia il procedimento di eliminazione seguito. Sappiamo comunque che per ogni matrice $\mathbf{A}$ esistono una matrice in forma ridotta $\mathbf{U}$ e una matrice invertibile $\mathbf{F}$ tali che $\mathbf{FA} = \mathbf{U}$ (si vedano il Lemma 4.5 (ii) e il Teorema 6.9 del Capitolo 1).

Affronteremo il problema più in generale, considerando due matrici $\mathbf{A}$ e $\mathbf{B}$ di dimensioni $m \times n$ tali che esista $\mathbf{F}$ invertibile di ordine m tale che $\mathbf{FA} = \mathbf{B}$. Fino al Teorema 5.5 ci metteremo in questa ipotesi.

Scriviamo $\mathbf{A} = [\mathbf{a}_1 \ \dots \ \mathbf{a}_n]$ e $\mathbf{B} = [\mathbf{b}_1 \ \dots \ \mathbf{b}_n]$. Gli insiemi di vettori $\mathscr{A} = \{\mathbf{a}_1; \dots; \mathbf{a}_n\}$ e $\mathscr{B} = \{\mathbf{b}_1; \dots; \mathbf{b}_n\}$ sono insiemi di generatori di $C(\mathbf{A})$ e $C(\mathbf{B})$ rispettivamente. Da essi perciò possiamo estrarre sottoinsiemi che sono basi. Dato un sottoinsieme di uno dei due è chiaro chi sia il sottoinsieme corrispondente nell'altro; per esempio, il sottoinsieme corrispondente a $\{\mathbf{a}_1; \mathbf{a}_3\}$ è $\{\mathbf{b}_1; \mathbf{b}_3\}$.

Ricordiamo infine che $\mathbf{b}_i = \mathbf{Fa}_i$.

Proposizione 5.3. *Un vettore* $\mathbf{v} \in \mathbb{C}^m$ *è combinazione lineare dell'insieme delle colonne di* $\mathbf{A}$ *se e solo se* $\mathbf{Fv}$ *è combinazione lineare dell'insieme delle colonne di* $\mathbf{B}$ *con gli stessi coefficienti.*

Dimostrazione. Se $\mathbf{v} = \sum_{i=1}^{n} \alpha_i \mathbf{a}_i$, allora $\mathbf{Fv} = \sum_{i=1}^{n} \alpha_i \mathbf{F}\mathbf{a}_i = \sum_{i=1}^{n} \alpha_i \mathbf{b}_i$.

Viceversa, se $\mathbf{Fv} = \sum_{i=1}^{n} \alpha_i \mathbf{b}_i$, abbiamo anche

$$\mathbf{v} = \mathbf{F}^{-1}(\mathbf{Fv}) = \mathbf{F}^{-1}\Bigl(\sum_{i=1}^{n} \alpha_i \mathbf{b}_i\Bigr) = \sum_{i=1}^{n} \alpha_i \mathbf{F}^{-1}\mathbf{b}_i = \sum_{i=1}^{n} \alpha_i \mathbf{a}_i$$

e la dimostrazione è completa. □

Osservazione 5.4. La Proposizione precedente si può generalizzare parlando di un insieme di colonne qualunque di $\mathbf{A}$ e del corrispondente insieme di colonne di $\mathbf{B}$. Sia infatti $\mathbf{A}' = [\mathbf{a}_{i_1}\ \mathbf{a}_{i_2}\ \dots\ \mathbf{a}_{i_k}]$ una matrice ottenuta da $\mathbf{A}$ cancellando alcune colonne e sia $\mathbf{B}' = [\mathbf{b}_{i_1}\ \mathbf{b}_{i_2}\ \dots\ \mathbf{b}_{i_k}]$ la matrice formata dalle colonne corrispondenti di $\mathbf{B}$. Per come è definito il prodotto di matrici, abbiamo evidentemente che

$$\mathbf{B}' = \mathbf{F}\mathbf{A}'$$

e quindi possiamo applicare a questa situazione la Proposizione 5.3.

Ciò che abbiamo visto è che la moltiplicazione per $\mathbf{F}$ definisce un'applicazione $f\colon \mathrm{C}(\mathbf{A}) \to \mathrm{C}(\mathbf{B})$ che è lineare proprio perché è la moltiplicazione tra matrici. Inoltre f è biiettiva: infatti, per simmetria, la moltiplicazione per $\mathbf{F}^{-1}$ induce un'applicazione lineare $g\colon \mathrm{C}(\mathbf{B}) \to \mathrm{C}(\mathbf{A})$. È immediato verificare che g è l'inversa di f.

Un'altra facile osservazione è che $\mathrm{N}(\mathbf{A}) = \mathrm{N}(\mathbf{B})$. Infatti, se $\mathbf{Av} = \mathbf{0}$, si ha $\mathbf{Bv} = \mathbf{FAv} = \mathbf{F0} = \mathbf{0}$; analogamente il viceversa, usando che $\mathbf{A} = \mathbf{F}^{-1}\mathbf{B}$.

Da questo discende che $\operatorname{rk}\mathbf{A} = \operatorname{rk}\mathbf{B}$, usando il teorema nullità + rango. Infatti

$$\begin{aligned} n &= \dim \mathrm{N}(\mathbf{A}) + \operatorname{rk}\mathbf{A} \\ &= \dim \mathrm{N}(\mathbf{B}) + \operatorname{rk}\mathbf{B} \end{aligned}$$

Abbiamo anche un'altra conseguenza, che riguarda come trovare sottoinsiemi linearmente indipendenti dell'insieme delle colonne di $\mathbf{A}$ una volta noti sottoinsiemi linearmente indipendenti dell'insieme delle colonne di $\mathbf{B}$. Si noti che usiamo la Proposizione 5.3 nella forma esposta nell'Osservazione 5.4.

Teorema 5.5. *Sia* $\mathbf{B} = \mathbf{FA}$, *con* $\mathbf{F}$ *matrice invertibile. Allora un sottoinsieme di colonne di* $\mathbf{A}$ *è linearmente indipendente se e solo se il corrispondente sottoinsieme di colonne di* $\mathbf{B}$ *è linearmente indipendente.*

Una sottoinsieme di colonne di $\mathbf{A}$ *è una base di* $\mathrm{C}(\mathbf{A})$ *se e solo se il sottoinsieme corrispondente di colonne di* $\mathbf{B}$ *è una base di* $\mathrm{C}(\mathbf{B})$.

Dimostrazione. Se $\mathscr{A}$ è un sottoinsieme di colonne di $\mathbf{A}$, allora il sottoinsieme di colonne di $\mathbf{B}$ corrispondente è precisamente $f[\mathscr{A}]$, dove f è l'applicazione lineare $f\colon \mathrm{C}(\mathbf{A}) \to$

$C(\mathbf{B})$ indotta dalla moltiplicazione per $\mathbf{F}$. Siccome f è iniettiva, supponendo che $\mathscr{A}$ sia linearmente indipendente, abbiamo che $f[\mathscr{A}]$ è linearmente indipendente, per 4.11.

Il viceversa si ottiene considerando l'applicazione lineare $g = f^{-1}$.

Se $\mathscr{A}$ è una base di $C(\mathbf{A})$, allora ha $k = \operatorname{rk}\mathbf{A}$ elementi. Siccome il sottoinsieme corrispondente è linearmente indipendente e ha $k = \operatorname{rk}\mathbf{B}$ elementi, esso è una base di $C(\mathbf{B})$ per 3.15. □

Da questa discussione ricaviamo dunque una procedura per determinare una base di $C(\mathbf{A})$.

(1) Eseguiamo l'eliminazione di Gauss su $\mathbf{A}$, ottenendo una matrice in forma ridotta $\mathbf{U}$ e una matrice invertibile $\mathbf{F}$ tali che $\mathbf{U} = \mathbf{FA}$.

(2) Le colonne dominanti di $\mathbf{U}$ formano una base di $C(\mathbf{U})$.

(3) Le colonne di $\mathbf{A}$ corrispondenti alle colonne dominanti di $\mathbf{U}$ formano una base di $C(\mathbf{A})$.

È bene ricordare che, in generale, gli spazi delle colonne di $\mathbf{A}$ e di $\mathbf{U}$ sono *diversi*. Essi hanno però la stessa dimensione.

Un caso diverso è quando $\mathbf{B} = \mathbf{AG}$, con $\mathbf{G}$ matrice invertibile. In tal caso $C(\mathbf{B}) = C(\mathbf{A})$. Sia infatti $\mathbf{G} = [\gamma_{ij}]$ e scriviamo $\mathbf{A} = [\mathbf{a}_1 \ \dots \ \mathbf{a}_n]$, $\mathbf{B} = [\mathbf{b}_1 \ \dots \ \mathbf{b}_n]$. Allora, per 2.13 del Capitolo 1, si ha

$$\mathbf{b}_i = \sum_{j=1}^{n} \gamma_{ji}\mathbf{a}_j \qquad (i = 1, \dots, n)$$

da cui segue che ogni colonna di $\mathbf{B}$ è combinazione lineare dell'insieme delle colonne di $\mathbf{A}$, perciò $C(\mathbf{B}) \subseteq C(\mathbf{A})$. L'inclusione inversa discende dall'uguaglianza $\mathbf{A} = \mathbf{BG}^{-1}$.

Da questa osservazione ricaviamo il seguente risultato.

Teorema 5.6. *Sia* $\mathbf{B} = \mathbf{FA}$, *con* $\mathbf{F}$ *matrice invertibile. Allora* $C(\mathbf{B}^H) = C(\mathbf{A}^H)$, *cioè gli spazi delle righe di* $\mathbf{A}$ *e* $\mathbf{B}$ *coincidono. In particolare ciò accade quando* $\mathbf{B} = \mathbf{U}$, *forma ridotta di* $\mathbf{A}$.

Dimostrazione. L'uguaglianza $\mathbf{B} = \mathbf{FA}$ è equivalente a $\mathbf{B}^H = \mathbf{A}^H\mathbf{F}^H$. Si applichi quanto appena visto. □

È ora di spiegare perché $C(\mathbf{A}^H)$ si chiama "spazio delle righe" di $\mathbf{A}$. Ciò è dovuto al fatto che noi privilegiamo gli spazi $\mathbb{C}^n$ dei vettori colonna rispetto agli spazi $\mathbb{C}_n$ dei vettori riga, quindi pensiamo alle righe di $\mathbf{A}$ come alle colonne di $\mathbf{A}^T$. Questo esaurisce la spiegazione per le matrici reali.

Nel caso di matrici complesse, il modo di esprimere l'ortogonalità tra vettori di $\mathbb{C}^n$ (che vedremo nel Capitolo 3) forza a considerare non già $\mathbf{A}^T$ ma $\mathbf{A}^H$. Questo non crea alcun problema ai fini di considerazioni su dipendenza e indipendenza lineare e insiemi di generatori, quindi di dimensione. Infatti un insieme di righe di $\mathbf{A}$ è linearmente indipendente se e solo se le stesse righe di $\overline{\mathbf{A}}$ lo sono (basta coniugare tutto), quindi se e solo se le stesse colonne di $(\overline{\mathbf{A}})^T = \mathbf{A}^H$ lo sono.

Come caso particolarmente importante, segnaliamo il seguente risultato.

Proposizione 5.7. *Sia* $\mathbf{U}$ *una forma ridotta della matrice* $\mathbf{A}$*. Una base di* $C(\mathbf{U}^H) = C(\mathbf{A}^H)$ *è data dalle colonne non nulle di* $\mathbf{U}^H$*.*

Dimostrazione. Basta provare che le colonne non nulle di $\mathbf{U}^H$ sono linearmente indipendenti, ovvero che le righe non nulle di $\mathbf{U}$ sono linearmente indipendenti. La verifica di questo fatto è analoga a quanto visto nell'Esempio 2.17. □

Da questi ultimi risultati si deduce che

> il numero di righe non nulle di una forma ridotta $\mathbf{U}$ della matrice $\mathbf{A}$ coincide con la dimensione di $C(\mathbf{A}^H)$, cioè con $\operatorname{rk}\mathbf{A}^H$.

Teorema 5.8. *Per ogni matrice* $\mathbf{A}$*, si ha* $\operatorname{rk}\mathbf{A} = \operatorname{rk}\mathbf{A}^H$*.*

Dimostrazione. Sia $\mathbf{U}$ una forma ridotta di $\mathbf{A}$, $\mathbf{U} = \mathbf{FA}$ con $\mathbf{F}$ invertibile. Allora

$$\operatorname{rk}\mathbf{A} = \dim C(\mathbf{A}) = \dim C(\mathbf{U}) = \dim C(\mathbf{U}^H) = \dim C(\mathbf{A}^H) = \operatorname{rk}\mathbf{A}^H,$$

dove l'uguaglianza centrale dipende dal fatto che il numero di colonne dominanti di $\mathbf{U}$ coincide con il numero delle sue righe non nulle. □

Se $\mathbf{A}$ ha dimensioni $m \times n$, lo spazio nullo sinistro è dato dai vettori $\mathbf{w} \in \mathbb{C}^m$ tali che $\mathbf{A}^H\mathbf{w} = 0$ o, equivalentemente, $\mathbf{w}^H\mathbf{A} = 0$. Ciò ne giustifica il nome. Ci interessa ora valutarne la dimensione.

Proposizione 5.9. *La dimensione dello spazio nullo di una matrice* $\mathbf{A}$ *di dimensioni* $m \times n$ *è* $n - \operatorname{rk}\mathbf{A}$*. La dimensione dello spazio nullo sinistro di* $\mathbf{A}$ *è* $m - \operatorname{rk}\mathbf{A}$*.*

Dimostrazione. Si tratta di applicare il teorema nullità + rango. Per definizione, $N(\mathbf{A}) = N(f_{\mathbf{A}})$ dove $f_{\mathbf{A}} \colon \mathbb{C}^n \to \mathbb{C}^m$. Allora

$$\dim N(\mathbf{A}) = n - \dim C(\mathbf{A}) = n - \operatorname{rk}\mathbf{A}.$$

Analogamente, $N(\mathbf{A}^H) = N(f_{\mathbf{A}^H})$, dove $f_{\mathbf{A}^H} \colon \mathbb{C}^m \to \mathbb{C}^n$. Allora

$$\dim N(\mathbf{A}^H) = m - \dim C(\mathbf{A}^H) = m - \operatorname{rk}\mathbf{A}.$$ □

Da quanto visto finora si può ricavare un importante risultato che lega tra di loro, a due a due, i quattro sottospazi fondamentali di una matrice; esso potrà essere anche migliorato nel Capitolo 3, quando avremo a disposizione la nozione di ortogonalità.

Teorema 5.10. *Data una matrice* $\mathbf{A}$ *di dimensioni* $m \times n$ *si ha:*

$$\mathbb{C}^m = C(\mathbf{A}) \oplus N(\mathbf{A}^H),$$
$$\mathbb{C}^n = C(\mathbf{A}^H) \oplus N(\mathbf{A}).$$

Dimostrazione. È sufficiente verificare la prima uguaglianza; infatti la seconda si ricava dalla prima sostituendo $\mathbf{A}$ con $\mathbf{A}^H$. Cominciamo dimostrando che $\mathrm{C}(\mathbf{A}) \cap \mathrm{N}(\mathbf{A}^H) = \{\mathbf{0}\}$. Se $\mathbf{y} \in \mathrm{C}(\mathbf{A}) \cap \mathrm{N}(\mathbf{A}^H)$, allora $\mathbf{y} = \mathbf{A}\mathbf{v}$ per un vettore $\mathbf{v} \in \mathbb{C}^n$ e $\mathbf{A}^H\mathbf{y} = \mathbf{0}$. Se ne ricava $\mathbf{A}^H\mathbf{A}\mathbf{v} = \mathbf{0}$ il che comporta, come già visto nella dimostrazione del Teorema 4.12 del Capitolo 1, che $\mathbf{y} = \mathbf{A}\mathbf{v} = \mathbf{0}$. Dalle Proposizioni 3.17 e 5.7, ricaviamo

$$\dim \mathrm{C}(\mathbf{A}) \oplus \mathrm{N}(\mathbf{A}^H) = \dim \mathrm{C}(\mathbf{A}) + \dim \mathrm{N}(\mathbf{A}^H) = \operatorname{rk}\mathbf{A} + (m - \operatorname{rk}\mathbf{A}) = m$$

e perciò, per quanto osservato dopo il Teorema 3.15, possiamo concludere che $\mathbb{C}^m = \mathrm{C}(\mathbf{A}) \oplus \mathrm{N}(\mathbf{A}^H)$. □

Rimane solo da descrivere una procedura per calcolare una base dello spazio nullo di una matrice $m \times n$. Osserviamo che lo spazio nullo di $\mathbf{A}$ coincide con quello di una sua forma ridotta $\mathbf{U}$: infatti, poiché $\mathbf{U} = \mathbf{F}\mathbf{A}$ con $\mathbf{F}$ invertibile, $\mathbf{A}\mathbf{v} = \mathbf{0}$ se e solo se $\mathbf{U}\mathbf{v} = \mathbf{F}\mathbf{A}\mathbf{v} = \mathbf{0}$. I vettori dello spazio nullo di $\mathbf{A}$ sono le soluzioni del sistema omogeneo $\mathbf{U}\mathbf{x} = \mathbf{0}$ e ci basterà trovare fra esse $n - \operatorname{rk}\mathbf{A}$ vettori linearmente indipendenti.

Una soluzione del sistema omogeneo si ottiene dando valori arbitrari alle incognite non dominanti, ottenendo in corrispondenza i valori delle incognite dominanti. Abbiamo un modo per scrivere $d = n - \operatorname{rk}\mathbf{A}$ vettori distinti: se le incognite non dominanti sono $x_{i_1}, x_{i_2}, \dots, x_{i_d}$, possiamo dare a una di esse il valore 1 e alle altre il valore 0. Questa assegnazione si può fare in d modi diversi, ottenendo i vettori $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_d$.

Questo insieme di vettori è linearmente indipendente: infatti a essi corrispondono, nell'applicazione che sceglie le componenti $i_1, i_2, \dots, i_d$ (si veda l'esempio 4.1 (3)), i vettori della base canonica di $\mathbb{C}^d$, che formano un insieme linearmente indipendente. Si noti che è particolarmente conveniente usare, nel calcolo della base dello spazio nullo, la forma ridotta ottenuta con l'eliminazione in avanti e all'indietro.

Esempio 5.11. Applichiamo a un esempio concreto quanto visto in questo Paragrafo. Consideriamo la seguente matrice 3×4 (si vedano anche gli esempi 5.4 e 5.5 del Capitolo 3):

$$\mathbf{A} = \begin{bmatrix} 1 & i & 6 & 8i \\ 2i & -2 & 0 & 8 \\ 1 & i & 6 & 8i \end{bmatrix}.$$

Vogliamo determinare i quattro sottospazi fondamentali con relative basi. L'eliminazione di Gauss produce la seguente forma ridotta di $\mathbf{A}$:

$$\mathbf{U} = \begin{bmatrix} 1 & i & 6 & 8i \\ 0 & 0 & 1 & 2i \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Da quanto descritto dopo il Teorema 5.5, si ricava che $\mathrm{C}(\mathbf{A})$ ha come base le colonne di $\mathbf{A}$ corrispondenti alle colonne dominanti di $\mathbf{U}$, quindi

$$\mathrm{C}(\mathbf{A}) = \left\langle \begin{bmatrix} 1 \\ 2i \\ 1 \end{bmatrix}; \begin{bmatrix} 6 \\ 0 \\ 6 \end{bmatrix} \right\rangle.$$

Un facile calcolo mostra che

$$\mathrm{N}(\mathbf{A}) = \mathrm{N}(\mathbf{U}) = \left\langle \begin{bmatrix} -2i \\ 0 \\ -i \\ 1 \end{bmatrix}; \begin{bmatrix} -i \\ 1 \\ 0 \\ 0 \end{bmatrix} \right\rangle.$$

La Proposizione 5.7 mostra che

$$\mathrm{C}(\mathbf{A}^H) = \mathrm{C}(\mathbf{U}^H) = \left\langle \begin{bmatrix} 1 \\ -i \\ 6 \\ -8i \end{bmatrix}; \begin{bmatrix} 0 \\ 0 \\ 1 \\ -2i \end{bmatrix} \right\rangle$$

dove i due vettori della base sono i vettori H-trasposti delle due righe non nulle di $\mathbf{U}$. Infine un altro facile calcolo mostra che

$$\mathrm{N}(\mathbf{A}^H) = \left\langle \begin{bmatrix} 1 \\ 0 \\ -1 \end{bmatrix} \right\rangle.$$

Il lettore verifichi che quanto previsto dal Teorema 5.10 si verifica. □

Il teorema di Rouché-Capelli

I concetti di rango e di spazio delle colonne di una matrice permettono di dare una veste precisa alle questioni sulla risolubilità di un sistema lineare. Il teorema che enunceremo è in realtà già stato dimostrato nel Capitolo 1, in forma leggermente diversa. Invitiamo il lettore a indagare sulle somiglianze e sulle differenze.

Un sistema lineare di m equazioni in n incognite si può scrivere nella forma $\mathbf{A}\mathbf{x} = \mathbf{b}$ e sappiamo che esso è risolubile se e solo se $\mathbf{b} \in \mathrm{C}(\mathbf{A})$. La matrice $\mathbf{A}$ è la *matrice dei coefficienti* del sistema, la matrice $[\mathbf{A} \mid \mathbf{b}]$ è la *matrice aumentata*.

Il sistema è allora risolubile se e solo se $\mathbf{b}$ è combinazione lineare dell'insieme delle prime n colonne della matrice aumentata. Quanto abbiamo visto nel teorema 5.5 mostra allora quello che già sappiamo: supponendo che $[\mathbf{U} \mid \mathbf{c}]$ sia una forma ridotta della matrice aumentata del sistema, il sistema è risolubile se e solo se $\mathbf{c}$ è non dominante. Infatti ciò accade se e solo se l'ultima colonna di $[\mathbf{A} \mid \mathbf{b}]$ è combinazione lineare dell'insieme delle colonne precedenti.

Un altro modo di vedere la faccenda usa il concetto di rango; si tratta di un aspetto utile nella teoria, anche perché finora l'unico modo che abbiamo visto per calcolare il rango di una matrice è di eseguire l'eliminazione.

Osserviamo che, chiaramente, $\mathrm{C}(\mathbf{A}) \subseteq \mathrm{C}([\mathbf{A} \mid \mathbf{b}])$. Dunque $\operatorname{rk}\mathbf{A} \le \operatorname{rk}[\mathbf{A} \mid \mathbf{b}]$. Di quanto può aumentare il rango della matrice aumentata? Poniamo $k = \operatorname{rk}\mathbf{A}$; ciò significa che fra le colonne di $\mathbf{A}$ possiamo sceglierne k a formare una base. Ma allora $\mathrm{C}([\mathbf{A} \mid \mathbf{b}])$ ha un insieme di generatori con $k+1$ elementi (la base di $\mathrm{C}(\mathbf{A})$ a cui aggiungiamo $\mathbf{b}$). Quindi $\dim \mathrm{C}([\mathbf{A} \mid \mathbf{b}]) \le k+1$.

Il sistema omogeneo associato a quello dato, cioè $\mathbf{A}\mathbf{x} = \mathbf{0}$, fornisce un altro dato. Supponiamo che $\mathbf{v}_0$ sia una soluzione di $\mathbf{A}\mathbf{x} = \mathbf{b}$ e sia $\mathbf{u}$ una soluzione del sistema omogeneo associato, in altre parole un elemento di $\mathrm{N}(\mathbf{A})$. Abbiamo allora

$$\mathbf{A}(\mathbf{u}+\mathbf{v}_0) = \mathbf{A}\mathbf{u}+\mathbf{A}\mathbf{v}_0 = \mathbf{0}+\mathbf{b} = \mathbf{b}$$

e quindi $\mathbf{u}+\mathbf{v}_0$ è una soluzione del sistema dato. Viceversa, se $\mathbf{v}$ è una soluzione del sistema dato e poniamo $\mathbf{u} = \mathbf{v}-\mathbf{v}_0$, abbiamo

$$\mathbf{A}\mathbf{u} = \mathbf{A}(\mathbf{v}-\mathbf{v}_0) = \mathbf{A}\mathbf{v}-\mathbf{A}\mathbf{v}_0 = \mathbf{b}-\mathbf{b} = \mathbf{0},$$

cioè $\mathbf{u} \in \mathrm{N}(\mathbf{A})$ ed è quindi soluzione del sistema omogeneo.

Abbiamo quindi visto che la differenza fra due soluzioni del sistema dato è un elemento dello spazio nullo della matrice dei coefficienti. Quindi una volta nota *una soluzione particolare* del sistema, tutte le altre si ottengono sommando a essa un elemento dello spazio nullo. Perciò, per conoscere tutte le soluzioni, basta conoscerne una e avere a disposizione una base dello spazio nullo, la cui dimensione è precisamente $n-\operatorname{rk}\mathbf{A}$.

È a questo che ci si riferisce quando si dice che le soluzioni di un sistema lineare, se esistono, dipendono da un numero di parametri pari al numero delle incognite meno il numero di incognite dominanti: questi parametri sono i coefficienti che possiamo assegnare agli elementi di una base dello spazio nullo per costruire una loro combinazione lineare.

Teorema 5.12 (Rouché-Capelli)**.** *Sia* $\mathbf{A}\mathbf{x} = \mathbf{b}$ *un sistema lineare di* m *equazioni in* n *incognite. Il sistema è risolubile se e solo se*

$$\operatorname{rk}\mathbf{A} = \operatorname{rk}[\mathbf{A} \mid \mathbf{b}]$$

e, in tal caso, le soluzioni del sistema dipendono da $n-\operatorname{rk}\mathbf{A}$ *parametri. In particolare il sistema ammette una e una sola soluzione se e solo se*

$$\operatorname{rk}\mathbf{A} = \operatorname{rk}[\mathbf{A} \mid \mathbf{b}] = n.$$

□

6. Coordinate e matrici associate alle applicazioni lineari

In tutta questa sezione supporremo che gli spazi vettoriali che menzioneremo siano non nulli (cioè di dimensione > 0), oltre che finitamente generati.

Nel contesto che tratteremo, a differenza di quanto fatto in precedenza, l'ordine in cui si considerano gli elementi di una base è importante. Perciò quando tratteremo di coordinate e, in seguito, di matrici associate ad applicazioni lineari, supporremo che una base sia definita sia dandone gli elementi che fissandone l'ordine in cui sono considerati. Non useremo notazioni diverse da prima, ma daremo risalto a questo fatto parlando di *basi ordinate*.

Se $\mathscr{B}$ è una base dello spazio vettoriale V, ogni elemento di V si può scrivere *in modo unico* come combinazione lineare dei vettori di $\mathscr{B}$.

Infatti, se $\mathscr{B} = \{\mathbf{v}_1; \dots; \mathbf{v}_n\}$ e

$$\mathbf{v} = \sum_{i=1}^{n} \alpha_i \mathbf{v}_i = \sum_{i=1}^{n} \beta_i \mathbf{v}_i$$

allora

$$\mathbf{0} = \mathbf{v} - \mathbf{v} = \sum_{i=1}^{n} \alpha_i \mathbf{v}_i - \sum_{i=1}^{n} \beta_i \mathbf{v}_i = \sum_{i=1}^{n} (\alpha_i - \beta_i) \mathbf{v}_i$$

e, per l'indipendenza lineare, $\alpha_i = \beta_i$ $(i = 1, \dots, n)$.

Se poi consideriamo $\mathscr{B}$ come base *ordinata*, possiamo definire un'applicazione $\mathrm{C}_{\mathscr{B}} \colon V \to \mathbb{C}^n$ ponendo

$$\mathrm{C}_{\mathscr{B}}(\mathbf{v}) = \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix} \quad \text{se e solo se} \quad \mathbf{v} = \sum_{i=1}^{n} \alpha_i \mathbf{v}_i.$$

È proprio il fatto di aver fissato l'ordine dei vettori di $\mathscr{B}$ a permetterci di dare questa definizione.

Questa applicazione si chiama *applicazione delle coordinate rispetto alla base ordinata* $\mathscr{B}$. Diremo che $\mathrm{C}_{\mathscr{B}}(\mathbf{v})$ è il *vettore delle coordinate di* $\mathbf{v}$ *rispetto alla base ordinata* $\mathscr{B}$.

Proposizione 6.1. *L'applicazione delle coordinate* $\mathrm{C}_{\mathscr{B}} \colon V \to \mathbb{C}^n$ *è lineare e biiettiva.*

Dimostrazione. Sia $\mathscr{B} = \{\mathbf{v}_1; \dots; \mathbf{v}_n\}$. Siano $\mathbf{u}, \mathbf{v} \in V$ e poniamo

$$\mathrm{C}_{\mathscr{B}}(\mathbf{u}) = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix}, \qquad \mathrm{C}_{\mathscr{B}}(\mathbf{v}) = \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix}.$$

Questo significa che

$$\mathbf{u} = \sum_{i=1}^{n} \alpha_i \mathbf{v}_i, \qquad \mathbf{v} = \sum_{i=1}^{n} \beta_i \mathbf{v}_i,$$

da cui

$$\mathbf{u} + \mathbf{v} = \sum_{i=1}^{n} (\alpha_i + \beta_i) \mathbf{v}_i$$

e quindi che

$$\mathrm{C}_{\mathscr{B}}(\mathbf{u} + \mathbf{u}) = \begin{bmatrix} \alpha_1 + \beta_1 \\ \vdots \\ \alpha_n + \beta_n \end{bmatrix} = \mathrm{C}_{\mathscr{B}}(\mathbf{u}) + \mathrm{C}_{\mathscr{B}}(\mathbf{v}).$$

Lasciamo al lettore la verifica che $C_{\mathscr{B}}(\alpha\mathbf{u}) = \alpha\, C_{\mathscr{B}}(\mathbf{u})$ per ogni $\mathbf{u} \in V$ e ogni scalare α.

Inoltre $C_{\mathscr{B}}$ è chiaramente suriettiva: per definizione

$$\begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = C_{\mathscr{B}}\Bigl(\sum_{i=1}^{n} \alpha_i \mathbf{v}_i\Bigr).$$

Per il teorema nullità + rango, la dimensione dello spazio nullo di $C_{\mathscr{B}}$ è zero. □

L'applicazione delle coordinate rispetto a una base è lo strumento che rende possibile trattare ogni questione su spazi vettoriali attraverso matrici, proprio perché è lineare e biiettiva. Infatti un insieme di vettori $\mathscr{A}$ in V è linearmente indipendente se e solo se l'insieme $C_{\mathscr{B}}[\mathscr{A}]$ è linearmente indipendente e quest'ultimo è un insieme di vettori in $\mathbb{C}^n$ e dunque si può trattare con i metodi matriciali.

Analogamente un vettore $\mathbf{v} \in V$ è combinazione lineare dei vettori di $\mathscr{A}$ se e solo se $C_{\mathscr{B}}(\mathbf{v})$ è combinazione lineare dei vettori di $C_{\mathscr{B}}[\mathscr{A}]$ (esercizio).

Questa situazione è analoga a quella discussa quando abbiamo costruito un'applicazione lineare biiettiva tra $C(\mathbf{A})$ e $C(\mathbf{B})$, dove $\mathbf{B} = \mathbf{FA}$ per una matrice $\mathbf{F}$ invertibile.

Esempi 6.2. (1) Nelle notazioni precedenti, abbiamo che

$$C_{\mathscr{B}}(\mathbf{v_i}) = \mathbf{e}_i \qquad (i = 1, 2, \dots, n).$$

Infatti possiamo scrivere

$$\mathbf{v}_i = 0\mathbf{v}_1 + \dots + 1\mathbf{v}_i + \dots + 0\mathbf{v}_n$$

e dunque

$$C_{\mathscr{B}}(\mathbf{v_i}) = [0 \ \dots \ 0 \ \overset{\overset{i}{\downarrow}}{1} \ 0 \ \dots \ 0]^T = \mathbf{e}_i.$$

Dunque il vettore delle coordinate di un vettore della base $\mathscr{B}$ è il corrispondente vettore della base canonica di $\mathbb{C}^n$.

(2) L'insieme $\mathscr{B} = \{2; 1 - X; 1 + X^2\}$ è una base di $\mathscr{P}_3(\mathbb{C})$ (lo si verifichi). Vogliamo calcolare $C_{\mathscr{B}}(4 - 2X + 3X^2)$. Per fare questo occorre scrivere

$$4 - 2X + 3X^2 = \alpha \cdot 2 + \beta(1 - X) + \gamma(1 + X^2)$$

che equivale al sistema lineare

$$\begin{bmatrix} 2 & 1 & 1 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \\ \gamma \end{bmatrix} = \begin{bmatrix} 4 \\ -2 \\ 3 \end{bmatrix}$$

e scrivendo la soluzione otteniamo

$$C_{\mathscr{B}}(4 - 2X + 3X^2) = \begin{bmatrix} -1/2 & 2 & 3 \end{bmatrix}^T.$$

(3) Se lo spazio vettoriale V è $\mathbb{C}^n$, possiamo considerarne la base canonica $\mathscr{E}$. Secondo la definizione, $\mathrm{C}_{\mathscr{E}}(\mathbf{v})$ è la colonna formata dai coefficienti che servono a scrivere $\mathbf{v}$ come combinazione lineare di $\mathscr{E}$. Ma

$$\begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix} = \alpha_1\mathbf{e}_1 + \alpha_2\mathbf{e}_2 + \dots + \alpha_n\mathbf{e}_n$$

e quindi $\mathrm{C}_{\mathscr{E}}(\mathbf{v}) = \mathbf{v}$. In altre parole $\mathrm{C}_{\mathscr{E}}$ è l'applicazione *identità*. □

È ovvio che se $\mathscr{B}$ e $\mathscr{D}$ sono basi ordinate distinte di V, le applicazioni delle coordinate saranno diverse. È tuttavia altrettanto chiaro che ci deve essere un modo per calcolare le coordinate di un vettore rispetto a una base conoscendo quelle rispetto a un'altra base.

Assumiamo che questa trasformazione delle coordinate si possa ottenere tramite la moltiplicazione per una matrice, cioè che esista una matrice quadrata $\mathbf{M}$ di ordine $n = \dim V$ tale che, per ogni $\mathbf{v} \in V$,

$$\mathrm{C}_{\mathscr{B}}(\mathbf{v}) = \mathbf{M}\,\mathrm{C}_{\mathscr{D}}(\mathbf{v}).$$

Abbiamo dati sufficienti per determinare $\mathbf{M}$? Sappiamo calcolare $\mathrm{C}_{\mathscr{D}}(\mathbf{w}_i)$, dove $\mathscr{D} = \{\mathbf{w}_1;\dots;\mathbf{w}_n\}$, infatti

$$\mathrm{C}_{\mathscr{D}}(\mathbf{w}_i) = \mathbf{e}_i.$$

Ma allora, la nostra ipotesi impone che

$$\mathrm{C}_{\mathscr{B}}(\mathbf{w}_i) = \mathbf{M}\,\mathrm{C}_{\mathscr{D}}(\mathbf{w}_i) = \mathbf{M}\mathbf{e}_i = i\text{-esima colonna di } \mathbf{M}.$$

Dunque possiamo scrivere $\mathbf{M}$ nel modo seguente:

$$\mathbf{M} = \begin{bmatrix} \mathrm{C}_{\mathscr{B}}(\mathbf{w}_1) & \mathrm{C}_{\mathscr{B}}(\mathbf{w}_2) & \dots & \mathrm{C}_{\mathscr{B}}(\mathbf{w}_n) \end{bmatrix}$$

e ci resta solo da vedere che effettivamente la matrice $\mathbf{M}$ così definita è adeguata alla nostra ipotesi.

Teorema 6.3. *Siano $\mathscr{B}$ e $\mathscr{D}$ basi dello spazio vettoriale V. Allora esiste una e una sola matrice $\mathbf{M}_{\mathscr{B}\leftarrow\mathscr{D}}$ tale che, per ogni $\mathbf{v} \in V$,*

$$\mathrm{C}_{\mathscr{B}}(\mathbf{v}) = \mathbf{M}_{\mathscr{B}\leftarrow\mathscr{D}}\,\mathrm{C}_{\mathscr{D}}(\mathbf{v}).$$

La matrice $\mathbf{M}_{\mathscr{B}\leftarrow\mathscr{D}}$ è invertibile e la sua inversa è $\mathbf{M}_{\mathscr{D}\leftarrow\mathscr{B}}$.

Dimostrazione. Nella discussione precedente abbiamo mostrato l'unicità della matrice $\mathbf{M}_{\mathscr{B}\leftarrow\mathscr{D}}$: se una tale matrice esiste essa è proprio

$$\mathbf{M}_{\mathscr{B}\leftarrow\mathscr{D}} = \begin{bmatrix} \mathrm{C}_{\mathscr{B}}(\mathbf{w}_1) & \mathrm{C}_{\mathscr{B}}(\mathbf{w}_2) & \dots & \mathrm{C}_{\mathscr{B}}(\mathbf{w}_n) \end{bmatrix}.$$

Facciamo vedere che questa matrice funziona come voluto. Sia $\mathbf{v} \in V$ e poniamo

$$\mathrm{C}_{\mathscr{D}}(\mathbf{v}) = [\beta_1\ \beta_2\ \dots\ \beta_n]^T.$$

Allora $\mathbf{v} = \sum_{i=1}^{n} \beta_i \mathbf{w}_i$; possiamo usare la linearità di $\mathrm{C}_{\mathscr{B}}$ e il fatto che, *per definizione*, $\mathbf{M}_{\mathscr{B}\leftarrow\mathscr{D}}\mathbf{e}_i = \mathrm{C}_{\mathscr{B}}(\mathbf{w}_i)$:

$$\begin{aligned}
\mathrm{C}_{\mathscr{B}}(\mathbf{v}) &= \sum_{i=1}^{n} \beta_i\, \mathrm{C}_{\mathscr{B}}(\mathbf{w}_i) = \sum_{i=1}^{n} \beta_i \mathbf{M}_{\mathscr{B}\leftarrow\mathscr{D}}\mathbf{e}_i \\
&= \mathbf{M}_{\mathscr{B}\leftarrow\mathscr{D}}\Bigl(\sum_{i=1}^{n} \beta_i \mathbf{e}_i\Bigr) = \mathbf{M}_{\mathscr{B}\leftarrow\mathscr{D}} \begin{bmatrix} \beta_1 \\ \beta_2 \\ \dots \\ \beta_n \end{bmatrix} \\
&= \mathbf{M}_{\mathscr{B}\leftarrow\mathscr{D}}\, \mathrm{C}_{\mathscr{D}}(\mathbf{v}).
\end{aligned}$$

Rimane da mostrare che $\mathbf{M}_{\mathscr{B}\leftarrow\mathscr{D}}$ è invertibile. Osserviamo alcune questioni importanti su quanto abbiamo visto.

(1) Ciò che abbiamo dimostrato vale per due basi qualunque. In particolare la matrice $\mathbf{M}_{\mathscr{D}\leftarrow\mathscr{B}}$ esiste ed è unica.
(2) Per verificare che, data una certa matrice $\mathbf{M}$, si ha $\mathbf{M} = \mathbf{M}_{\mathscr{B}\leftarrow\mathscr{D}}$, basta dimostrare che, per ogni $\mathbf{v} \in V$, si ha $\mathbf{M}\,\mathrm{C}_{\mathscr{D}}(\mathbf{v}) = \mathrm{C}_{\mathscr{B}}(\mathbf{v})$.
(3) Non abbiamo in nessun punto usato che $\mathscr{B}$ e $\mathscr{D}$ siano diverse; quindi la matrice $\mathbf{M}_{\mathscr{B}\leftarrow\mathscr{B}}$ esiste ed è unica.

Quale sarà la matrice $\mathbf{M}_{\mathscr{B}\leftarrow\mathscr{B}}$? Siccome $\mathbf{I}\,\mathrm{C}_{\mathscr{B}}(\mathbf{v}) = \mathrm{C}_{\mathscr{B}}(\mathbf{v})$ l'osservazione (2) dice che $\mathbf{M}_{\mathscr{B}\leftarrow\mathscr{B}} = \mathbf{I}$. Ora proviamo a eseguire il prodotto $(\mathbf{M}_{\mathscr{B}\leftarrow\mathscr{D}}\mathbf{M}_{\mathscr{D}\leftarrow\mathscr{B}})\,\mathrm{C}_{\mathscr{B}}(\mathbf{v})$:

$$(\mathbf{M}_{\mathscr{B}\leftarrow\mathscr{D}}\mathbf{M}_{\mathscr{D}\leftarrow\mathscr{B}})\,\mathrm{C}_{\mathscr{B}}(\mathbf{v}) = \mathbf{M}_{\mathscr{B}\leftarrow\mathscr{D}}(\mathbf{M}_{\mathscr{D}\leftarrow\mathscr{B}}\,\mathrm{C}_{\mathscr{B}}(\mathbf{v})) = \mathbf{M}_{\mathscr{B}\leftarrow\mathscr{D}}\,\mathrm{C}_{\mathscr{D}}(\mathbf{v}) = \mathrm{C}_{\mathscr{B}}(\mathbf{v}).$$

Dunque la matrice $\mathbf{M}_{\mathscr{B}\leftarrow\mathscr{D}}\mathbf{M}_{\mathscr{D}\leftarrow\mathscr{B}}$ coincide con la matrice $\mathbf{M}_{\mathscr{B}\leftarrow\mathscr{B}} = \mathbf{I}$. Perciò abbiamo dimostrato che $\mathbf{M}_{\mathscr{B}\leftarrow\mathscr{D}}\mathbf{M}_{\mathscr{D}\leftarrow\mathscr{B}} = \mathbf{I}$. Analogamente $\mathbf{M}_{\mathscr{D}\leftarrow\mathscr{B}}\mathbf{M}_{\mathscr{B}\leftarrow\mathscr{D}} = \mathbf{I}$. □

La matrice $\mathbf{M}_{\mathscr{B}\leftarrow\mathscr{D}}$ si chiama *matrice del cambiamento di base*. Consigliamo al lettore di non cercare di imparare a memoria le formule, ma di ricordare il procedimento con cui si è costruita $\mathbf{M}_{\mathscr{B}\leftarrow\mathscr{D}}$: si vuole che $\mathrm{C}_{\mathscr{B}}(\mathbf{v}) = \mathbf{M}_{\mathscr{B}\leftarrow\mathscr{D}}\,\mathrm{C}_{\mathscr{D}}(\mathbf{v})$ ed è facile calcolare le coordinate dei vettori della base $\mathscr{D}$ rispetto a $\mathscr{D}$, perché sono proprio i vettori della base canonica di $\mathbb{C}^n$. Inoltre $\mathbf{A}\mathbf{e}_i$ è la i-esima colonna della matrice $\mathbf{A}$.

Un caso particolare di queste matrici si ha quando $V = \mathbb{C}^n$ e una delle basi è la base canonica $\mathscr{E}$. Vogliamo dunque calcolare $\mathbf{M}_{\mathscr{E}\leftarrow\mathscr{B}}$, dove $\mathscr{B}$ è un'altra base di $\mathbb{C}^n$. Secondo la definizione, posto $\mathscr{B} = \{\mathbf{v}_1; \dots; \mathbf{v}_n\}$, dobbiamo calcolare $\mathrm{C}_{\mathscr{E}}(\mathbf{v}_i)$ e questo è facile, per quanto visto nell'esempio 6.2 (3): $\mathrm{C}_{\mathscr{E}}(\mathbf{v}_i) = \mathbf{v}_i$. Dunque

$$\mathbf{M}_{\mathscr{E}\leftarrow\mathscr{B}} = [\mathbf{v}_1\ \mathbf{v}_2\ \dots\ \mathbf{v}_n].$$

Per esercizio si verifichi che, data un'altra base $\mathscr{D}$ di $\mathbb{C}^n$, si ha

$$\mathbf{M}_{\mathscr{B}\leftarrow\mathscr{D}} = \mathbf{M}_{\mathscr{E}\leftarrow\mathscr{B}}^{-1}\mathbf{M}_{\mathscr{E}\leftarrow\mathscr{D}}.$$

Più in generale, si dimostri che, se $\mathscr{B}$, $\mathscr{D}$ e $\mathscr{F}$ sono basi dello spazio vettoriale V, si ha

$$\mathbf{M}_{\mathscr{B}\leftarrow\mathscr{F}} = \mathbf{M}_{\mathscr{B}\leftarrow\mathscr{D}}\mathbf{M}_{\mathscr{D}\leftarrow\mathscr{F}}.$$

Come abbiamo visto nella sezione precedente, le coordinate permettono di trasferire questioni sugli spazi vettoriali a questioni su matrici. Il caso principale è quello delle applicazioni lineari. Con una tecnica analoga a quella per le matrici del cambiamento di base, assoceremo a un'applicazione lineare una matrice.

Teorema 6.4. *Sia $f\colon V \to W$ un'applicazione lineare tra spazi vettoriali; siano $\mathscr{B}$ una base di V e $\mathscr{D}$ una base di W. Se $n = \dim V$ e $m = \dim W$, esiste una e una sola matrice $\mathbf{A}$ di dimensioni $m \times n$ tale che, per ogni $\mathbf{v} \in V$,*

$$\mathrm{C}_{\mathscr{D}}(f(\mathbf{v})) = \mathbf{A}\,\mathrm{C}_{\mathscr{B}}(\mathbf{v}).$$

Dimostrazione. Come nel caso delle matrici del cambiamento di base vediamo prima l'unicità di $\mathbf{A}$. Poniamo $\mathscr{B} = \{\mathbf{v}_1;\dots;\mathbf{v}_n\}$ e ricordiamo che $\mathrm{C}_{\mathscr{B}}(\mathbf{v}_i) = \mathbf{e}_i$. Dunque dobbiamo avere

$$\mathrm{C}_{\mathscr{D}}(f(\mathbf{v}_i)) = \mathbf{A}\,\mathrm{C}_{\mathscr{B}}(\mathbf{v}_i) = \mathbf{A}\mathbf{e}_i = i\text{-esima colonna di } \mathbf{A}.$$

Perciò, se la matrice $\mathbf{A}$ esiste, deve essere

$$\mathbf{A} = \begin{bmatrix}\mathrm{C}_{\mathscr{D}}(f(\mathbf{v}_1)) & \mathrm{C}_{\mathscr{D}}(f(\mathbf{v}_2)) & \dots & \mathrm{C}_{\mathscr{D}}(f(\mathbf{v}_n))\end{bmatrix}.$$

Facciamo vedere che questa matrice fa proprio al caso nostro. Sia $\mathbf{v} \in V$ e scriviamo $\mathbf{v} = \sum_{i=1}^{n} \alpha_i\mathbf{v}_i$, cioè $\mathrm{C}_{\mathscr{B}}(\mathbf{v}) = [\alpha_1 \ \dots \ \alpha_n]^T$. Allora

$$\begin{aligned}
\mathrm{C}_{\mathscr{D}}(f(\mathbf{v})) = \mathrm{C}_{\mathscr{D}}\Bigl(f\Bigl(\sum_{i=1}^{n}\alpha_i\mathbf{v}_i\Bigr)\Bigr) &= \sum_{i=1}^{n}\alpha_i\,\mathrm{C}_{\mathscr{D}}(f(\mathbf{v}_i)) \\
&= \sum_{i=1}^{n}\alpha_i\mathbf{A}\mathbf{e}_i = \mathbf{A}\Bigl(\sum_{i=1}^{n}\alpha_i\mathbf{e}_i\Bigr) \\
&= \mathbf{A}\,\mathrm{C}_{\mathscr{B}}(\mathbf{v}),
\end{aligned}$$

come si desiderava. □

La matrice $\mathbf{A}$ così trovata si chiama *matrice associata a f rispetto alla base $\mathscr{B}$ sul dominio e alla base $\mathscr{D}$ sul codominio.* L'unicità dice che, ogni volta che si trovi una matrice che svolge il compito della matrice associata, allora essa *è* la matrice associata.

Esempio 6.5. Prendiamo un'applicazione lineare $f\colon \mathbb{C}^n \to \mathbb{C}^m$. Se su dominio e codominio prendiamo le basi canoniche $\mathscr{E}_n$ e $\mathscr{E}_m$, possiamo calcolare la matrice associata a f. Sarà la matrice $\mathbf{A}$ di dimensioni $m \times n$ tale che, per ogni $\mathbf{v} \in \mathbb{C}^n$,

$$\mathrm{C}_{\mathscr{E}_m}(f(\mathbf{v})) = \mathbf{A}\,\mathrm{C}_{\mathscr{E}_n}(\mathbf{v}) \qquad \text{cioè} \qquad f(\mathbf{v}) = \mathbf{A}\mathbf{v}$$

per le proprietà della base canonica. Dunque ogni applicazione lineare $\mathbb{C}^n \to \mathbb{C}^m$ è la moltiplicazione per una matrice. □

Vediamo un primo uso della matrice associata: il rango di un'applicazione lineare si può calcolare tramite il rango della sua matrice associata.

Proposizione 6.6. *Sia $f\colon V \to W$ un'applicazione lineare tra spazi vettoriali; siano $\mathscr{B}$ una base di V e $\mathscr{D}$ una base di W. Se $\mathbf{A}$ è la matrice associata a f rispetto a queste basi, allora*

$$\dim \operatorname{Im}(f) = \operatorname{rk}\mathbf{A}.$$

Di conseguenza $\dim \mathrm{N}(f) = \dim V - \operatorname{rk}\mathbf{A}$.

Dimostrazione. Poniamo $\mathscr{B} = \{\mathbf{v}_1; \dots; \mathbf{v}_n\}$. Sia $k = \operatorname{rk}\mathbf{A}$; allora sappiamo trovare un insieme di k colonne di $\mathbf{A}$ linearmente indipendenti. Per non complicare le notazioni supponiamo che l'insieme sia quello delle prime k colonne. Allora l'insieme

$$\{\mathrm{C}_{\mathscr{D}}(f(\mathbf{v}_1)); \mathrm{C}_{\mathscr{D}}(f(\mathbf{v}_2)); \dots; \mathrm{C}_{\mathscr{D}}(f(\mathbf{v}_k))\}$$

è linearmente indipendente e quindi anche l'insieme

$$\{f(\mathbf{v}_1); f(\mathbf{v}_2); \dots; f(\mathbf{v}_k)\}$$

è linearmente indipendente. Siccome è un insieme di vettori in $\operatorname{Im}(f)$ ne segue che $\dim \operatorname{Im}(f) \le k$.

La disuguaglianza inversa si dimostra in modo analogo. Siccome $f[\mathscr{B}]$ è un insieme di generatori di $\operatorname{Im}(f)$, da essa possiamo estrarre una base. Possiamo allora riordinare i vettori di $\mathscr{B}$ in modo che la base estratta sia $\{f(\mathbf{v}_1); \dots; f(\mathbf{v}_{k'})\}$ e ne deduciamo che $\{\mathrm{C}_{\mathscr{D}}(f(\mathbf{v}_1)); \dots; \mathrm{C}_{\mathscr{D}}(f(\mathbf{v}_{k'}))\}$ è un insieme linearmente indipendente in $\mathbb{C}^n$. Questi vettori sono k' colonne di $\mathbf{A}$, quindi $\dim \operatorname{Im}(f) = k' \le \operatorname{rk}\mathbf{A}$, come si voleva. □

Nella dimostrazione abbiamo usato il fatto che un'applicazione lineare biiettiva, in particolare l'applicazione delle coordinate o la sua inversa, trasforma insiemi linearmente indipendenti in insiemi linearmente indipendenti.

Talvolta è data la matrice associata a un'applicazione lineare rispetto a basi che non sono quelle che ci interessano; quale sarà la relazione fra due matrici associate?

Fissiamo le notazioni: avremo l'applicazione lineare $f\colon V \to W$; le basi $\mathscr{B}$ e $\mathscr{B}'$ di V; le basi $\mathscr{D}$ e $\mathscr{D}'$ di W; la matrice $\mathbf{A}$ associata a f rispetto alle basi $\mathscr{B}$ e $\mathscr{D}$; la matrice $\mathbf{A}'$ associata a f rispetto alle basi $\mathscr{B}'$ e $\mathscr{D}'$.

Assumiamo di conoscere $\mathbf{A}'$ e cerchiamo di calcolare $\mathbf{A}$, usando ovviamente le matrici dei cambiamenti di base. Ci serve una matrice $\mathbf{A}$ con la proprietà che, per ogni $\mathbf{v} \in V$,

$$\mathrm{C}_{\mathscr{D}}(f(\mathbf{v})) = \mathbf{A}\,\mathrm{C}_{\mathscr{B}}(\mathbf{v}).$$

Abbiamo a disposizione le seguenti uguaglianze, valide per ogni $\mathbf{v} \in V$ e ogni $\mathbf{w} \in W$:

$$(1) \qquad \mathrm{C}_{\mathscr{D}'}(f(\mathbf{v})) = \mathbf{A}'\,\mathrm{C}_{\mathscr{B}'}(\mathbf{v})$$

$$(2) \qquad \mathrm{C}_{\mathscr{B}}(\mathbf{v}) = \mathbf{M}_{\mathscr{B}\leftarrow\mathscr{B}'}\,\mathrm{C}_{\mathscr{B}'}(\mathbf{v})$$

$$(3) \qquad \mathrm{C}_{\mathscr{D}}(\mathbf{w}) = \mathbf{M}_{\mathscr{D}\leftarrow\mathscr{D}'}\,\mathrm{C}_{\mathscr{D}'}(\mathbf{w})$$

Abbiamo allora, indicando sopra il segno di uguaglianza quale relazione stiamo impiegando,

$$\mathrm{C}_{\mathscr{D}}(f(\mathbf{v})) \overset{(3)}{=} \mathbf{M}_{\mathscr{D}\leftarrow\mathscr{D}'}\mathrm{C}_{\mathscr{D}'}(f(\mathbf{v})) \overset{(1)}{=} \mathbf{M}_{\mathscr{D}\leftarrow\mathscr{D}'}\mathbf{A}'\mathrm{C}_{\mathscr{B}'}(\mathbf{v}) \overset{(2)}{=} \mathbf{M}_{\mathscr{D}\leftarrow\mathscr{D}'}\mathbf{A}'\mathbf{M}^{-1}_{\mathscr{B}\leftarrow\mathscr{B}'}\mathrm{C}_{\mathscr{B}}(\mathbf{v}).$$

Per l'unicità della matrice associata, avremo

$$\mathbf{A} = \mathbf{M}_{\mathscr{D}\leftarrow\mathscr{D}'}\mathbf{A}'\mathbf{M}^{-1}_{\mathscr{B}\leftarrow\mathscr{B}'}.$$

Abbiamo quindi già la dimostrazione del risultato seguente.

Teorema 6.7. *Sia $f\colon V \to W$ un'applicazione lineare, siano $\mathscr{B}$ e $\mathscr{B}'$ due basi di V, $\mathscr{D}$ e $\mathscr{D}'$ due basi di W. Se $\mathbf{A}$ (risp., $\mathbf{A}'$) denota la matrice associata a f rispetto alle basi $\mathscr{B}$ e $\mathscr{D}$ (risp., $\mathscr{B}'$ e $\mathscr{D}'$), allora $\mathbf{A}$ e $\mathbf{A}'$ sono legate dalla relazione*

$$\mathbf{A} = \mathbf{M}_{\mathscr{D}\leftarrow\mathscr{D}'}\mathbf{A}'\mathbf{M}^{-1}_{\mathscr{B}\leftarrow\mathscr{B}'}. \qquad \square$$

Ancora una volta raccomandiamo di non imparare a memoria la formula, ma di impadronirsi del procedimento.

Esempio 6.8. La matrice associata all'applicazione lineare $f\colon \mathbb{C}^3 \to \mathbb{C}^2$ rispetto alla base

$$\mathscr{B} = \left\{ \mathbf{v}_1 = \begin{bmatrix} 1 \\ 1 \\ -1 \end{bmatrix}; \mathbf{v}_2 = \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix}; \mathbf{v}_3 = \begin{bmatrix} -1 \\ 1 \\ 1 \end{bmatrix} \right\}$$

sul dominio $\mathbb{C}^3$ e alla base

$$\mathscr{D} = \left\{ \mathbf{w}_1 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}; \mathbf{w}_2 = \begin{bmatrix} 1 \\ -1 \end{bmatrix} \right\}$$

sul codominio $\mathbb{C}^2$ sia

$$\mathbf{B} = \begin{bmatrix} 1 & 2 & 0 \\ 2 & -1 & 1 \end{bmatrix}.$$

Desideriamo conoscere la matrice $\mathbf{A}$ associata a f rispetto alle basi canoniche su dominio e codominio. Scriviamo dunque le formule necessarie, dove poniamo $\mathbf{P} = \mathbf{M}_{\mathscr{E}_3\leftarrow\mathscr{B}}$ e $\mathbf{S} = \mathbf{M}_{\mathscr{E}_2\leftarrow\mathscr{D}}$ per brevità:

$$\begin{aligned}
&(0) \qquad \mathrm{C}_{\mathscr{E}_2}(f(\mathbf{v})) = \mathbf{A}\,\mathrm{C}_{\mathscr{E}_3}(\mathbf{v}),\\
&(1) \qquad \mathrm{C}_{\mathscr{D}}(f(\mathbf{v})) = \mathbf{B}\,\mathrm{C}_{\mathscr{B}}(\mathbf{v}),\\
&(2) \qquad \mathrm{C}_{\mathscr{E}_3}(\mathbf{v}) = \mathbf{P}\,\mathrm{C}_{\mathscr{B}}(\mathbf{v}),\\
&(3) \qquad \mathrm{C}_{\mathscr{E}_2}(\mathbf{w}) = \mathbf{S}\,\mathrm{C}_{\mathscr{D}}(\mathbf{w}).
\end{aligned}$$

Abbiamo indicato con $\mathscr{E}_2$ e $\mathscr{E}_3$ le basi canoniche di $\mathbb{C}^2$ e $\mathbb{C}^3$ rispettivamente; secondo quanto appreso, la matrice $\mathbf{P} = \mathbf{M}_{\mathscr{E}_3\leftarrow\mathscr{B}}$ si scrive come

$$\mathbf{P} = [\mathrm{C}_{\mathscr{E}_3}(\mathbf{v}_1)\ \mathrm{C}_{\mathscr{E}_3}(\mathbf{v}_2)\ \mathrm{C}_{\mathscr{E}_3}(\mathbf{v}_3)] = [\mathbf{v}_1\ \mathbf{v}_2\ \mathbf{v}_3],$$

mentre $\mathbf{S} = \mathbf{M}_{\mathscr{E}_2 \leftarrow \mathscr{D}}$ si scrive come

$$\mathbf{S} = [\mathrm{C}_{\mathscr{E}_2}(\mathbf{w}_1)\ \mathrm{C}_{\mathscr{E}_2}(\mathbf{w}_2)] = [\mathbf{w}_1\ \mathbf{w}_2].$$

Vogliamo dunque esprimere una relazione del genere di (0), attraverso le altre tre relazioni. Sia $\mathbf{v} \in \mathbb{C}^3$; allora

$$\begin{aligned} \mathrm{C}_{\mathscr{E}_2}(f(\mathbf{v})) &= \mathbf{S}\,\mathrm{C}_{\mathscr{D}}(f(\mathbf{v})) \\ &= \mathbf{SB}\,\mathrm{C}_{\mathscr{B}}(\mathbf{v}) \\ &= \mathbf{SBP}^{-1}\,\mathrm{C}_{\mathscr{E}_3}(\mathbf{v}) \end{aligned}$$

e dunque

$$\mathbf{A} = \mathbf{SBP}^{-1}.$$

Calcoliamo l'inversa di $\mathbf{P}$:

$$\left[\begin{array}{ccc|ccc} 1 & 1 & -1 & 1 & 0 & 0 \\ 1 & -1 & 1 & 0 & 1 & 0 \\ -1 & 1 & 1 & 0 & 0 & 1 \end{array}\right] \to \dots \to \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1/2 & 1/2 & 0 \\ 0 & 1 & 0 & 1/2 & 0 & 1/2 \\ 0 & 0 & 1 & 0 & 1/2 & 1/2 \end{array}\right]$$

dunque

$$\mathbf{P}^{-1} = \begin{bmatrix} 1/2 & 1/2 & 0 \\ 1/2 & 0 & 1/2 \\ 0 & 1/2 & 1/2 \end{bmatrix}$$

e quindi la matrice cercata è

$$\mathbf{A} = \mathbf{SBP}^{-1} = \begin{bmatrix} 2 & 2 & 1 \\ 1 & -1 & 1 \end{bmatrix}.$$

L'importanza di conoscere la matrice associata rispetto alle basi canoniche risiede nel fatto che, per ogni $\mathbf{v} \in \mathbb{C}^3$,

$$f(\mathbf{v}) = \mathrm{C}_{\mathscr{E}_2}(f(\mathbf{v})) = \mathbf{A}\,\mathrm{C}_{\mathscr{E}_3}(\mathbf{v}) = \mathbf{Av}$$

cioè $f(\mathbf{v}) = \mathbf{Av}$ e quindi f coincide con la pre-moltiplicazione per $\mathbf{A}$. □

Osserviamo che, quando l'applicazione lineare $f\colon V \to W$ è biiettiva, anche l'inversa $f^{-1}\colon W \to V$ è lineare. Questo è ovvio nei casi già incontrati, ma è vero in generale. Supponiamo infatti $\mathbf{w}_1, \mathbf{w}_2 \in W$ e siano α_1 e α_2 scalari. Allora

$$\mathbf{w}_1 = f(\mathbf{v}_1) \quad \text{e} \quad \mathbf{w}_2 = f(\mathbf{v}_2)$$

dove $\mathbf{v}_1 = f^{-1}(\mathbf{w}_1)$ e $\mathbf{v}_2 = f^{-1}(\mathbf{w}_2)$. Abbiamo

$$\begin{aligned} f^{-1}(\alpha_1\mathbf{w}_1 + \alpha_2\mathbf{w}_2) &= f^{-1}(\alpha_1 f(\mathbf{v}_1) + \alpha_2 f(\mathbf{v}_2)) \\ &= f^{-1}(f(\alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2)) \\ &= \alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2 \\ &= \alpha_1 f^{-1}(\mathbf{w}_1) + \alpha_2 f^{-1}(\mathbf{w}_2). \end{aligned}$$

Definizione. Un'applicazione lineare $f: V \to W$ si dice un *isomorfismo* se è biiettiva, cioè iniettiva e suriettiva. Se esiste un isomorfismo $f: V \to W$ diremo che V e W sono *isomorfi.*

Il fatto che due spazi vettoriali finitamente generati siano isomorfi è equivalente al fatto che abbiano la stessa dimensione.

Proposizione 6.9. *Siano V e W spazi vettoriali finitamente generati. Allora V e W sono isomorfi se e solo se* $\dim V = \dim W$.

Dimostrazione. Supponiamo che $f: V \to W$ sia un isomorfismo e sia $\mathscr{B}$ una base di V. Allora $f[\mathscr{B}]$ è un insieme linearmente indipendente in W e quindi $\dim V \le \dim W$. Considerando f^{-1}, otteniamo che $\dim W \le \dim V$.

Supponiamo, viceversa, che $\dim V = \dim W$ e siano $\mathscr{B} = \{\mathbf{v}_1; \dots \mathbf{v}_n\}$, $\mathscr{D} = \{\mathbf{w}_1; \dots; \mathbf{w}_n\}$ basi di V e W rispettivamente. Per il Teorema 4.14, esiste un'unica applicazione lineare $f: V \to W$ tale che

$$f(\mathbf{v}_i) = \mathbf{w}_i \qquad (i = 1, \dots, n).$$

Allora f è suriettiva perché $\operatorname{Im}(f) \supseteq \langle \mathscr{D} \rangle = W$ e, per il Teorema nullità + rango, f è iniettiva. □

In alcuni casi è possibile trovare isomorfismi fra due spazi vettoriali che danno informazioni supplementari. Diamo alcuni esempi di isomorfismi importanti.

Esempi 6.10. (1) Se $\mathbf{A}$ e $\mathbf{B}$ sono matrici $m \times n$ e $\mathbf{B} = \mathbf{FA}$, con $\mathbf{F}$ invertibile, allora $C(\mathbf{A})$ è isomorfo a $C(\mathbf{B})$.

Sia infatti $\mathbf{v} \in C(\mathbf{A})$; allora $\mathbf{v} = \sum_{i=1}^n \alpha_i \mathbf{a}_i$, dove abbiamo posto $\mathbf{A} = [\mathbf{a}_1 \ \dots \ \mathbf{a}_n]$. Allora

$$\mathbf{Fv} = \sum_{i=1}^n \alpha_i \mathbf{Fa}_i = \sum_{i=1}^n \alpha_i \mathbf{b}_i \in C(\mathbf{B}),$$

dove $\mathbf{B} = [\mathbf{b}_1 \ \dots \ \mathbf{b}_n]$. Quindi ponendo $f(\mathbf{v}) = \mathbf{Fv}$, per $\mathbf{v} \in C(\mathbf{A})$, otteniamo un'applicazione $f: C(\mathbf{A}) \to C(\mathbf{B})$ che è evidentemente lineare. Analogamente abbiamo l'applicazione $g: C(\mathbf{B}) \to C(\mathbf{A})$ definita da $g(\mathbf{w}) = \mathbf{F}^{-1}\mathbf{w}$ e, chiaramente, g è l'inversa di f.

Abbiamo in realtà già usato questo esempio; qui l'isomorfismo fra i due spazi è definito in modo naturale.

(2) Sia $\mathbf{A}$ una matrice $m \times n$. Siccome $\dim C(\mathbf{A}^H) = \dim C(\mathbf{A})$, gli spazi vettoriali $C(\mathbf{A}^H)$ e $C(\mathbf{A})$ sono isomorfi. Anche in questo caso esiste un isomorfismo definito in modo naturale. Consideriamo infatti $\mathbf{A} = [\mathbf{a}_1 \ \dots \ \mathbf{a}_n]$. Allora, $\mathbf{A}^H\mathbf{a}_i \in C(\mathbf{A}^H)$, quindi abbiamo l'applicazione $f: C(\mathbf{A}) \to C(\mathbf{A}^H)$ definita da $f(\mathbf{v}) = \mathbf{A}^H\mathbf{v}$.

Per il Teorema nullità + rango ci basta dimostrare che f è iniettiva. Ora, $\mathbf{v} \in C(\mathbf{A})$ se e solo se $\mathbf{v} = \mathbf{Au}$, per un opportuno $\mathbf{u} \in \mathbb{C}^n$. Se $f(\mathbf{v}) = \mathbf{0}$, abbiamo $\mathbf{0} = \mathbf{A}^H\mathbf{Au}$ e quindi

$$0 = \mathbf{u}^H\mathbf{A}^H\mathbf{Au} = (\mathbf{Au})^H\mathbf{Au} = \mathbf{v}^H\mathbf{v}$$

da cui ricaviamo, come in 4.12 del Capitolo 1, che $\mathbf{v} = \mathbf{0}$. □

Esercizi

Paragrafo 1

2.1. Si esegua la verifica delle regole di calcolo nello spazio vettoriale $\mathscr{C}([a,b])$.

2.2. Nello spazio vettoriale $\mathbb{C}^3$ si considerino i seguenti sottoinsiemi:

$$
\begin{aligned}
&(1)\quad X_1 = \{[\alpha_1\ \alpha_2\ \alpha_3]^T \mid \alpha_2 = 0\}\\
&(2)\quad X_2 = \{[\alpha_1\ \alpha_2\ \alpha_3]^T \mid \alpha_1 + \alpha_2 - \alpha_3 = 1\}\\
&(3)\quad X_3 = \{[\alpha_1\ \alpha_2\ \alpha_3]^T \mid \alpha_1 + \alpha_2 - \alpha_3 = 0\}\\
&(4)\quad X_4 = \{[\alpha_1\ \alpha_2\ \alpha_3]^T \mid \alpha_1^2 - \alpha_2^2 = 0\}
\end{aligned}
$$

e si dica quali sono sottospazi e quali no.

2.3. Si considerino i seguenti sottoinsiemi dello spazio vettoriale $\mathscr{C}([-1,1])$:

$$
\begin{aligned}
&(1)\quad X_1 = \{f \in \mathscr{C}([-1,1]) \mid f(0) = 0\}\\
&(2)\quad X_2 = \{f \in \mathscr{C}([-1,1]) \mid f(0) = 1\}\\
&(3)\quad X_3 = \{f \in \mathscr{C}([-1,1]) \mid f(-1) + f(1) = 0\}\\
&(4)\quad X_4 = \{f \in \mathscr{C}([-1,1]) \mid f(-1) = f(1)\}
\end{aligned}
$$

e si dica quali sono sottospazi e quali no.

2.4. Sia $\mathbf{A} \in \mathrm{M}_n(\mathbb{C})$ e si consideri

$$U = \{\mathbf{X} \in \mathrm{M}_n(\mathbb{C}) \mid \mathbf{AX} = \mathbf{XA}\}.$$

Si dimostri che U è un sottospazio di $\mathrm{M}_n(\mathbb{C})$.

2.5. Siano U_1 e U_2 sottospazi dello spazio vettoriale V. Si esegua la verifica delle proprietà che rendono $U_1 + U_2$ un sottospazio di V.

2.6. Si provi che le matrici reali e simmetriche $n \times n$ formano un sottospazio dello spazio reale $\mathrm{M}_n(\mathbb{R})$, mentre le matriche complesse hermitiane $n \times n$ non formano un sottospazio dello spazio vettoriale complesso $\mathrm{M}_n(\mathbb{C})$.

2.7. Si provi che l'insieme $\mathscr{U}$ delle matrici triangolari superiori e l'insieme $\mathscr{L}$ delle matrici triangolari inferiori sono sottospazi di $\mathrm{M}_n(\mathbb{C})$. Si determinino i sottospazi $\mathscr{U} \cap \mathscr{L}$ e $\mathscr{U} + \mathscr{L}$.

Paragrafo 2

2.8. Si indichi una base di $\mathrm{M}_{m\times n}(\mathbb{R})$. Si dimostri, viceversa, che lo spazio vettoriale $\mathscr{C}([a,b])$ delle funzioni reali continue sull'intervallo $[a,b]$ non è finitamente generato.

2.9. Si consideri, come nell'esercizio 2.4, $n = 2$ e $\mathbf{A} = \left[\begin{smallmatrix} 1 & -1 \\ 0 & 0 \end{smallmatrix}\right]$. Si verifichi che l'insieme

$$\left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}; \begin{bmatrix} 1 & -1 \\ 0 & 0 \end{bmatrix}; \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}; \begin{bmatrix} 2 & 1 \\ 0 & 3 \end{bmatrix} \right\}$$

è un insieme di generatori di U.

2.10. Si dimostri, per induzione, che ogni insieme di colonne dominanti di una matrice in forma ridotta è linearmente indipendente.

2.11. Si provi che in una matrice $\mathbf{U}$ in forma ridotta una colonna non dominante è combinazione lineare delle colonne che la precedono.

2.12. Si trovi una base per lo spazio vettoriale delle matrici reali simmetriche $n \times n$.

2.13. Si trovi una base per lo spazio vettoriale delle matrici reali anti-simmetriche $n \times n$.

2.14. Si determini una base del sottospazio U di $\mathrm{M}_2(\mathbb{C})$ dell'esercizio 2.9.

Paragrafo 3

2.15. Si usi la Proposizione 3.17 per determinare la dimensione del sottospazio $U_1 + U_2$ di $\mathbb{C}^4$, dove

$$U_1 = \{ [x_1 \ x_2 \ x_3 \ x_4]^T \mid x_1 - 2x_2 + x_3 - x_4 = 0 \},$$

$$U_2 = \left\langle \begin{bmatrix} 1 \\ 2 \\ 3 \\ 1 \end{bmatrix}; \begin{bmatrix} -1 \\ 0 \\ 2 \\ 2 \end{bmatrix}; \begin{bmatrix} 0 \\ 2 \\ 5 \\ 3 \end{bmatrix} \right\rangle.$$

2.16. Sia U un sottospazio di $\mathbb{C}^n$ e si consideri l'insieme U' delle matrici $\mathbf{A} \in \mathrm{M}_{m\times n}(\mathbb{C})$ tali che ogni colonna di $\mathbf{A}$ appartiene a U. Si dimostri che, se $\mathscr{B} = \{\mathbf{u}_1; \mathbf{u}_2; \dots; \mathbf{u}_k\}$ è una base di U, allora le matrici in cui una sola colonna è in $\mathscr{B}$ e le altre sono nulle è una base di U'. Si calcoli quindi la dimensione di U'.

2.17. Si dimostri, per induzione su k, la Proposizione 3.19.

2.18. Si dimostri che i sottospazi U_1, U_2, ..., U_k dello spazio vettoriale V sono indipendenti se e solo se, per ogni $i \le k$, $U_i \cap \sum_{j \ne i} U_j = \{\mathbf{0}\}$.

2.19. Dati tre sottospazi U, V e W di uno spazio vettoriale finitamente generato, si provi che

$$\begin{aligned} \dim U + \dim V + \dim W &= \dim(U + V + W) + \dim(V \cap W) + \dim(U \cap (V + W)) \\ &= \dim(U \cap V \cap W) + \dim(V + W) + \dim(U + (V \cap W)). \end{aligned}$$

2.20. Sia $\{\mathbf{v}_1; \mathbf{v}_2; \dots; \mathbf{v}_n\}$ una base dello spazio vettoriale V. L'insieme

$$\{\mathbf{v}_1 - \mathbf{v}_2; \mathbf{v}_2 - \mathbf{v}_3; \dots; \mathbf{v}_{n-1} - \mathbf{v}_n; \mathbf{v}_n - \mathbf{v}_1\}$$

è anch'esso una base di V?

Paragrafo 4

2.21. Sia $f\colon V \to W$ un'applicazione lineare, con V e W finitamente generati. Si dimostri che, se $\dim V = \dim W$, allora f è iniettiva se e solo se f è suriettiva.

Si dimostri che, se $\dim V \neq \dim W$ e f è iniettiva (rispettivamente, suriettiva), allora f non è suriettiva (rispettivamente, iniettiva).

2.22. Si dia un esempio di applicazione lineare iniettiva ma non suriettiva avente dominio e codominio uguali. Suggerimento: il dominio non può essere finitamente generato; si cerchi dunque un'applicazione lineare $f\colon \mathscr{P}(\mathbb{C}) \to \mathscr{P}(\mathbb{C})$.

2.23. Sia $\mathbf{F}$ una matrice $m \times n$. Si dimostri che l'applicazione $f\colon \mathrm{M}_{n\times p} \to \mathrm{M}_{m\times p}$ definita da $f(\mathbf{X}) = \mathbf{FX}$ è lineare. Si calcoli la dimensione dell'immagine di f in termini del rango di F. Suggerimento: una matrice $\mathbf{X} = [\mathbf{x}_1\ \mathbf{x}_2\ \dots\ \mathbf{x}_p]$ appartiene allo spazio nullo di f se e solo se $\mathbf{x}_i \in \mathrm{N}(\mathbf{F})$ $(i = 1, 2, \dots, p)$; si applichino l'esercizio 2.11 e il Teorema nullità + rango.

2.24. Siano $f\colon V \to W$ un'applicazione lineare e U un sottospazio di W. Si provi che $f^{\leftarrow}(U) = \{\mathbf{v} \in V \mid f(\mathbf{v}) \in U\}$ è un sottospazio di V.

2.25. Sia U un sottospazio dello spazio vettoriale V. Per ogni $\mathbf{v}, \mathbf{v}' \in V$ e $\alpha \in \mathbb{C}$, si ponga

$$[\mathbf{v}] = \{\mathbf{v} + \mathbf{u} \mid \mathbf{u} \in U\}, \qquad [\mathbf{v}] + [\mathbf{v}'] = [\mathbf{v} + \mathbf{v}'], \quad \alpha[\mathbf{v}] = [\alpha\mathbf{v}].$$

Si provi che in tal modo l'insieme $W = \{\,[\mathbf{v}] \mid \mathbf{v} \in V\,\}$ diventa uno spazio vettoriale.

2.26. Nelle notazioni dell'Esercizio precedente, si provi che l'applicazione $\pi\colon V \to W$ definita ponendo $\pi(\mathbf{v}) = [\mathbf{v}]$ è lineare e suriettiva e che $\mathrm{N}(\pi) = U$.

2.27. Dimostrare per induzione il Corollario 4.4.

2.28. Si mostri che l'applicazione lineare $f_{\mathbf{A}}$ dell'Esempio 4.6 (1) coincide con la trasformazione di un generico vettore di $\mathbb{R}^2$ nel suo simmetrico rispetto alla retta $y = x$.

2.29. Si mostri che l'applicazione lineare $f_{\mathbf{A}}$ dell'Esempio 4.6 (2) coincide con la rotazione del generico vettore di $\mathbb{R}^2$ in senso antiorario di un angolo di α radianti.

2.30. Dimostrazione con applicazioni lineari della Proposizione 3.17. Sia $U_1 \times U_2$ lo spazio vettoriale formato dalle coppie $(\mathbf{u}_1, \mathbf{u}_2)$ $(\mathbf{u}_i \in U_i)$ con le ovvie operazioni. Sia $\varphi\colon U_1 \times U_2 \to V$ l'applicazione definita ponendo $\varphi(\mathbf{u}_1, \mathbf{u}_2) = \mathbf{u}_1 - \mathbf{u}_2$. Provare che: φ è lineare; $\mathrm{Im}(\varphi) = U_1 + U_2$; $\mathrm{N}(\varphi)$ è isomorfo a $U_1 \cap U_2$. Concludere con il Teorema nullità + rango.

Paragrafo 5

2.31. Siano $\mathbf{A}$ e $\mathbf{B}$ due matrici in $\mathrm{M}_{m\times n}(\mathbb{C})$. Provare che valgono le inclusioni $\mathrm{C}(\mathbf{A}+\mathbf{B}) \subseteq \mathrm{C}(\mathbf{A}) + \mathrm{C}(\mathbf{B})$ e $\mathrm{N}(\mathbf{A}) \cap \mathrm{N}(\mathbf{B}) \subseteq \mathrm{N}(\mathbf{A}+\mathbf{B})$.

2.32. Si supponga che nell'Esercizio precedente risulti $\mathrm{rk}(\mathbf{A}+\mathbf{B}) = \mathrm{rk}\,\mathbf{A} + \mathrm{rk}\,\mathbf{B}$. Si provi che allora $\mathrm{C}(\mathbf{A}) \cap \mathrm{C}(\mathbf{B}) = \{\mathbf{0}\}$, $\mathrm{C}(\mathbf{A}+\mathbf{B}) = \mathrm{C}(\mathbf{A}) \oplus \mathrm{C}(\mathbf{B})$ e $\mathrm{N}(\mathbf{A}) \cap \mathrm{N}(\mathbf{B}) = \mathrm{N}(\mathbf{A}+\mathbf{B})$ (si usi la Proposizione 3.17).

2.33. Nelle ipotesi dell'Esercizio precedente si provi che $\mathrm{N}(\mathbf{A}) + \mathrm{N}(\mathbf{B}) = \mathbb{C}^n$.

Paragrafo 6

2.34. Si consideri l'applicazione lineare $f\colon \mathrm{M}_{2\times 3}(\mathbb{C}) \to \mathrm{M}_{2\times 3}(\mathbb{C})$ definita da $f(\mathbf{X}) = \mathbf{AX}$, dove $\mathbf{A}$ è una matrice 2×2. Si scriva la matrice associata a f rispetto alla base di $\mathrm{M}_{2\times 3}(\mathbb{C})$ formata dalle matrici con un solo coefficiente uguale a 1 e gli altri nulli.

2.35. Date due matrici $\mathbf{A}$ e $\mathbf{A}'$ di $\mathrm{M}_n(\mathbb{C})$ si dice che $\mathbf{A}$ *è simile ad* $\mathbf{A}'$ se esiste una matrice invertibile $\mathbf{S} \in \mathrm{M}_n(\mathbb{C})$ tale che $\mathbf{A} = \mathbf{S}\mathbf{A}'\mathbf{S}^{-1}$. Si provi che la relazione di similitudine è una relazione di equivalenza, cioè che: (1) $\mathbf{A}$ è simile a $\mathbf{A}$; (2) se $\mathbf{A}$ è simile a $\mathbf{A}'$, allora $\mathbf{A}'$ è simile a $\mathbf{A}$; (3) se $\mathbf{A}$ è simile a $\mathbf{A}'$ e $\mathbf{A}'$ è simile a $\mathbf{A}''$, allora $\mathbf{A}$ è simile a $\mathbf{A}''$.

2.36. Si provi che, se nel Teorema 6.7 si suppone $V = W$, $\mathscr{B} = \mathscr{D}$ e $\mathscr{B}' = \mathscr{D}'$, allora $\mathbf{A}$ è simile ad $\mathbf{A}'$.

2.37. Dati due spazi vettoriali V e W, si provi che l'insieme delle applicazioni lineari da V in W, dotato delle operazioni

$$(f+g)(\mathbf{v}) = f(\mathbf{v}) + g(\mathbf{v}), \qquad (\alpha f)(\mathbf{v}) = \alpha f(\mathbf{v})$$

dove $f\colon V \to W$ e $g\colon V \to W$ sono lineari e $\alpha \in \mathbb{C}$, è uno spazio vettoriale che si denota con $\mathrm{Hom}_{\mathbb{C}}(V, W)$.

2.38. Siano $\mathscr{B}$ una base dello spazio vettoriale V e $\mathscr{D}$ una base dello spazio vettoriale W. Si considerino le applicazioni $\Phi\colon \mathrm{Hom}_{\mathbb{C}}(V, W) \to \mathrm{M}_{m\times n}(\mathbb{C})$ (dove $n = \dim V$ e $m = \dim W$) e $\Psi\colon \mathrm{M}_{m\times n}(\mathbb{C}) \to \mathrm{Hom}_{\mathbb{C}}(V, W)$ definite ponendo $\Phi(f) = \mathbf{A}$, matrice associata a f rispetto alle basi $\mathscr{B}$ e $\mathscr{D}$ e $\Psi(\mathbf{A}) = \mathrm{C}_{\mathscr{D}}^{-1}\mathbf{A}\mathrm{C}_{\mathscr{B}}$ sono lineari e una inversa dell'altra.

2.39. Si provi che, se nell'Esercizio precedente si prende $V = W$ e $\mathscr{B} = \mathscr{D}$, allora $\Phi(f \circ g) = \Phi(f)\Phi(g)$ e $\Psi(\mathbf{AB}) = \Psi(\mathbf{A}) \circ \Psi(\mathbf{B})$.

Capitolo 3

Norme, prodotti interni e ortogonalità

Questo Capitolo inizia con delle generalizzazioni dei concetti geometrici di lunghezza di un segmento e di angolo. L'ambito in cui vengono ottenute è quello degli spazi vettoriali euclidei. In questo contesto sorge in modo naturale il problema di studiare le proiezioni ortogonali, e, nel caso specifico degli spazi $\mathbb{R}^n$ e $\mathbb{C}^n$, le matrici che le realizzano. Viene poi descritto l'algoritmo di Gram-Schmidt, che applicato a una base di uno spazio vettoriale euclideo ne produce una con vettori a due a due ortogonali, ossia una base ortogonale. Ciò fornisce lo strumento essenziale per ottenere una decomposizione QR di una matrice, secondo pilastro portante dell'Algebra Lineare. Il Capitolo si chiude con la descrizione del metodo dei minimi quadrati, che viene applicato per l'approssimazione di dati sperimentali per un fenomeno descritto da un'equazione polinomiale.

1. Norme di vettori

In questo Capitolo impiegheremo, per aiutare l'intuizione, l'interpretazione geometrica di $\mathbb{R}^2$ e $\mathbb{R}^3$ quali spazi di dimensione due e tre rispettivamente, forniti di un sistema di coordinate. Rimandiamo il lettore all'Appendice C per i primi elementi di questa interpretazione. In particolare ricordiamo che, fissato su di un piano π un sistema di riferimento ortogonale e monometrico Oxy, la posizione che associa a ogni punto P di π il vettore $\mathbf{v} = [a\ b]^T$, dove a e b sono rispettivamente l'ascissa e l'ordinata di P rispetto a Oxy, definisce una corrispondenza biunivoca tra l'insieme dei punti di π e gli elementi di $\mathbb{R}^2$. Per il teorema di Pitagora, la distanza di P da O, ossia la misura della lunghezza del segmento OP, è data da

$$|OP| = \sqrt{|a|^2 + |b|^2} = \sqrt{a^2 + b^2} = \sqrt{\begin{bmatrix} a & b \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix}} = \sqrt{\mathbf{v}^T \mathbf{v}}.$$

Dunque la funzione definita su $\mathbb{R}^2$ da $f(\mathbf{v}) = \sqrt{\mathbf{v}^T\mathbf{v}}$ esprime algebricamente la lunghezza di un vettore nel piano. Introduciamo ora il concetto di *norma* come generalizzazione di quello di "lunghezza".

Per far ciò, poniamo in evidenza alcune proprietà di cui gode la funzione $f(\mathbf{v}) = \sqrt{\mathbf{v}^T\mathbf{v}}$ definita su $\mathbb{R}^2$, e successivamente chiamiamo norma ogni funzione definita su di un qualsiasi spazio vettoriale V che soddisfi tali proprietà.

Le tre proprietà di $f(\mathbf{v}) = \sqrt{\mathbf{v}^T\mathbf{v}}$, per $\mathbf{v} \in \mathbb{R}^2$, su cui intendiamo porre l'accento sono le seguenti:

(1) $f\left(\begin{bmatrix} a \\ b \end{bmatrix}\right) = \sqrt{a^2+b^2} \geq 0$ per ogni $a, b \in \mathbb{R}$, ed $f\left(\begin{bmatrix} a \\ b \end{bmatrix}\right) = \sqrt{a^2+b^2} = 0$ se e solo se $a = b = 0$.

(2) se $\alpha \in \mathbb{R}$,

$$f\left(\alpha\begin{bmatrix} a \\ b \end{bmatrix}\right) = f\left(\begin{bmatrix} \alpha a \\ \alpha b \end{bmatrix}\right) = \sqrt{(\alpha a)^2 + (\alpha b)^2} = |\alpha|\sqrt{a^2+b^2} = |\alpha| f\left(\begin{bmatrix} a \\ b \end{bmatrix}\right),$$

per ogni $a, b \in \mathbb{R}$.

(3) per ogni $a, b, c, d \in \mathbb{R}$,

$$f\left(\begin{bmatrix} a \\ b \end{bmatrix}\right) + f\left(\begin{bmatrix} c \\ d \end{bmatrix}\right) = f\left(\begin{bmatrix} a+c \\ b+d \end{bmatrix}\right) \leq f\left(\begin{bmatrix} a \\ b \end{bmatrix}\right) + f\left(\begin{bmatrix} c \\ d \end{bmatrix}\right).$$

Per verificare (3), cominciamo con l'osservare che $2acbd \leq b^2c^2 + a^2d^2$, per cui

$$\begin{aligned} ac + bd &\leq \sqrt{(ac+bd)^2} = \sqrt{a^2c^2 + 2acbd + b^2d^2} \leq \sqrt{a^2c^2 + b^2c^2 + a^2d^2 + b^2d^2} \\ &= \sqrt{(a^2+b^2)(c^2+d^2)} = \sqrt{\begin{bmatrix} a & b \end{bmatrix}\begin{bmatrix} a \\ b \end{bmatrix}}\sqrt{\begin{bmatrix} c & d \end{bmatrix}\begin{bmatrix} c \\ d \end{bmatrix}}. \end{aligned}$$

L'ultima disuguaglianza comporta

$$\begin{aligned} \begin{bmatrix} a+c & b+d \end{bmatrix}\begin{bmatrix} a+c \\ b+d \end{bmatrix} &= (a+c)^2 + (b+d)^2 = (a^2+b^2) + (c^2+d^2) + 2(ac+bd) \\ &\leq \begin{bmatrix} a & b \end{bmatrix}\begin{bmatrix} a \\ b \end{bmatrix} + \begin{bmatrix} c & d \end{bmatrix}\begin{bmatrix} c \\ d \end{bmatrix} + 2\sqrt{\begin{bmatrix} a & b \end{bmatrix}\begin{bmatrix} a \\ b \end{bmatrix}}\sqrt{\begin{bmatrix} c & d \end{bmatrix}\begin{bmatrix} c \\ d \end{bmatrix}} \\ &= \left(\sqrt{\begin{bmatrix} a & b \end{bmatrix}\begin{bmatrix} a \\ b \end{bmatrix}} + \sqrt{\begin{bmatrix} c & d \end{bmatrix}\begin{bmatrix} c \\ d \end{bmatrix}}\right)^2, \end{aligned}$$

e quindi

$$\sqrt{\begin{bmatrix} a+c & b+d \end{bmatrix}\begin{bmatrix} a+c \\ b+d \end{bmatrix}} \leq \sqrt{\begin{bmatrix} a & b \end{bmatrix}\begin{bmatrix} a \\ b \end{bmatrix}} + \sqrt{\begin{bmatrix} c & d \end{bmatrix}\begin{bmatrix} c \\ d \end{bmatrix}},$$

che è appunto (3).

La proprietà (3) esprime algebricamente il fatto che la lunghezza della diagonale di un parallelogramma è minore o uguale alla somma delle lunghezze di due suoi lati adiacenti: si ricordi che se P e Q sono i punti del piano corrispondenti ai vettori $\mathbf{v}, \mathbf{w} \in \mathbb{R}^2$, allora il punto che corrisponde al vettore $\mathbf{v} + \mathbf{w}$ è il quarto vertice, diciamolo R, del parallelogramma in cui i segmenti OP e OQ sono due lati. In altre parole, (3) esprime il fatto che nel triangolo OQR la lunghezza dell'ipotenusa OR è minore o uguale alla somma delle lunghezze dei due cateti OQ e QR. Per questo motivo si chiama *disuguaglianza triangolare* (si veda la Figura 3.1).

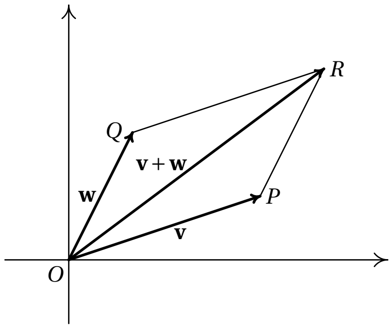


Figura 3.1: Disuguaglianza triangolare

Prendiamo ora tali proprietà della lunghezza di un segmento nel piano come assiomi per le lunghezze dei vettori in un generico spazio vettoriale (ricordiamo che il termine "spazio vettoriale" senza alcuna specificazione denoterà sempre spazi vettoriali complessi). Tutte le definizioni e i risultati valgono con ovvie modifiche per spazi vettoriali reali.

Definizione. Sia V uno spazio vettoriale. Una funzione $\|\cdot\|\colon V \to \mathbb{R}_{\geq 0}$ si dice una *norma* su V se soddisfa le tre seguenti proprietà:

(1) $\|\mathbf{v}\| > 0$, per ogni $\mathbf{0} \neq \mathbf{v} \in V$, e $\|\mathbf{0}\| = 0$.

(2) $\|\alpha\mathbf{v}\| = |\alpha|\,\|\mathbf{v}\|$ per ogni scalare $\alpha \in \mathbb{C}$ e ogni $\mathbf{v} \in V$.

(3) $\|\mathbf{v} + \mathbf{w}\| \leq \|\mathbf{v}\| + \|\mathbf{w}\|$ per ogni $\mathbf{v}, \mathbf{w} \in V$ (disuguaglianza triangolare).

Esempio 1.1. Abbiamo visto che la funzione $f(\mathbf{v}) = \sqrt{\mathbf{v}^T\mathbf{v}}$ definita su $\mathbb{R}^2$ verifica le proprietà (1), (2) e (3), per cui è una norma sullo spazio vettoriale reale $V = \mathbb{R}^2$. Essa si chiama *norma euclidea* di $\mathbb{R}^2$ e si indica con il simbolo $\|\cdot\|_2$ (si scrive cioè $\|\mathbf{v}\|_2 = \sqrt{\mathbf{v}^T\mathbf{v}}$ per ogni $\mathbf{v} \in \mathbb{R}^2$).

Più in generale la funzione

$$\begin{aligned} \|\cdot\|_2 \colon \mathbb{C}^n &\to \mathbb{R}_{\geq 0} \\ \mathbf{v} &\mapsto \sqrt{\mathbf{v}^H\mathbf{v}} \end{aligned}$$

è una norma sullo spazio vettoriale complesso $V = \mathbb{C}^n$, e si chiama la *norma euclidea di* $\mathbb{C}^n$.

Per esempio:

$$\left\| \begin{bmatrix} 1 \\ -2i \\ 2+i \end{bmatrix} \right\|_2 = \sqrt{\begin{bmatrix} 1 \\ -2i \\ 2+i \end{bmatrix}^H \begin{bmatrix} 1 \\ -2i \\ 2+i \end{bmatrix}} = \sqrt{\begin{bmatrix} 1 & 2i & 2-i \end{bmatrix} \begin{bmatrix} 1 \\ -2i \\ 2+i \end{bmatrix}}$$
$$= \sqrt{1+4+(2-i)(2+i)} = \sqrt{1+4+4+1} = \sqrt{10}. \qquad \square$$

Verifichiamo che la funzione $\|\mathbf{v}\|_2 = \sqrt{\mathbf{v}^H\mathbf{v}}$ definita su $\mathbb{C}^n$ soddisfa le proprietà (1), (2) e (3) (la dimostrazione che tali proprietà sono soddisfatte anche da $\|\mathbf{v}\|_2 = \sqrt{\mathbf{v}^T\mathbf{v}}$ definita su $\mathbb{R}^n$ seguirà allora dal fatto che se $\mathbf{v} \in \mathbb{R}^n$ si ha che $\mathbf{v} \in \mathbb{C}^n$ e $\mathbf{v}^H = \mathbf{v}^T$). Se

$$\mathbf{v} = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} \in \mathbb{C}^n,$$

allora

$$\begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix}^H \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} = \sum_{1\le i\le n} \overline{v_i} v_i = \sum_{1\le i\le n} |v_i|^2.$$

Dunque $\|\cdot\|_2$ soddisfa la proprietà (1) poiché per ogni $z \in \mathbb{C}$ si ha $|z| \in \mathbb{R}_{\ge 0}$, la somma di numeri reali non negativi è non negativa ed è nulla se e solo se ciascun addendo è nullo, e infine 0 è l'unico numero complesso che ha modulo uguale a 0.

Per verificare che $\|\cdot\|_2$ soddisfa la proprietà (2), basta osservare che se $\mathbf{v} \in \mathbb{C}^n$ e $\alpha \in \mathbb{C}$, si ha

$$(\alpha\mathbf{v})^H(\alpha\mathbf{v}) = \overline{\alpha}\mathbf{v}^H\alpha\mathbf{v} = \overline{\alpha}\alpha\mathbf{v}^H\mathbf{v} = |\alpha|^2\mathbf{v}^H\mathbf{v}.$$

Mentre per provare che vale la disuguaglianza triangolare per la norma euclidea di $\mathbb{R}^2$ abbiamo potuto fare un semplice calcolo diretto, la verifica che la norma euclidea di $\mathbb{C}^n$ soddisfa la proprietà (3) è meno immediata e necessita del risultato che ora enunciamo, e che dimostreremo in un contesto più generale nel Paragrafo 2.

Disuguaglianza di Cauchy-Schwarz. *Siano* $\mathbf{v}, \mathbf{w} \in \mathbb{C}^n$. *Allora si ha:*

$$|\mathbf{v}^H\mathbf{w}| \le \|\mathbf{v}\|_2\|\mathbf{w}\|_2.$$

Vogliamo dunque provare che vale la disuguaglianza triangolare per $\|\cdot\|_2$ definita su $\mathbb{C}^n$.

Poiché per ogni $\mathbf{v}, \mathbf{w} \in \mathbb{C}^n$ si ha che $\|\mathbf{v}\|_2$, $\|\mathbf{w}\|_2$ e $\|\mathbf{v}+\mathbf{w}\|_2$ sono numeri reali non negativi, verificare la proprietà (3) equivale a provare che $\|\mathbf{v}+\mathbf{w}\|_2^2 \le (\|\mathbf{v}\|_2 + \|\mathbf{w}\|_2)^2$ per ogni $\mathbf{v}, \mathbf{w} \in \mathbb{C}^n$. Pertanto, essendo

$$\|\mathbf{v}+\mathbf{w}\|_2^2 = (\mathbf{v}+\mathbf{w})^H(\mathbf{v}+\mathbf{w}) = \mathbf{v}^H\mathbf{v} + \mathbf{v}^H\mathbf{w} + \mathbf{w}^H\mathbf{v} + \mathbf{w}^H\mathbf{w},$$

(da cui in particolare segue che $\mathbf{v}^H\mathbf{w}+\mathbf{w}^H\mathbf{v}$ è un numero reale), ed essendo

$$(\|\mathbf{v}\|_2+\|\mathbf{w}\|_2)^2 = \|\mathbf{v}\|_2^2+\|\mathbf{w}\|_2^2+2\|\mathbf{v}\|_2\|\mathbf{w}\|_2 = \mathbf{v}^H\mathbf{v}+\mathbf{w}^H\mathbf{w}+2\|\mathbf{v}\|_2\|\mathbf{w}\|_2,$$

ci possiamo ricondurre a verificare la seguente disuguaglianza tra numeri reali:

$$\mathbf{v}^H\mathbf{w}+\mathbf{w}^H\mathbf{v} \le 2\|\mathbf{v}\|_2\|\mathbf{w}\|_2. \tag{*}$$

Dalla disuguaglianza triangolare del modulo di numeri complessi otteniamo innanzitutto:

$$\mathbf{v}^H\mathbf{w}+\mathbf{w}^H\mathbf{v} \le |\mathbf{v}^H\mathbf{w}+\mathbf{w}^H\mathbf{v}| \le |\mathbf{v}^H\mathbf{w}|+|\mathbf{w}^H\mathbf{v}|. \tag{1}$$

Ricordiamo ora che se $z\in\mathbb{C}$, allora $z^H=\overline{z}$ per cui $|z^H|=|z|$. In particolare da $(\mathbf{w}^H\mathbf{v})^H = \mathbf{v}^H(\mathbf{w}^H)^H = \mathbf{v}^H\mathbf{w}$ otteniamo che $|\mathbf{w}^H\mathbf{v}|=|\mathbf{v}^H\mathbf{w}|$.

Assieme alla Disuguaglianza di Cauchy-Schwarz ciò comporta

$$|\mathbf{v}^H\mathbf{w}|+|\mathbf{w}^H\mathbf{v}| = 2|\mathbf{v}^H\mathbf{w}| \le 2\|\mathbf{v}\|_2\|\mathbf{w}\|_2, \tag{2}$$

per cui (*) segue da (1) e (2). La dimostrazione che $\|\cdot\|_2$ è una norma è così completata.

Anche nel piano, la norma euclidea non è l'unica norma adottata per la misura delle distanze. Il prossimo esempio, nel caso particolare di uno spazio vettoriale reale di dimensione 2, esprime la distanza minima che occorre percorrere da un punto a un altro di una città in cui le strade siano a due a due perpendicolari o parallele.

Esempio 1.2. Le funzioni

$$\begin{aligned} &\|\cdot\|_1 : \mathbb{C}^n \to \mathbb{R}_{\ge 0} \quad \text{definita da} \quad \|\mathbf{v}\|_1 = |v_1|+|v_2|+\cdots+|v_n| \\ &\|\cdot\|_1 : \mathbb{R}^n \to \mathbb{R}_{\ge 0} \quad \text{definita da} \quad \|\mathbf{v}\|_1 = |v_1|+|v_2|+\cdots+|v_n| \end{aligned}$$

per ogni $\mathbf{v}=[v_1\ v_2\ \dots\ v_n]^T \in \mathbb{C}^n$ (o, rispettivamente, in $\mathbb{R}^n$) sono due norme sugli spazi vettoriali $\mathbb{C}^n$ e $\mathbb{R}^n$.

La verifica che soddisfano le proprietà (1), (2) e (3) è lasciata come esercizio (si veda l'Esercizio 3.1) e dipende esclusivamente dalle proprietà del modulo di un numero complesso o reale. In particolare la proprietà (3) segue dalla disuguaglianza triangolare del modulo.

Per esempio:

$$\left\| \begin{bmatrix} 1 \\ -2i \\ 2+i \end{bmatrix} \right\|_1 = |1|+|-2i|+|2+i| = 1+2+\sqrt{4+1} = 3+\sqrt{5}. \qquad \square$$

Quando si è interessati a misurare le variazioni massime da un valore medio, si usa la norma definita nell'Esempio successivo.

Esempio 1.3. Le funzioni

$$\|\cdot\|_\infty\colon \mathbb{C}^n \to \mathbb{R}_{\geq 0} \quad \text{definita da} \quad \|\mathbf{v}\|_\infty = \max\{|v_1|, |v_2|, \dots, |v_n|\}$$
$$\|\cdot\|_\infty\colon \mathbb{R}^n \to \mathbb{R}_{\geq 0} \quad \text{definita da} \quad \|\mathbf{v}\|_\infty = \max\{|v_1|, |v_2|, \dots, |v_n|\}$$

per ogni $\mathbf{v} = [v_1\ v_2\ \dots\ v_n]^T \in \mathbb{C}^n$ (o, rispettivamente, in $\mathbb{R}^n$) sono due norme sugli spazi vettoriali $\mathbb{C}^n$ e $\mathbb{R}^n$.

Per esempio:

$$\left\| \begin{bmatrix} 1 \\ -2i \\ 2+i \end{bmatrix} \right\|_\infty = \max\{|1|, |-2i|, |2+i|\} = \max\{1, 2, \sqrt{5}\} = \sqrt{5}. \qquad \square$$

Verifichiamo solo che vale la proprietà (3), essendo le altre due verifiche banali.

Siano $\mathbf{v} = [v_1\ v_2\ \dots\ v_n]^T$, $\mathbf{w} = [w_1\ w_2\ \dots\ w_n] \in \mathbb{C}^n$ (risp. $\mathbb{R}^n$), e $k \in \{1, \dots, n\}$ tale che

$$\|\mathbf{v}+\mathbf{w}\|_\infty = \max\{|v_1 + w_1|, |v_2 + w_2|, \dots, |v_n + w_n|\} = |v_k + w_k|.$$

Applicando la disuguaglianza triangolare del modulo di numeri si ottiene

$$|v_k + w_k| \leq |v_k| + |w_k| \leq \max\{|v_1|, |v_2|, \dots, |v_n|\} + \max\{|w_1|, |w_2|, \dots, |w_n|\} = \|\mathbf{v}\|_\infty + \|\mathbf{w}\|_\infty,$$

e quindi la proprietà (3).

Osservazione 1.4. Se $\mathbf{v} = [v_1\ v_2\ \dots\ v_n]^T \in \mathbb{C}^n$ allora

$$\max\{|v_1|, |v_2|, \dots, |v_n|\} \leq \sqrt{\mathbf{v}^H\mathbf{v}} = \sqrt{\sum_{1\leq i\leq n} |v_i|^2} \leq \sum_{1\leq i\leq n} |v_i|,$$

quindi

$$\|\mathbf{v}\|_\infty \leq \|\mathbf{v}\|_2 \leq \|\mathbf{v}\|_1 \quad \text{per ogni } \mathbf{v} \in \mathbb{C}^n.$$

Citiamo possibili generalizzazioni delle norme $\|\cdot\|_1$ e $\|\cdot\|_2$, tralasciando la dimostrazione che verificano le proprietà (1), (2) e (3). In particolare la disuguaglianza triangolare prende nel loro caso il nome di disuguaglianza di Minkowski, e la sua verifica richiede l'uso della disuguaglianza di Hölder, di cui il Teorema di Schwarz è un caso particolare.

Esempio 1.5. Sia p un numero intero, $p \geq 1$. La funzione

$$\|\cdot\|_p\colon \mathbb{C}^n \to \mathbb{R}_{\geq 0} \quad \text{definita da} \quad \|\mathbf{v}\|_p = \Big(\sum_{1\leq i\leq n} |v_i|^p\Big)^{\frac{1}{p}}$$

per ogni $\mathbf{v} = [v_1\ v_2\ \dots\ v_n]^T \in \mathbb{C}^n$ è una norma sullo spazio vettoriale $\mathbb{C}^n$ (si vedano gli Esercizi 3.11 e 3.12).

Per esempio:

$$\left\| \begin{bmatrix} 1 \\ -2i \\ 2+i \end{bmatrix} \right\|_3 = \sqrt[3]{|1|^3 + |-2i|^3 + |2+i|^3} = \sqrt[3]{1^3 + 2^3 + (\sqrt{5})^3} = \sqrt[3]{9 + 5\sqrt{5}}. \qquad \square$$

Si noti che ponendo $p = 1$ nella definizione delle norme dell'Esempio 1.5 si ottiene la definizione di $\|\cdot\|_1$, e ponendo $p = 2$ quella della norma euclidea.

A partire da quella euclidea si possono costruire altre norme nel modo descritto nel prossimo esempio.

Esempio 1.6. Sia $\mathbf{B}$ una matrice complessa invertibile $n \times n$, e sia $\mathbf{A}$ la matrice hermitiana di ordine n definita da $\mathbf{A} = \mathbf{B}\mathbf{B}^H$. La funzione

$$\|\cdot\|_{\mathbf{A}} : \mathbb{C}^n \to \mathbb{R}_{\geq 0} \quad \text{definita da} \quad \|\mathbf{v}\|_{\mathbf{A}} = \sqrt{\mathbf{v}^H\mathbf{A}\mathbf{v}} = \sqrt{\mathbf{v}^H\mathbf{B}\mathbf{B}^H\mathbf{v}} = \|\mathbf{B}^H\mathbf{v}\|_2,$$

per ogni $\mathbf{v} \in \mathbb{C}^n$, è una norma sullo spazio vettoriale $\mathbb{C}^n$ (la verifica che $\|\cdot\|_{\mathbf{A}}$ soddisfa le proprietà (1), (2) e (3) è lasciata come esercizio; si veda l'Esercizio 3.7). Si osservi che per provare (1) si deve sfruttare l'ipotesi che la matrice $\mathbf{B}$ è invertibile. □

Esempio 1.7. Sia $\mathscr{C}([a,b])$ lo spazio vettoriale reale delle funzioni reali continue definite nell'intervallo $[a,b]$, con $a, b \in \mathbb{R}$ e $a < b$. La funzione

$$\|\cdot\|_2 : \mathscr{C}([a,b]) \to \mathbb{R}_{\geq 0} \quad \text{definita da} \quad \|f\|_2 = \sqrt{\int_a^b f(t)^2\, dt}$$

per ogni $f \in \mathscr{C}([a,b])$, è una norma su $\mathscr{C}([a,b])$. □

Lasciamo al lettore per esercizio la verifica che le tre proprietà delle norme sono soddisfatte. In particolare per provare la terza si impiega una disuguaglianza che corrisponde a quella di Cauchy-Schwarz già enunciata (si veda l'Esercizio 3.9).

Disuguaglianza di Schwarz per le funzioni continue. *Siano $f, g \in \mathscr{C}([a,b])$. Allora si ha:*

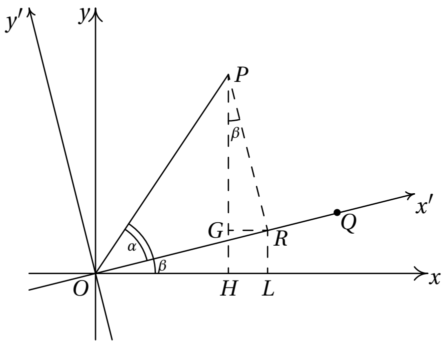
$$\left|\int_a^b f(t)g(t)\, dt\right| \leq \sqrt{\int_a^b f(t)^2\, dt}\sqrt{\int_a^b g(t)^2\, dt}$$

2. Prodotti interni

Siano Oxy un sistema di riferimento ortogonale e monometrico nel piano, e P e Q due punti del piano distinti da O. Per fissare le idee si suppongano entrambi nel primo quadrante, come in Figura 3.2.

Si consideri il sistema di riferimento ortogonale monometrico $Ox'y'$ che ha la stessa origine O del precedente e il semiasse positivo delle ascisse x' contenente il punto Q. Se β è l'angolo, misurato in senso antiorario, tra l'asse positivo delle ascisse di Oxy e la retta passante per O e per Q, allora $Ox'y'$ si ottiene ruotando in senso antiorario Oxy intorno a O dell'angolo β.

Siano $\mathbf{v} = [x_P \ y_P]^T$ e $\mathbf{w} = [x_Q \ y_Q]^T$ i vettori delle coordinate di P e Q rispetto al sistema di riferimento Oxy, e $\mathbf{v}' = [x'_P \ y'_P]^T$ e $\mathbf{w}' = [x'_Q \ y'_Q]^T$ quelli rispetto a $Ox'y'$.



$$
\begin{aligned}
x_P &= |OH| = |OL| - |HL| = |OR|\cos\beta - |GR| \\
&= x'_P \cos\beta - |PR| \operatorname{sen}\beta \\
&= x'_P \cos\beta - y'_P \operatorname{sen}\beta \\
y_P &= |PH| = |PG| + |GH| = |PR|\cos\beta + |RL| \\
&= y'_P \cos\beta + |OR| \operatorname{sen}\beta \\
&= x'_P \operatorname{sen}\beta + y'_P \cos\beta
\end{aligned}
$$

Figura 3.2: Proiezioni ortogonali

Da considerazioni trigonometriche elementari si ricava che la relazione tra $\mathbf{v}$ e $\mathbf{v}'$, e tra $\mathbf{w}$ e $\mathbf{w}'$ è data da

$$\mathbf{v} = \mathbf{R}_\beta \mathbf{v}' \quad \text{e} \quad \mathbf{w} = \mathbf{R}_\beta \mathbf{w}',$$

dove

$$\mathbf{R}_\beta = \begin{bmatrix} \cos\beta & -\operatorname{sen}\beta \\ \operatorname{sen}\beta & \cos\beta \end{bmatrix}.$$

La matrice $\mathbf{R}_\beta$ si chiama *matrice di rotazione* dell'angolo β (si veda anche il Capitolo 6, Paragrafo 1). Si noti che la relazione $(\cos\beta)^2 + (\operatorname{sen}\beta)^2 = 1$ implica $\mathbf{R}_\beta^T \mathbf{R}_\beta = \mathbf{I}_2$, per cui si ottiene

$$\mathbf{v}^T \mathbf{w} = (\mathbf{R}_\beta \mathbf{v}')^T (\mathbf{R}_\beta \mathbf{w}') = (\mathbf{v}')^T \mathbf{R}_\beta^T \mathbf{R}_\beta \mathbf{w}' = (\mathbf{v}')^T \mathbf{w}'. \tag{1}$$

D'altra parte, se α è l'angolo tra la retta passante per O e Q e la retta passante per O e P, allora, indicando con $|OP|$ e $|OQ|$ le misure dei segmenti OP e OQ rispettivamente, si ha anche

$$\mathbf{v}' = \begin{bmatrix} |OP|\cos\alpha \\ |OP|\operatorname{sen}\alpha \end{bmatrix} \qquad \text{e} \qquad \mathbf{w}' = \begin{bmatrix} |OQ| \\ 0 \end{bmatrix},$$

e quindi

$$
\begin{aligned}
(\mathbf{v}')^T \mathbf{w}' &= \begin{bmatrix} |OP|\cos\alpha & |OP|\operatorname{sen}\alpha \end{bmatrix} \begin{bmatrix} |OQ| \\ 0 \end{bmatrix} \\
&= |OP||OQ|\cos\alpha = \|\mathbf{v}\|_2 \|\mathbf{w}\|_2 \cos\alpha.
\end{aligned} \tag{2}
$$

Poiché $\mathbf{v} \neq \mathbf{0}$ implica $\|\mathbf{v}\|_2 \neq 0$, avremo anche $\|\mathbf{w}\| \neq 0$ e da (1) e (2) si ricava la seguente relazione:

$$\cos\alpha = \frac{\mathbf{v}^T \mathbf{w}}{\|\mathbf{v}\|_2 \|\mathbf{w}\|_2} \quad \text{per ogni } \mathbf{v}, \mathbf{w} \in \mathbb{R}^2 \setminus \{\mathbf{0}\}. \tag{*}$$

In particolare se P e Q sono punti del piano appartenenti alla circonferenza di centro O e raggio 1, si ottiene:

$$\cos\alpha = \mathbf{v}^T \mathbf{w} \quad \text{per ogni } \mathbf{v}, \mathbf{w} \in \mathbb{R}^2 \text{ con } \|\mathbf{v}\|_2 = \|\mathbf{w}\|_2 = 1.$$

Dunque la funzione reale definita su $\mathbb{R}^2 \times \mathbb{R}^2$ da $f(\mathbf{v},\mathbf{w}) = \mathbf{v}^T\mathbf{w}$ esprime, se ristretta al prodotto cartesiano dell'insieme dei vettori di norma 1, il coseno dell'angolo compreso tra due vettori.

Introduciamo ora il concetto di *prodotto interno* come generalizzazione della funzione $f(\mathbf{v},\mathbf{w}) = \mathbf{v}^T\mathbf{w}$, e poi, a partire dalla definizione di prodotto interno e dalla relazione (*), definiremo il concetto di *angolo* tra vettori come generalizzazione di quello tra vettori di $\mathbb{R}^2$.

Definizione. Sia V uno spazio vettoriale. Si chiama *prodotto interno* su V ogni funzione

$$(\cdot \mid \cdot)\colon V \times V \to \mathbb{C}$$

che soddisfi le seguenti proprietà:

(1) $(\mathbf{v} \mid \mathbf{w}) = \overline{(\mathbf{w} \mid \mathbf{v})}$ per ogni $\mathbf{v},\mathbf{w} \in V$;

(2) $(\mathbf{v} \mid \alpha\mathbf{w} + \beta\mathbf{z}) = \alpha(\mathbf{v} \mid \mathbf{w}) + \beta(\mathbf{v} \mid \mathbf{z})$ per ogni $\mathbf{v},\mathbf{w},\mathbf{z} \in V$ e ogni $\alpha,\beta \in \mathbb{C}$;

(3) $(\mathbf{v} \mid \mathbf{v}) \in \mathbb{R}_{>0}$ se $\mathbf{v} \neq 0$.

Nel caso in cui V sia uno spazio vettoriale reale, un prodotto interno su V è una funzione

$$(\cdot \mid \cdot)\colon V \times V \to \mathbb{R}$$

con le proprietà

(1′) $(\mathbf{v} \mid \mathbf{w}) = (\mathbf{w} \mid \mathbf{v})$ per ogni $\mathbf{v},\mathbf{w} \in V$;

(2′) $(\mathbf{v} \mid \alpha\mathbf{w} + \beta\mathbf{z}) = \alpha(\mathbf{v} \mid \mathbf{w}) + \beta(\mathbf{v} \mid \mathbf{z})$ per ogni $\mathbf{v},\mathbf{w},\mathbf{z} \in V$ e ogni $\alpha,\beta \in \mathbb{R}$;

(3′) $(\mathbf{v} \mid \mathbf{v}) \in \mathbb{R}_{>0}$ se $\mathbf{v} \neq 0$.

Si osservi che dalle proprietà segue facilmente $(\mathbf{0} \mid \mathbf{w}) = 0 = (\mathbf{v} \mid \mathbf{0})$ per ogni $\mathbf{v},\mathbf{w} \in V$.

La proprietà (1) si esprime dicendo che la funzione $(\cdot \mid \cdot)$ è "hermitiana" (ed è "simmetrica" se V è uno spazio vettoriale reale). Le proprietà (2) e (3) si esprimono dicendo che la funzione $(\cdot \mid \cdot)$ è "lineare nella seconda componente" e "definita positiva", rispettivamente.

Si noti che dalle proprietà (1) e (2) segue che se $(\cdot \mid \cdot)$ è un prodotto interno su uno spazio vettoriale V su $\mathbb{C}$ (risp. su $\mathbb{R}$), allora si ha

(4) $(\alpha\mathbf{u} + \beta\mathbf{v} \mid \mathbf{w}) = \overline{\alpha}(\mathbf{u} \mid \mathbf{w}) + \overline{\beta}(\mathbf{v} \mid \mathbf{w})$ per ogni $\mathbf{u},\mathbf{v},\mathbf{w} \in V$ e ogni $\alpha,\beta \in \mathbb{C}$;

(4′) $(\alpha\mathbf{u} + \beta\mathbf{v} \mid \mathbf{w}) = \alpha(\mathbf{u} \mid \mathbf{w}) + \beta(\mathbf{v} \mid \mathbf{w})$ per ogni $\mathbf{u},\mathbf{v},\mathbf{w} \in V$ e ogni $\alpha,\beta \in \mathbb{R}$.

Definizione. Uno spazio vettoriale su cui sia definito un prodotto interno $(\cdot \mid \cdot)$ si chiama uno *spazio vettoriale euclideo.*

Esempio 2.1. Le funzioni

$$(\cdot \mid \cdot)\colon \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C} \quad \text{definita da} \quad (\mathbf{v} \mid \mathbf{w}) = \mathbf{v}^H\mathbf{w} \quad \text{per ogni } \mathbf{v},\mathbf{w} \in \mathbb{C}^n$$
$$(\cdot \mid \cdot)\colon \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R} \quad \text{definita da} \quad (\mathbf{v} \mid \mathbf{w}) = \mathbf{v}^T\mathbf{w} \quad \text{per ogni } \mathbf{v},\mathbf{w} \in \mathbb{R}^n$$

sono rispettivamente un prodotto interno sullo spazio vettoriale $\mathbb{C}^n$, e un prodotto interno sullo spazio vettoriale (reale) $\mathbb{R}^n$. Si chiamano il *prodotto interno standard di* $\mathbb{C}^n$ *e di* $\mathbb{R}^n$.

Per esempio, il prodotto interno standard dei due vettori

$$\begin{bmatrix} -7 \\ 2 \\ 1 \end{bmatrix}, \begin{bmatrix} 3 \\ 6 \\ 5 \end{bmatrix} \in \mathbb{R}^3$$

è

$$\begin{bmatrix} -7 \\ 2 \\ 1 \end{bmatrix}^T \begin{bmatrix} 3 \\ 6 \\ 5 \end{bmatrix} = \begin{bmatrix} -7 & 2 & 1 \end{bmatrix} \begin{bmatrix} 3 \\ 6 \\ 5 \end{bmatrix} = -21 + 12 + 5 = -4,$$

ed il prodotto interno standard dei due vettori

$$\begin{bmatrix} 1+4i \\ 2-i \\ i \end{bmatrix}, \begin{bmatrix} 3-i \\ 6+2i \\ 5 \end{bmatrix} \in \mathbb{C}^3$$

è

$$\begin{aligned} \begin{bmatrix} 1+4i \\ 2-i \\ i \end{bmatrix}^H \begin{bmatrix} 3-i \\ 6+2i \\ 5 \end{bmatrix} &= \begin{bmatrix} 1-4i & 2+i & -i \end{bmatrix} \begin{bmatrix} 3-i \\ 6+2i \\ 5 \end{bmatrix} \\ &= (1-4i)(3-i) + (2+i)(6+2i) + 5(-i) = 9-8i \end{aligned}$$ □

Verifichiamo che la funzione definita su $\mathbb{C}^n \times \mathbb{C}^n$ da $(\mathbf{v} \mid \mathbf{w}) = \mathbf{v}^H\mathbf{w}$ soddisfa le proprietà (1), (2) e (3). Dal momento che i numeri reali sono i numeri complessi che coincidono con il proprio coniugato da ciò seguirà che anche la funzione definita su $\mathbb{R}^n \times \mathbb{R}^n$ da $(\mathbf{v} \mid \mathbf{w}) = \mathbf{v}^T\mathbf{w}$ è un prodotto interno.

La proprietà (1) segue dal fatto che, essendo $\mathbf{v}^H\mathbf{w} \in \mathbb{C}$, si ha $(\mathbf{v}^H\mathbf{w})^H = \overline{\mathbf{v}^H\mathbf{w}}$, per cui

$$\mathbf{v}^H\mathbf{w} = \overline{(\mathbf{v}^H\mathbf{w})^H} = \overline{\mathbf{w}^H(\mathbf{v}^H)^H} = \overline{\mathbf{w}^H\mathbf{v}};$$

la (2) segue dalle proprietà (PS_1) e (Pp) del Capitolo 1, Paragrafo 1; infine la proprietà (3) dall'osservazione che

$$(\mathbf{v} \mid \mathbf{v}) = \|\mathbf{v}\|_2^2.$$

Esempio 2.2. Sia $V = \mathrm{M}_{m\times n}(\mathbb{C})$ e, per $\mathbf{A}, \mathbf{B} \in \mathrm{M}_{m\times n}(\mathbb{C})$ si ponga $(\mathbf{A} \mid \mathbf{B}) = \mathrm{Tr}(\mathbf{A}^H\mathbf{B})$. Si può facilmente verificare che questo è un prodotto interno e che $(\mathbf{A} \mid \mathbf{A}) = \sum_{i,j} |a_{ij}|^2$. □

Esempio 2.3. Sia $\mathscr{C}([a,b])$ lo spazio vettoriale reale delle funzioni reali continue definite nell'intervallo $[a,b]$, con $a, b \in \mathbb{R}$ e $a < b$. La funzione

$$(\cdot \mid \cdot) \colon \mathscr{C}([a,b]) \times \mathscr{C}([a,b]) \to \mathbb{R}, \qquad (f \mid g) = \int_a^b f(t)g(t)\,dt$$

è un prodotto interno sullo spazio vettoriale reale $V = \mathscr{C}([a,b])$.

Per esempio, il prodotto interno delle funzioni $f(t) = t$ e $g(t) = t^2 + 1$ ristrette all'intervallo $[0,2]$ è

$$\int_0^2 t(t^2+1)\,dt = \int_0^2 t^3\,dt + \int_0^2 t\,dt = \frac{1}{4}\cdot 2^4 + \frac{1}{2}\cdot 2^2 = 2^2 + 2 = 6.$$

La verifica che la funzione appena definita soddisfa le proprietà (1), (2) e (3) è immediata. Infatti, la proprietà (1) segue dal fatto che $f(t)g(t) = g(t)f(t)$ per ogni $t \in [a,b]$, la (2) dalla linearità dell'integrale, e infine la (3) dall'osservazione che

$$(f \mid f) = \|f\|_2^2$$

dove $\|f\|_2$ è la norma di $f \in \mathscr{C}([a,b])$ definita nell'Esempio 1.7. □

Esempio 2.4. Sia $\mathbf{B}$ una matrice complessa $n \times n$ invertibile e sia $\mathbf{A}$ la matrice hermitiana di ordine n definita da $\mathbf{A} = \mathbf{B}\mathbf{B}^H$. La funzione

$$(\cdot \mid \cdot)_{\mathbf{A}} \colon \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C} \quad \text{definita da} \quad (\mathbf{v} \mid \mathbf{w})_{\mathbf{A}} = \mathbf{v}^H\mathbf{A}\mathbf{w} \quad \text{per ogni } \mathbf{v}, \mathbf{w} \in \mathbb{C}^n$$

è un prodotto interno su $\mathbb{C}^n$.

La verifica che essa soddisfa le proprietà (1), (2) e (3) è lasciata come esercizio (si veda l'Esercizio 3.9). Per provare la proprietà (3) conviene osservare che

$$(\mathbf{v} \mid \mathbf{v})_{\mathbf{A}} = \|\mathbf{B}^H\mathbf{v}\|_2^2, \quad \text{per ogni } \mathbf{v} \in \mathbb{C}^n.$$ □

In effetti, l'Esempio 2.4 descrive ogni prodotto interno su $\mathbb{C}^n$ o $\mathbb{R}^n$, come specifichiamo nella seguente osservazione: per ogni prodotto interno $(\cdot \mid \cdot)$ definito su $\mathbb{C}^n$ o $\mathbb{R}^n$ esiste una matrice invertibile $n \times n$ $\mathbf{B}$ tale che posto $\mathbf{A} = \mathbf{B}\mathbf{B}^H$ si abbia $(\cdot \mid \cdot) = (\cdot \mid \cdot)_{\mathbf{A}}$, dove $(\cdot \mid \cdot)_{\mathbf{A}}$ è il prodotto interno definito nell'Esempio 2.4. Questo fatto è un caso particolare del seguente risultato valido per ogni spazio vettoriale euclideo di dimensione n.

Teorema 2.5. *Sia V uno spazio vettoriale euclideo con base $\mathscr{B} = \{\mathbf{v}_1; \mathbf{v}_2; \dots; \mathbf{v}_n\}$. Allora, per ogni $\mathbf{v}, \mathbf{w} \in V$, risulta: $(\mathbf{v} \mid \mathbf{w}) = C_{\mathscr{B}}(\mathbf{v})^H \mathbf{A} C_{\mathscr{B}}(\mathbf{w})$, dove $\mathbf{A} = [(\mathbf{v}_i \mid \mathbf{v}_j)]$ è una matrice del tipo $\mathbf{A} = \mathbf{B}\mathbf{B}^H$, con $\mathbf{B}$ invertibile.*

Dimostrazione. Dalle proprietà (2) e (4) del prodotto interno $(\cdot \mid \cdot)$ definito su V si ottiene che se $\mathbf{v} = \sum_{1\le i\le n} \alpha_i \mathbf{v}_i$, $\mathbf{w} = \sum_{1\le j\le n} \beta_j \mathbf{v}_j \in V$, allora

$$(\mathbf{v} \mid \mathbf{w}) = \Big(\sum_{1\le i\le n} \alpha_i \mathbf{v}_i \;\Big|\; \sum_{1\le j\le n} \beta_j \mathbf{v}_j \Big) = \sum_{\substack{1\le i\le n \\ 1\le j\le n}} \overline{\alpha}_i \beta_j (\mathbf{v}_i \mid \mathbf{v}_j).$$

Quindi, una volta fissata la base $\mathscr{B}$ di V, il prodotto interno $(\cdot \mid \cdot)$ è completamente individuato dalla matrice $n \times n$ $\mathbf{A} = [a_{ij}]$, dove $a_{ij} = (\mathbf{v}_i \mid \mathbf{v}_j)$.

La matrice **A** si chiama *matrice di Gram* del prodotto interno rispetto alla base $\mathscr{B}$ di V:

$$(\mathbf{v} \mid \mathbf{w}) = \sum_{\substack{1\le i\le n\\ 1\le j\le n}} \overline{\alpha}_i \beta_j a_{ij} = \begin{bmatrix} \overline{\alpha}_1 & \overline{\alpha}_2 & \dots & \overline{\alpha}_n \end{bmatrix} \mathbf{A} \begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{bmatrix}$$

$$= \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix}^H \mathbf{A} \begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{bmatrix} = \mathrm{C}_{\mathscr{B}}(\mathbf{v})^H \mathbf{A} \mathrm{C}_{\mathscr{B}}(\mathbf{w}) = (\mathrm{C}_{\mathscr{B}}(\mathbf{v}) \mid \mathrm{C}_{\mathscr{B}}(\mathbf{w}))_{\mathbf{A}}$$

Come nell'Esempio 2.4 la matrice **A** ammette una fattorizzazione del tipo $\mathbf{A} = \mathbf{B}\mathbf{B}^H$, dove **B** è un'opportuna matrice invertibile $n \times n$. La dimostrazione di quest'ultimo fatto verrà data solo nel Teorema 3.5 del Capitolo 6 e dipende dalle due seguenti proprietà di **A**:

(1) **A** è hermitiana, poiché

$$\overline{a}_{ij} = \overline{(\mathbf{v}_i \mid \mathbf{v}_j)} = (\mathbf{v}_j \mid \mathbf{v}_i) = a_{ji} \quad \text{per ogni } i, j = 1, \dots, n$$

per la proprietà (1) del prodotto interno.

(2) $\mathbf{x}^H \mathbf{A} \mathbf{x} \in \mathbb{R}_{>0}$ per ogni $\mathbf{0} \neq \mathbf{x} \in \mathbb{C}^n$: per ogni $\mathbf{0} \neq \mathbf{x} \in \mathbb{C}^n$ esiste $\mathbf{0} \neq \mathbf{v} \in V$ tale che $\mathrm{C}_{\mathscr{B}}(\mathbf{v}) = \mathbf{x}$, e $(\mathrm{C}_{\mathscr{B}}(\mathbf{v}) \mid \mathrm{C}_{\mathscr{B}}(\mathbf{v}))_{\mathbf{A}} > 0$ per la proprietà (3) del prodotto interno. □

In particolare possiamo prendere $V = \mathbb{C}^n$ e la base canonica $\mathscr{E} = \{\mathbf{e}_1; \mathbf{e}_2; \dots; \mathbf{e}_n\}$. Allora $\mathrm{C}_{\mathscr{E}}(\mathbf{v}) = \mathbf{v}$ per ogni $\mathbf{v} \in V$. Quindi per ogni prodotto interno $(\cdot \mid \cdot)$ definito su $\mathbb{C}^n$ si ha

$$(\mathbf{v} \mid \mathbf{w}) = (\mathbf{v} \mid \mathbf{w})_{\mathbf{A}} \quad \text{per ogni } \mathbf{v}, \mathbf{w} \in \mathbb{C}^n$$

dove **A** è la matrice di Gram di $(\cdot \mid \cdot)$ rispetto alla base canonica $\mathscr{E}$ di $\mathbb{C}^n$.

Nel paragrafo precedente abbiamo enunciato due casi particolari del seguente teorema.

Teorema 2.6 (Disuguaglianza di Cauchy-Schwarz)**.** *Sia V uno spazio vettoriale euclideo. Allora si ha*

$$|(\mathbf{v} \mid \mathbf{w})| \le \sqrt{(\mathbf{v} \mid \mathbf{v})}\sqrt{(\mathbf{w} \mid \mathbf{w})} \quad \textit{per ogni } \mathbf{v}, \mathbf{w} \in V.$$

Dimostrazione. Proviamo il Teorema nel caso in cui V sia uno spazio vettoriale complesso: il caso reale segue da questo e dal fatto che ogni numero reale coincide con il proprio coniugato.

Poiché la disuguaglianza che vogliamo provare è vera se $(\mathbf{v} \mid \mathbf{w}) = 0$, possiamo supporre che sia $(\mathbf{v} \mid \mathbf{w}) \neq 0$. In particolare, per la proprietà (4) del prodotto interno, possiamo supporre che $\mathbf{v} \neq \mathbf{0}$, e quindi, per la (3), che $(\mathbf{v} \mid \mathbf{v}) > 0$.

Sia $\alpha \in \mathbb{C}$. Dalle proprietà (2), (2.1) e (3) otteniamo:

$$\begin{aligned}0 &\le (\mathbf{v}+\alpha\mathbf{w} \mid \mathbf{v}+\alpha\mathbf{w}) = (\mathbf{v}\mid\mathbf{v}) + (\mathbf{v}\mid\alpha\mathbf{w}) + (\alpha\mathbf{w}\mid\mathbf{v}) + (\alpha\mathbf{w}\mid\alpha\mathbf{w})\\ &= (\mathbf{v}\mid\mathbf{v}) + \alpha(\mathbf{v}\mid\mathbf{w}) + \overline{\alpha}(\mathbf{w}\mid\mathbf{v}) + \alpha\overline{\alpha}(\mathbf{w}\mid\mathbf{w}) \qquad (*)\\ &= (\mathbf{v}\mid\mathbf{v}) + \alpha(\mathbf{v}\mid\mathbf{w}) + \overline{\alpha}(\mathbf{w}\mid\mathbf{v}) + |\alpha|^2(\mathbf{w}\mid\mathbf{w})\end{aligned}$$

In particolare, prendendo $\alpha = -\frac{(\mathbf{v}|\mathbf{v})}{(\mathbf{v}|\mathbf{w})}$, dalle proprietà (1) e (3) si ottiene che

$$\overline{\alpha} = -\overline{(\mathbf{v}\mid\mathbf{v})}/\overline{(\mathbf{v}\mid\mathbf{w})} = -(\mathbf{v}\mid\mathbf{v})/(\mathbf{w}\mid\mathbf{v})$$

e $|\alpha|^2 = (\mathbf{v}\mid\mathbf{v})^2/|(\mathbf{v}\mid\mathbf{w})|^2$. Sostituendo in (*) si ricava

$$\begin{aligned}0 &\le (\mathbf{v}\mid\mathbf{v}) - \frac{(\mathbf{v}\mid\mathbf{v})}{(\mathbf{v}\mid\mathbf{w})}(\mathbf{v}\mid\mathbf{w}) - \frac{(\mathbf{v}\mid\mathbf{v})}{(\mathbf{w}\mid\mathbf{v})}(\mathbf{w}\mid\mathbf{v}) + \frac{(\mathbf{v}\mid\mathbf{v})^2}{|(\mathbf{v}\mid\mathbf{w})|^2}(\mathbf{w}\mid\mathbf{w})\\ &= -(\mathbf{v}\mid\mathbf{v}) + \frac{(\mathbf{v}\mid\mathbf{v})^2}{|(\mathbf{v}\mid\mathbf{w})|^2}(\mathbf{w}\mid\mathbf{w}),\end{aligned}$$

e quindi

$$(\mathbf{v}\mid\mathbf{v}) \le \frac{(\mathbf{v}\mid\mathbf{v})^2}{|(\mathbf{v}\mid\mathbf{w})|^2}(\mathbf{w}\mid\mathbf{w}).$$

La disuguaglianza di Cauchy-Schwarz segue ora da quest'ultima moltiplicandone ambo i membri per il numero reale positivo $|(\mathbf{v}\mid\mathbf{w})|^2/(\mathbf{v}\mid\mathbf{v})$ ed estraendo la radice quadrata. □

Le disuguaglianze di Cauchy-Schwarz enunciate nel paragrafo precedente si ottengono da quella appena dimostrata specificandola ai prodotti interni degli Esempi 2.1 e 2.3: basta osservare, come abbiamo fatto per provare che per essi vale la proprietà (3), che $(\mathbf{v}\mid\mathbf{v}) = \|\mathbf{v}\|_2^2$ per ogni $\mathbf{v} \in \mathbb{R}^n$ o $\mathbb{C}^n$, e $(f \mid f) = \|f\|_2^2$ per ogni $f \in \mathscr{C}([a,b])$.

Quest'ultima osservazione porta a un'altra considerazione: a partire dai prodotti interni definiti negli Esempi 2.1 e 2.3, si possono definire le norme $\|\cdot\|_2$ in $\mathbb{R}^n$ e $\mathbb{C}^n$, e la norma $\|\cdot\|_2$ in $\mathscr{C}([a,b])$ ponendo

$$\begin{aligned}\|\mathbf{v}\|_2 &= \sqrt{(\mathbf{v}\mid\mathbf{v})} \quad \text{per ogni } \mathbf{v} \in \mathbb{R}^n \text{ o } \mathbb{C}^n,\\ \|f\|_2 &= \sqrt{(f\mid f)} \quad \text{per ogni } f \in \mathscr{C}([a,b]).\end{aligned}$$

Si dice che la norma euclidea di $\mathbb{R}^n$ e di $\mathbb{C}^n$ è "indotta" dai prodotti interni dell'Esempio 2.1, e che la norma $\|\cdot\|_2$ di $\mathscr{C}([a,b])$ è "indotta" dal prodotto interno dell'Esempio 2.3.

Più in generale, se V è uno spazio vettoriale euclideo, allora la funzione

$$\|\cdot\|\colon V \to \mathbb{R}_{\ge 0}$$

definita da $\|\mathbf{v}\| = \sqrt{(\mathbf{v}\mid\mathbf{v})}$ è una norma su V, e si chiama la *norma indotta dal prodotto interno* $(\cdot \mid \cdot)$. La verifica che essa soddisfa le tre proprietà delle norme si ottiene ricalcando quella che abbiamo fatto negli Esempi 1.1 e 1.6, tenendo conto delle proprietà del prodotto interno e della disuguaglianza di Schwarz (si veda l'Esercizio 3.9).

Esempio 2.7. Sia $\mathbf{B}$ una matrice complessa $n \times k$ di rango uguale a n, e sia $\mathbf{A}$ la matrice hermitiana di ordine n definita da $\mathbf{A} = \mathbf{B}\mathbf{B}^H$. La norma $\|\cdot\|_{\mathbf{A}}$ definita su $\mathbb{C}^n$ da $\|\mathbf{v}\|_{\mathbf{A}} = \|\mathbf{B}^H\mathbf{v}\|_2$ per ogni $\mathbf{v} \in \mathbb{C}^n$ (si veda l'Esempio 1.6) è la norma indotta dal prodotto interno $(\cdot \mid \cdot)_{\mathbf{A}}$ definito nell'Esempio 2.4. $\square$

Osservazione 2.8. Non tutte le norme sono norme indotte da prodotti interni. Siano infatti $\|\cdot\|$ una norma definita su $\mathbb{C}^n$ ed $\mathscr{E}$ la base canonica di $\mathbb{C}^n$. Per quanto visto nell'Osservazione 2.5 e nell'Esempio 2.7, la norma $\|\cdot\|$ è indotta da un prodotto interno se e solo se esiste una matrice invertibile $n \times n$ $\mathbf{B}$ tale che, posto $\mathbf{A} = \mathbf{B}\mathbf{B}^H$, si abbia

$$\|\mathbf{v}\|^2 = (\mathbf{v} \mid \mathbf{v})_{\mathbf{A}} = \|\mathbf{v}\|_{\mathbf{A}}^2 = \|\mathbf{B}^H\mathbf{v}\|_2^2 = \mathbf{v}^H\mathbf{A}\mathbf{v}, \quad \text{per ogni } \mathbf{v} \in V. \tag{$\bullet$}$$

Se dunque $\mathbf{v}, \mathbf{w} \in V$ e la norma $\|\cdot\|$ soddisfa la condizione ($\bullet$), si ottiene

$$\begin{aligned} \|\mathbf{v}+\mathbf{w}\|^2 &= (\mathbf{v}+\mathbf{w})^H\mathbf{A}(\mathbf{v}+\mathbf{w}) = \mathbf{v}^H\mathbf{A}\mathbf{v} + \mathbf{w}^H\mathbf{A}\mathbf{w} + \mathbf{v}^H\mathbf{A}\mathbf{w} + \mathbf{w}^H\mathbf{A}\mathbf{v} \\ \|\mathbf{v}-\mathbf{w}\|^2 &= (\mathbf{v}-\mathbf{w})^H\mathbf{A}(\mathbf{v}-\mathbf{w}) = \mathbf{v}^H\mathbf{A}\mathbf{v} + \mathbf{w}^H\mathbf{A}\mathbf{w} - \mathbf{v}^H\mathbf{A}\mathbf{w} - \mathbf{w}^H\mathbf{A}\mathbf{v} \end{aligned} \tag{$\bullet\bullet$}$$

che sommate membro a membro danno

$$\|\mathbf{v}+\mathbf{w}\|^2 + \|\mathbf{v}-\mathbf{w}\|^2 = 2\|\mathbf{v}\|^2 + 2\|\mathbf{w}\|^2. \tag{$\bullet\bullet\bullet$}$$

Se ne deduce che ogni norma $\|\cdot\|$ che non soddisfi alla condizione ($\bullet\bullet\bullet$) non può essere indotta da un prodotto interno.

Per esempio, se $V = \mathbb{R}^2$ le norme $\|\cdot\|_1$ e $\|\cdot\|_\infty$ definite negli Esempi 1.2 e 1.3 non sono indotte da prodotti interni. Se si considerano infatti $\mathbf{v} = [1\ 1]^T$ e $\mathbf{w} = [-1\ 2]^T$, si ha $\mathbf{v}+\mathbf{w} = [0\ 3]^T$ e $\mathbf{v}-\mathbf{w} = [2\ {-1}]^T$. Dunque

$$\begin{gathered} \|\mathbf{v}+\mathbf{w}\|_1 = \|\mathbf{v}-\mathbf{w}\|_1 = \|\mathbf{w}\|_1 = 3 \quad \text{e} \quad \|\mathbf{v}\|_1 = 2 \\ \|\mathbf{v}-\mathbf{w}\|_\infty = \|\mathbf{w}\|_\infty = 2, \quad \|\mathbf{v}+\mathbf{w}\|_\infty = 3 \quad \text{e} \quad \|\mathbf{v}\|_\infty = 1 \end{gathered}$$

ed entrambe $\|\cdot\|_1$ e $\|\cdot\|_\infty$ non soddisfano ($\bullet\bullet\bullet$).

È possibile dimostrare che la condizione ($\bullet\bullet\bullet$) non è solo una condizione necessaria affinché una norma sia indotta da un prodotto interno, ma è anche sufficiente: ogni norma che la soddisfa è la norma indotta da un opportuno prodotto interno.

Poiché in $\mathbb{R}^2$ essa esprime il fatto che in un parallelogramma la somma delle aree dei quadrati costruiti sulle diagonali è uguale alla somma delle aree dei quadrati costruiti sui lati, si chiama *identità del parallelogramma.*

Ritorniamo ora alla relazione

$$\cos\alpha = \frac{\mathbf{v}^T\mathbf{w}}{\|\mathbf{v}\|_2\|\mathbf{w}\|_2} \tag{*}$$

che abbiamo trovato tra due vettori $\mathbf{v}$, $\mathbf{w}$ di $\mathbb{R}^2$ e il coseno dell'angolo tra essi compreso.

Abbiamo introdotto il concetto di prodotto interno come generalizzazione della funzione $(\mathbf{v} \mid \mathbf{w}) = \mathbf{v}^T\mathbf{w}$, definito la norma indotta da un prodotto interno e osservato che la norma euclidea è la norma indotta dal prodotto interno standard. Possiamo quindi, impiegando (*) introdurre una generalizzazione del concetto di angolo tra due vettori.

Definizione. Siano V uno spazio vettoriale euclideo e $\|\cdot\|$ la norma indotta dal prodotto interno $(\cdot \mid \cdot)$ definito su V. Allora per ogni $\mathbf{v}, \mathbf{w} \in V \setminus \{\mathbf{0}\}$ si pone

$$\cos\widehat{\mathbf{vw}} = \frac{(\mathbf{v} \mid \mathbf{w})}{\|\mathbf{v}\| \cdot \|\mathbf{w}\|}.$$

Si osservi che il numero $\cos\widehat{\mathbf{vw}}$ ora definito è un numero complesso, e per la disuguaglianza di Schwarz ha *modulo* minore o uguale a 1. Solo nel caso in cui V sia uno spazio vettoriale reale, si può porre

$$\alpha = \arccos\Big(\frac{(\mathbf{v} \mid \mathbf{w})}{\|\mathbf{v}\| \cdot \|\mathbf{w}\|}\Big)$$

e α si chiama *angolo* tra i vettori $\mathbf{v}$ e $\mathbf{w}$.

3. Ortogonalità e proiezioni ortogonali

Sia V uno spazio vettoriale euclideo. Si dice che il vettore $\mathbf{w}$ di V è *ortogonale* al vettore $\mathbf{u}$ di V, e si scrive $\mathbf{w} \perp \mathbf{u}$, se il coseno dell'angolo compreso tra $\mathbf{w}$ e $\mathbf{u}$ è 0, oppure se almeno uno tra $\mathbf{w}$ e $\mathbf{u}$ è il vettore nullo. Dunque se $\mathbf{w}, \mathbf{u} \in V$ si ha

$$\mathbf{w} \perp \mathbf{u} \iff (\mathbf{w} \mid \mathbf{u}) = 0 \iff (\mathbf{u} \mid \mathbf{w}) = 0 \iff \mathbf{u} \perp \mathbf{w},$$

e in tal caso si dice che i due vettori sono tra loro *ortogonali*.

Si dice inoltre che il vettore $\mathbf{w} \in V$ è *ortogonale al sottospazio U* di V, e si scrive $\mathbf{w} \perp U$, se $\mathbf{w}$ è ortogonale *a ogni vettore* $\mathbf{u} \in U$. L'insieme di tutti i vettori di V ortogonali a U si chiama il *complemento ortogonale di U in V* e si indica con il simbolo $U^\perp$.

Si osservi che per ogni $\mathbf{w}_1, \mathbf{w}_2 \in U^\perp$, $\mathbf{u} \in U$ e α_1, α_2 scalari, si ha, per la linearità del prodotto interno, che

$$(\mathbf{u} \mid \alpha_1\mathbf{w}_1 + \alpha_2\mathbf{w}_2) = \alpha_1(\mathbf{u} \mid \mathbf{w}_1) + \alpha_2(\mathbf{u} \mid \mathbf{w}_2) = \alpha_1 \cdot 0 + \alpha_2 \cdot 0 = 0,$$

per cui $U^\perp$ è un sottospazio di V.

Inoltre, essendo ogni vettore ortogonale a quello nullo e il vettore nullo l'unico vettore ortogonale a tutti gli altri, si ha:

$$\{\mathbf{0}\}^\perp = V \qquad \text{e} \qquad V^\perp = \{\mathbf{0}\}.$$

Dalla linearità del prodotto interno segue anche che per verificare che un vettore $\mathbf{w}$ di V è ortogonale a un sottospazio U di V è sufficiente verificare che $\mathbf{w}$ sia ortogonale ai vettori che compongono un insieme di generatori di U. Infatti se $\{\mathbf{u}_1; \mathbf{u}_2; \ldots; \mathbf{u}_k\}$ è un insieme di generatori di U, allora

$$\begin{aligned}\mathbf{w} \in U^\perp &\iff 0 = (\mathbf{w} \mid \alpha_1\mathbf{u}_1 + \cdots + \alpha_k\mathbf{u}_k) = \alpha_1(\mathbf{w} \mid \mathbf{u}_1) + \cdots + \alpha_k(\mathbf{w} \mid \mathbf{u}_k) \quad \forall \alpha_1, \ldots, \alpha_k \\ &\iff (\mathbf{w} \mid \mathbf{u}_i) = 0 \text{ per ogni } i = 1, \ldots, k \iff \mathbf{w} \perp \mathbf{u}_i \text{ per ogni } i = 1, \ldots, k.\end{aligned}$$

Esempio 3.1. Siano $V = \mathbb{R}^3$ dotato del prodotto interno standard $(\mathbf{v} \mid \mathbf{z}) = \mathbf{v}^T\mathbf{z}$, $\mathscr{E} = \{\mathbf{e}_1; \mathbf{e}_2; \mathbf{e}_3\}$ la base canonica di V e $U = \langle \mathbf{e}_1 \rangle$. Allora

$$\begin{aligned} U^{\perp} &= \{\mathbf{w} \in \mathbb{R}^3 \mid \mathbf{w} \perp \mathbf{e}_1\} = \{\mathbf{w} \in \mathbb{R}^3 \mid \mathbf{w}^T\mathbf{e}_1 = 0\} \\ &= \left\{ \begin{bmatrix} x \\ y \\ z \end{bmatrix} \in \mathbb{R}^3 \mid \begin{bmatrix} x & y & z \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = 0 \right\} = \left\{ \begin{bmatrix} 0 \\ y \\ z \end{bmatrix} \mid y, z \in \mathbb{R} \right\} = \langle \mathbf{e}_2; \mathbf{e}_3 \rangle. \end{aligned}$$

Analogamente, se $Z = \langle \mathbf{e}_1; \mathbf{e}_3 \rangle$ allora

$$\begin{aligned} Z^{\perp} &= \{\mathbf{w} \in \mathbb{R}^3 \mid \mathbf{w} \perp \mathbf{e}_1 \text{ e } \mathbf{w} \perp \mathbf{e}_3\} = \{\mathbf{w} \in \mathbb{R}^3 \mid \mathbf{w}^T\mathbf{e}_1 = 0 = \mathbf{w}^T\mathbf{e}_3\} \\ &= \left\{ \begin{bmatrix} 0 \\ y \\ 0 \end{bmatrix} \mid y \in \mathbb{R} \right\} = \langle \mathbf{e}_2 \rangle. \end{aligned}$$ □

Sappiamo che fissando un sistema di riferimento ortogonale e monometrico $Oxyz$ nello spazio tridimensionale euclideo si stabilisce una corrispondenza biunivoca tra l'insieme dei suoi punti e i vettori di V (si veda l'Appendice C). In questo modo alle rette e ai piani contenenti l'origine O del sistema di riferimento, pensati come insiemi dei loro punti, corrispondono i sottospazi di V di dimensione 1 e 2 rispettivamente.

In particolare a $U = \langle \mathbf{e}_1 \rangle$ corrisponde l'insieme dei punti dell'asse x, e a $U^{\perp}$ corrisponde l'insieme dei punti del piano Oyz, che è il piano perpendicolare all'asse x contenente O.

Inoltre a $Z = \langle \mathbf{e}_1; \mathbf{e}_3 \rangle$ corrisponde l'insieme dei punti del piano Oxz e a $Z^{\perp}$ l'insieme dei punti dell'asse y, ossia la retta passante per O perpendicolare al piano Oxz.

In generale, se V è un sottospazio di dimensione 1 di $\mathbb{R}^3$ corrispondente all'insieme dei punti di una retta r passante per O, il suo complemento ortogonale $V^{\perp}$ è il sottospazio di dimensione 2 di $\mathbb{R}^3$ corrispondente all'insieme dei punti del piano perpendicolare a r e contenente O.

Inoltre, se W è un sottospazio di dimensione 2 di $\mathbb{R}^3$ corrispondente all'insieme dei punti di un piano π contenente O, il suo complemento ortogonale $W^{\perp}$ è il sottospazio di dimensione 1 di $\mathbb{R}^3$ corrispondente all'insieme dei punti della retta perpendicolare a π e passante per O.

Nel considerare il seguente risultato si ricordi che nel Capitolo 2 lo spazio delle righe di una matrice $\mathbf{A}$ è stato definito come $\mathrm{C}(\mathbf{A}^H)$, cioè lo spazio delle colonne della sua H-trasposta. Esso completa il Teorema 5.10 del Capitolo 2.

Proposizione 3.2. *Sia* $\mathbf{A}$ *una matrice complessa* $m \times n$. *Allora:*

(1) $\mathrm{N}(\mathbf{A})$ *è il complemento ortogonale di* $\mathrm{C}(\mathbf{A}^H)$ *in* $\mathbb{C}^n$*;*

(2) $\mathrm{N}(\mathbf{A}^H)$ *è il complemento ortogonale di* $\mathrm{C}(\mathbf{A})$ *in* $\mathbb{C}^m$*.*

Dimostrazione. Suddividendo la matrice $\mathbf{A}$ in blocchi riga, si ha che

$$\mathbf{A} = \begin{bmatrix} \mathbf{r}_1^T \\ \mathbf{r}_2^T \\ \vdots \\ \mathbf{r}_m^T \end{bmatrix} \quad \text{e} \quad \mathbf{A}^H = \begin{bmatrix} \overline{\mathbf{r}_1} & \overline{\mathbf{r}_2} & \dots & \overline{\mathbf{r}_m} \end{bmatrix}, \quad \text{con } \mathbf{r}_i \in \mathbb{C}^n \text{ per } i = 1, \dots, m.$$

Allora se $\mathbf{v} \in V$ si ha

$$\begin{aligned} \mathbf{v} \in \mathrm{N}(\mathbf{A}) &\iff \mathbf{0} = \mathbf{A}\mathbf{v} = \begin{bmatrix} \mathbf{r}_1^T \\ \mathbf{r}_2^T \\ \vdots \\ \mathbf{r}_m^T \end{bmatrix} \mathbf{v} = \begin{bmatrix} \mathbf{r}_1^T\mathbf{v} \\ \mathbf{r}_2^T\mathbf{v} \\ \vdots \\ \mathbf{r}_m^T\mathbf{v} \end{bmatrix} \\ &\iff 0 = \mathbf{r}_i^T\mathbf{v} = \overline{\mathbf{r}_i}^H\mathbf{v} = (\overline{\mathbf{r}_i} \mid \mathbf{v}) \quad \text{per } i = 1, \dots, m \\ &\iff \mathbf{v} \in \mathrm{C}(\mathbf{A}^H)^\perp. \end{aligned}$$

Considerando ora $\mathbf{A}^H$ al posto di $\mathbf{A}$, si ottiene che $\mathrm{N}(\mathbf{A}^H)$ è il complemento ortogonale in $\mathbb{C}^m$ di $\mathrm{C}((\mathbf{A}^H)^H) = \mathrm{C}(\mathbf{A})$. □

In particolare, se $U = \langle \mathbf{u}_1; \dots; \mathbf{u}_n \rangle$ è un sottospazio di $\mathbb{C}^m$ dotato del prodotto interno standard, allora la matrice $m \times n$ $\mathbf{A} = [\mathbf{u}_1\ \mathbf{u}_2\ \dots\ \mathbf{u}_n]$ è tale che $U = \mathrm{C}(\mathbf{A})$, e da ciò segue che

$$U^\perp = \mathrm{C}(\mathbf{A})^\perp = \mathrm{N}(\mathbf{A}^H).$$

Rimandiamo al Capitolo 2 per le definizioni e le proprietà della somma e della somma diretta di sottospazi di uno spazio vettoriale.

Nella seguente Proposizione elenchiamo alcune proprietà del complemento ortogonale di un sottospazio, lasciandone come esercizio la facile dimostrazione (si veda l'Esercizio 3.23).

Proposizione 3.3. *Sia V uno spazio vettoriale euclideo.*

(1) $U \cap U^\perp = \{\mathbf{0}\}$ *per ogni sottospazio U di V.*

(2) *Se U e W sono sottospazi di V e U è contenuto in W, allora $W^\perp$ è contenuto in $U^\perp$.*

(3) *Se U_1 e U_2 sono sottospazi di V allora $(U_1 + U_2)^\perp = U_1^\perp \cap U_2^\perp$.* □

Esempio 3.4. Sia $V = \mathbb{C}^3$ dotato del prodotto interno standard. Abbiamo visto nell'Esempio 3.1 che

$$\langle \mathbf{e}_1; \mathbf{e}_3 \rangle^\perp = \langle \mathbf{e}_2 \rangle \subseteq \langle \mathbf{e}_2; \mathbf{e}_3 \rangle = \langle \mathbf{e}_1 \rangle^\perp.$$

È facile verificare che $\langle \mathbf{e}_3 \rangle^\perp = \langle \mathbf{e}_1; \mathbf{e}_2 \rangle$, quindi

$$(\langle \mathbf{e}_1 \rangle + \langle \mathbf{e}_3 \rangle)^\perp = \langle \mathbf{e}_1; \mathbf{e}_3 \rangle^\perp = \langle \mathbf{e}_2 \rangle = \langle \mathbf{e}_2; \mathbf{e}_3 \rangle \cap \langle \mathbf{e}_1; \mathbf{e}_2 \rangle = \langle \mathbf{e}_1 \rangle^\perp \cap \langle \mathbf{e}_3 \rangle^\perp.$$ □

Il nostro prossimo obiettivo è dimostrare che ogni spazio vettoriale euclideo è somma diretta di un suo qualunque sottospazio e del suo complemento ortogonale. La dimostrazione sarà per induzione sulla dimensione del sottospazio; il lemma seguente fornisce il primo passo dell'induzione.

Lemma 3.5. *Per ogni* $\mathbf{0} \neq \mathbf{u} \in V$ *si ha* $V = \langle \mathbf{u} \rangle \oplus \langle \mathbf{u} \rangle^{\perp}$.

Dimostrazione. Per ogni $\mathbf{v} \in V$ si ha:

$$\mathbf{v} - \frac{(\mathbf{u} \mid \mathbf{v})}{(\mathbf{u} \mid \mathbf{u})}\mathbf{u} \in \langle \mathbf{u} \rangle^{\perp}$$

perché

$$\left(\mathbf{v} - \frac{(\mathbf{u} \mid \mathbf{v})}{(\mathbf{u} \mid \mathbf{u})}\mathbf{u} \,\middle|\, \mathbf{u}\right) = (\mathbf{v} \mid \mathbf{u}) - \frac{(\mathbf{v} \mid \mathbf{u})}{(\mathbf{u} \mid \mathbf{u})}(\mathbf{u} \mid \mathbf{u}) = 0,$$

e

$$\mathbf{v} = \frac{(\mathbf{u} \mid \mathbf{v})}{(\mathbf{u} \mid \mathbf{u})}\mathbf{u} + \left(\mathbf{v} - \frac{(\mathbf{u} \mid \mathbf{v})}{(\mathbf{u} \mid \mathbf{u})}\mathbf{u}\right).$$

La tesi segue quindi dalla Proposizione 3.3 (1). □

Il risultato del Lemma 3.5 si estende da sottospazi di dimensione 1 di V a sottospazi di dimensione qualunque.

Proposizione 3.6. *Per ogni sottospazio* U *di uno spazio euclideo* V *si ha* $V = U \oplus U^{\perp}$, *da cui in particolare si ottiene che* $\dim U^{\perp} = \dim V - \dim U$.

Dimostrazione. È sufficiente provare che $V = U \oplus U^{\perp}$, perché la formula sulle dimensioni segue poi dalla Proposizione 3.17 del Capitolo 2.

Procediamo per induzione su $\dim V$ e osserviamo che non è restrittivo supporre $U \neq \{\mathbf{0}\}$.

Se $\dim V = 1$, allora $V = U$ e non c'è nulla da dimostrare. Si supponga ora che la proposizione sia vera per ogni spazio di dimensione minore di $\dim V$ e si fissi $\mathbf{u} \in U$ con $\mathbf{u} \neq \mathbf{0}$.

Poiché per il Lemma 3.5 è $V = \langle \mathbf{u} \rangle \oplus \langle \mathbf{u} \rangle^{\perp}$, posto $W = \langle \mathbf{u} \rangle^{\perp}$ si ha

$$U = \langle \mathbf{u} \rangle \oplus (U \cap W)$$

e quindi anche, per la Proposizione 3.3 (3), $U^{\perp} = W \cap (U \cap W)^{\perp}$.

Poiché $\dim W < \dim V$ e $W \cap (U \cap W)^{\perp}$ è il complemento ortogonale di $U \cap W$ in W, dall'ipotesi induttiva segue che

$$W = (U \cap W) \oplus (W \cap (U \cap W)^{\perp}) = (U \cap W) \oplus U^{\perp},$$

per cui si ottiene $V = \langle \mathbf{u} \rangle \oplus W = \langle \mathbf{u} \rangle \oplus (U \cap W) \oplus U^{\perp} = U \oplus U^{\perp}$. □

Si confronti la Proposizione 3.6 con il Teorema 5.10 del Capitolo 2 e la precedente Proposizione 3.2.

Corollario 3.7. *Per ogni sottospazio U di V si ha $U^{\perp\perp} = U$*

Dimostrazione. Poiché si ha banalmente che U è un sottospazio di $U^{\perp\perp}$, dalla Proposizione 3.6 segue

$$\dim U^{\perp\perp} = \dim V - \dim U^{\perp} = \dim V - (\dim V - \dim U) = \dim U,$$

pertanto la conclusione segue da quanto osservato dopo il Teorema 3.15 del Capitolo 2. □

La Proposizione 3.6 e il Corollario 3.7 sono in realtà equivalenti (si veda l'Esercizio 3.19).

Uno spazio vettoriale V è somma diretta di due suoi sottospazi W e Z se e solo se ogni vettore di V si scrive in uno e un solo modo come somma di un vettore di W e uno di Z (si veda la Proposizione 3.18 del Capitolo 2). Abbiamo quindi provato che, una volta fissato un sottospazio U di V, ogni vettore $\mathbf{v} \in V$ individua completamente due vettori, $\mathbf{u} \in U$ e $\mathbf{w} \in U^{\perp}$, tali che $\mathbf{v} = \mathbf{u} + \mathbf{w}$.

Esempio 3.8. Siano $V = \mathbb{R}^3$ dotato del prodotto interno standard e $U = \langle \mathbf{e}_1; \mathbf{e}_3 \rangle$, per cui, come abbiamo visto nell'Esempio 3.1, $U^{\perp} = \langle \mathbf{e}_2 \rangle$.

Ogni vettore $\mathbf{v} = [x_0\ y_0\ z_0]^T \in \mathbb{R}^3$ si decompone nella somma del vettore $[x_0\ 0\ z_0]^T \in U$ con il vettore $[0\ y_0\ 0]^T \in U^{\perp}$, completamente individuati da $\mathbf{v}$.

Se P è il punto che corrisponde al vettore $\mathbf{v}$, e Q ed R sono rispettivamente le sue proiezioni ortogonali sul piano Oxz e sull'asse y, allora Q corrisponde a $\mathbf{u}$ ed R a $\mathbf{w}$. In altre parole, il vettore $\mathbf{v}$, rappresentato dal segmento orientato OP, è la somma dei vettori $\mathbf{u}$ e $\mathbf{w}$, dove $\mathbf{u}$ è rappresentato dalla proiezione ortogonale OQ di OP sul piano Oxz, e $\mathbf{w}$ è rappresentato dal segmento OR, perpendicolare al piano Oxz (si veda la Figura 3.3). □

Possiamo generalizzare a questo punto il concetto geometrico di proiezione ortogonale di un vettore di $\mathbb{R}^3$ (identificato con il segmento che lo rappresenta nello spazio euclideo) su di un piano o su di una retta.

Sia U un sottospazio di V. Lasciamo come esercizio la facile verifica del fatto che, essendo $V = U \oplus U^{\perp}$ per la Proposizione 3.6, l'applicazione $P_U\colon V \to V$ che associa a ogni $\mathbf{v} \in V$ l'unico vettore $\mathbf{u} \in U$ tale che $\mathbf{v} = \mathbf{u} + \mathbf{w}$ con $\mathbf{w} \in U^{\perp}$ definisce un'applicazione lineare.

Si osservi che P_U è l'unica applicazione lineare di V le cui restrizioni a U e a $U^{\perp}$ siano rispettivamente l'identità e la funzione identicamente nulla.

Definizione. Sia U un sottospazio dello spazio vettoriale euclideo V. L'applicazione lineare $P_U\colon V \to V$ tale che

(po$_1$) $P_U(\mathbf{u}) = \mathbf{u}$ per ogni $\mathbf{u} \in U$,

(po$_2$) $P_U(\mathbf{w}) = \mathbf{0}$ per ogni $\mathbf{w} \in U^{\perp}$,

si chiama *proiezione ortogonale di V su U*. L'immagine $P_U(\mathbf{v})$ tramite P_U di un vettore $\mathbf{v} \in V$ si chiama *la proiezione ortogonale del vettore $\mathbf{v}$ sul sottospazio U di V*.

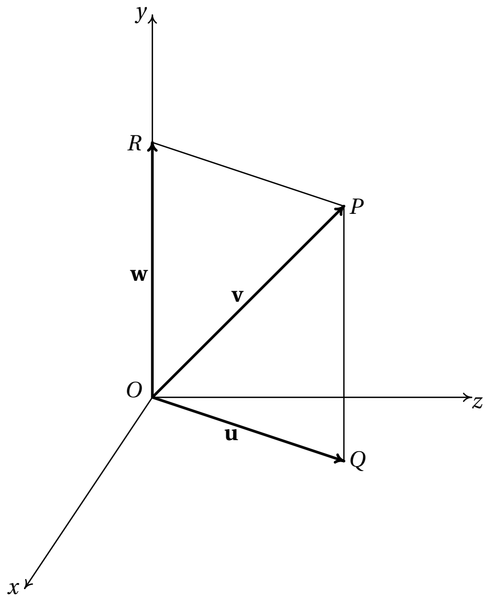


Figura 3.3: Proiezioni ortogonali e decomposizione in somma

Proposizione 3.9. *Siano U un sottospazio dello spazio vettoriale euclideo V e $P_U : V \to V$ la proiezione ortogonale di V su U. Per ogni $\mathbf{v} \in V$ si ha:*

(1) $P_U(\mathbf{v}) = \mathbf{v}$ *se e solo se* $\mathbf{v} \in U$;

(2) $\mathbf{v} - P_U(\mathbf{v}) = \mathbf{w} \in U^\perp$.

Dimostrazione. Dalla linearità di P_U si ottiene che, se $\mathbf{v} \in V$ e $\mathbf{u} \in U$ e $\mathbf{w} \in U^\perp$ sono tali che $\mathbf{v} = \mathbf{u} + \mathbf{w}$, allora

$$P_U(\mathbf{v}) = P_U(\mathbf{u}) + P_U(\mathbf{w}) = \mathbf{u} + \mathbf{0} = \mathbf{u}.$$

Ciò prova (1) e anche che $\mathbf{v} - P_U(\mathbf{v}) = \mathbf{w} \in U^\perp$, ossia (2). $\square$

Nel caso di $V = \mathbb{R}^3$ dotato del prodotto interno standard e U un sottospazio di dimensione 2 (si veda l'Esempio 3.6), identificando i vettori con i segmenti orientati uscenti dall'origine che li rappresentano, $P_U(\mathbf{v})$ è quindi proprio la proiezione ortogonale in senso geometrico di $\mathbf{v}$ sul piano che rappresenta U.

Ricordiamo che in geometria la distanza di un punto P da un piano π è la lunghezza minima di un segmento congiungente P a un punto di π. Se H è il punto di π intercettato dalla perpendicolare per P a π, per ogni punto T di π diverso da H si ha che la lunghezza del segmento PT è strettamente maggiore di quella del segmento PH. Quindi la distanza di P da π è la lunghezza del segmento PH (si veda la Figura 3.4).

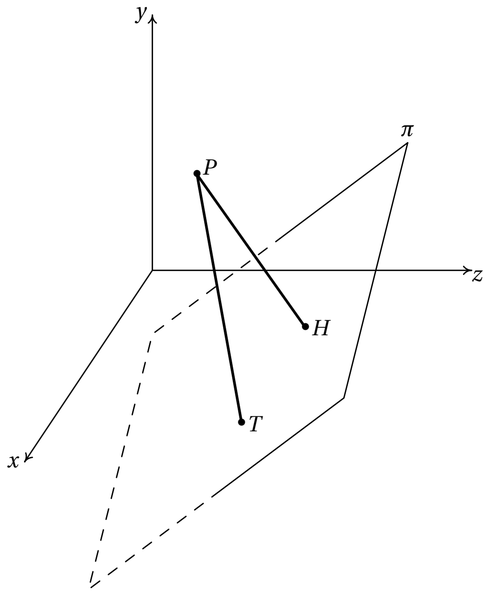


Figura 3.4: Distanza di un punto da un piano

Per esempio, se $U = \langle \mathbf{e}_1; \mathbf{e}_3 \rangle$ è come nell'Esempio 3.8 e $\mathbf{v} = [5\ 4\ 3]^T$, allora $\mathbf{v} = \mathbf{u} + \mathbf{w}$ con

$$\mathbf{u} = \begin{bmatrix} 5 \\ 0 \\ 3 \end{bmatrix} \in U, \qquad \mathbf{w} = \begin{bmatrix} 0 \\ 4 \\ 0 \end{bmatrix} \in U^{\perp} = \langle \mathbf{e}_2 \rangle$$

la distanza del punto P corrispondente a $\mathbf{v}$ dal piano corrispondente a U è

$$\|\mathbf{v} - P_U(\mathbf{v})\|_2 = \|\mathbf{w}\|_2 = \left\| \begin{bmatrix} 0 \\ 4 \\ 0 \end{bmatrix} \right\|_2 = 4.$$

Vogliamo generalizzare quanto abbiamo ora visto in $\mathbb{R}^3$.

Teorema 3.10. *Siano U un sottospazio dello spazio vettoriale euclideo V e $P_U \colon V \to V$ la proiezione ortogonale di V su U; sia inoltre $\|\cdot\|$ la norma indotta dal prodotto interno di V. Per ogni $\mathbf{v} \in V$ si ha:*

(1) *Se $\mathbf{v} \notin U$ allora $\|P_U(\mathbf{v})\| < \|\mathbf{v}\|$, e se $\mathbf{v} \notin U^{\perp}$ allora $\|\mathbf{v} - P_U(\mathbf{v})\| < \|\mathbf{v}\|$.*

(2) $\|\mathbf{v} - P_U(\mathbf{v})\| < \|\mathbf{v} - \mathbf{z}\|$ *per ogni $\mathbf{z} \in U$ con $\mathbf{z} \neq P_U(\mathbf{v})$.*

(3) $P_U(P_U(\mathbf{v})) = P_U(\mathbf{v})$.

(4) $(\mathbf{v} \mid P_U(\mathbf{z})) = (P_U(\mathbf{v}) \mid \mathbf{z})$.

Dimostrazione. Per la Proposizione 3.5 esistono $\mathbf{u} \in U$ e $\mathbf{w} \in U^{\perp}$ tali che $\mathbf{v} = \mathbf{u} + \mathbf{w}$. Da

$$\begin{aligned}\|\mathbf{u}+\mathbf{w}\|^2 &= (\mathbf{u}+\mathbf{w} \mid \mathbf{u}+\mathbf{w}) = (\mathbf{u} \mid \mathbf{u}) + (\mathbf{u} \mid \mathbf{w}) + (\mathbf{w} \mid \mathbf{u}) + (\mathbf{w} \mid \mathbf{w}) \\ &= (\mathbf{u} \mid \mathbf{u}) + (\mathbf{w} \mid \mathbf{w}) = \|\mathbf{u}\|^2 + \|\mathbf{w}\|^2\end{aligned}$$

si deduce che

$$\begin{aligned}\|\mathbf{u}+\mathbf{w}\|^2 > \|\mathbf{w}\|^2 \quad &\text{se} \quad \mathbf{u} \neq \mathbf{0}, \\ \|\mathbf{u}+\mathbf{w}\|^2 > \|\mathbf{u}\|^2 \quad &\text{se} \quad \mathbf{w} \neq \mathbf{0},\end{aligned}$$

ossia che

$$\begin{aligned}\|\mathbf{u}+\mathbf{w}\| > \|\mathbf{w}\| \quad &\text{se} \quad \mathbf{v} \notin U^{\perp}, \\ \|\mathbf{u}+\mathbf{w}\| > \|\mathbf{u}\| \quad &\text{se} \quad \mathbf{v} \notin U.\end{aligned}$$

Poiché abbiamo visto che $P_U(\mathbf{v}) = \mathbf{u}$, ciò prova (1).

In particolare, se $\mathbf{z} \neq P_U(\mathbf{v})$, si ha che $\mathbf{v}_1 = \mathbf{v} - \mathbf{z} \notin U^{\perp}$, e un'applicazione di (1) dà $\|\mathbf{v}_1 - P_U(\mathbf{v}_1)\| < \|\mathbf{v}_1\|$. Si ottiene quindi (2) osservando che $P_U(\mathbf{v}_1) = P_U(\mathbf{v}) - \mathbf{z}$.

Il punto (3) segue da $P_U(\mathbf{v}) \in U$ e dalla definizione di P_U.

Proviamo ora (4). Poiché P_U è una applicazione lineare, dalla linearità del prodotto interno e da $V = U \oplus U^{\perp}$ segue che per provare (4) non è restrittivo supporre $\mathbf{v}, \mathbf{z} \in U \cup U^{\perp}$.

Se $\mathbf{v}, \mathbf{z} \in U$ allora $P_U(\mathbf{v}) = \mathbf{v}$ e $P_U(\mathbf{z}) = \mathbf{z}$ e non vi è nulla da dimostrare.

Supponiamo $\mathbf{z} \in U^{\perp}$. Allora si ha che $P_U(\mathbf{z}) = \mathbf{0}$, per cui $(\mathbf{v} \mid P_U(\mathbf{z})) = (\mathbf{v} \mid \mathbf{0}) = 0$, e anche, essendo $P_U(\mathbf{v}) \in U$, che $(P_U(\mathbf{v}) \mid \mathbf{z}) = 0$. Quindi (4) è soddisfatta.

Analogamente, se $\mathbf{v} \in U^{\perp}$ si ha $(P_U(\mathbf{v}) \mid \mathbf{z}) = (\mathbf{0} \mid \mathbf{z}) = 0$ e anche, essendo $P_U(\mathbf{z}) \in U$, che $(\mathbf{v} \mid P_U(\mathbf{z})) = 0$. □

Dal punto (2) della Proposizione 3.8, si deduce che se $\mathbf{z}_1 \in U$ è tale che $\|\mathbf{v} - \mathbf{z}_1\| \leq \|\mathbf{v} - \mathbf{z}\|$ per ogni $\mathbf{z} \in U$ allora $\mathbf{z}_1 = P_U(\mathbf{v})$. Per questo motivo si dice che $P_U(\mathbf{v})$ è il vettore di U che meglio approssima $\mathbf{v}$ rispetto alla norma indotta dal prodotto interno di V; se tale norma coincide con la norma euclidea (per cui $\|\mathbf{v}\|_2 = (\sum |v_i|^2)^{\frac{1}{2}}$), si dice che $P_U(\mathbf{v})$ meglio approssima $\mathbf{v}$ "ai minimi quadrati".

In analogia con il caso $\mathbb{R}^3$, si pone la seguente definizione.

Definizione. Nelle notazioni della Proposizione 3.8, il numero $\|\mathbf{v} - P_U(\mathbf{v})\|$ si chiama *la distanza del vettore* $\mathbf{v}$ *dal sottospazio U di V*, e si indica con il simbolo $d(\mathbf{v}, U)$.

4. Basi ortogonali e basi ortonormali

Sia V uno spazio vettoriale euclideo. Generalizziamo il concetto di ortogonalità tra due vettori, introdotto nel paragrafo precedente, a un insieme finito di vettori.

Definizione. Un insieme di vettori $\{\mathbf{v}_1; \mathbf{v}_2; \ldots; \mathbf{v}_k\}$ di $k \geq 2$ vettori di V si dice *ortogonale* se $\mathbf{v}_i \perp \mathbf{v}_j$ per ogni $i, j = 1, \ldots, k$ con $i \neq j$, ossia se è costituito da vettori a due a due ortogonali. Si conviene poi che ogni insieme costituito da un unico vettore è un insieme ortogonale. In particolare, una *base ortogonale* di V è una base di V che sia anche un insieme ortogonale.

Esempio 4.1. La base canonica $\mathscr{E} = \{\mathbf{e}_1; \mathbf{e}_2; \ldots; \mathbf{e}_n\}$ di $\mathbb{C}^n$ è una base ortogonale di $\mathbb{C}^n$ dotato del prodotto interno standard: infatti, se $n > 1$,

$$(\mathbf{e}_i \mid \mathbf{e}_j) = \mathbf{e}_i^H \mathbf{e}_j = 0 \quad \text{per ogni } i \neq j. \qquad \square$$

Come ci si può aspettare guardando a semplici esempi in $\mathbb{R}^3$, l'ortogonalità è una condizione più forte dell'indipendenza lineare.

Proposizione 4.2. *Un insieme ortogonale $\mathscr{S} = \{\mathbf{v}_1; \mathbf{v}_2; \ldots; \mathbf{v}_k\}$ costituito da vettori non nulli è linearmente indipendente.*

Dimostrazione. Si consideri una combinazione lineare nulla degli elementi di $\mathscr{S}$:

$$\mathbf{0} = \alpha_1 \mathbf{v}_1 + \alpha_2 \mathbf{v}_2 + \cdots + \alpha_{k-1} \mathbf{v}_{k-1} + \alpha_k \mathbf{v}_k.$$

Per ogni $j \in \{1, \ldots, k\}$, dalla linearità del prodotto interno e da $\mathbf{v}_j \perp \mathbf{v}_i$ per ogni $i \neq j$, si ottiene

$$\begin{aligned} 0 = (\mathbf{v}_j \mid \mathbf{0}) &= (\mathbf{v}_j \mid \alpha_1 \mathbf{v}_1 + \alpha_2 \mathbf{v}_2 + \cdots + \alpha_{k-1} \mathbf{v}_{k-1} + \alpha_k \mathbf{v}_k) \\ &= \alpha_1 (\mathbf{v}_j \mid \mathbf{v}_1) + \alpha_2 (\mathbf{v}_j \mid \mathbf{v}_2) + \cdots + \alpha_{k-1} (\mathbf{v}_j \mid \mathbf{v}_{k-1}) + \alpha_k (\mathbf{v}_j \mid \mathbf{v}_k) \\ &= \alpha_j (\mathbf{v}_j \mid \mathbf{v}_j). \end{aligned}$$

Da ciò si deduce, essendo $(\mathbf{v}_j \mid \mathbf{v}_j) \neq 0$ poiché $\mathbf{v}_j$ è supposto non nullo, che $\alpha_j = 0$.

Al variare di $j \in \{1, \ldots, k\}$ si ottiene che tutti i coefficienti della combinazione lineare sono uguali a 0, ossia che $\mathscr{S}$ è linearmente indipendente. $\square$

La seguente proposizione prova l'esistenza di basi ortogonali di V. Nel prossimo paragrafo illustreremo un algoritmo, detto *algoritmo di Gram-Schmidt*, che permette di costruire una base ortogonale di V a partire da una base generica. Per tutto il Capitolo, anche se non sarà detto esplicitamente, ogni spazio vettoriale considerato sarà euclideo.

Proposizione 4.3. *Se $V \neq \{\mathbf{0}\}$, allora V ammette una base ortogonale.*

Dimostrazione. Procediamo per induzione su $n = \dim V \geq 1$.

Se $n = 1$ ogni base di V è costituita da un unico vettore, e quindi per definizione è un base ortogonale di V.

Supponiamo ora che $n > 1$ e che ogni spazio vettoriale euclideo U di dimensione $n - 1$ ammetta una base ortogonale (ipotesi induttiva).

Siano $\mathbf{0} \neq \mathbf{v} \in V$ e $U = \langle \mathbf{v} \rangle^\perp$ il complemento ortogonale di $\langle \mathbf{v} \rangle$ in V. Dalla Proposizione 3.5 si ottiene che $V = \langle \mathbf{v} \rangle \oplus U$ e $\dim U = \dim V - 1 = n - 1$. Per ipotesi induttiva, dal momento che la restrizione a U del prodotto interno di V è un prodotto interno per U, esiste una base ortogonale $\{\mathbf{u}_1; \mathbf{u}_2; \dots; \mathbf{u}_{n-1}\}$ di U. Per definizione, i vettori che la compongono, se in numero maggiore di uno, sono a due a due ortogonali, inoltre ciascuno di essi, stando nel complemento ortogonale di $\langle \mathbf{v} \rangle$ è ortogonale a $\mathbf{v}$. L'insieme $\mathscr{B} = \{\mathbf{v}; \mathbf{u}_1; \mathbf{u}_2; \dots; \mathbf{u}_{n-1}\}$ è dunque un insieme ortogonale costituito da vettori non nulli, che quindi, per la Proposizione 4.2, è linearmente indipendente. Poiché $\mathscr{B}$ ha $n = \dim V$ elementi, esso è una base.

Con ciò concludiamo che $\mathscr{B}$ è una base ortogonale di V. □

Il vantaggio dell'impiego di basi ortogonali rispetto a basi generiche sta nella possibilità di un calcolo immediato dei coefficienti delle combinazioni lineari dei loro vettori. Più precisamente, vale il risultato seguente.

Proposizione 4.4. *Siano U un sottospazio di V e $\mathscr{B} = \{\mathbf{u}_1; \mathbf{u}_2; \dots; \mathbf{u}_k\}$ una base ortogonale di U. Allora per ogni vettore $\mathbf{u}$ di U si ha*

$$\mathbf{u} = \alpha_1 \mathbf{u}_1 + \alpha_2 \mathbf{u}_2 + \dots + \alpha_k \mathbf{u}_k$$

con

$$\alpha_i = \frac{(\mathbf{u}_i \mid \mathbf{u})}{(\mathbf{u}_i \mid \mathbf{u}_i)}$$

per ogni $i = 1, \dots, k$.

Dimostrazione. Poiché $\mathscr{B}$ è una base di U e $\mathbf{u} \in U$, esistono scalari α_1, α_2, ..., α_k tali che

$$\mathbf{u} = \alpha_1 \mathbf{u}_1 + \alpha_2 \mathbf{u}_2 + \dots + \alpha_k \mathbf{u}_k.$$

Con un procedimento analogo a quello adottato nella dimostrazione della Proposizione 4.2, per ogni $i \in \{1, \dots, k\}$, dalla linearità del prodotto interno e da $\mathbf{u}_j \perp \mathbf{u}_i$ per ogni $j \neq i$, si ottiene

$$\begin{aligned}
(\mathbf{u}_i \mid \mathbf{u}) &= (\mathbf{u}_i \mid \alpha_1 \mathbf{u}_1 + \alpha_2 \mathbf{u}_2 + \dots + \alpha_k \mathbf{u}_k) \\
&= \alpha_1 (\mathbf{u}_i \mid \mathbf{u}_1) + \alpha_2 (\mathbf{u}_i \mid \mathbf{u}_2) + \dots + \alpha_k (\mathbf{u}_i \mid \mathbf{u}_k) \\
&= \alpha_i (\mathbf{u}_i \mid \mathbf{u}_i).
\end{aligned}$$

Se ne deduce, essendo $(\mathbf{u}_i \mid \mathbf{u}_i) \neq 0$, che

$$\alpha_i = \frac{(\mathbf{u}_i \mid \mathbf{u})}{(\mathbf{u}_i \mid \mathbf{u}_i)}.$$ □

Esempio 4.5. Sia $\mathbb{R}^3$ dotato del prodotto interno standard e consideriamo

$$\mathscr{B} = \left\{ \mathbf{v}_1 = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}; \mathbf{v}_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}; \mathbf{v}_3 = \begin{bmatrix} 1 \\ 0 \\ -1 \end{bmatrix} \right\},$$

$$\mathscr{B}' = \left\{ \mathbf{v}'_1 = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}; \mathbf{v}'_2 = \begin{bmatrix} 1 \\ 2 \\ 0 \end{bmatrix}; \mathbf{v}'_3 = \begin{bmatrix} 1 \\ 1 \\ -1 \end{bmatrix} \right\}.$$

Lasciamo come esercizio la verifica che $\mathscr{B}$ e $\mathscr{B}'$ sono due basi di V, inoltre che $\mathscr{B}$ è ortogonale, mentre $\mathscr{B}'$ non lo è.

Vogliamo esprimere $\mathbf{v} = [3\ 4\ 5]^T$ come combinazione lineare degli elementi di $\mathscr{B}$ e come combinazione lineare degli elementi di $\mathscr{B}'$. Cerchiamo quindi gli scalari α_1, α_2, α_3, β_1, β_2, β_3 tali che

$$\mathbf{v} = \alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2 + \alpha_3\mathbf{v}_3 = \beta_1\mathbf{v}'_1 + \beta_2\mathbf{v}'_2 + \beta_3\mathbf{v}'_3.$$

Per trovare β_1, β_2, β_3, non abbiamo altra scelta che risolvere un sistema lineare, procedimento che può richiedere anche calcoli laboriosi. In questo caso specifico, da

$$\begin{bmatrix}3\\4\\5\end{bmatrix} = \mathbf{v} = \beta_1\mathbf{v}'_1 + \beta_2\mathbf{v}'_2 + \beta_3\mathbf{v}'_3 = \beta_1\begin{bmatrix}1\\0\\1\end{bmatrix} + \beta_2\begin{bmatrix}1\\2\\0\end{bmatrix} + \beta_3\begin{bmatrix}1\\1\\-1\end{bmatrix} = \begin{bmatrix}\beta_1+\beta_2+\beta_3\\2\beta_2+\beta_3\\\beta_1-\beta_3\end{bmatrix}$$

otteniamo il sistema lineare che ha come matrice aumentata

$$\left[\begin{array}{ccc|c}1 & 1 & 1 & 3\\0 & 2 & 1 & 4\\1 & 0 & -1 & 5\end{array}\right]$$

e ha come unica soluzione $[7/3\ 10/3\ -8/3]$.

Per trovare α_1, α_2 e α_3, invece, possiamo procedere direttamente calcolando

$$\alpha_1 = \frac{\mathbf{v}_1^T\mathbf{v}}{\mathbf{v}_1^T\mathbf{v}_1} = 4, \qquad \alpha_2 = \frac{\mathbf{v}_2^T\mathbf{v}}{\mathbf{v}_2^T\mathbf{v}_2} = 4, \qquad \alpha_3 = \frac{\mathbf{v}_3^T\mathbf{v}}{\mathbf{v}_3^T\mathbf{v}_3} = -1. \qquad \square$$

È naturale chiedersi che significato ha il vettore $\alpha_1\mathbf{v}_1 + \cdots + \alpha_n\mathbf{v}_n$ della Proposizione 4.4, dove $\alpha_i = \frac{(\mathbf{u}_i|\mathbf{u})}{(\mathbf{u}_i|\mathbf{u}_i)}$, per ogni i, nel caso il vettore $\mathbf{u}$ non appartenga al sottospazio U. La risposta sta nel risultato seguente.

Proposizione 4.6. *Siano U un sottospazio di V e $\mathscr{B} = \{\mathbf{u}_1;\mathbf{u}_2;\dots;\mathbf{u}_k\}$ una base ortogonale di U. Per ogni vettore $\mathbf{v} \in V$ si ha*

$$P_U(\mathbf{v}) = \frac{(\mathbf{u}_1 \mid \mathbf{v})}{(\mathbf{u}_1 \mid \mathbf{u}_1)}\mathbf{u}_1 + \frac{(\mathbf{u}_2 \mid \mathbf{v})}{(\mathbf{u}_2 \mid \mathbf{u}_2)}\mathbf{u}_2 + \cdots + \frac{(\mathbf{u}_k \mid \mathbf{v})}{(\mathbf{u}_k \mid \mathbf{u}_k)}\mathbf{u}_k.$$

Dimostrazione. Applicando la Proposizione 4.4 a $P_U(\mathbf{v}) \in U$ si ottiene

$$P_U(\mathbf{v}) = \frac{(\mathbf{u}_1 \mid P_U(\mathbf{v}))}{(\mathbf{u}_1 \mid \mathbf{u}_1)}\mathbf{u}_1 + \frac{(\mathbf{u}_2 \mid P_U(\mathbf{v}))}{(\mathbf{u}_2 \mid \mathbf{u}_2)}\mathbf{u}_2 + \cdots + \frac{(\mathbf{u}_k \mid P_U(\mathbf{v}))}{(\mathbf{u}_k \mid \mathbf{u}_k)}\mathbf{u}_k.$$

Poiché abbiamo visto che $\mathbf{v} = P_U(\mathbf{v}) + \mathbf{w}$ per un opportuno $\mathbf{w} \in U^\perp$, dalla linearità del prodotto interno otteniamo

$$(\mathbf{u}_i \mid \mathbf{v}) = (\mathbf{u}_i \mid P_U(\mathbf{v}) + \mathbf{w}) = (\mathbf{u}_i \mid P_U(\mathbf{v})) + (\mathbf{u}_i \mid \mathbf{w}) = (\mathbf{u}_i \mid P_U(\mathbf{v}))$$

per ogni $i = 1, \dots, k$, e quindi la tesi. $\square$

Osservazione 4.7. Siano U un sottospazio non nullo di V ed $\mathscr{S} = \{\mathbf{u}_1;\dots;\mathbf{u}_k\}$ un insieme di generatori di U che sia anche un insieme ortogonale. Allora l'insieme che si ottiene da $\mathscr{S}$ togliendo gli eventuali vettori nulli è una base ortogonale di U e per ogni $\mathbf{v} \in V$ si ha (si veda l'Esercizio 3.27)

$$P_U(\mathbf{v}) = \alpha_1\mathbf{u}_1 + \dots + \alpha_k\mathbf{u}_k$$

dove

$$\alpha_i = \begin{cases} 0 & \text{se } \mathbf{u}_i = \mathbf{0} \\ \frac{(\mathbf{u}_i|\mathbf{v})}{(\mathbf{u}_i|\mathbf{u}_i)} & \text{se } \mathbf{u}_i \neq \mathbf{0} \end{cases}$$

per ogni $i = 1,\dots,k$.

Per il calcolo della proiezione ortogonale di un vettore $\mathbf{v} \in V$ su un sottospazio U di V, occorre quindi saper effettivamente costruire una base ortogonale di U, la cui esistenza è assicurata dalla Proposizione 4.3.

Se i calcoli possono essere semplificati dall'impiego di basi ortogonali, lo sono ancora di più quando si usano basi ortonormali.

Diremo che un vettore $\mathbf{v} \in V$ viene *normalizzato* quando al posto di $\mathbf{v}$ si considera il vettore

$$\frac{1}{\|\mathbf{v}\|}\mathbf{v} = \frac{\mathbf{v}}{\|\mathbf{v}\|},$$

dove $\|\cdot\|$ è la norma indotta dal prodotto interno. Ovviamente un vettore è normalizzato se e solo se ha norma uguale a 1 e inoltre

$$\left\langle \frac{\mathbf{v}}{\|\mathbf{v}\|} \right\rangle = \langle \mathbf{v} \rangle.$$

Definizione. Una base $\mathscr{B} = \{\mathbf{v}_1;\mathbf{v}_2;\dots;\mathbf{v}_n\}$ di V si dice una *base ortonormale* se è ortogonale e ogni suo vettore è normalizzato, ossia se

$$\mathbf{v}_i \perp \mathbf{v}_j \quad \text{per} \quad i \neq j \quad \text{e} \quad \|\mathbf{v}_i\| = 1 \quad \text{per ogni } i = 1,\dots,n.$$

Esempio 4.8. La base canonica $\{\mathbf{e}_1;\mathbf{e}_2;\dots;\mathbf{e}_n\}$ di $\mathbb{C}^n$, è una base ortonormale di $\mathbb{C}^n$ dotato del prodotto interno standard, essendo ortogonale (si veda l'Esempio 4.1) ed essendo $\|\mathbf{e}_i\|_2 = 1$, per ogni $i = 1,\dots,n$. □

Ovviamente, da ogni base ortogonale di V se ne ottiene una ortonormale normalizzandone tutti i vettori.

Osservazione 4.9. Siano U un sottospazio di V e $\mathscr{B} = \{\mathbf{u}_1;\mathbf{u}_2;\dots;\mathbf{u}_k\}$ una base ortonormale di U. Dal momento che per ogni $i = 1,\dots,k$ si ha che $(\mathbf{u}_i \mid \mathbf{u}_i) = \|\mathbf{u}_i\|^2 = 1$, la Proposizione 4.4 si semplifica nel seguente modo:

$$\mathbf{u} = (\mathbf{u}_1 \mid \mathbf{u})\mathbf{u}_1 + (\mathbf{u}_2 \mid \mathbf{u})\mathbf{u}_2 + \dots + (\mathbf{u}_k \mid \mathbf{u})\mathbf{u}_k.$$

Analogamente, se $\mathbf{v} \in V$ dalla Proposizione 4.6 si ottiene:

$$P_U(\mathbf{v}) = (\mathbf{u}_1 \mid \mathbf{v})\mathbf{u}_1 + (\mathbf{u}_2 \mid \mathbf{v})\mathbf{u}_2 + \dots + (\mathbf{u}_k \mid \mathbf{v})\mathbf{u}_k.$$

5. L'algoritmo di Gram-Schmidt

Sia V uno spazio vettoriale euclideo. Descriviamo un algoritmo che, applicato a un insieme di generatori di V, fornisce un insieme di generatori che sia anche un insieme ortogonale (si dice un *insieme ortogonale di generatori*). Se $V \neq \{\mathbf{0}\}$, l'insieme che si ottiene togliendo da quest'ultimo insieme gli eventuali vettori nulli è una base ortogonale di V (si veda l'Osservazione 4.7).

Lemma 5.1. *Siano U un sottospazio di V e $\mathscr{S}_U = \{\mathbf{u}_1;\dots;\mathbf{u}_r\}$ un insieme ortogonale di generatori di U. Siano poi $\mathbf{v} \in V$ e $W = U + \langle \mathbf{v} \rangle$. Allora posto*

$$\mathbf{u}_{r+1} = \mathbf{v} - P_U(\mathbf{v}) = \mathbf{v} - \alpha_1\mathbf{u}_1 - \alpha_2\mathbf{u}_2 - \cdots - \alpha_r\mathbf{u}_r,$$

dove

$$\alpha_i = \begin{cases} 0 & \textit{se } \mathbf{u}_i = \mathbf{0} \\ \dfrac{(\mathbf{u}_i \mid \mathbf{v})}{(\mathbf{u}_i \mid \mathbf{u}_i)} & \textit{se } \mathbf{u}_i \neq \mathbf{0} \end{cases}$$

per ogni $i = 1,\dots,r$, si ha che $\mathscr{S}_W = \{\mathbf{u}_1;\dots;\mathbf{u}_r;\mathbf{u}_{r+1}\}$ è un insieme ortogonale di generatori di W.

Dimostrazione. Se $U = \{\mathbf{0}\}$, l'asserto è ovvio.

Sia ora $U \neq \{\mathbf{0}\}$. Per l'Osservazione 4.7 si ha che $P_U(\mathbf{v}) = \alpha_1\mathbf{u}_1 + \cdots + \alpha_r\mathbf{u}_r$, per cui

$$\mathbf{u}_{r+1} = \mathbf{v} - P_U(\mathbf{v}) = \mathbf{v} - \alpha_1\mathbf{u}_1 - \cdots - \alpha_r\mathbf{u}_r \in U + \langle \mathbf{v} \rangle$$

e $\langle \mathscr{S}_W \rangle$ è un sottospazio di W. Poiché $\mathscr{S}_U$ è un insieme ortogonale e sappiamo che $\mathbf{v} - P_U(\mathbf{v}) \in U^\perp$, allora anche $\mathscr{S}_W$ è un insieme ortogonale. Infine da

$$\mathbf{v} = P_U(\mathbf{v}) + \mathbf{u}_{r+1} = \alpha_1\mathbf{u}_1 + \alpha_2\mathbf{u}_2 + \cdots + \alpha_r\mathbf{u}_r + \mathbf{u}_{r+1}$$

otteniamo che W è contenuto in $\langle \mathscr{S}_W \rangle$, per cui $W = \langle \mathscr{S}_W \rangle$, ossia $\mathscr{S}_W$ è un insieme di generatori di W. □

Teorema 5.2 (Algoritmo di Gram-Schmidt)**.** *Sia $\mathscr{S} = \{\mathbf{v}_1;\dots;\mathbf{v}_m\}$ un insieme di generatori di V. Si ponga*

$$V_0 = \{\mathbf{0}\} \quad e \quad V_k = \langle \mathbf{v}_1;\dots;\mathbf{v}_k \rangle \quad \textit{per ogni } 1 \le k \le m,$$

e sia $P_{V_k}\colon V \to V$ la proiezione ortogonale di V su V_k per ogni $0 \le k \le m$. Allora l'insieme

$\mathscr{S}^* = \{\mathbf{u}_1; \mathbf{u}_2; \dots; \mathbf{u}_m\}$ *dei vettori*

$$\begin{aligned}
&\mathbf{u}_1 = \mathbf{v}_1 - P_{V_0}(\mathbf{v}_1) = \mathbf{v}_1\\
&\mathbf{u}_2 = \mathbf{v}_2 - P_{V_1}(\mathbf{v}_2) = \mathbf{v}_2 - \alpha_{12}\mathbf{u}_1,\\
&\mathbf{u}_3 = \mathbf{v}_3 - P_{V_2}(\mathbf{v}_3) = \mathbf{v}_3 - \alpha_{13}\mathbf{u}_1 - \alpha_{23}\mathbf{u}_2,\\
&\vdots\\
&\mathbf{u}_k = \mathbf{v}_k - P_{V_{k-1}}(\mathbf{v}_k) = \mathbf{v}_k - \alpha_{1k}\mathbf{u}_1 - \alpha_{2k}\mathbf{u}_2 - \alpha_{3k}\mathbf{u}_3 - \dots - \alpha_{k-1,k}\mathbf{u}_{k-1},\\
&\vdots\\
&\mathbf{u}_m = \mathbf{v}_m - P_{V_{m-1}}(\mathbf{v}_m) = \mathbf{v}_m - \alpha_{1m}\mathbf{u}_1 - \alpha_{2m}\mathbf{u}_2 - \alpha_{3m}\mathbf{u}_3 - \dots - \alpha_{m-1,m}\mathbf{u}_{m-1},
\end{aligned}$$

dove, per ogni $i, j = 1, \dots, m$ con $i < j$, i coefficienti α_{ij} sono definiti da

$$\alpha_{ij} = \begin{cases} 0 & \text{se } \mathbf{u}_i = \mathbf{0} \\ \dfrac{(\mathbf{u}_i \mid \mathbf{v}_j)}{(\mathbf{u}_i \mid \mathbf{u}_i)} & \text{se } \mathbf{u}_i \neq \mathbf{0} \end{cases}$$

è un insieme ortogonale di generatori di V.

Dimostrazione. Poiché $\mathbf{u}_1 = \mathbf{v}_1$ allora $\mathscr{S}_{V_1} = \{\mathbf{u}_1\}$ è un insieme ortogonale di generatori di V_1.

La dimostrazione del Teorema consiste ora in $m-1$ passaggi, ciascuno dei quali è un'applicazione del Lemma 5.1.

Al primo passaggio lo si applica a $U = V_1$, $\mathscr{S}_{V_1} = \{\mathbf{u}_1\}$ e $\mathbf{v} = \mathbf{v}_2$ ottenendo così che $\mathscr{S}_{V_2} = \{\mathbf{u}_1; \mathbf{u}_2\}$ è un insieme ortogonale di generatori di V_2.

Al secondo passaggio lo si applica a $U = V_2$, $\mathscr{S}_{V_2} = \{\mathbf{u}_1; \mathbf{u}_2\}$ (che per il passaggio precedente è un insieme ortogonale di generatori di V_2) e $\mathbf{v} = \mathbf{v}_3$ ottenendo così che $\mathscr{S}_{V_3} = \{\mathbf{u}_1; \mathbf{u}_2; \mathbf{u}_3\}$ è un insieme ortogonale di generatori di V_3.

Procedendo in questo modo, all'$(m-1)$-esimo passaggio, sapendo dal passaggio precedente che $\mathscr{S}_{V_{m-1}} = \{\mathbf{u}_1; \mathbf{u}_2; \dots; \mathbf{u}_{m-1}\}$ è un insieme ortogonale di generatori di V_{m-1}, si applica il Lemma 5.1 a $U = V_{m-1}$, $\mathscr{S}_{V_{m-1}} = \{\mathbf{u}_1; \mathbf{u}_2; \dots; \mathbf{u}_{m-1}\}$ e $\mathbf{v} = \mathbf{v}_m$ ottenenedo così che $\mathscr{S}_{V_m} = \{\mathbf{u}_1; \dots; \mathbf{u}_{m-1}; \mathbf{u}_m\}$ è un insieme ortogonale di generatori di $V_m = V$. □

Osservazione 5.3. L'insieme $\{\mathbf{u}_1; \dots; \mathbf{u}_n\}$ che si ottiene applicando l'algoritmo di Gram-Schmidt a un insieme linearmente indipendente $\{\mathbf{v}_1; \dots; \mathbf{v}_n\}$ non contiene vettori nulli.

Infatti se, con le notazioni del Lemma 5.1, esistesse $1 < i \leq n$ tale che $\mathbf{u}_i = \mathbf{0}$, da $\mathbf{u}_i = \mathbf{v}_i - P_{V_{i-1}}(\mathbf{v}_i)$ si otterrebbe $\mathbf{v}_i \in V_{i-1}$. In tal caso, come anche nel caso in cui a essere nullo fosse il vettore $\mathbf{u}_1 = \mathbf{v}_1$, si avrebbe che $\{\mathbf{v}_1; \dots; \mathbf{v}_i\}$ sarebbe linarmente dipendente, mentre è un sottoinsieme dell'insieme linearmente indipendente $\{\mathbf{v}_1; \dots; \mathbf{v}_n\}$.

Esempio 5.4. Sia V il sottospazio di $\mathbb{C}^3$, dotato del prodotto interno standard, generato dall'insieme di vettori

$$\mathscr{S} = \left\{ \mathbf{v}_1 = \begin{bmatrix} 1 \\ 2i \\ 1 \end{bmatrix}; \mathbf{v}_2 = \begin{bmatrix} i \\ -2 \\ i \end{bmatrix}; \mathbf{v}_3 = \begin{bmatrix} 6 \\ 0 \\ 6 \end{bmatrix}; \mathbf{v}_4 = \begin{bmatrix} 8i \\ 8 \\ 8i \end{bmatrix} \right\}.$$

Applichiamo l'algoritmo di Gram-Schmidt ai vettori di $\mathscr{S}$. Otterremo i vettori $\mathbf{u}_1$, $\mathbf{u}_2$, $\mathbf{u}_3$, $\mathbf{u}_4$, ciascuno dei quali è legato a quelli che lo precedono e al corrispondente elemento di $\mathscr{S}$ dalle seguenti relazioni:

$$\begin{aligned}
\mathbf{u}_1 &= \mathbf{v}_1, \\
\mathbf{u}_2 &= \mathbf{v}_2 - \alpha_{12}\mathbf{u}_1, \\
\mathbf{u}_3 &= \mathbf{v}_3 - \alpha_{13}\mathbf{u}_1 - \alpha_{23}\mathbf{u}_2, \\
\mathbf{u}_4 &= \mathbf{v}_4 - \alpha_{14}\mathbf{u}_1 - \alpha_{24}\mathbf{u}_2 - \alpha_{34}\mathbf{u}_3,
\end{aligned}$$

dove per $1 \le i < j \le 4$ i coefficienti α_{ij} sono dati dalla formula

$$\alpha_{ij} = \begin{cases} 0 & \text{se } \mathbf{u}_i = \mathbf{0} \\ \dfrac{(\mathbf{u}_i \mid \mathbf{v}_j)}{(\mathbf{u}_i \mid \mathbf{u}_i)} & \text{se } \mathbf{u}_i \neq \mathbf{0} \end{cases}$$

(GS1) Poniamo innanzitutto

$$\mathbf{u}_1 = \mathbf{v}_1 = \begin{bmatrix} 1 \\ 2i \\ 1 \end{bmatrix}.$$

(GS2) Per costruire $\mathbf{u}_2$, dobbiamo calcolare il coefficiente α_{12}, che, essendo $\mathbf{u}_1 \neq \mathbf{0}$, è dato da

$$\alpha_{12} = \frac{(\mathbf{u}_1 \mid \mathbf{v}_2)}{(\mathbf{u}_1 \mid \mathbf{u}_1)} = \frac{\mathbf{u}_1^H \mathbf{v}_2}{\mathbf{u}_1^H \mathbf{u}_1} = \frac{\begin{bmatrix} 1 & -2i & 1 \end{bmatrix} \begin{bmatrix} i \\ -2 \\ i \end{bmatrix}}{\begin{bmatrix} 1 & -2i & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 2i \\ 1 \end{bmatrix}} = \frac{6i}{6} = i.$$

Dunque si ha

$$\mathbf{u}_2 = \mathbf{v}_2 - i\mathbf{u}_1 = \begin{bmatrix} i \\ -2 \\ i \end{bmatrix} - i \begin{bmatrix} 1 \\ 2i \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}.$$

(GS3) Per costruire $\mathbf{u}_3$, dobbiamo, essendo già a conoscenza di $\mathbf{u}_1$ e $\mathbf{u}_2$, calcolare i coefficienti α_{13} e α_{23}. Essendo $\mathbf{u}_1 \neq \mathbf{0}$, il primo è dato da

$$\alpha_{13} = \frac{(\mathbf{u}_1 \mid \mathbf{v}_3)}{(\mathbf{u}_1 \mid \mathbf{u}_1)} = \frac{\mathbf{u}_1^H \mathbf{v}_3}{\mathbf{u}_1^H \mathbf{u}_1} = \frac{\begin{bmatrix} 1 & -2i & 1 \end{bmatrix} \begin{bmatrix} 6 \\ 0 \\ 6 \end{bmatrix}}{\begin{bmatrix} 1 & -2i & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 2i \\ 1 \end{bmatrix}} = \frac{12}{6} = 2,$$

mentre, essendo $\mathbf{u}_2 = \mathbf{0}$, si prende $\alpha_{23} = 0$. Dunque si ha

$$\mathbf{u}_3 = \mathbf{v}_3 - 2\mathbf{u}_1 = \begin{bmatrix} 6 \\ 0 \\ 6 \end{bmatrix} - 2 \begin{bmatrix} 1 \\ 2i \\ 1 \end{bmatrix} = \begin{bmatrix} 4 \\ -4i \\ 4 \end{bmatrix}.$$

(GS4) Infine, per costruire $\mathbf{u}_4$, dopo aver già determinato $\mathbf{u}_1$, $\mathbf{u}_2$ e $\mathbf{u}_3$, dobbiamo calcolare i coefficienti α_{14}, α_{24} e α_{34}. Essendo $\mathbf{u}_1 \neq \mathbf{0}$ e $\mathbf{u}_3 \neq \mathbf{0}$, per ottenere il primo e il terzo si calcola:

$$\alpha_{14} = \frac{(\mathbf{u}_1 \mid \mathbf{v}_4)}{(\mathbf{u}_1 \mid \mathbf{u}_1)} = \frac{\mathbf{u}_1^H \mathbf{v}_4}{\mathbf{u}_1^H \mathbf{u}_1} = \frac{\begin{bmatrix} 1 & -2i & 1 \end{bmatrix} \begin{bmatrix} 8i \\ 8 \\ 8i \end{bmatrix}}{\begin{bmatrix} 1 & -2i & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 2i \\ 1 \end{bmatrix}} = \frac{0}{6} = 0,$$

$$\alpha_{34} = \frac{(\mathbf{u}_3 \mid \mathbf{v}_4)}{(\mathbf{u}_3 \mid \mathbf{u}_3)} = \frac{\mathbf{u}_3^H \mathbf{v}_4}{\mathbf{u}_3^H \mathbf{u}_3} = \frac{\begin{bmatrix} 4 & 4i & 4 \end{bmatrix} \begin{bmatrix} 8i \\ 8 \\ 8i \end{bmatrix}}{\begin{bmatrix} 4 & 4i & 4 \end{bmatrix} \begin{bmatrix} 4 \\ -4i \\ 4 \end{bmatrix}} = \frac{96i}{48} = 2i,$$

mentre, essendo $\mathbf{u}_2 = \mathbf{0}$, si prende $\alpha_{24} = 0$. In definitiva si ricava

$$\mathbf{u}_4 = \mathbf{v}_4 - 2i\mathbf{u}_3 = \begin{bmatrix} 8i \\ 8 \\ 8i \end{bmatrix} - 2i \begin{bmatrix} 4 \\ -4i \\ 4 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}.$$

Pertanto

$$\mathscr{S}^* = \left\{ \mathbf{u}_1 = \begin{bmatrix} 1 \\ 2i \\ 1 \end{bmatrix}; \mathbf{u}_2 = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}; \mathbf{u}_3 = \begin{bmatrix} 4 \\ -4i \\ 4 \end{bmatrix}; \mathbf{u}_4 = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \right\}$$

è un insieme ortogonale di generatori di V e l'insieme

$$\left\{ \mathbf{u}_1 = \begin{bmatrix} 1 \\ 2i \\ 1 \end{bmatrix}; \mathbf{u}_3 = \begin{bmatrix} 4 \\ -4i \\ 4 \end{bmatrix} \right\}$$

che si ottiene da $\mathscr{S}^*$ togliendo il vettore nullo è una base ortogonale di V. □

Useremo il procedimento che abbiamo illustrato nel prossimo paragrafo per trovare una decomposizione $\mathbf{A} = \mathbf{Q}_0\mathbf{R}_0$ di una matrice $\mathbf{A}$. Nel caso però in cui l'obiettivo sia quello di ottenere una base ortogonale di $V = \langle \mathscr{S} \rangle$ a partire da $\mathscr{S}$, può risultare più conveniente procedere diversamente.

Infatti, trovando prima a partire da $\mathscr{S}$ una generica base $\mathscr{B}$ di V, può accadere che $\mathscr{B}$ abbia un numero di elementi minore di quello di $\mathscr{S}$. In tal caso l'applicazione dell'algoritmo di Gram-Schmidt agli elementi di $\mathscr{B}$ necessita di in un numero minore di passaggi rispetto a quella effettuata sugli elementi di $\mathscr{S}$, e l'insieme che si ottiene da $\mathscr{B}$ è già una base ortogonale di V.

Esempio 5.5. Riprendiamo il sottoinsieme $\mathscr{S}$ di $\mathbb{C}^3$ dell'Esempio 5.4. È opportuno per quanto segue cambiare le notazioni e porre

$$\mathscr{S} = \left\{ \mathbf{w}_1 = \begin{bmatrix} 1 \\ 2i \\ 1 \end{bmatrix}; \mathbf{w}_2 = \begin{bmatrix} i \\ -2 \\ i \end{bmatrix}; \mathbf{w}_3 = \begin{bmatrix} 6 \\ 0 \\ 6 \end{bmatrix}; \mathbf{w}_4 = \begin{bmatrix} 8i \\ 8 \\ 8i \end{bmatrix} \right\}.$$

Troviamo una generica base $\mathscr{B}$ di $V = \langle \mathscr{S} \rangle$.

Per esempio possiamo cercare una base dello spazio delle colonne $C(\mathbf{A})$ di una matrice $\mathbf{A}$ che abbia come colonne gli elementi di $\mathscr{S}$ (per cui $\mathrm{C}(\mathbf{A}) = \langle \mathscr{S} \rangle = V$). Se

$$\mathbf{A} = \begin{bmatrix} 1 & i & 6 & 8i \\ 2i & -2 & 0 & 8 \\ 1 & i & 6 & 8i \end{bmatrix},$$

con un'eliminazione di Gauss su $\mathbf{A}$ si ottiene una sua forma ridotta di Gauss $\mathbf{U}$:

$$\mathbf{A} = \begin{bmatrix} 1 & i & 6 & 8i \\ 2i & -2 & 0 & 8 \\ 1 & i & 6 & 8i \end{bmatrix} \to \begin{bmatrix} 1 & i & 6 & 8i \\ 0 & 0 & -12i & 24 \\ 0 & 0 & 0 & 0 \end{bmatrix} \to \begin{bmatrix} 1 & i & 6 & 8i \\ 0 & 0 & 1 & 2i \\ 0 & 0 & 0 & 0 \end{bmatrix} = \mathbf{U}.$$

Poiché le colonne dominanti di $\mathbf{U}$ sono la prima e la terza, allora una base $\mathscr{B}$ dello spazio delle colonne di $\mathbf{A}$, e quindi di V, è

$$\mathscr{B} = \left\{ \mathbf{w}_1 = \begin{bmatrix} 1 \\ 2i \\ 1 \end{bmatrix}; \mathbf{w}_3 = \begin{bmatrix} 6 \\ 0 \\ 6 \end{bmatrix} \right\}.$$

Dopo aver posto $\mathbf{v}_1 = \mathbf{w}_1$ e $\mathbf{v}_2 = \mathbf{w}_3$ applichiamo l'algoritmo di Gram-Schmidt a $\{\mathbf{v}_1; \mathbf{v}_2\}$.

(GS1) Prendiamo innanzitutto

$$\mathbf{u}_1 = \mathbf{v}_1 = \begin{bmatrix} 1 \\ 2i \\ 1 \end{bmatrix}.$$

(GS2) Per determinare $\mathbf{u}_2 = \mathbf{v}_2 - \alpha_{12}\mathbf{u}_1$, dobbiamo calcolare il coefficiente α_{12}, che, essendo $\mathbf{u}_1 \neq \mathbf{0}$ è dato da

$$\alpha_{12} = \frac{(\mathbf{u}_1 \mid \mathbf{v}_2)}{(\mathbf{u}_1 \mid \mathbf{u}_1)} = \frac{\mathbf{u}_1^H \mathbf{v}_2}{\mathbf{u}_1^H \mathbf{u}_1} = \frac{\begin{bmatrix} 1 & -2i & 1 \end{bmatrix} \begin{bmatrix} 6 \\ 0 \\ 6 \end{bmatrix}}{\begin{bmatrix} 1 & -2i & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 2i \\ 1 \end{bmatrix}} = \frac{12}{6} = 2,$$

per cui

$$\mathbf{u}_2 = \mathbf{v}_2 - 2\mathbf{u}_1 = \begin{bmatrix} 6 \\ 0 \\ 6 \end{bmatrix} - 2 \begin{bmatrix} 1 \\ 2i \\ 1 \end{bmatrix} = \begin{bmatrix} 4 \\ -4i \\ 4 \end{bmatrix}$$

e quindi

$$\left\{ \mathbf{u}_1 = \begin{bmatrix} 1 \\ 2i \\ 1 \end{bmatrix}; \mathbf{u}_2 = \begin{bmatrix} 4 \\ -4i \\ 4 \end{bmatrix} \right\}$$

è una base ortogonale di V.

Volendo trovare una base ortonormale di V, si normalizzano i vettori di una base ortogonale:

$$\|\mathbf{u}_1\|_2 = \sqrt{\mathbf{u}_1^H \mathbf{u}_1} = \left(\begin{bmatrix} 1 & -2i & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 2i \\ 1 \end{bmatrix} \right)^{1/2} = \sqrt{1+4+1} = \sqrt{6},$$

$$\|\mathbf{u}_2\|_2 = \sqrt{\mathbf{u}_2^H \mathbf{u}_2} = \left(\begin{bmatrix} 4 & 4i & 4 \end{bmatrix} \begin{bmatrix} 4 \\ -4i \\ 4 \end{bmatrix} \right)^{1/2} = \sqrt{16+16+16} = 4\sqrt{3},$$

per cui

$$\left\{ \frac{\mathbf{u}_1}{\|\mathbf{u}_1\|_2} = \frac{1}{\sqrt{6}} \begin{bmatrix} 1 \\ 2i \\ 1 \end{bmatrix}; \frac{\mathbf{u}_2}{\|\mathbf{u}_2\|_2} = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 \\ -i \\ 1 \end{bmatrix} \right\}$$

è una base ortonormale di V. $\square$

6. Matrici di proiezione e decomposizione QR

Chiameremo *matrice di proiezione* ogni matrice (complessa o reale) idempotente ed hermitiana, ossia ogni matrice $\mathbf{P}$ tale che $\mathbf{P}^2 = \mathbf{P} = \mathbf{P}^H$. La motivazione della scelta del nome è data dal seguente teorema che caratterizza le matrici di proiezione come quelle matrici la cui pre-moltiplicazione concida con la proiezione ortogonale di $\mathbb{C}^n$ su di un opportuno sottospazio U. Il discorso può essere ripetuto in modo del tutto analogo nel caso reale.

Teorema 6.1. *Una matrice quadrata* $\mathbf{P}$ *complessa di ordine* n *è una matrice di proiezione se e solo se esiste un sottospazio* U *di* $\mathbb{C}^n$*, tale che per ogni* $\mathbf{v} \in \mathbb{C}^n$ *si abbia* $\mathbf{Pv} = P_U(\mathbf{v})$. *In tal caso risulta* $U = \mathrm{C}(\mathbf{P})$*, lo spazio delle colonne di* $\mathbf{P}$.

Dimostrazione. Sia $\mathbf{P}$ una matrice di proiezione, ossia tale che $\mathbf{P}^2 = \mathbf{P} = \mathbf{P}^H$.

Da $\mathbf{P}$ hermitiana segue che $\mathrm{N}(\mathbf{P}^H) = \mathrm{N}(\mathbf{P})$, per cui, essendo $\mathrm{C}(\mathbf{P})^\perp = \mathrm{N}(\mathbf{P}^H)$ (si veda la Proposizione 3.2) si ha che $\mathbb{C}^n = \mathrm{C}(\mathbf{P}) \oplus \mathrm{N}(\mathbf{P})$ per la Proposizione 3.6. Da $\mathbf{P}^2 = \mathbf{P}$ segue poi che $\mathbf{P}(\mathbf{Pe}_i) = \mathbf{Pe}_i$ per ogni $i = 1, \dots, n$, dove $\{\mathbf{e}_1; \dots; \mathbf{e}_n\}$ è la base canonica di $\mathbb{C}^n$. Dunque, ricordando che $\mathbf{Pe}_i$ è la i-esima colonna di $\mathbf{P}$, si ottiene che la pre-moltiplicazione per $\mathbf{P}$ è una applicazione lineare di $\mathbb{C}^n$ che ristretta a $\mathrm{C}(\mathbf{P})$ è l'identità e ristretta a $\mathrm{N}(\mathbf{P})$ è l'applicazione nulla. Pertanto la pre-moltiplicazione per $\mathbf{P}$ è la proiezione ortogonale di $\mathbb{C}^n$ su $\mathrm{C}(\mathbf{P})$.

Viceversa siano U un sottospazio di $\mathbb{C}^n$ e $\mathbf{P}$ una matrice tale che

$$\mathbf{Pv} = P_U(\mathbf{v}) \quad \text{per ogni } \mathbf{v} \in \mathbb{C}^n. \tag{*}$$

Si osservi che esiste ed è unica una matrice $\mathbf{P}$ soddisfacente la condizione (*):

$$\mathbf{P} = \begin{bmatrix} \mathbf{Pe}_1 & \mathbf{Pe}_2 & \dots & \mathbf{Pe}_n \end{bmatrix} = \begin{bmatrix} P_U(\mathbf{e}_1) & P_U(\mathbf{e}_2) & \dots & P_U(\mathbf{e}_n) \end{bmatrix}.$$

Prendendo $V = \mathbb{C}^n$ con il prodotto interno standard in 3.10 (3) e (4), si ottiene che $\mathbf{P}^2 = \mathbf{P} = \mathbf{P}^H$, ossia che $\mathbf{P}$ è una matrice di proiezione. La prima parte del teorema dà ora $U = \mathrm{C}(\mathbf{P})$. $\square$

Affinché la pre-moltiplicazione per una matrice complessa quadrata $\mathbf{A}$ di ordine n sia la proiezione di $\mathbb{C}^n$ sullo spazio delle colonne $\mathrm{C}(\mathbf{A})$ di $\mathbf{A}$ occorre che $\mathbf{A}$ soddisfi entrambe le condizioni $\mathbf{A} = \mathbf{A}^2$ e $\mathbf{A} = \mathbf{A}^H$, come mostrano i due esempi che seguono.

Esempio 6.2. La matrice reale $\mathbf{A} = \begin{bmatrix} 0 & 0 \\ 2 & 1 \end{bmatrix}$ è idempotente ma non simmetrica. Il suo spazio delle colonne $\mathrm{C}(\mathbf{A})$ è il sottospazio di $\mathbb{C}^2$ generato da $\mathbf{e}_2$, e il complemento ortogonale in $\mathbb{C}^2$ di $\mathrm{C}(\mathbf{A})$ è il sottospazio di $\mathbb{C}^2$ generato da $\mathbf{e}_1$. Pertanto la proiezione ortogonale di $\mathbf{v} = \mathbf{e}_1$ su $\mathrm{C}(\mathbf{A})$ è il vettore nullo. Invece, pre-moltiplicando per $\mathbf{A}$ il vettore $\mathbf{v}$ si ottiene

$$\mathbf{Av} = \mathbf{Ae}_1 = 2\mathbf{e}_2 \neq \mathbf{0} = P_{\mathrm{C}(\mathbf{A})}(\mathbf{v}).$$ $\square$

Esempio 6.3. La matrice reale

$$\mathbf{B} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 0 \\ 1 & 0 & 2 \end{bmatrix}$$

è simmetrica ma non idempotente. Se $\mathbf{u}$ è la sua prima colonna, si ha

$$\mathbf{B}\mathbf{u} \neq \mathbf{u} = P_{C(\mathbf{B})}(\mathbf{u}). \qquad \square$$

Lemma 6.4. *Sia* $\mathbf{Q}$ *una matrice* $n \times k$*. Allora* $\mathbf{Q}^H\mathbf{Q} = \mathbf{I}_k$ *se e solo se le colonne di* $\mathbf{Q}$ *sono ortonormali.*

Dimostrazione. Se $\mathbf{Q} = [\mathbf{u}_1 \ \dots \ \mathbf{u}_k]$, allora

$$\mathbf{Q}^H = \begin{bmatrix} \mathbf{u}_1^H \\ \vdots \\ \mathbf{u}_k^H \end{bmatrix},$$

per cui, calcolando il prodotto $\mathbf{Q}^H\mathbf{Q}$ a blocchi, si ottiene che l'elemento di posto (i, j) di $\mathbf{Q}^H\mathbf{Q}$ è $\mathbf{u}_i^H\mathbf{u}_j$. Quindi

$$\mathbf{Q}^H\mathbf{Q} = \mathbf{I}_k \iff (\mathbf{u}_i \mid \mathbf{u}_j) = \begin{cases} 0 & \text{se } i \neq j \\ 1 & \text{se } i = j \end{cases}$$

ossia se e solo se le colonne di $\mathbf{Q}$ sono ortonormali. $\square$

Il teorema che segue fornisce uno strumento per il calcolo effettivo della matrice di proiezione su di un sottospazio U di $\mathbb{C}^n$.

Teorema 6.5. *Una matrice quadrata* $\mathbf{P}$ *complessa di ordine* n *e rango* k *è una matrice di proiezione se e solo se* $\mathbf{P} = \mathbf{Q}\mathbf{Q}^H$ *dove* $\mathbf{Q}$ *è una matrice* $n \times k$ *le cui colonne sono i vettori di una base ortonormale del sottospazio* U *di* $\mathbb{C}^n$ *tale che* $\mathbf{P}\mathbf{v} = P_U(\mathbf{v})$ *per ogni* $\mathbf{v} \in \mathbb{C}^n$*.*

Dimostrazione. Sia $\mathbf{P}$ una matrice di proiezione, ossia tale che $\mathbf{P}^2 = \mathbf{P} = \mathbf{P}^H$.

Per il Teorema 6.1 esiste un sottospazio U di $\mathbb{C}^n$ tale che $\mathbf{P}\mathbf{v} = P_U(\mathbf{v})$ per ogni $\mathbf{v} \in \mathbb{C}^n$. Poiché inoltre $U = C(\mathbf{P})$ allora $k = \dim U$.

Dalla Proposizione 4.6 segue che se $\mathscr{B} = \{\mathbf{u}_1; \dots; \mathbf{u}_k\}$ è una base ortonormale di U, allora

$$P_U(\mathbf{v}) = \sum_{i=1,\dots,k} (\mathbf{u}_i \mid \mathbf{v})\mathbf{u}_i \quad \text{per ogni } \mathbf{v} \in \mathbb{C}^n.$$

Quindi si ottiene:

$$\begin{aligned} \mathbf{P}\mathbf{v} = P_U(\mathbf{v}) &= \sum_{i=1,\dots,k} (\mathbf{u}_i \mid \mathbf{v})\mathbf{u}_i = \sum_{i=1,\dots,k} \mathbf{u}_i^H\mathbf{v}\mathbf{u}_i = \sum_{i=1,\dots,k} \mathbf{u}_i\mathbf{u}_i^H\mathbf{v} \\ &= \Big(\sum_{i=1,\dots,k} \mathbf{u}_i\mathbf{u}_i^H\Big)\mathbf{v} = \mathbf{Q}\mathbf{Q}^H\mathbf{v} \end{aligned}$$

dove $\mathbf{Q} = [\mathbf{u}_1 \ \dots \ \mathbf{u}_k]$ è una matrice che ha come colonne i vettori di $\mathscr{B}$.

Viceversa se $\mathbf{P} = \mathbf{Q}\mathbf{Q}^H$ dove $\mathbf{Q}$ è una matrice con colonne ortonormali, allora $\mathbf{P}^H = (\mathbf{Q}\mathbf{Q}^H)^H = (\mathbf{Q}^H)^H\mathbf{Q}^H = \mathbf{Q}\mathbf{Q}^H = \mathbf{P}$ e dal Lemma 6.3 si ottiene anche

$$\mathbf{P}^2 = \mathbf{Q}\mathbf{Q}^H\mathbf{Q}\mathbf{Q}^H = \mathbf{Q}\mathbf{I}_k\mathbf{Q}^H = \mathbf{Q}\mathbf{Q}^H = \mathbf{P}.$$

Dunque $\mathbf{P}$ è una matrice di proiezione. Resta da provare che le colonne di $\mathbf{Q}$ sono i vettori di una base ortonormale di $U = \mathrm{C}(\mathbf{P})$, ossia che $\mathrm{C}(\mathbf{Q}) = \mathrm{C}(\mathbf{P})$. Ciò segue da

$$\mathrm{C}(\mathbf{P}) = \langle \mathbf{P}\mathbf{e}_i : i = 1, \dots, n\rangle = \langle \mathbf{Q}(\mathbf{Q}^H \mathbf{e}_i) : i = 1, \dots, n\rangle \subseteq \mathrm{C}(\mathbf{Q})$$

e da $\dim \mathrm{C}(\mathbf{P}) = \mathrm{rk}\,\mathbf{P} = k = \mathrm{rk}\,\mathbf{Q} = \dim \mathrm{C}(\mathbf{Q})$. □

Dal Teorema 6.5 segue che $\mathbf{P}$ dipende dal sottospazio $\mathrm{C}(\mathbf{P}) = \mathrm{C}(\mathbf{Q})$, ma è indipendente dalla particolare base ortonormale di esso che si sceglie per costruire $\mathbf{Q}$, come è illustrato dall'esempio seguente.

Esempio 6.6. Si consideri il sottospazio $U = \langle \mathbf{v}_1 = [1\ 1\ 1]^T ; \mathbf{v}_2 = [0\ 1\ 0]^T\rangle$ di $\mathbb{R}^3$. Applicando l'algoritmo di Gram-Schmidt a $\{\mathbf{v}_1; \mathbf{v}_2\}$ e normalizzando poi i vettori che si ottengono, si costruisce una base ortonormale di U:

$$\mathscr{B}_1 = \left\{ \frac{1}{\sqrt{3}} \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} ; \frac{1}{\sqrt{6}} \begin{bmatrix} -1 \\ 2 \\ -1 \end{bmatrix} \right\}.$$

Per il Teorema 6.5, posto

$$\mathbf{Q}_1 = \begin{bmatrix} 1/\sqrt{3} & -1/\sqrt{6} \\ 1/\sqrt{3} & 2/\sqrt{6} \\ 1/\sqrt{3} & -1/\sqrt{6} \end{bmatrix},$$

la matrice di proiezione su U è:

$$\mathbf{P}_1 = \mathbf{Q}_1\mathbf{Q}_1^H = \begin{bmatrix} 1/\sqrt{3} & -1/\sqrt{6} \\ 1/\sqrt{3} & 2/\sqrt{6} \\ 1/\sqrt{3} & -1/\sqrt{6} \end{bmatrix} \begin{bmatrix} 1/\sqrt{3} & 1/\sqrt{3} & 1/\sqrt{3} \\ -1/\sqrt{6} & 2/\sqrt{6} & -1/\sqrt{6} \end{bmatrix} = \begin{bmatrix} 1/2 & 0 & 1/2 \\ 0 & 1 & 0 \\ 1/2 & 0 & 1/2 \end{bmatrix}.$$

D'altra parte, se $\mathbf{w}_1 = \mathbf{v}_1 - \mathbf{v}_2$, si ha che $\mathbf{w}_1 \perp \mathbf{v}_2$ e $U = \langle \mathbf{w}_1, \mathbf{v}_2\rangle$. Quindi, normalizzando $\mathbf{w}_1 = [1\ 0\ 1]^T$, si ricava che anche

$$\mathscr{B}_2 = \left\{ \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} ; \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \right\}$$

è una base ortonormale di U. Anche se la matrice

$$\mathbf{Q}_2 = \begin{bmatrix} 1/\sqrt{2} & 0 \\ 0 & 1 \\ 1/\sqrt{2} & 0 \end{bmatrix},$$

costruita a partire dalla base ortonormale $\mathscr{B}_2$ di U, è diversa da $\mathbf{Q}_1$, costruita a partire dalla base ortonormale $\mathscr{B}_1$ di U, si ha che

$$\mathbf{P}_2 = \mathbf{Q}_2\mathbf{Q}_2^H = \begin{bmatrix} 1/\sqrt{2} & 0 \\ 0 & 1 \\ 1/\sqrt{2} & 0 \end{bmatrix} \begin{bmatrix} 1/\sqrt{2} & 0 & 1/\sqrt{2} \\ 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1/2 & 0 & 1/2 \\ 0 & 1 & 0 \\ 1/2 & 0 & 1/2 \end{bmatrix} = \mathbf{P}_1.$$ □

Siano U un sottospazio di $\mathbb{C}^n$ e $\mathbf{P}$ la matrice di proiezione su U. Sappiamo che essendo $\mathbb{C}^n = U \oplus U^\perp$, per la Proposizione 3.6, per ogni $\mathbf{v} \in \mathbb{C}^n$ esistono $\mathbf{u} \in U$ e $\mathbf{w} \in U^\perp$ tali che $\mathbf{v} = \mathbf{u} + \mathbf{w}$. Dal Teorema 6.1 segue che $\mathbf{Pv} = P_U(\mathbf{v}) = \mathbf{u}$, e quindi

$$(\mathbf{I}_n - \mathbf{P})\mathbf{v} = \mathbf{v} - \mathbf{Pv} = \mathbf{v} - \mathbf{u} = \mathbf{w} = P_{U^\perp}(\mathbf{v}).$$

Pertanto, sempre per il Teorema 6.1, abbiamo dimostrato il risultato seguente.

Proposizione 6.7. *Dato un sottospazio U di $\mathbb{C}^n$ con matrice di proiezione $\mathbf{P}$, la matrice di proiezione sul complemento ortogonale $U^\perp$ di U è $\mathbf{I}_n - \mathbf{P}$.* □

Osservazione 6.8. Siano U_1 e U_2 due sottospazi di $\mathbb{C}^n$ tra loro ortogonali, e siano $\mathbf{P}_1$ e $\mathbf{P}_2$ le matrici di proiezione su U_1 e U_2 rispettivamente. Poiché da $U_1 \perp U_2$ segue che $U_1 \cap U_2 = \{\mathbf{0}\}$, allora (si veda l'Esercizio 3.24) si ha $\mathbf{0} = P_{\{\mathbf{0}\}}(\mathbf{v}) = P_{U_1 \cap U_2}(\mathbf{v}) = P_{U_1}(P_{U_2}(\mathbf{v})) = \mathbf{P}_1(\mathbf{P}_2(\mathbf{v}))$, e, analogamente, $\mathbf{0} = P_{U_2}(P_{U_1}(\mathbf{v})) = \mathbf{P}_2(\mathbf{P}_1(\mathbf{v}))$ per ogni $\mathbf{v} \in \mathbb{C}^n$.

Se ne deduce che $\mathbf{P}_1\mathbf{P}_2 = \mathbb{O} = \mathbf{P}_2\mathbf{P}_1$, ossia che il prodotto di due matrici di proiezione su due sottospazi di $\mathbb{C}^n$ tra loro ortogonali è la matrice nulla.

Mostriamo ora come ogni matrice $\mathbf{A}$ possa essa fattorizzata nel prodotto di una matrice a colonne ortogonali e una matrice unitriangolare superiore. Tale decomposizione si chiama *decomposizione QR non normalizzata di* $\mathbf{A}$. Partendo da essa, costruiremo poi una fattorizzazione di $\mathbf{A}$ nel prodotto di una matrice a colonne ortonormali e una matrice a scala per righe (*decomposizione QR normalizzata di* $\mathbf{A}$).

Sia $\mathbf{A} = [\mathbf{v}_1\ \mathbf{v}_2\ \dots\ \mathbf{v}_n]$ una matrice (reale o complessa) $m \times n$. Applicando l'algoritmo di Gram-Schmidt alle colonne $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n$ di $\mathbf{A}$ si ottengono i vettori $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_n$ definiti nel modo seguente:

$$\begin{aligned}
&\mathbf{u}_1 = \mathbf{v}_1\\
&\mathbf{u}_2 = \mathbf{v}_2 - \alpha_{12}\mathbf{u}_1\\
&\vdots\\
&\mathbf{u}_k = \mathbf{v}_k - \alpha_{1k}\mathbf{u}_1 - \alpha_{2k}\mathbf{u}_2 - \alpha_{3k}\mathbf{u}_3 - \dots - \alpha_{k-1,k}\mathbf{u}_{k-1} \quad \text{per ogni } 1 < k \le n,
\end{aligned}$$

con

$$\alpha_{ij} = \begin{cases} 0 & \text{se } \mathbf{u}_i = \mathbf{0} \\ \dfrac{(\mathbf{u}_i \mid \mathbf{v}_j)}{(\mathbf{u}_i \mid \mathbf{u}_i)} & \text{se } \mathbf{u}_i \neq \mathbf{0} \end{cases}$$

per ogni $1 \le i \neq j \le n$, dove il prodotto interno è quello standard.

Siano $\mathbf{Q}_0 = [\mathbf{u}_1\ \mathbf{u}_2\ \dots\ \mathbf{u}]$ la matrice che ha come come colonne i vettori $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_n$ ed $\mathbf{R}_0$ la seguente matrice unitriangolare superiore costruita con i coefficienti α_{ij}:

$$\mathbf{R}_0 = \begin{bmatrix} 1 & \alpha_{12} & \dots & \alpha_{1,n-1} & \alpha_{1n} \\ 0 & 1 & \dots & \alpha_{2,n-1} & \alpha_{2n} \\ \dots & & & & \\ 0 & 0 & \dots & 1 & \alpha_{n-1,n} \\ 0 & 0 & \dots & 0 & 1 \end{bmatrix}.$$

Per ogni $k = 1, \dots, n$ si ha

$$\begin{aligned}\mathbf{Q}_0(\mathbf{R}_0\mathbf{e}_k) &= \mathbf{Q}_0(\mathbf{e}_k + \sum_{i=1,\dots,k-1} \alpha_{ik}\mathbf{e}_i) = \mathbf{Q}_0\mathbf{e}_k + \sum_{i=1,\dots,k-1} \alpha_{ik}\mathbf{Q}_0\mathbf{e}_i\\ &= \mathbf{u}_k + \sum_{i=1,\dots,k-1} \alpha_{ik}\mathbf{u}_i = \mathbf{v}_k = \mathbf{A}\mathbf{e}_k,\end{aligned}$$

per cui $\mathbf{A} = \mathbf{Q}_0\mathbf{R}_0$. Abbiamo quindi provato il seguente risultato.

Teorema 6.9 (Decomposizione QR non normalizzata di $\mathbf{A}$)**.** *Sia* $\mathbf{A}$ *una matrice* $m \times n$*. Allora esistono una matrice* $m \times n$ $\mathbf{Q}_0$ *a colonne ortogonali e una matrice unitriangolare superiore di ordine* n $\mathbf{R}_0$ *tali che* $\mathbf{A} = \mathbf{Q}_0\mathbf{R}_0$*.* □

Osservazione 6.10. Sia $\mathbf{A} = \mathbf{Q}_0\mathbf{R}_0$ una decomposizione QR non normalizzata di una matrice $m \times n$ $\mathbf{A}$ di rango k. Poiché $\mathbf{R}_0$ è invertibile, da $\mathbf{A} = \mathbf{Q}_0\mathbf{R}_0$ segue che $C(\mathbf{A}) = C(\mathbf{Q}_0)$. In particolare, essendo le colonne di $\mathbf{Q}_0$ ortogonali e $k = \operatorname{rk}\mathbf{A} = \dim C(\mathbf{A})$, dalla Proposizione 4.2 si ottiene che $n-k$ colonne di $\mathbf{Q}_0$ sono nulle. Inoltre, se $k > 1$, per come abbiamo costruito $\mathbf{Q}_0$ e dal Teorema 5.3, segue che se $V_{k-1} = \langle \mathbf{u}_1; \dots; \mathbf{u}_{k-1}\rangle$ allora $V_{k-1} = \langle \mathbf{v}_1; \dots; \mathbf{v}_{k-1}\rangle$ e

$$\mathbf{u}_k = \mathbf{v}_k - P_{V_{k-1}}(\mathbf{v}_k).$$

Ciò mostra che ogni vettore $\mathbf{u}_k$ ottenuto con l'algoritmo di Gram-Schmidt non è altro che la proiezione ortogonale di $\mathbf{v}_k$ sul sottospazio complemento ortogonale di V_{k-1}. Inoltre, per il Teorema 3.10, $\|\mathbf{u}_k\|_2$ è la distanza di $\mathbf{u}_k$ da V_{k-1} (si veda la Definizione al termine del Paragrafo).

Esempio 6.11. Sia

$$\mathbf{A} = \begin{bmatrix} 1 & i & 6 & 8i \\ 2i & -2 & 0 & 8 \\ 1 & i & 6 & 8i \end{bmatrix}.$$

Applicando l'algoritmo di Gram-Schmidt all'insieme $\{\mathbf{v}_1; \mathbf{v}_2; \mathbf{v}_3; \mathbf{v}_4\}$ delle colonne di $\mathbf{A}$ si ottengono i vettori (si veda l'Esempio 5.4)

$$\mathbf{u}_1 = \mathbf{v}_1 = \begin{bmatrix} 1 \\ 2i \\ 1 \end{bmatrix},$$

$$\mathbf{u}_2 = \mathbf{v}_2 - \alpha_{12}\mathbf{u}_1 = \mathbf{v}_2 - i\mathbf{u}_1 = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix},$$

$$\mathbf{u}_3 = \mathbf{v}_3 - \alpha_{13}\mathbf{u}_1 - \alpha_{23}\mathbf{u}_2 = \mathbf{v}_3 - 2\mathbf{u}_1 = \begin{bmatrix} 4 \\ -4i \\ 4 \end{bmatrix},$$

$$\mathbf{u}_4 = \mathbf{v}_4 - \alpha_{14}\mathbf{u}_1 - \alpha_{24}\mathbf{u}_2 - \alpha_{34}\mathbf{u}_3 = \mathbf{v}_4 - 2i\mathbf{u}_3 = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}.$$

Pertanto posto

$$\mathbf{Q}_0 = \begin{bmatrix} 1 & 0 & 4 & 0 \\ 2i & 0 & -4i & 0 \\ 1 & 0 & 4 & 0 \end{bmatrix} \quad \text{e} \quad \mathbf{R}_0 = \begin{bmatrix} 1 & i & 2 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 2i \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

si ha che $\mathbf{A} = \mathbf{Q}_0\mathbf{R}_0$ è una decomposizione QR non normalizzata di $\mathbf{A}$. □

Se $\mathbf{Q}_1$ è la matrice $m \times k$ ottenuta da $\mathbf{Q}_0$ sopprimendone le colonne nulle ed $\mathbf{R}_1$ è la matrice $k \times n$ ottenuta da $\mathbf{R}_0$ sopprimendone le righe di indice corrispondente a quello delle colonne nulle di $\mathbf{Q}_0$, allora $\mathbf{Q}_0\mathbf{R}_0 = \mathbf{Q}_1\mathbf{R}_1$ (si eseguano i prodotti $\mathbf{Q}_0\mathbf{R}_0$ e $\mathbf{Q}_1\mathbf{R}_1$ a blocchi, suddividendo $\mathbf{Q}_0$ e $\mathbf{Q}_1$ in righe ed $\mathbf{R}_0$ ed $\mathbf{R}_1$ in colonne). Sia $\mathbf{D}$ la matrice diagonale di ordine k i cui gli elementi diagonali sono le norme euclidee delle colonne di $\mathbf{Q}_1$. Poiché le colonne di $\mathbf{Q}_1$ sono vettori non nulli, le loro norme euclidee sono diverse da 0, per cui $\mathbf{D}$ è invertibile, e posto $\mathbf{Q} = \mathbf{Q}_1\mathbf{D}^{-1}$ ed $\mathbf{R} = \mathbf{D}\mathbf{R}_1$ si ha $\mathbf{Q}_1\mathbf{R}_1 = \mathbf{Q}\mathbf{R}$. Abbiamo quindi provato il seguente risultato.

Teorema 6.12 (Decomposizione QR normalizzata di $\mathbf{A}$)**.** *Sia* $\mathbf{A}$ *una matrice* $m \times n$ *di rango* k. *Allora esistono una matrice* $m \times k$ $\mathbf{Q}$ *a colonne ortonormali e una matrice a scala per righe* $k \times n$ $\mathbf{R}$ *tali che* $\mathbf{A} = \mathbf{Q}\mathbf{R}$. □

Osservazione 6.13. Sia $\mathbf{A} = \mathbf{Q}\mathbf{R}$ una decomposizione QR normalizzata di una matrice $m \times n$ $\mathbf{A}$ di rango k. Poiché la i-esima colonna di $\mathbf{Q}$, per $i = 1, \dots, k$, è la i-esima colonna di $\mathbf{Q}_1$ normalizzata, allora

$$\mathrm{C}(\mathbf{Q}) = \mathrm{C}(\mathbf{Q}_1) = \mathrm{C}(\mathbf{Q}_0) = \mathrm{C}(\mathbf{A})$$

e le colonne di $\mathbf{Q}$ formano una base ortonormale di $\mathrm{C}(\mathbf{A})$.

Si osservi inoltre che essendo $\mathbf{R}_0$ invertibile, le sue colonne sono linearmente indipendenti. Dunque anche le colonne di $\mathbf{R}_1$ sono linearmente indipendenti, per cui $\mathrm{rk}\mathbf{R}_1 = k \le n$. Da $\mathbf{D}$ invertibile ed $\mathbf{R} = \mathbf{D}\mathbf{R}_1$ segue infine che $\mathrm{rk}\mathbf{R} = k$. Pertanto la decomposizione $\mathbf{A} = \mathbf{Q}\mathbf{R}$ è una decomposizione a rango pieno di $\mathbf{A}$.

Esempio 6.14. Si consideri di nuovo la matrice dell'Esempio 6.11

$$\mathbf{A} = \begin{bmatrix} 1 & i & 6 & 8i \\ 2i & -2 & 0 & 8 \\ 1 & i & 6 & 8i \end{bmatrix}.$$

Partendo dalla decomposizione QR non normalizzata di $\mathbf{A}$, $\mathbf{A} = \mathbf{Q}_0\mathbf{R}_0$, si costruiscono prima le matrici

$$\mathbf{Q}_1 = \begin{bmatrix} 1 & 4 \\ 2i & -4i \\ 1 & 4 \end{bmatrix} \quad \text{e} \quad \mathbf{R}_1 = \begin{bmatrix} 1 & i & 2 & 0 \\ 0 & 0 & 1 & 2i \end{bmatrix}.$$

Poiché

$$\|\mathbf{u}_1\|_2 = \sqrt{\begin{bmatrix}1 & -2i & 1\end{bmatrix}\begin{bmatrix}1\\2i\\1\end{bmatrix}} = \sqrt{1+4+1} = \sqrt{6}$$

$$\|\mathbf{u}_3\|_2 = \sqrt{\begin{bmatrix}4 & 4i & 4\end{bmatrix}\begin{bmatrix}4\\-4i\\4\end{bmatrix}} = \sqrt{16+16+16} = 4\sqrt{3},$$

allora

$$\mathbf{D} = \begin{bmatrix}\sqrt{6} & 0\\ 0 & 4\sqrt{3}\end{bmatrix} \quad \text{e} \quad \mathbf{D}^{-1} = \begin{bmatrix}1/\sqrt{6} & 0\\ 0 & 1/4\sqrt{3}\end{bmatrix}.$$

Posto

$$\mathbf{Q} = \mathbf{Q}_1\mathbf{D}^{-1} = \begin{bmatrix}1/\sqrt{6} & 1/\sqrt{3}\\ 2i/\sqrt{6} & -i/\sqrt{3}\\ 1/\sqrt{6} & 1/\sqrt{3}\end{bmatrix} \quad \text{e} \quad \mathbf{R} = \mathbf{D}\mathbf{R}_1 = \begin{bmatrix}\sqrt{6} & \sqrt{6}i & 2\sqrt{6} & 0\\ 0 & 0 & 4\sqrt{3} & 8\sqrt{3}i\end{bmatrix}$$

si ha che $\mathbf{A} = \mathbf{QR}$ è una decomposizione QR normalizzata di $\mathbf{A}$. □

7. Approssimazione ai minimi quadrati

Se un sistema lineare $\mathbf{Ax} = \mathbf{b}$ ha la matrice dei coefficienti $\mathbf{A}$ (quadrata) invertibile, allora il vettore $\mathbf{A}^{-1}\mathbf{b}$ è l'unica soluzione del sistema. Ricordando che, data una generica matrice $m \times n$ $\mathbf{A}$, la sua pseudo-inversa $\mathbf{A}^+$ generalizza per certi aspetti la matrice inversa, è naturale porsi la seguente domanda: dato il sistema lineare $\mathbf{Ax} = \mathbf{b}$, con $\mathbf{A}$ matrice qualunque, quale significato ha il vettore $\mathbf{A}^+\mathbf{b}$?

Nella prima parte di questo paragrafo daremo una risposta esauriente a tale domanda.

Sia pertanto $\mathbf{A}$ una matrice complessa $m \times n$ e sia $\mathbf{b} \in \mathbb{C}^m$. Ricordiamo che il sistema $\mathbf{Ax} = \mathbf{b}$ ha soluzione se e solo se $\mathbf{b} \in \mathrm{C}(\mathbf{A})$, lo spazio delle colonne di $\mathbf{A}$. Dal Teorema 3.10 (2), applicato a $\mathbf{v} = \mathbf{b}$ e $U = \mathrm{C}(\mathbf{A})$, sappiamo che esiste un unico vettore in $\mathrm{C}(\mathbf{A})$ che ha distanza euclidea minima da $\mathbf{b}$; tale vettore coincide con la proiezione ortogonale $\mathbf{b}_0$ del vettore $\mathbf{b}$ su $\mathrm{C}(\mathbf{A})$, e $\mathbf{b} = \mathbf{b}_0$ se e solo se $\mathbf{b} \in \mathrm{C}(\mathbf{A})$. Il teorema seguente caratterizza le soluzioni del sistema compatibile $\mathbf{Ax} = \mathbf{b}_0$.

Teorema 7.1. *Dato il sistema lineare* $\mathbf{Ax} = \mathbf{b}$, *con* $\mathbf{A}$ *matrice* $m \times n$, *e detto* $\mathbf{b}_0$ *il vettore proiezione di* $\mathbf{b}$ *su* $\mathrm{C}(\mathbf{A})$, *le seguenti condizioni per un vettore* $\mathbf{v} \in \mathbb{C}^n$ *sono equivalenti:*

(a) $\mathbf{Av} = \mathbf{b}_0$;

(b) $\|\mathbf{Av} - \mathbf{b}\|_2 < \|\mathbf{Au} - \mathbf{b}\|_2$ *per ogni vettore* $\mathbf{u} \in \mathbb{C}^n$ *tale che* $\mathbf{Av} \neq \mathbf{Au}$;

(c) $\mathbf{A}^H\mathbf{Av} = \mathbf{A}^H\mathbf{b}$;

(d) $\mathbf{Rv} = \mathbf{Q}^H\mathbf{b}$, *dove* $\mathbf{A} = \mathbf{QR}$ *è una decomposizione* QR *normalizzata.*

Dimostrazione. (a) $\Longleftrightarrow$ (b) Discende dalla caratterizzazione della proiezione $\mathbf{b}_0$ di $\mathbf{b}$ su $C(\mathbf{A})$ (si veda il Teorema 3.10 (2)) e dal fatto che un vettore appartiene a $C(\mathbf{A})$ se e solo se è del tipo $\mathbf{Au}$ per un opportuno vettore $\mathbf{u} \in \mathbb{C}^n$.

(c) $\Longleftrightarrow$ (a) Ricordando che $C(\mathbf{A})^\perp = N(\mathbf{A}^H)$ (si veda la Proposizione 3.2), si ha

$$\mathbf{A}^H\mathbf{Av} = \mathbf{A}^H\mathbf{b} \iff \mathbf{Av} - \mathbf{b} \in N(\mathbf{A}^H) = C(\mathbf{A})^\perp.$$

Inoltre, poiché $\mathbf{b} = \mathbf{Av} + (\mathbf{b} - \mathbf{Av})$ e $\mathbf{Av} \in C(\mathbf{A})$, dalla Proposizione 3.6 segue che

$$\mathbf{Av} - \mathbf{b} \in C(\mathbf{A})^\perp \iff \mathbf{Av} = \mathbf{b}_0.$$

In conclusione si ottiene che $\mathbf{A}^H\mathbf{Av} = \mathbf{A}^H\mathbf{b}$ se e solo se $\mathbf{Av} = \mathbf{b}_0$.

(c) $\Longleftrightarrow$ (d) Le uguaglianze $\mathbf{A} = \mathbf{QR}$ e $\mathbf{A}^H\mathbf{Av} = \mathbf{A}^H\mathbf{b}$ sono equivalenti all'uguaglianza $\mathbf{R}^H\mathbf{Q}^H\mathbf{QRv} = \mathbf{R}^H\mathbf{Q}^H\mathbf{b}$. Ma, essendo $\mathbf{R}^H$ dotata di inversa sinistra e $\mathbf{Q}^H\mathbf{Q} = \mathbf{I}$, tale uguaglianza equivale a $\mathbf{Rv} = \mathbf{Q}^H\mathbf{b}$. $\square$

Il sistema $\mathbf{A}^H\mathbf{Ax} = \mathbf{A}^H\mathbf{b}$ si chiama il *sistema delle equazioni normali* associato al sistema $\mathbf{Ax} = \mathbf{b}$. Il Teorema 7.1 dice che il sistema delle equazioni normali è risolubile e ha esattamente le soluzioni del sistema $\mathbf{Ax} = \mathbf{b}_0$.

Possiamo ora dare la risposta alla domanda posta all'inizio di questo Paragrafo.

Teorema 7.2. *Dato il sistema lineare* $\mathbf{Ax} = \mathbf{b}$ *e detto* $\mathbf{b}_0$ *il vettore proiezione di* $\mathbf{b}$ *su* $C(\mathbf{A})$*, il vettore* $\mathbf{A}^+\mathbf{b}$ *è l'unica soluzione del sistema* $\mathbf{Ax} = \mathbf{b}_0$ *di norma euclidea minima.*

Dimostrazione. Proviamo innanzitutto che il vettore $\mathbf{A}^+\mathbf{b}$ è soluzione del sistema $\mathbf{Ax} = \mathbf{b}_0$.

Per il Teorema 7.1 ciò accade se e solo se $\mathbf{A}^H\mathbf{AA}^+\mathbf{b} = \mathbf{A}^H\mathbf{b}$. Ma $\mathbf{A}^H\mathbf{AA}^+ = \mathbf{A}^H$, per la proprietà ($\mathrm{pi}_5$) del Paragrafo 4 del Capitolo 1, da cui l'asserto.

Proviamo ora che, se $\mathbf{u} \in \mathbb{C}^n$ è un'altra soluzione di $\mathbf{Ax} = \mathbf{b}_0$ diversa da $\mathbf{A}^+\mathbf{b}$, allora $\|\mathbf{u}\|_2 > \|\mathbf{A}^+\mathbf{b}\|_2$.

Osserviamo preliminarmente che $\mathbf{A}^+\mathbf{b} \in N(\mathbf{A})^\perp$. Infatti, se $\mathbf{w} \in N(\mathbf{A})$, risulta

$$\begin{aligned}\mathbf{w}^H\mathbf{A}^+\mathbf{b} &= \mathbf{w}^H\mathbf{A}^+\mathbf{AA}^+\mathbf{b} = \mathbf{w}^H(\mathbf{A}^+\mathbf{A})^H\mathbf{A}^+\mathbf{b} = \mathbf{w}^H A^H(\mathbf{A}^+)^H\mathbf{A}^+\mathbf{b}\\ &= (\mathbf{Aw})^H(\mathbf{A}^+)^H\mathbf{A}^+\mathbf{b} = 0.\end{aligned}$$

Osserviamo poi che, essendo $\mathbf{A}^+\mathbf{b}$ una soluzione del sistema $\mathbf{Ax} = \mathbf{b}_0$, ogni altra soluzione $\mathbf{u}$ è del tipo $\mathbf{u} = \mathbf{A}^+\mathbf{b} + \mathbf{y}$, dove $\mathbf{y} \in N(\mathbf{A})$. Ora, se $\mathbf{u} \neq \mathbf{A}^+\mathbf{b}$, risulta $\mathbf{y} \neq \mathbf{0}$. Poiché $\mathbf{y} \in N(\mathbf{A})$ e $\mathbf{A}^+\mathbf{b} \in N(\mathbf{A})^\perp$, si ha

$$\|\mathbf{u}\|_2^2 = \|\mathbf{A}^+\mathbf{b}\|_2^2 + \|\mathbf{y}\|_2^2 > \|\mathbf{A}^+\mathbf{b}\|_2^2,$$

da cui l'asserto. $\square$

In virtù di quanto provato nel Teorema 7.2 e poiché la norma euclidea di un vettore si ottiene dalla somma dei quadrati dei moduli delle sue coordinate (estraendone la radice quadrata), il vettore $\mathbf{A}^+\mathbf{b}$ si chiama *soluzione ai minimi quadrati* del sistema $\mathbf{Ax} = \mathbf{b}$.

Esempio 7.3. Si consideri la matrice dell'Esempio 4.21 del Capitolo 1

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

che ha come pseudo-inversa la matrice $\mathbf{A}^+ = \frac{1}{70}\mathbf{A}^T$. Il sistema $\mathbf{Ax} = [1\ 1]^T$ non ha soluzioni, perché

$$\begin{bmatrix} 1 \\ 1 \end{bmatrix} \notin \mathrm{C}(\mathbf{A}) = \left\langle \begin{bmatrix} 2 \\ 1 \end{bmatrix} \right\rangle.$$

Il vettore proiezione di $[1\ 1]^T$ su $\mathrm{C}(\mathbf{A})$ è il vettore

$$\mathbf{b}_0 = \frac{\begin{bmatrix} 1 & 1 \end{bmatrix}\begin{bmatrix} 2 \\ 1 \end{bmatrix}}{\begin{bmatrix} 2 & 1 \end{bmatrix}\begin{bmatrix} 2 \\ 1 \end{bmatrix}} \begin{bmatrix} 2 \\ 1 \end{bmatrix} = \begin{bmatrix} 6/5 \\ 3/5 \end{bmatrix}.$$

La soluzione ai minimi quadrati del sistema $\mathbf{Ax} = [1\ 1]^T$ è il vettore

$$\mathbf{A}^+ \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{70} A^T \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{3}{70} \begin{bmatrix} 2 \\ 0 \\ 1 \\ 3 \end{bmatrix},$$

la cui norma euclidea

$$\left\| \mathbf{A}^+ \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\|_2 = \frac{3}{70}\sqrt{14}$$

è minima tra le norme euclidee delle soluzioni del sistema $\mathbf{Ax} = \mathbf{b}_0$. □

Data la matrice $m \times n$ $\mathbf{A}$, qualora la sua pseudo-inversa $\mathbf{A}^+$ sia nota, è facile calcolare la proiezione di un vettore di $\mathbb{C}^m$ sulle spazio delle colonne $\mathrm{C}(\mathbf{A})$ e quella di un vettore di $\mathbb{C}^n$ sulle spazio delle righe $\mathrm{C}(\mathbf{A}^H)$ di $\mathbf{A}$.

Corollario 7.4. *Data la matrice $m \times n$ $\mathbf{A}$, si ha che*

(a) *la proiezione di $\mathbf{b} \in \mathbb{C}^m$ su $\mathrm{C}(\mathbf{A})$ è il vettore $\mathbf{AA}^+\mathbf{b}$;*

(b) *la proiezione di $\mathbf{v} \in \mathbb{C}^n$ su $\mathrm{C}(\mathbf{A}^H)$ è il vettore $\mathbf{A}^+\mathbf{Av}$.*

Dimostrazione. (a) Se $\mathbf{b}_0$ è la proiezione di $\mathbf{b}$ su $\mathrm{C}(\mathbf{A})$, dal Teorema 7.2 segue che $\mathbf{b}_0 = \mathbf{AA}^+\mathbf{b}$.

Per (a), la proiezione di $\mathbf{v}$ su $\mathrm{C}(\mathbf{A}^H)$ è $\mathbf{A}^H(\mathbf{A}^H)^+\mathbf{v}$. Ma risulta

$$\mathbf{A}^H(\mathbf{A}^H)^+\mathbf{v} = \mathbf{A}^H(\mathbf{A}^+)^H\mathbf{v} = (\mathbf{A}^+\mathbf{A})^H\mathbf{v} = \mathbf{A}^+\mathbf{Av}$$ □

La seconda parte di questo paragrafo sarà dedicata a illustrare il *metodo dei minimi quadrati*, che è il modo più usato per approssimare dati sperimentali. Applicheremo questo metodo a un fenomeno descritto da una equazione polinomiale del tipo:

$$Y = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n, \tag{1}$$

dove sono da determinarsi i coefficienti a_i dell'equazione. Effettuando N misurazioni del fenomeno per N valori distinti $x_1, x_2, \dots, x_N$ della variabile indipendente X si ottengono N valori $y_1, y_2, \dots, y_N$ della variabile dipendente Y. Se il numero N di misurazioni è minore o uguale a n, esistono infiniti polinomi $a_0 + a_1X + a_2X^2 + \dots + a_nX^n$ che assumono negli N punti $x_1, x_2, \dots, x_N$ rispettivamente i valori $y_1, y_2, \dots, y_N$ (si pensi alle infinite rette per un punto, o alle infinite parabole per due punti). Se $N = n + 1$, esiste esattamente un polinomio soddisfacente a tali requisiti (si pensi alla retta per due punti, o alla parabola per tre punti; si veda l'Esercizio 3.53).

Nel caso che si presenta usualmente in cui si effettuano molte più misurazioni rispetto al grado dell'equazione polinomiale, non esiste in generale il polinomio cercato.

Ci si chiede: qual è il polinomio che meglio approssima i dati ottenuti?

Esempio 7.5. Si vuole determinare la retta di equazione $Y = a + bX$ che meglio approssima i quattro punti di $\mathbb{R}^2$:

$$P_1 = (1,1), \qquad P_2 = (3,2), \qquad P_3 = (0,1), \qquad P_4 = (2,3).$$

Dalla discussione che segue si vedrà che la retta cercata ha equazione $Y = 1 + \frac{1}{2}X$, che è la retta che minimizza le somme dei quadrati delle differenze tra le ordinate dei punti P_i e le ordinate dei punti dei punti Q_i, dove per ogni $i = 1,2,3,4$, Q_i è il punto sulla retta che ha ascissa uguale all'ascissa di P_i.

Si vedrà che i coefficienti $(1, \frac{1}{2})$ del polinomio che rappresenta la retta corrispondono alle coordinate del vettore $\mathbf{A}^+\mathbf{y}$ soluzione ai minimi quadrati del sistema $\mathbf{Ax} = \mathbf{y}$, dove $\mathbf{y} = [1\ 2\ 1\ 3]^T$ è il vettore delle ordinate dei punti P_i e $\mathbf{A}$ è la matrice che ha 1 sulla prima colonna e le ascisse dei punti P_i sulla seconda colonna:

$$\mathbf{A} = \begin{bmatrix} 1 & 1 \\ 1 & 3 \\ 1 & 0 \\ 1 & 2 \end{bmatrix}.$$

Lasciamo verificare al lettore che in questo caso

$$\mathbf{A}^+ = \frac{1}{10}\begin{bmatrix} 4 & -2 & 7 & 1 \\ -1 & 3 & -3 & 1 \end{bmatrix},$$

e quindi che

$$\mathbf{A}^+\mathbf{y} = \begin{bmatrix} 1 \\ 1/2 \end{bmatrix}. \qquad \square$$

Riprendiamo la domanda formulata prima dell'Esempio 7.5. Una risposta convincente è che il polinomio $a_0 + a_1X + a_2X^2 + \dots + a_nX^n$ che meglio approssima i dati ottenuti è quello che minimizza la quantità

$$\sum_{i=1,\dots,N} \left(y_i - (a_0 + a_1x_i + a_2x_i^2 + \dots + a_nx_i^n)\right)^2, \tag{2}$$

cioè la somma dei quadrati degli errori commessi nelle misurazioni rispetto ai valori ipotizzati come reali. Posto

$$\mathbf{y} = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_N \end{bmatrix} \qquad \text{(vettore dei dati misurati)}$$

$$\mathbf{x} = \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_n \end{bmatrix} \qquad \text{(vettore incognito)}$$

$$\mathbf{A} = \begin{bmatrix} 1 & x_1 & x_1^2 & \dots & x_1^n \\ 1 & x_2 & x_2^2 & \dots & x_2^n \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & x_N & x_N^2 & \dots & x_N^n \end{bmatrix} \qquad \text{(matrice } N \times (n+1))$$

è immediato verificare che la quantità da minimizzare in (2) corrisponde a $\|\mathbf{y} - \mathbf{Ax}\|_2^2$. Per il Teorema 7.1 i vettori $\mathbf{v}$ per cui la norma $\|\mathbf{y} - \mathbf{Av}\|_2$ è minima sono tutte e sole le soluzioni del sistema delle equazioni normali $\mathbf{A}^H\mathbf{Ax} = \mathbf{A}^H\mathbf{y}$.

Ma nel caso in esame in cui $N \geq n+1$ accade che:

la matrice $\mathbf{A}^H\mathbf{A}$ ha rango $n+1$, per cui $(\mathbf{A}^H\mathbf{A})^{-1}\mathbf{A}^H = \mathbf{A}^+$ e $\mathbf{A}^+\mathbf{y}$ è l'unica soluzione del sistema $\mathbf{Ax} = \mathbf{y}_0$ (dove $\mathbf{y}_0$ è la proiezione di $\mathbf{y}$ su $C(\mathbf{A})$) e quindi l'unico vettore che minimizza $\|\mathbf{y} - \mathbf{Ax}\|_2$.

Per provare quanto asserito è sufficiente dimostrare che la matrice quadrata di ordine $n+1$

$$\mathbf{V} = \begin{bmatrix} 1 & x_1 & x_1^2 & \dots & x_1^n \\ 1 & x_2 & x_2^2 & \dots & x_2^n \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & x_{n+1} & x_{n+1}^2 & \dots & x_{n+1}^n \end{bmatrix}$$

è invertibile, perché in tal caso le colonne della matrice $\mathbf{A}$ risultano linearmente indipendenti, il che comporta che $\mathrm{rk}\mathbf{A} = n+1 = \mathrm{rk}\mathbf{A}^H\mathbf{A}$. La matrice $\mathbf{V}$ è la matrice di Vandermonde ottenuta dagli $n+1$ valori *distinti* $x_1, x_2, \dots, x_{n+1}$. Vedremo nel Capitolo 4 che $\mathbf{V}$ è effettivamente invertibile.

Esercizi

Paragrafo 1

3.1. Si verifichi che $\|\cdot\|_1$ definita nell'Esempio 1.2 è una norma.

3.2. Si verifichi che per ogni $\mathbf{v} \in \mathbb{C}^n$ si ha $\|\mathbf{v}\|_2 \leq \sqrt{n}\|\mathbf{v}\|_\infty$.

3.3. Si verifichi che per ogni $\mathbf{v} \in \mathbb{C}^n$ si ha $\mathrm{Tr}(\mathbf{v}\mathbf{v}^H) = \|\mathbf{v}\|_2^2$.

3.4. Siano d un numero reale strettamente positivo, V uno spazio vettoriale e $\|\cdot\|$ una norma definita su V. Si chiama *intorno* di $\mathbf{0} \in V$ di raggio d rispetto alla norma $\|\cdot\|$ l'insieme

$$\mathscr{I}_{\|\cdot\|,d} = \{\mathbf{v} \in V \mid \|\mathbf{v}\| \leq d\}.$$

Se $V = \mathbb{R}^2$, si disegnino su di un piano su cui si sia fissato un sistema di riferimento ortogonale e monometrico Oxy gli insiemi dei punti che rappresentano gli elementi di $\mathscr{I}_{\|\cdot\|_2,1}$, $\mathscr{I}_{\|\cdot\|_1,1}$ e $\mathscr{I}_{\|\cdot\|_\infty,1}$ rispettivamente.

3.5. Sia $\|\cdot\|$ una norma definita su di uno spazio vettoriale reale V e sia α un numero reale strettamente positivo. Si verifichi che la funzione $\|\cdot\|_\alpha$ definita da $\|\mathbf{v}\|_\alpha = \alpha\|\mathbf{v}\|$ è una norma su V.

3.6. Si provi che se f e g sono due norme definite sullo spazio vettoriale V anche $f+g$ lo è.

3.7. Si provi che la funzione $\|\cdot\|_{\mathbf{A}}$ definita nell'Esempio 1.6 è una norma su $\mathbb{C}^n$.

3.8. Si verifichi che la funzione $\varphi\colon \mathbb{R}^2 \to \mathbb{R}_{\geq 0}$ definita da

$$\varphi\left(\begin{bmatrix} a_0 \\ a_1 \end{bmatrix}\right) = |a_0 + a_1| + |a_0 - a_1|$$

è una norma.

3.9. Si provi la disuguaglianza di Schwarz per le funzioni continue e, tramite questa, si provi la disuguaglianza triangolare per la norma definita nell'Esempio 1.7.

3.10. Siano p e q numeri reali positivi tali che $p^{-1} + q^{-1} = 1$. Si provi che, dati due numeri reali positivi x e y, risulta $xy \leq p^{-1}x^p + q^{-1}y^q$.

3.11. Con quanto visto nell'Esercizio precedente, si provi la *disuguaglianza di Hölder*: dati $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ e $p, q > 0$ con $p^{-1} + q^{-1} = 1$,

$$|\mathbf{x}^T\mathbf{y}| \leq \|\mathbf{x}\|_p \cdot \|\mathbf{y}\|_q.$$

(Suggerimento: si dimostri prima il caso in cui $\|\mathbf{x}\|_p = 1 = \|\mathbf{y}\|_q$.)

3.12. Impiegando la disuguaglianza di Hölder, si provi la *disuguaglianza di Minkowski*: dati $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ e $p \geq 1$,

$$\|\mathbf{x} + \mathbf{y}\|_p \leq \|\mathbf{x}\|_p + \|\mathbf{y}\|_p.$$

Paragrafo 2

3.13. Si verifichi che la funzione $(\cdot \mid \cdot)_{\mathbf{A}}$ definita nell'Esempio 2.4 è un prodotto interno su $\mathbb{C}^n$.

3.14. Si provi che se V è uno spazio vettoriale euclideo allora la funzione definita da $\|\mathbf{v}\| = \sqrt{(\mathbf{v} \mid \mathbf{v})}$ per ogni $\mathbf{v} \in V$ è una norma su V (la norma indotta dal prodotto interno $(\cdot \mid \cdot)$ definito su V).

3.15. Si verifichi che la funzione $(\cdot \mid \cdot)\colon \mathbb{C}^2 \times \mathbb{C}^2 \to \mathbb{C}$ definita da

$$\left(\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \middle| \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}\right) = \overline{x_1}y_1 + 2\overline{x_2}y_2$$

è un prodotto interno.

3.16. Siano V uno spazio vettoriale euclideo reale e $\|\cdot\|$ la norma indotta dal prodotto interno $(\cdot \mid \cdot)$ definito su V. Si provi che vale l'identità di polarizzazione

$$(\mathbf{v} \mid \mathbf{w}) = \frac{\|\mathbf{v}+\mathbf{w}\|^2 - \|\mathbf{v}-\mathbf{w}\|^2}{4} \quad \text{per ogni } \mathbf{v}, \mathbf{w} \in V.$$

3.17. Si provi che la funzione $f\colon \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}$ definita da

$$f(\mathbf{v}, \mathbf{w}) = \frac{\|\mathbf{v}+\mathbf{w}\|_1^2 - \|\mathbf{v}-\mathbf{w}\|_1^2}{4} \quad \text{per ogni } \mathbf{v}, \mathbf{w} \in \mathbb{R}^2$$

non è un prodotto interno su $\mathbb{R}^2$.

3.18. Siano V uno spazio vettoriale euclideo reale e $\|\cdot\|$ la norma indotta dal prodotto interno $(\cdot \mid \cdot)$ definito su V. Si provi che per ogni $\mathbf{v}, \mathbf{w} \in V$ si ha:

$$(\mathbf{v} \mid \mathbf{w}) = \frac{1}{2}(\|\mathbf{v}+\mathbf{w}\|^2 - \|\mathbf{v}\|^2 - \|\mathbf{w}\|^2)$$

3.19. Si provi che la funzione $f\colon \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}$ definita da

$$f(\mathbf{v}, \mathbf{w}) = \frac{1}{2}(\|\mathbf{v}+\mathbf{w}\|_\infty^2 - \|\mathbf{v}\|_\infty^2 - \|\mathbf{w}\|_\infty^2) \quad \text{per ogni } \mathbf{v}, \mathbf{w} \in \mathbb{R}^2$$

non è un prodotto interno su $\mathbb{R}^2$.

3.20. Dati nel piano cartesiano tre punti distinti O, A e B, per un teorema di trigonometria (Teorema di Carnot) si ha che

$$|AB|^2 = |OA|^2 + |OB|^2 - 2|OA|\,|OB|\cos\alpha$$

dove α è l'angolo compreso tra i segmenti OA e OB. Se $\mathbf{v}, \mathbf{w} \in \mathbb{R}^2 \setminus \{\mathbf{0}\}$ e $\alpha = \widehat{\mathbf{v}\mathbf{w}}$, si deduca dal teorema di Carnot che

$$\cos\alpha = \frac{\mathbf{v}^T\mathbf{w}}{\|\mathbf{v}\|_2\|\mathbf{w}\|_2}.$$

3.21. Si verifichi che nello spazio vettoriale $\mathrm{M}_n(\mathbb{C})$ resta definito un prodotto interno ponendo $(\mathbf{A} \mid \mathbf{B}) = \mathrm{Tr}(\mathbf{A}^H\mathbf{B})$.

Paragrafo 3

3.22. Siano V uno spazio vettoriale euclideo, $\|\cdot\|$ la norma indotta dal prodotto interno $(\cdot \mid \cdot)$ definito su V e $\mathbf{u}, \mathbf{v} \in V$. Si provi che se $\mathbf{u} \perp \mathbf{v}$ allora $\|\mathbf{u}+\mathbf{v}\|^2 = \|\mathbf{u}\|^2 + \|\mathbf{v}\|^2$. Viceversa, se $\|\mathbf{u}+\mathbf{v}\|^2 = \|\mathbf{u}\|^2 + \|\mathbf{v}\|^2$ allora $(\mathbf{u} \mid \mathbf{v}) + \overline{(\mathbf{u} \mid \mathbf{v})} = 0$. In particolare, se V è reale allora $\mathbf{u} \perp \mathbf{v}$ se e solo se $\|\mathbf{u}+\mathbf{v}\|^2 = \|\mathbf{u}\|^2 + \|\mathbf{v}\|^2$.

3.23. Si dimostri la Proposizione 3.3.

3.24. Si provi per induzione su $\dim V$ che per ogni sottospazio U di V da $U^{\perp\perp} = U$ si deduce $V = U \oplus U^{\perp}$ (ossia la Proposizione 3.6 e il Corollario 3.7 sono equivalenti).

3.25. Si provi che per ogni sottospazio U di V si ha $U^{\perp} = ((U^{\perp})^{\perp})^{\perp}$.

3.26. Siano U_1 e U_2 due sottospazi di V. Si usi la Proposizione 3.3 per provare che

$$(U_1 \cap U_2)^{\perp} = U_1^{\perp} + U_2^{\perp}.$$

3.27. Siano U e W sottospazi di V con U contenuto in W. Si provi che $W = U \oplus (U^{\perp} \cap W)$.

3.28. Siano U e W sottospazi di V tali che $(\mathbf{u} \mid \mathbf{w}) = 0$ per ogni $\mathbf{u} \in U$ e ogni $\mathbf{w} \in W$ (si dice che il sottospazio U di V è ortogonale al sottospazio W di V, e si scrive $U \perp W$). Si provi che per ogni $\mathbf{v} \in V$ si ha

$$P_{U+W}(\mathbf{v}) = P_U(\mathbf{v}) + P_W(\mathbf{v}).$$

3.29. Siano U e W sottospazi di V. Si provi che per ogni $\mathbf{v} \in V$ si ha

$$P_{U\cap W}(\mathbf{v}) = P_W(P_U(\mathbf{v})) = P_U(P_W(\mathbf{v})).$$

3.30. Si provi che la norma $\|\cdot\|_1$ su $\mathbb{R}^2$ non è indotta da alcun prodotto interno, mostrando che non esiste un vettore del sottospazio di $\mathbb{R}^2$ generato dal vettore $\mathbf{v} = [1\ 1]^T$ che ha distanza minima dal vettore $\mathbf{u} = [0\ 1]^T$ (si veda il Teorema 3.10).

3.31. Siano U e V sottospazi di $\mathbb{C}^n$. Si provi che

$$\mathbb{C}^n = (U \cap (U^{\perp} + V^{\perp})) \oplus (V \oplus (U^{\perp} \cap V^{\perp})).$$

Paragrafo 4

3.32. Si provi che l'insieme delle colonne di una matrice complessa $m \times n$ $\mathbf{A}$ è un sottoinsieme ortogonale di $\mathbb{C}^m$ (rispetto al prodotto interno standard) se e solo se la matrice $\mathbf{A}^H\mathbf{A}$ è diagonale.

3.33. Sia $\mathbf{Q}$ una matrice $m \times k$ a colonne ortonormali. Si verifichi che $\mathbf{Q}^+ = \mathbf{Q}^H$.

3.34. Si provi l'Osservazione 4.7.

3.35. Una matrice reale $\mathbf{A}$ si dice ortogonale se $\mathbf{A}^{-1} = \mathbf{A}^T$. Si provi che una matrice reale $\mathbf{A}$ è ortogonale se e solo se l'insieme delle sue colonne è una base ortonormale di $C(\mathbf{A})$, o, equivalentemente, se e solo se l'insieme delle sue righe è una base ortonormale di $C(\mathbf{A}^H)$.

3.36. Siano V uno spazio vettoriale e $\mathscr{B} = \{\mathbf{v}_1; \mathbf{v}_2; \dots; \mathbf{v}_n\}$ una base di V. Si definisca un prodotto interno $(\cdot \mid \cdot)_{\mathscr{B}}$ di V rispetto al quale la base $\mathscr{B}$ risulti ortonormale.

Paragrafo 5

Nei seguenti tre esercizi si applica quanto sarà provato nell'Esempio 1.10 del Capitolo 6, cioè che, dati due vettori distinti $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$, di uguale norma euclidea, esiste una matrice reale ortogonale $\mathbf{H}$ tale che $\mathbf{Hu} = \mathbf{v}$.

3.37. Sia $\mathbf{A} \in \mathrm{M}_{m\times n}(\mathbb{R})$, con $m \geq n$, decomposta a blocchi

$$\mathbf{A} = \begin{bmatrix} \mathbf{R} & \mathbf{B} \\ \mathbb{O} & \mathbf{C} \end{bmatrix}$$

con $\mathbf{R}$ triangolare superiore $i \times i$ ($i \leq n$) con coefficienti diagonali ≥ 0. Si provi che esiste una matrice diagonale $\mathbf{Q} = \mathbf{Diag}(\mathbf{I}_i, \mathbf{H})$ tale che

$$\mathbf{QA} = \begin{bmatrix} \mathbf{R} & \mathbf{B} \\ \mathbb{O} & \mathbf{C}' \end{bmatrix}$$

con $\mathbf{C}'$ avente come prima colonna $r\mathbf{e}_1$, dove $r \geq 0$ ed $\mathbf{e}_1$ è il primo vettore coordinato di $\mathbb{R}^n$.

3.38. Sia $\mathbf{A} \in \mathrm{M}_{m\times n}(\mathbb{R})$, con $m \geq n$. Iterando l'applicazione dell'Esercizio 3.37, si ricavino n matrici ortogonali $\mathbf{Q}_0, \mathbf{Q}_1, \dots, \mathbf{Q}_n$ tali che, posto $\mathbf{A}_0 = \mathbf{A}$ e, per $0 \leq i < n$, risulti $\mathbf{Q}_i\mathbf{A}_i = \mathbf{A}_{i+1}$, dove

$$\mathbf{A}_i = \begin{bmatrix} \mathbf{R}_i & \mathbf{B}_i \\ \mathbb{O} & \mathbf{C}_i \end{bmatrix}$$

e $\mathbf{R}_i \in \mathrm{M}_i(\mathbb{R})$ è triangolare superiore con coefficienti diagonali ≥ 0.

3.39. Sia $\mathbf{A} \in \mathrm{M}_{m\times n}(\mathbb{R})$, con $m \geq n$. Mediante l'Esercizio 3.38 trovare una dimostrazione alternativa del fatto che si ha una decomposizione $\mathbf{A} = \mathbf{QR}$ con $\mathbf{Q}$ matrice reale $m \times n$ a colonne ortonormali e $\mathbf{R}$ triangolare superiore $n \times n$ con coefficienti diagonali ≥ 0.

3.40. Si provi che, se nell'Esercizio 3.39 risulta $\mathrm{rk}\mathbf{A} = n$, allora la decomposizione ottenuta è una decomposizione QR normalizzata, cioè $\mathrm{C}(\mathbf{A}) = \mathrm{C}(\mathbf{Q})$.

Paragrafo 6

3.41. Si verifichi che per ogni matrice $\mathbf{A}$ le matrici $\mathbf{A}^+\mathbf{A}$ e $\mathbf{AA}^+$ sono matrici di proiezione.

3.42. Sia $\mathbf{P}$ una matrice di proiezione. Si provi che $\mathrm{rk}\mathbf{P} = \mathrm{Tr}(\mathbf{P})$. (Suggerimento: $\mathbf{P} = \sum_{1\leq i\leq k} \mathbf{u}_i^H\mathbf{u}_i$, con $\|\mathbf{u}_i\|_2 = 1$ per $1 \leq i \leq k$; in realtà tale risultato vale per ogni matrice idempotente.)

3.43. Sia $\mathbf{P} = \mathbf{QR}$ una decomposizione QR normalizzata della matrice di proiezione $\mathbf{P}$. Si provi che $\mathbf{R} = \mathbf{Q}^H$.

3.44. Provare che, se $\mathbf{A} \in \mathrm{M}_n(\mathbb{R})$ è invertibile, allora la decomposizione QR normalizzata di $\mathbf{A} = \mathbf{QR}$ è unica (con $\mathbf{Q}$ unitaria e $\mathbf{R}$ triangolare superiore con coefficienti diagonali reali positivi).

3.45. Un'applicazione lineare $f\colon V \to V$ di uno spazio vettoriale V in sé stesso è una *proiezione* (non necessariamente ortogonale) se $f = f \circ f$. Provare che, in tal caso, $V = \mathrm{Im}(f) \oplus \mathrm{N}(f)$.

3.46. Nelle ipotesi dell'Esercizio precedente, sia $g\colon V \to V$ un'altra applicazione lineare. Provare che:

- $f \circ g = g \circ f$ se e solo se $g(\mathrm{Im}(f)) \subseteq \mathrm{Im}(f)$ e $g(\mathrm{N}(f)) \subseteq \mathrm{N}(f)$;
- $f \circ g = f \circ g \circ f$ se e solo se $g(\mathrm{N}(f)) \subseteq \mathrm{N}(f)$;
- $g \circ f = f \circ g \circ f$ se e solo se $g(\mathrm{Im}(f)) \subseteq \mathrm{Im}(f)$.

3.47. Una matrice $\mathbf{P} \in \mathrm{M}_n(\mathbb{C})$ è una matrice di proiezione (cioè $\mathbf{P} = \mathbf{P}^2 = \mathbf{P}^H$) se e solo se $\mathbf{P} = \mathbf{P}^H\mathbf{P}$ o anche se e solo se $\mathbf{P} = \mathbf{P}^2 = \mathbf{P}^+$.

Paragrafo 7

3.48. Sia $\mathbf{A} = \mathbf{QR}$ una decomposizione QR normalizzata della matrice $\mathbf{A}$. Si provi che le soluzioni delle equazioni normali del sistema $\mathbf{Ax} = \mathbf{b}$ sono tutte e sole le soluzioni del sistema $\mathbf{Rx} = \mathbf{Q}^H\mathbf{b}$.

3.49. Sia $\mathbf{A} = \mathbf{QR}$ una decomposizione QR normalizzata della matrice $\mathbf{A}$. Si provi che $\mathbf{AA}^+ = \mathbf{QQ}^H$ e $\mathbf{A}^+\mathbf{A} = \mathbf{R}^+\mathbf{R}$.

3.50. Dato il sistema $\mathbf{Ax} = \mathbf{b}$, le soluzioni delle equazioni normali a esso associate coincidono con le soluzioni del sistema $\mathbf{A}^+\mathbf{A} = \mathbf{A}^+\mathbf{b}$.

3.51. Data $\mathbf{A} \in \mathrm{M}_{m\times n}(\mathbb{C})$, si chiama 1-*inversa* di $\mathbf{A}$ ogni matrice $\mathbf{B}$ tale che $\mathbf{ABA} = \mathbf{A}$. Provare che ciò equivale al fatto che, per ogni $\mathbf{v} \in \mathrm{C}(\mathbf{A})$, $\mathbf{Bv}$ sia soluzione del sistema $\mathbf{Ax} = \mathbf{v}$.

3.52. Provare che esiste un'unica matrice 1-inversa di una matrice $\mathbf{A}$ se e solo se $\mathbf{A}$ è quadrata e invertibile.

3.53. Utilizzando la matrice di Vandermonde ottenuta dai numeri $x_1, x_2, \dots, x_{n+1}$, si provi che esiste uno e un solo polinomio di grado n che interpola $n+1$ punti del piano reale con distinte ascisse $x_1, x_2, \dots, x_{n+1}$. (Si veda l'Esercizio 4.16 per la definizione di matrice di Vandermonde.)

Capitolo 4

Il determinante

Le prime apparizioni della nozione di determinante si hanno nella seconda metà del 1600, prima in un trattato del 1674 del matematico giapponese Seki Kowa, noto anche con il nome di Takakazu, poi in una lettera di Leibniz a l'Hôpital del 1693. La prima pubblicazione in Europa sui determinanti è dovuta a Cramer nel 1750. Uno sviluppo sistematico della teoria del determinante si ha però solo nella prima metà del 1800 con Cauchy e Jacobi.

Delle diverse possibili definizioni di determinante noi preferiremo quella legata al suo comportamento rispetto alle matrici elementari da noi introdotte nel Capitolo 1. Proveremo l'esistenza e l'unicità di funzioni determinanti che assumono un valore preassegnato nella matrice identità e studieremo le loro principali proprietà. Daremo poi due diversi metodi, i più usati, per il calcolo dei determinanti: il primo fa ricorso all'eliminazione di Gauss, il secondo è il cosiddetto "sviluppo di Laplace" del determinante. Infine vedremo il determinante nel classico modo legato alle permutazione e alla loro segnatura.

1. Funzioni determinanti

Ogni matrice $\mathbf{A} \in \mathrm{M}_2(\mathbb{R})$ può essere considerata come una trasformazione f del piano in sé: identificando un punto come un vettore colonna $\mathbf{P} = [a\ b]^T \in \mathbb{R}^2$, a esso possiamo associare il punto

$$f(\mathbf{P}) = \mathbf{A}\begin{bmatrix} a \\ b \end{bmatrix}.$$

La composizione di due trasformazioni di questo tipo corrisponde come sappiamo al prodotto delle matrici associate.

Vediamo come casi particolari le trasformazioni indotte dalle matrici elementari introdotte nel Capitolo 1: se $\mathbf{A} = \mathbf{E}_{12}$, questa trasformazione è la riflessione attorno alla bisettrice del primo e terzo quadrante. In una trasformazione del genere, i percorsi cambiano senso di percorrenza: se immaginiamo di percorrere un triangolo in senso antiorario, il triangolo trasformato verrà percorso in senso orario.

Se invece $\mathbf{A} = \mathbf{E}_1(c)$, avremo $f([a\ b]^T) = [ca\ b]^T$. Se proviamo a confrontare l'area di un triangolo con quella del triangolo trasformato, troviamo che la seconda è c volte la prima. Per esempio, il triangolo di vertici $[0\ 0]^T$, $[1\ 0]^T$, $[1\ 1]^T$ ha area $1/2$. Il triangolo trasformato ha vertici $[0\ 0]^T$, $[c\ 0]^T$, $[c\ 1]^T$ e ha area $c/2$.

Proviamo invece il caso $\mathbf{A} = \mathbf{E}_{21}(d)$. Il trasformato dello stesso triangolo di prima ha vertici $[0\ 0]^T$, $[1\ d]^T$, $[1\ 1+d]^T$ che ha area ancora $1/2$.

Non è difficile verificare che lo stesso accade per ogni triangolo: le trasformazioni $\mathbf{E}_i(c)$ moltiplicano le aree per c, le trasformazioni $\mathbf{E}_{ij}(d)$ non modificano le aree.

Si potrebbe eseguire un calcolo simile nello spazio tridimensionale. Si vedrebbe che le trasformazioni $\mathbf{E}_i(c)$ moltiplicano i volumi per c e che le $\mathbf{E}_{ij}(d)$ non li modificano. Invece le trasformazioni $\mathbf{E}_{ij}$ cambiano l'orientazione: una mano destra diventa una mano sinistra.

Se poi la matrice $\mathbf{A}$ non è invertibile, l'immagine della trasformazione dello spazio è tutta contenuta in un piano (o addirittura in una retta e, se la matrice $\mathbf{A}$ è nulla, in un punto): in tal caso i volumi si annullano.

Queste considerazioni stanno alla base della definizione che segue.

Definizione. Un'applicazione $\varphi\colon \mathrm{M}_n(\mathbb{C}) \to \mathbb{C}$ si dice una *funzione determinante* se ha le proprietà seguenti:

(D_1) per ogni $\mathbf{A} \in \mathrm{M}_n(\mathbb{C})$, $\varphi(\mathbf{A}\mathbf{E}_i(c)) = c\varphi(\mathbf{A})$;

(D_2) per ogni $\mathbf{A} \in \mathrm{M}_n(\mathbb{C})$, $\varphi(\mathbf{A}\mathbf{E}_{ij}(d)) = \varphi(\mathbf{A})$;

(D_3) per ogni $\mathbf{A} \in \mathrm{M}_n(\mathbb{C})$, $\varphi(\mathbf{A}\mathbf{E}_{ij}) = -\varphi(\mathbf{A})$.

Dimostreremo che una tale applicazione è essenzialmente unica. Il succo della definizione è che il comportamento della funzione φ è buono rispetto alle trasformazioni elementari sulle colonne. Notiamo che avremmo potuto altrettanto bene considerare la pre-moltiplicazione per matrici elementari, esaminando il comportamento di φ rispetto alle trasformazioni elementari sulle righe. Vedremo infatti che sarà comunque $\varphi(\mathbf{A}) = \varphi(\mathbf{A}^T)$.

Lemma 1.1. *Se $\varphi\colon \mathrm{M}_n(\mathbb{C}) \to \mathbb{C}$ è una funzione determinante e $\mathbf{A} \in \mathrm{M}_n(\mathbb{C})$ ha una colonna nulla, allora $\varphi(\mathbf{A}) = 0$.*

Dimostrazione. Supponiamo che la colonna nulla sia la i-esima. Allora $\mathbf{A} = \mathbf{A}\mathbf{E}_i(2)$ e, per la proprietà (D_1), $\varphi(\mathbf{A}) = \varphi(\mathbf{A}\mathbf{E}_i(2)) = 2\varphi(\mathbf{A})$, da cui la tesi. □

Lemma 1.2. *Se $\varphi\colon \mathrm{M}_n(\mathbb{C}) \to \mathbb{C}$ è una funzione determinante e $\mathbf{A} \in \mathrm{M}_n(\mathbb{C})$ è non invertibile, allora $\varphi(\mathbf{A}) = 0$.*

Dimostrazione. Siccome $\mathbf{A}$ non è invertibile, una colonna è combinazione lineare delle altre; non è restrittivo supporre che sia la prima, usando la proprietà (D_3) per scambiare le colonne, eventualmente: infatti $\varphi(\mathbf{A})$ può cambiare di segno, ma dovendo provare che $\varphi(\mathbf{A}) = 0$ ciò non ha rilevanza.

Abbiamo allora, scritta $\mathbf{A} = [\mathbf{a}_1\ \mathbf{a}_2\ \dots\ \mathbf{a}_n]$,

$$\mathbf{a}_1 = \alpha_2\mathbf{a}_2 + \alpha_3\mathbf{a}_3 + \cdots + \alpha_n\mathbf{a}_n.$$

Applicando nell'ordine le trasformazioni elementari $\mathbf{E}_{21}(-\alpha_2), \mathbf{E}_{31}(-\alpha_3), \dots, \mathbf{E}_{n1}(-\alpha_n)$, la matrice $\mathbf{B}$ che otteniamo ha la prima colonna nulla, quindi, per il lemma precedente, $\varphi(\mathbf{B}) = 0$. Ma

$$\mathbf{B} = \mathbf{A}\mathbf{E}_{21}(-\alpha_2)\mathbf{E}_{31}(-\alpha_3)\dots\mathbf{E}_{n1}(-\alpha_n)$$

e quindi, per la proprietà (D_2), $\varphi(A) = 0$. □

Teorema 1.3. *Dato $a \in \mathbb{C}$, esiste al più una funzione determinante $\varphi\colon \mathrm{M}_n(\mathbb{C}) \to \mathbb{C}$ tale che $\varphi(\mathbf{I}_n) = a$.*

Dimostrazione. L'applicazione φ è determinata una volta che ne conosciamo il valore sulle matrici invertibili, per il lemma precedente. Ora, una matrice invertibile $\mathbf{A}$ è prodotto di matrici elementari (si veda l'Esercizio 1.42), quindi, per le proprietà imposte alla funzione determinante φ, possiamo calcolare $\varphi(\mathbf{A})$ una volta che conosciamo il valore di φ sulle matrici elementari:

(1) $\varphi(\mathbf{E}_i(c)) = \varphi(\mathbf{I}\mathbf{E}_i(c)) = c\varphi(\mathbf{I}) = ca$;

(2) $\varphi(\mathbf{E}_{ij}(d)) = \varphi(\mathbf{I}\mathbf{E}_{ij}(d)) = \varphi(\mathbf{I}) = a$;

(3) $\varphi(\mathbf{E}_{ij}) = \varphi(\mathbf{I}\mathbf{E}_{ij}) = -\varphi(\mathbf{I}) = -a$. □

Prima di dimostrare l'esistenza di una funzione determinante, vediamo due proprietà importanti.

Teorema 1.4 (Binet)**.** *Se $\varphi\colon \mathrm{M}_n(\mathbb{C}) \to \mathbb{C}$ è una funzione determinante con $\varphi(\mathbf{I}_n) = 1$ e $\mathbf{A}, \mathbf{B} \in \mathrm{M}_n(\mathbb{C})$, allora $\varphi(\mathbf{AB}) = \varphi(\mathbf{A})\varphi(\mathbf{B})$.*

Dimostrazione. Fissiamo una matrice $\mathbf{C} \in \mathrm{M}_n(\mathbb{C})$ e definiamo $\psi\colon \mathrm{M}_n(\mathbb{C}) \to \mathbb{C}$ con

$$\psi(\mathbf{X}) = \varphi(\mathbf{CX}).$$

Allora

$$\begin{aligned}
\psi(\mathbf{X}\mathbf{E}_i(c)) &= \varphi(\mathbf{C}\mathbf{X}\mathbf{E}_i(c)) = c\varphi(\mathbf{CX}) = c\psi(\mathbf{X});\\
\psi(\mathbf{X}\mathbf{E}_{ij}(d)) &= \varphi(\mathbf{C}\mathbf{X}\mathbf{E}_{ij}(d)) = \varphi(\mathbf{CX}) = \psi(\mathbf{X});\\
\psi(\mathbf{X}\mathbf{E}_{ij}) &= \varphi(\mathbf{C}\mathbf{X}\mathbf{E}_{ij}) = -\varphi(\mathbf{CX}) = -\psi(\mathbf{X}).
\end{aligned}$$

Dunque ψ è una funzione determinante e $\psi(\mathbf{I}) = \varphi(\mathbf{C})$.

Se consideriamo la funzione $\psi'\colon \mathrm{M}_n(\mathbb{C}) \to \mathbb{C}$ definita da

$$\psi'(\mathbf{X}) = \varphi(\mathbf{C})\varphi(\mathbf{X}),$$

con verifiche del tutto analoghe alle precedenti troviamo che anche ψ' è una funzione determinante e che $\psi'(\mathbf{I}) = \varphi(\mathbf{C})$. Dunque $\psi = \psi'$. Calcolando per $\mathbf{C} = \mathbf{A}$ e $\mathbf{X} = \mathbf{B}$, abbiamo la tesi. □

Teorema 1.5. *Se $\varphi\colon \mathrm{M}_n(\mathbb{C}) \to \mathbb{C}$ è una funzione determinante e $\mathbf{A} \in \mathrm{M}_n(\mathbb{C})$, allora*

$$\varphi(\mathbf{A}^T) = \varphi(\mathbf{A}).$$

Dimostrazione. La tesi è ovvia se $\mathbf{A}$ è non invertibile, perché in tal caso lo è anche $\mathbf{A}^T$. Supponiamo allora $\mathbf{A}$ invertibile e scriviamola come prodotto di matrici elementari $\mathbf{A} = \mathbf{E}_1\mathbf{E}_2\dots\mathbf{E}_r$ che dà

$$\mathbf{A}^T = \mathbf{E}_r^T \dots \mathbf{E}_2^T \mathbf{E}_1^T,$$

perciò

$$\varphi(\mathbf{A}^T) = \varphi(\mathbf{E}_r^T)\dots\varphi(\mathbf{E}_2^T)\varphi(\mathbf{E}_1^T)$$

e abbiamo la tesi, poiché $\mathbf{E}_i(c)^T = \mathbf{E}_i(c)$, $\mathbf{E}_{ij}(d)^T = \mathbf{E}_{ji}(d)$ e $\mathbf{E}_{ij}^T = \mathbf{E}_{ij}$. □

Con la stessa tecnica si dimostra anche il risultato seguente.

Teorema 1.6. *Supponiamo esista una funzione determinante* $\varphi^{(n)}\colon \mathrm{M}_n(\mathbb{C}) \to \mathbb{C}$ *tale che* $\varphi^{(n)}(\mathbf{I}) = 1$. *Allora, per ogni* $a \in \mathbb{C}$, *l'unica funzione determinante* $\varphi_a\colon \mathrm{M}_n(\mathbb{C}) \to \mathbb{C}$ *tale che* $\varphi_a(\mathbf{I}) = a$ *si ottiene ponendo, per* $\mathbf{A} \in \mathrm{M}_n(\mathbb{C})$,

$$\varphi_a(\mathbf{A}) = a\varphi^{(n)}(\mathbf{A}).$$ □

Nella sezione successiva dimostreremo che una funzione determinante come quella del teorema *esiste* e quindi saremo autorizzati a chiamarla *la funzione determinante*. Useremo allora una notazione abbreviata che vale per ogni matrice: se $\mathbf{A} \in \mathrm{M}_n(\mathbb{C})$, invece di scrivere $\varphi^{(n)}(\mathbf{A})$ scriveremo $\det\mathbf{A}$; questo numero sarà chiamato *determinante* di $\mathbf{A}$.

2. Esistenza di funzioni determinanti

Quanto abbiamo visto finora dice che le funzioni determinanti hanno alcune proprietà molto importanti, purché tali funzioni esistano. Ci sono vari modi di dimostrarne l'esistenza; quello che scegliamo ci permetterà di dare anche un metodo per il calcolo.

Quanto abbiamo visto prima riguardo all'unicità delle funzioni determinanti potrebbe apparire una dimostrazione anche dell'esistenza: si scrive una matrice invertibile $\mathbf{A}$ come prodotto di matrici elementari e le proprietà richieste permetterebbero di calcolarne il determinante. Tuttavia la scrittura di $\mathbf{A}$ come prodotto di matrici elementari non è affatto unica, quindi occorrerebbe verificare che da due scritture del genere si ricava lo stesso numero, cosa tutt'altro che facile. Per questo preferiamo seguire una strada diversa.

Teorema 2.1. *Per ogni* $n \geq 1$ *esiste una funzione determinante* $\varphi^{(n)}\colon \mathrm{M}_n(\mathbb{C}) \to \mathbb{C}$ *tale che* $\varphi^{(n)}(I) = 1$.

Dimostrazione. L'asserto è ovvio per $n = 1$: l'applicazione identità di $\mathrm{M}_1(\mathbb{C}) = \mathbb{C} \to \mathbb{C}$ soddisfa alle richieste. Perciò faremo induzione su n.

Supponiamo dunque $n > 1$ e di avere già a disposizione la funzione determinante $\varphi^{(n-1)}$, che quindi possiamo calcolare su ogni matrice che si ottiene da una data matrice $n \times n$ cancellandone una riga e una colonna. Fissiamo alcune notazioni: se

$\mathbf{A} \in \mathrm{M}_n(\mathbb{C})$, denoteremo con a_{ij} il suo coefficiente di posto (i, j) e con $\mathbf{A}_{ij}$ la matrice che si ottiene da $\mathbf{A}$ cancellandone la i-esima riga e la j-esima colonna.

Vedremo che non occorre considerare tutte le *sottomatrici* così fatte, perché una funzione determinante assume lo stesso valore, oppure questo cambia di segno o viene moltiplicato per uno scalare, su matrici che si ottengono l'una dall'altra con trasformazioni elementari.

Definiamo allora, per $\mathbf{A} \in \mathrm{M}_n(\mathbb{C})$,

$$\varphi(\mathbf{A}) = \sum_{j=1}^{n} (-1)^{1+j} a_{1j} \varphi^{(n-1)}(\mathbf{A}_{1j})$$

e verifichiamo che questa è una funzione determinante.

Consideriamo $\mathbf{B} = \mathbf{A}\mathbf{E}_k(c)$; abbiamo

$$b_{1j} = \begin{cases} a_{1j} & \text{se } j \neq k, \\ ca_{1k} & \text{se } j = k, \end{cases} \qquad \mathbf{B}_{1j} = \begin{cases} \mathbf{A}_{1j}\mathbf{E}_k(c) & \text{se } j \neq k, \\ \mathbf{A}_{1k} & \text{se } j = k. \end{cases}$$

Perciò

$$\begin{aligned} \varphi(\mathbf{B}) &= \sum_{j=1}^{n} (-1)^{1+j} b_{1j} \varphi^{(n-1)}(\mathbf{B}_{1j}) \\ &= (-1)^{1+k} ca_{1k} \varphi^{(n-1)}(\mathbf{A}_{1k}) + \sum_{j \neq k}^{n} (-1)^{i+1} a_{1j} \varphi^{(n-1)}(\mathbf{A}_{1j}\mathbf{E}_k(c)) \\ &= c\varphi(\mathbf{A}) \end{aligned}$$

avendo applicato l'ipotesi induttiva per $\varphi^{(n-1)}$ e raccogliendo c.

Consideriamo $\mathbf{B} = \mathbf{A}\mathbf{E}_{12}$; nel caso generale si aggiungono solo complicazioni tecniche. Abbiamo

$$b_{1j} = \begin{cases} a_{12} & \text{se } j = 1, \\ a_{11} & \text{se } j = 2, \\ a_{1j} & \text{altrimenti}, \end{cases} \qquad \mathbf{B}_{1j} = \begin{cases} \mathbf{A}_{12} & \text{se } j = 1, \\ \mathbf{A}_{11} & \text{se } j = 2, \\ \mathbf{A}_{1j}\mathbf{E}_{12} & \text{altrimenti}. \end{cases}$$

Perciò

$$\begin{aligned} \varphi(\mathbf{B}) &= \sum_{j=1}^{n} (-1)^{1+j} b_{1j} \varphi^{(n-1)}(\mathbf{B}_{1j}) \\ &= (-1)^{1+1} b_{11} \varphi^{(n-1)}(\mathbf{B}_{11}) + (-1)^{1+2} b_{12} \varphi^{(n-1)}(\mathbf{B}_{12}) + \sum_{j=3}^{n} (-1)^{1+j} b_{1j} \varphi^{(n-1)}(\mathbf{B}_{1j}) \\ &= a_{12} \varphi^{(n-1)}(\mathbf{A}_{12}) - a_{11} \varphi^{(n-1)}(\mathbf{A}_{11}) + \sum_{j=3}^{n} (-1)^{1+j} a_{1j} \varphi^{(n-1)}(\mathbf{A}_{1j}\mathbf{E}_{12}) \\ &= -(a_{11} \varphi^{(n-1)}(\mathbf{A}_{11}) + a_{12} \varphi^{(n-1)}(\mathbf{A}_{12})) + (-1) \sum_{j=3}^{n} (-1)^{1+j} a_{1j} \varphi^{(n-1)}(\mathbf{A}_{1j}) \\ &= -\varphi(\mathbf{A}), \end{aligned}$$

applicando ancora una volta l'ipotesi induttiva.

Vediamo ora l'ultimo caso; ancora esaminiamo come caso particolare $\mathbf{B} = \mathbf{A}\mathbf{E}_{21}(d)$ per evitare le complicazioni tecniche. Abbiamo

$$b_{1j} = \begin{cases} a_{11} + d a_{12} & \text{se } j = 1, \\ a_{1j} & \text{se } j > 1, \end{cases} \qquad \mathbf{B}_{1j} = \begin{cases} \mathbf{A}_{11} & \text{se } j = 1, \\ \mathbf{X} & \text{se } j = 2, \\ \mathbf{A}_{1j}\mathbf{E}_{21}(d) & \text{se } j > 2. \end{cases}$$

Perciò

$$\begin{aligned} \varphi(\mathbf{B}) &= \sum_{j=1}^{n} (-1)^{1+j} b_{1j} \varphi^{(n-1)}(\mathbf{B}_{1j}) \\ &= (-1)^{1+1}(a_{11} + d a_{12})\varphi^{(n-1)}(\mathbf{A}_{11}) + (-1)^{1+2} a_{12} \varphi^{(n-1)}(\mathbf{X}) + \\ &\qquad + \sum_{j=3}^{n} (-1)^{1+j} a_{1j} \varphi^{(n-1)}(\mathbf{A}_{1j}\mathbf{E}_{21}(d)) \\ &= \varphi(\mathbf{A}) + d a_{12} \varphi^{(n-1)}(\mathbf{A}_{11}) + (-1)^{1+2} a_{12} \varphi^{(n-1)}(\mathbf{X}) - (-1)^{1+2} a_{12} \varphi^{(n-1)}(\mathbf{A}_{12}) \end{aligned}$$

e la tesi sarà dimostrata se proviamo che

$$\varphi^{(n-1)}(\mathbf{X}) = \varphi^{(n-1)}(\mathbf{A}_{12}) + d\varphi^{(n-1)}(\mathbf{A}_{11}).$$

Più in generale, dimostreremo che, posto $m = n-1$, $\varphi^{(m)}$ è *lineare nella prima colonna*, cioè che, se

$$\begin{aligned} \mathbf{X}' &= [\mathbf{x}'\ \mathbf{x}_2\ \mathbf{x}_3\ \dots\ \mathbf{x}_m], \\ \mathbf{X}'' &= [\mathbf{x}''\ \mathbf{x}_2\ \mathbf{x}_3\ \dots\ \mathbf{x}_m], \\ \mathbf{X} &= [\mathbf{x}' + \mathbf{x}''\ \mathbf{x}_2\ \mathbf{x}_3\ \dots\ \mathbf{x}_m], \end{aligned}$$

allora

$$\varphi^{(m)}(\mathbf{X}) = \varphi^{(m)}(\mathbf{X}') + \varphi^{(m)}(\mathbf{X}'').$$

Ricordiamo che sappiamo già che, se

$$\begin{aligned} \mathbf{Y} &= [\mathbf{y}\ \mathbf{y}_2\ \mathbf{y}_3\ \dots\ \mathbf{y}_m], \\ \mathbf{Y}' &= [\alpha\mathbf{y}\ \mathbf{y}_2\ \mathbf{y}_3\ \dots\ \mathbf{y}_m], \end{aligned}$$

allora

$$\varphi^{(m)}(\mathbf{Y}') = \alpha\varphi^{(m)}(\mathbf{Y})$$

(tutti i vettori considerati sono in $\mathbb{C}^m$). È chiaro che, quando consideriamo la forma della matrice $\mathbf{A}'$ che stiamo trattando, da questa linearità segue la tesi.

Possiamo senz'altro dare l'asserto per ovvio quando $m = 1$: la funzione $\varphi^{(1)}$ è l'identità su $\mathbb{C}$. Faremo pertanto induzione su m e dunque consideriamo l'asserto vero per $\varphi^{(m-1)}$. Fissiamo alcune notazioni: x_1', x_1'' e x_1 sono i coefficienti sulla prima riga di

$\mathbf{x}'$, $\mathbf{x}''$ e $\mathbf{x}$ rispettivamente; indicheremo con $\mathbf{y}'$, $\mathbf{y}''$, $\mathbf{y}$ e $\mathbf{y}_j$ $(j = 2, \dots, m)$ i vettori di $\mathbb{C}^{m-1}$ che si ottengono da quelli dati cancellando il coefficiente sulla prima riga.

Quando applichiamo la definizione di $\varphi^{(m)}$ alla matrice $\mathbf{X}$, dobbiamo cancellare via via una colonna, oltre alla prima riga; se cancelliamo la prima colonna, rimane la matrice

$$[\mathbf{y}_2\ \mathbf{y}_3\ \dots\ \mathbf{y}_m],$$

mentre se cancelliamo la seconda colonna otteniamo la matrice

$$[\mathbf{y}' + \mathbf{y}''\ \mathbf{y}_3\ \dots\ \mathbf{y}_m],$$

e così anche per le successive, alle quali potremo dunque applicare l'ipotesi induttiva. Con facili calcoli si ottiene allora la tesi. □

3. Come calcolare il determinante

Possiamo riassumere quanto visto nelle sezioni precedenti nel modo seguente:

Teorema 3.1. *Per ogni $n > 0$ esiste un'unica funzione determinante $\varphi^{(n)} \colon \mathrm{M}_n(\mathbb{C}) \to \mathbb{C}$ tale che $\varphi^{(n)}(\mathbf{I}_n) = 1$.*

Per semplicità di notazione, si scrive $\varphi^{(n)}(\mathbf{A}) = \det \mathbf{A}$; il numero $\det \mathbf{A}$ si chiama *determinante* di $\mathbf{A}$. Possiamo allora, usando le notazioni precedenti, trascrivere i risultati ottenuti nel modo seguente.

Teorema 3.2 (Binet)**.** *Se $\mathbf{A}, \mathbf{B} \in \mathrm{M}_n(\mathbb{C})$, allora*

$$\det(\mathbf{AB}) = (\det \mathbf{A})(\det \mathbf{B}).$$ □

Teorema 3.3. *Una matrice $\mathbf{A} \in \mathrm{M}_n(\mathbb{C})$ non è invertibile se e solo se $\det \mathbf{A} = 0$.* □

Teorema 3.4. *Per ogni $\mathbf{A} \in \mathrm{M}_n(\mathbb{C})$, $\det \mathbf{A} = \det(\mathbf{A}^T)$.* □

Esistono almeno due modi per calcolare il determinante di una matrice. Uno viene dalla definizione di funzione determinante, l'altro dalla dimostrazione di esistenza.

Primo metodo di calcolo del determinante. *Sia $\mathbf{A}$ una matrice $n \times n$ invertibile. Sia s il numero di scambi di riga e siano $c_1, c_2, \dots, c_n$ i pivot per ottenere da $\mathbf{A}$ una matrice in forma ridotta. Allora*

$$\det \mathbf{A} = (-1)^s c_1 c_2 \dots c_n.$$

Dimostrazione. Scriviamo $\mathbf{A} = \mathbf{P}^T \mathbf{LU}$, con $\mathbf{U}$ unitriangolare superiore, visto che $\mathbf{A}$ è invertibile; allora

- $\mathbf{P}$ è prodotto di s matrici del tipo $\mathbf{E}_{ij}$;
- $\mathbf{L}$ è prodotto di matrici elementari dove compaiono le matrici $\mathbf{E}_1(c_1)$, $\mathbf{E}_2(c_2)$, …, $\mathbf{E}_n(c_n)$ oltre a matrici del tipo $\mathbf{E}_{ij}(d)$;

- $\mathbf{U}$ è prodotto di matrici elementari del tipo $\mathbf{E}_{ij}(d)$.

Siccome det è una funzione determinante che vale 1 sulla matrice identità, il teorema di Binet permette di calcolare $\det\mathbf{A}$ come prodotto dei determinanti delle matrici elementari suddette. Le matrici $\mathbf{E}_{ij}(d)$ hanno determinante 1, quelle del tipo $\mathbf{E}_i(c)$ hanno determinante c e quelle del tipo $\mathbf{E}_{ij}$ hanno determinante -1, da cui si ha subito la conclusione. □

Vediamo alcune conseguenze del metodo di calcolo.

Corollario 3.5. *Se* $\mathbf{A}$ *è una matrice quadrata a coefficienti reali, allora* $\det\mathbf{A}$ *è un numero reale.*

Dimostrazione. Siccome l'eliminazione su $\mathbf{A}$ si può eseguire interamente con numeri reali, i pivot saranno reali e così il loro prodotto. □

Corollario 3.6. *Il determinante di una matrice triangolare è il prodotto degli elementi sulla diagonale.*

Dimostrazione. Una matrice triangolare non è invertibile se e solo se uno dei coefficienti sulla diagonale è nullo.

Se la matrice è invertibile e triangolare superiore, i pivot dell'eliminazione, che si può eseguire senza scambi di righe, sono esattamente i coefficienti sulla diagonale.

Per le triangolari inferiori, basta applicare la trasposizione. □

Corollario 3.7. *Se* $\mathbf{A} \in \mathrm{M}_n(\mathbb{C})$, *allora* $\det\overline{\mathbf{A}} = \overline{\det\mathbf{A}}$.

Dimostrazione. Se $\mathbf{A}$ è non invertibile, non c'è niente da dimostrare: il coniugato di zero è zero. Supponiamo allora che $\mathbf{A}$ sia invertibile e scriviamola nella forma $\mathbf{A} = \mathbf{P}^T\mathbf{L}\mathbf{U}$, con $\mathbf{L}$ triangolare inferiore e $\mathbf{U}$ unitriangolare superiore. Allora abbiamo $\overline{\mathbf{A}} = \mathbf{P}^T\overline{\mathbf{L}}\overline{\mathbf{U}}$; per il teorema di Binet

$$\det\overline{\mathbf{A}} = (\det\mathbf{P}^T)(\det\overline{\mathbf{L}})(\det\overline{\mathbf{U}})$$

e, per il corollario precedente, $\det\overline{\mathbf{U}} = 1$. Inoltre, siccome $\det\overline{\mathbf{L}}$ è il prodotto dei coefficienti sulla diagonale, vale $\det\overline{\mathbf{L}} = \overline{\det\mathbf{L}}$. □

Corollario 3.8. *Se* $\mathbf{A} \in \mathrm{M}_n(\mathbb{C})$, *allora* $\det(\mathbf{A}^H) = \overline{\det\mathbf{A}}$.

Dimostrazione. Basta ricordare che $\mathbf{A}^H = (\overline{\mathbf{A}})^T$. □

Veniamo ora al secondo metodo di calcolo, che ricaviamo dalla dimostrazione di esistenza. Ricordiamo che denotiamo con $\mathbf{A}_{ij}$ la matrice che si ottiene da $\mathbf{A}$ cancellandone la i-esima riga e la j-esima colonna (supponendo che $\mathbf{A}$ sia $n \times n$ e che $n > 1$). Il determinante di una matrice 1×1, cioè un numero, è il numero stesso.

Le formule che enunceremo si chiamano *sviluppo del determinante per righe o per colonne* e sono dovute a Laplace.

Secondo metodo di calcolo del determinante. *Sia* $\mathbf{A} \in \mathrm{M}_n(\mathbb{C})$, $n > 1$. *Allora*

$$\det \mathbf{A} = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det \mathbf{A}_{ij} \qquad (\textit{sviluppo secondo la } i\textit{-esima riga})$$

$$\det \mathbf{A} = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det \mathbf{A}_{ij} \qquad (\textit{sviluppo secondo la } j\textit{-esima colonna})$$

Dimostrazione. La prima delle due formule, nel caso $i = 1$, è esattamente la formula usata per dimostrare l'esistenza delle funzioni determinanti.

Prima di dimostrarla nel caso generale, proviamo a calcolare quanti scambi di righe occorrono per portare la i-esima riga sulla prima e *far scalare* le altre. Per esempio, supponiamo $n = 5$ e di voler portare la terza riga al posto della prima, la prima al posto della seconda e la seconda al posto della terza lasciando ferme la quarta e la quinta. Se la matrice è, scritta per righe,

$$\begin{bmatrix} \mathbf{R}_1 \\ \mathbf{R}_2 \\ \mathbf{R}_3 \\ \mathbf{R}_4 \\ \mathbf{R}_5 \end{bmatrix},$$

la vogliamo far diventare

$$\begin{bmatrix} \mathbf{R}_3 \\ \mathbf{R}_1 \\ \mathbf{R}_2 \\ \mathbf{R}_4 \\ \mathbf{R}_5 \end{bmatrix}.$$

Occorrerà impiegare la $\mathbf{E}_{13}$, poi la $\mathbf{E}_{23}$.

Supponiamo invece di voler portare la quarta riga in alto, ottenendo la matrice

$$\begin{bmatrix} \mathbf{R}_4 \\ \mathbf{R}_1 \\ \mathbf{R}_2 \\ \mathbf{R}_3 \\ \mathbf{R}_5 \end{bmatrix}.$$

Occorrerà la $\mathbf{E}_{14}$, poi la $\mathbf{E}_{34}$ e infine la $\mathbf{E}_{23}$.

Ci si accorge che, in ogni caso, il numero di scambi di riga necessari per portare in alto la i-esima riga è $i - 1$.

Se $\mathbf{B}$ è la matrice ottenuta portando la i-esima riga in alto e facendo scalare le altre, avremo che $\det \mathbf{B} = (-1)^{i-1} \det \mathbf{A}$, perché abbiamo applicato $i - 1$ scambi di righe. Inoltre $\mathbf{B}_{1j} = \mathbf{A}_{ij}$, quindi

$$\det \mathbf{A} = (-1)^{i-1} \det \mathbf{B} = \sum_{j=1}^{n} (-1)^{i-1} (-1)^{1+j} b_{1j} \det \mathbf{B}_{1j} = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det \mathbf{A}_{ij}.$$

La formula dello sviluppo per colonne segue dal fatto che $\det \mathbf{A} = \det(\mathbf{A}^T)$. □

Questo metodo di calcolo è utile quando la matrice $\mathbf{A}$ ha "molti zeri", ma non è molto efficiente nel caso generale. Infatti si richiedono n prodotti per il primo sviluppo; ciascuno dipende dal determinante di una matrice $(n-1) \times (n-1)$ e così via.

Dunque lo sviluppo completo per righe richiede un grande numero di moltiplicazioni: $n!$ (si legge *n fattoriale* e significa $n \cdot (n-1) \cdot (n-2) \cdot \dots \cdot 3 \cdot 2 \cdot 1$). Se consideriamo che $6! = 720$ e che $30! \approx 2{,}65 \cdot 10^{32}$ ci rendiamo conto che il metodo con l'eliminazione di Gauss è certamente più efficiente, perché richiede n^2 moltiplicazioni per il primo passo, $(n-1)^2$ per il secondo, e così via. In totale il numero di moltiplicazioni è uguale a $s_n = n(n+1)(2n+1)/6$.

Abbiamo $s_4 = 30$ e $4! = 24$; invece $s_5 = 55$ e $5! = 120$, $s_6 = 91$ e $6! = 720$. Come si vede, il metodo con l'eliminazione è di gran lunga più efficiente.

I determinanti hanno un uso anche nella risoluzione di sistemi lineari, con un metodo più teorico che pratico, visto che richiederebbe il calcolo di $n+1$ determinanti.

Cominciamo con una semplice considerazione: se supponiamo $j \neq k$, con $1 \leq j \leq n$ e $1 \leq k \leq n$, abbiamo

$$\sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det \mathbf{A}_{ik} = 0.$$

Infatti questa formula è lo sviluppo del determinante rispetto alla j-esima colonna della matrice che si ottiene da $\mathbf{A}$ sostituendo la j-esima colonna con la k-esima e lasciando invariate le altre. Questa matrice ha dunque due colonne uguali e quindi determinante zero, essendo ovviamente non invertibile. Possiamo allora scrivere

$$\sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det \mathbf{A}_{ik} = (\det \mathbf{A}) \delta_{jk}$$

dove $\delta_{jk} = 1$ se $j = k$ e $\delta_{jk} = 0$ se $j \neq k$ (sono cioè i coefficienti della matrice identità).

Questo permette di scrivere in modo esplicito l'inversa di una matrice invertibile $\mathbf{A}$ di ordine $n > 1$. Definiamo la sua *aggiunta* nel modo seguente: $\operatorname{adj} \mathbf{A} = [\alpha_{ij}]$ dove

$$\alpha_{ji} = (-1)^{i+j} \det \mathbf{A}_{ij}.$$

In altre parole il coefficiente di posto (j, i) della matrice $\operatorname{adj} \mathbf{A}$ si calcola moltiplicando per $(-1)^{i+j}$ il determinante della matrice ottenuta cancellando la i-esima riga e la j-esima colonna. Si faccia attenzione all'inversione degli indici.

Proposizione 3.9. *Se $\mathbf{A}$ è una matrice quadrata, allora* $(\operatorname{adj} \mathbf{A})\mathbf{A} = (\det \mathbf{A})\mathbf{I}$. *In particolare, se $\mathbf{A}$ è invertibile,* $\mathbf{A}^{-1} = (\det \mathbf{A})^{-1} \operatorname{adj} \mathbf{A}$.

Dimostrazione. Basta eseguire il calcolo di $(\operatorname{adj} \mathbf{A})\mathbf{A}$; il coefficiente di posto (k, j) in questo prodotto è

$$\sum_{i=1}^{n} \alpha_{ki} a_{ij} = \sum_{i=1}^{n} a_{ij} (-1)^{i+k} \det \mathbf{A}_{ik} = (\det \mathbf{A}) \delta_{jk},$$

quindi

$$(\operatorname{adj} \mathbf{A})\mathbf{A} = (\det \mathbf{A})\mathbf{I}_n. \qquad \square$$

Esempio 3.10. L'unico caso in cui questo metodo sia migliore del metodo dell'eliminazione per il calcolo dell'inversa è quando $n = 2$. Infatti in questo caso i determinanti per calcolare l'aggiunta sono semplici numeri. Se

$$\mathbf{A} = \begin{bmatrix} 1 & 3 \\ -2 & 4 \end{bmatrix},$$

allora $\det \mathbf{A} = 10$ e quindi, come si è già visto nel Capitolo 1,

$$\mathbf{A}^{-1} = \begin{bmatrix} 4/10 & -3/10 \\ 2/10 & 1/10 \end{bmatrix}$$

cioè: si scambiano gli elementi della diagonale e gli altri vengono cambiati di segno. Poi tutti i coefficienti vanno divisi per il determinante. □

Se $\mathbf{A}$ è una matrice $n \times n$ e $\mathbf{b} \in \mathbb{C}^n$, indichiamo con $\mathbf{A}(\mathbf{b}, j)$ la matrice che si ottiene da $\mathbf{A}$ sostituendone la j-esima colonna con $\mathbf{b}$.

Possiamo analizzare il sistema $\mathbf{Ax} = \mathbf{b}$ tenendo conto della teoria appena sviluppata e ottenere un classico risultato dovuto a Cramer.

Teorema 3.11 (Cramer)**.** *Siano $\mathbf{A}$ una matrice $n \times n$ invertibile e $\mathbf{b} \in \mathbb{C}^n$. Se la soluzione del sistema $\mathbf{Ax} = \mathbf{b}$ è $\mathbf{x} = [x_1\ x_2\ \dots\ x_n]^T$, allora*

$$x_k = \frac{\det \mathbf{A}(\mathbf{b}, k)}{\det \mathbf{A}} \qquad (k = 1, 2, \dots, n).$$

Dimostrazione. Scriviamo come prima $\operatorname{adj} \mathbf{A} = [\alpha_{ij}]$ e poniamo $\mathbf{b} = [b_1\ b_2\ \dots\ b_n]^T$. Sappiamo che $\mathbf{x} = \mathbf{A}^{-1}\mathbf{b}$, dunque

$$(\det \mathbf{A})\mathbf{x} = (\operatorname{adj} \mathbf{A})\mathbf{b},$$

e dunque

$$(\det \mathbf{A}) x_k = \sum_{j=1}^{n} \alpha_{kj} b_j = \sum_{j=1}^{n} (-1)^{j+k} b_j \det \mathbf{A}_{jk}$$

che è proprio lo sviluppo rispetto alla k-esima colonna della matrice $\mathbf{A}(\mathbf{b}, k)$. □

Esempio 3.12. Il sistema lineare

$$\begin{cases} ax + by = l \\ cx + dy = m \end{cases}$$

ha una ed una sola soluzione se e solo se $ad - bc \neq 0$ e in tal caso

$$x = \frac{\det \begin{bmatrix} a & l \\ c & m \end{bmatrix}}{\det \begin{bmatrix} a & b \\ c & d \end{bmatrix}} = \frac{am - cl}{ad - bc}, \qquad y = \frac{\det \begin{bmatrix} l & b \\ m & d \end{bmatrix}}{\det \begin{bmatrix} a & b \\ c & d \end{bmatrix}} = \frac{dl - bm}{ad - bc}.$$

È questa la nota *regola di Cramer*. Anche in questo caso il metodo è efficiente solo per sistemi 2×2. □

4. Conservazione della parità nelle permutazioni e determinanti

Vedremo in questa sezione un'applicazione delle proprietà dei determinanti. Diamo per noti i primi elementi della teoria delle permutazioni e la loro decomposizione in cicli disgiunti.

Proposizione 4.1. *Sia σ un elemento del gruppo delle permutazioni S_n, con $n > 1$. Allora σ è prodotto di trasposizioni.*

Dimostrazione. Basta dimostrarlo per ogni ciclo. Ma

$$(i_1 i_2 \dots i_k) = (i_1 i_k)(i_1 i_{k-1}) \dots (i_1 i_2)$$

nel caso in cui il ciclo abbia lunghezza almeno due. Se il ciclo ha lunghezza uno è l'identità, ma allora coincide con $(12)(12)$. □

Notiamo che si usa l'ipotesi $n > 1$, perché per $n = 1$ il gruppo S_1 non ha trasposizioni!

Teorema 4.2. *Sia $\sigma \in S_n$ e scriviamo*

$$\sigma = \alpha_1 \alpha_2 \dots \alpha_r = \beta_1 \beta_2 \dots \beta_s$$

come prodotto di trasposizioni in due modi distinti. Allora r e s sono entrambi pari o entrambi dispari.

Dimostrazione. Useremo una tecnica indiretta, associando a ogni permutazione una opportuna matrice $n \times n$. Ricordiamo che $\mathbf{e}_i$ denota la i-esima colonna dell'identità. Definiamo allora, per $\sigma \in S_n$,

$$\widehat{\sigma} = [\mathbf{e}_{\sigma(1)}\ \mathbf{e}_{\sigma(2)}\ \dots\ \mathbf{e}_{\sigma(n)}],$$

cioè la matrice che ha come colonne le colonne dell'identità permutate attraverso σ. Per esempio, se σ è la permutazione identità, allora $\widehat{\sigma}$ è la matrice identità. In ogni caso, è chiaro che $\widehat{\sigma}$ è una matrice di permutazione.

Ricordiamo anche che, se $\mathbf{A}$ e $\mathbf{B}$ sono matrici $n \times n$ e scriviamo $\mathbf{B} = [\mathbf{b}_1\ \mathbf{b}_2\ \dots\ \mathbf{b}_n]$, allora

$$\mathbf{AB} = [\mathbf{Ab}_1\ \mathbf{Ab}_2\ \dots\ \mathbf{Ab}_n]$$

e che il prodotto di $\mathbf{Ae}_i$ dà la i-esima colonna di $\mathbf{A}$. In particolare $\widehat{\sigma}\mathbf{e}_i = \mathbf{e}_{\sigma(i)}$.

Siano $\sigma, \tau \in S_n$; allora abbiamo

$$\widehat{\sigma}\widehat{\tau} = [\widehat{\sigma}\mathbf{e}_{\tau(1)}\ \widehat{\sigma}\mathbf{e}_{\tau(2)}\ \dots\ \widehat{\sigma}\mathbf{e}_{\tau(n)}] = [\mathbf{e}_{\sigma(\tau(1))}\ \mathbf{e}_{\sigma(\tau(2))}\ \dots\ \mathbf{e}_{\sigma(\tau(n))}] = \widehat{\sigma\tau}.$$

In altre parole abbiamo una relazione fra la composizione di permutazioni e il prodotto di matrici (si tratta di un omomorfismo del gruppo delle permutazioni nel gruppo delle matrici $n \times n$ invertibili) e questo ci permette di usare il teorema di Binet.

Osserviamo che ogni matrice $\widehat{\sigma}$ ha determinante 1 oppure -1, in quanto matrice di permutazione. Ne segue che, scrivendo $\sigma = \alpha_1\alpha_2\dots\alpha_r$ come prodotto di trasposizioni, abbiamo dapprima

$$\widehat{\sigma} = \widehat{\alpha_1}\widehat{\alpha_2}\dots\widehat{\alpha_r}$$

e, per il teorema di Binet,

$$\begin{aligned}\det\widehat{\sigma} &= \det(\widehat{\alpha_1}\widehat{\alpha_2}\dots\widehat{\alpha_r})\\ &= (\det\widehat{\alpha_1})(\det\widehat{\alpha_2})\dots(\det\widehat{\alpha_r})\\ &= (-1)^r\end{aligned}$$

da cui segue l'enunciato del teorema. □

Di fatto l'assegnazione $\sigma \mapsto \det\widehat{\sigma}$ definisce un omomorfismo di S_n nel gruppo $\{1,-1\}$ degli elementi invertibili di $\mathbb{Z}$ (rispetto alla moltiplicazione) che si suole chiamare *segnatura*: allora $\operatorname{sgn}\sigma = \det\widehat{\sigma}$. Questo omomorfismo è definito anche nel caso di $n = 1$.

L'introduzione della segnatura permette di scrivere un'altra formula per il determinante di una matrice.

Teorema 4.3. *Se $\mathbf{A} = [a_{ij}]$ è una matrice $n \times n$, allora*

$$\det\mathbf{A} = \sum_{\sigma\in S_n} (\operatorname{sgn}\sigma)\, a_{\sigma(1),1}a_{\sigma(2),2}\dots a_{\sigma(n),n}.$$

Per esempio, quando $n = 2$ le permutazioni sono l'identità ι e $\sigma = (12)$; quindi

$$\det\begin{bmatrix} a_{11} & a_{12}\\ a_{21} & a_{22}\end{bmatrix} = (\operatorname{sgn}\iota)\, a_{\iota(1),1}a_{\iota(2),2} + (\operatorname{sgn}\sigma)\, a_{\sigma(1),1}a_{\sigma(2),2} = a_{11}a_{22} - a_{21}a_{12}.$$

Per esercizio si scriva la formula esplicita per $n = 3$, considerando che S_n consiste della permutazione identità ι e di $\alpha = (12)$, $\beta = (13)$, $\gamma = (23)$, $\delta = (123)$, $\varepsilon = (132)$.

Dimostrazione. Si tratta di vedere che la funzione

$$\mathbf{A} \mapsto \varphi(\mathbf{A}) = \sum_{\sigma\in S_n} (\operatorname{sgn}\sigma)\, a_{\sigma(1),1}a_{\sigma(2),2}\dots a_{\sigma(n),n}$$

è una funzione determinante e che $\varphi(\mathbf{I}_n) = 1$. Porremo

$$\mathbf{A}[\sigma] = a_{\sigma(1),1}a_{\sigma(2),2}\dots a_{\sigma(n),n},$$

quindi

$$\varphi(\mathbf{A}) = \sum_{\sigma\in S_n} (\operatorname{sgn}\sigma)\mathbf{A}[\sigma].$$

(1) Poniamo $\mathbf{B} = \mathbf{A}\mathbf{E}_i(c)$ e $\mathbf{B} = [b_{ij}]$. Allora

$$\mathbf{B}[\sigma] = b_{\sigma(1),1}\dots b_{\sigma(i),i}\dots b_{\sigma(n),n} = a_{\sigma(1),1}\dots c a_{\sigma(i),i}\dots a_{\sigma(n),n} = c\mathbf{A}[\sigma],$$

quindi il caso è banale.

(2) Poniamo $\mathbf{C} = \mathbf{A}\mathbf{E}_{ij}$ e $\mathbf{C} = [c_{ij}]$. Avremo allora

$$\mathbf{C}[\sigma] = c_{\sigma(1),1} \dots c_{\sigma(i),i} \dots c_{\sigma(j),j} \dots c_{\sigma(n),n} = b_{\sigma(1),1} \dots b_{\sigma(j),i} \dots b_{\sigma(i),j} \dots b_{\sigma(n),n} = \mathbf{B}[\sigma\alpha],$$

dove $\alpha = (12)$. Perciò

$$\varphi(\mathbf{C}) = \sum_{\sigma \in S_n} (\operatorname{sgn}\sigma)\mathbf{C}[\sigma] = \sum_{\sigma \in S_n} (\operatorname{sgn}\sigma)\mathbf{B}[\sigma\alpha] = \sum_{\tau \in S_n} (\operatorname{sgn}(\tau\alpha^{-1}))\mathbf{B}[\tau] = -\sum_{\tau \in S_n} (\operatorname{sgn}\tau)\mathbf{B}[\tau],$$

dove abbiamo eseguito il cambio di indici $\sigma\alpha = \tau$ e applicato il fatto che $\operatorname{sgn}(\tau\alpha^{-1}) = (\operatorname{sgn}\tau)(\operatorname{sgn}(\alpha^{-1}))$ e che $\operatorname{sgn}(\alpha^{-1}) = \operatorname{sgn}(i\,j) = -1$.

(3) Poniamo $\mathbf{F} = \mathbf{A}\mathbf{E}_{ij}(d)$ e $\mathbf{F} = [f_{ij}]$. Avremo allora

$$\begin{aligned}\mathbf{F}[\sigma] &= f_{\sigma(1),1} \dots f_{\sigma(j),j} \dots f_{\sigma(n),n} = a_{\sigma(1),1} \dots (d a_{\sigma(j),i} + a_{\sigma(j),j} \dots a_{\sigma(n),n} \\ &= \mathbf{A}[\sigma] + d(a_{\sigma(1),1} \dots a_{\sigma(j),i} \dots a_{\sigma(n),n}).\end{aligned}$$

Poniamo

$$t_\sigma = a_{\sigma(1),1} \dots a_{\sigma(j),i} \dots a_{\sigma(n),n},$$

dove il coefficiente $a_{\sigma(j),i}$ sta al j-esimo posto. Si tratta di verificare che $\sum_\sigma (\operatorname{sgn}\sigma)\, t_\sigma = 0$. Infatti, posto $\alpha = (i\,j)$ e $\tau = \sigma\alpha$, abbiamo

$$t_\tau = t_\sigma$$

e nella sommatoria i due addendi compaiono con segni opposti. Dunque $\varphi(\mathbf{F}) = \varphi(\mathbf{A})$.

(4) Ci basta ora calcolare $\varphi(\mathbf{I}_n)$; nella sommatoria che lo definisce, solo un addendo ha tutti i fattori non nulli, precisamente quello con σ la permutazione identità. Questo addendo vale 1. □

Siccome $\det \mathbf{A} = \det(\mathbf{A}^T)$, abbiamo anche

$$\det \mathbf{A} = \sum_{\sigma \in S_n} (\operatorname{sgn}\sigma)\, a_{1,\sigma(1)}\, a_{2,\sigma(2)} \dots a_{n,\sigma(n)}.$$

Rimarchiamo ancora una volta che queste formule sono inapplicabili nella pratica: l'insieme delle permutazioni S_n ha $n!$ elementi e vengono richieste qui $n \cdot n!$ moltiplicazioni.

Esercizi

Paragrafo 1

4.1. Trovare una formula esplicita per l'area di un triangolo note le coordinate dei suoi vertici e verificare le asserzioni fatte sul cambiamento dell'area dopo una trasformazione lineare.

4.2. Trovare una formula esplicita per il volume di un parallelepipedo note le coordinate di quattro vertici su spigoli concorrenti e verificare le asserzioni fatte sul cambiamento di volume dopo una trasformazione lineare.

4.3. Si usino le proprietà delle funzioni determinanti per dimostrare che, moltiplicando una colonna di una matrice per uno scalare α, il determinante viene moltiplicato per α.

4.4. Si usino le proprietà delle funzioni determinanti per dimostrare che, scambiando due colonne di una matrice, il determinante viene moltiplicato per -1.

4.5. Dare le definizioni di funzione determinante usando la pre-moltiplicazione per matrici elementari e dimostrare le proprietà rilevanti.

4.6. Dimostrare senza l'uso del teorema di Binet che, date le matrici $n \times n$ $\mathbf{A}$ e $\mathbf{B}$, si ha $\varphi(AB) = \varphi(BA)$ per ogni funzione determinante φ.

Paragrafo 2

4.7. Usando l'unicità delle funzioni determinanti, dimostrare che $\det \mathbf{A} = \overline{\det \mathbf{A}^H}$.

4.8. Usando l'unicità delle funzioni determinanti, dimostrare che per ogni matrice $\mathbf{A}$ $n \times n$ si ha

$$\sum_{i=1}^{n} (-1)^{i+1} a_{i1} \det \mathbf{A}_{i2} = 0.$$

4.9. Dimostrare che, se $\mathbf{N}$ è nilpotente (cioè esiste $n > 0$ tale che $\mathbf{N}^n = \mathbb{O}$), allora $\mathbf{I} - \mathbf{N}$ è invertibile. Suggerimento: calcolare $(\mathbf{I} - \mathbf{N})(\mathbf{I} + \mathbf{N} + \mathbf{N}^2 + \cdots + \mathbf{N}^{n-1})$.

4.10. Si consideri la matrice $n \times n$ decomposta a blocchi

$$\mathbf{M} = \begin{bmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{C} & \mathbf{D} \end{bmatrix}$$

con $\mathbf{A}$ matrice invertibile $k \times k$. Si provi che

$$\mathbf{M} = \begin{bmatrix} \mathbf{I}_k & \mathbb{O} \\ \mathbf{CA}^{-1} & \mathbf{I}_{n-k} \end{bmatrix} \cdot \begin{bmatrix} \mathbf{A} & \mathbf{B} \\ \mathbb{O} & \mathbf{D} - \mathbf{CA}^{-1}\mathbf{B} \end{bmatrix}.$$

4.11. Nelle notazioni dell'esercizio precedente, la matrice $\mathbf{D} - \mathbf{CA}^{-1}\mathbf{B}$ si chiama *complemento di Schur* di $\mathbf{A}$ in $\mathbf{M}$ ed è denotato con $(\mathbf{M}|\mathbf{A})$. Si provi che $\det \mathbf{M} = \det \mathbf{A} \cdot \det(\mathbf{M}|\mathbf{A})$. Analogamente, se $\mathbf{D}$ è invertibile, posto $(\mathbf{M}|\mathbf{D}) = \mathbf{A} - \mathbf{BD}^{-1}\mathbf{C}$, si provi che $\det \mathbf{M} = \det \mathbf{D} \cdot (\mathbf{M}|\mathbf{D})$.

4.12. Nelle notazioni dei due esercizi precedenti, sia $n = 2k$ e i quattro blocchi di $\mathbf{M}$ siano tutti invertibili. Si provi che

$$\mathbf{M}^{-1} = \begin{bmatrix} (\mathbf{A} - \mathbf{BD}^{-1}\mathbf{C})^{-1} & (\mathbf{C} - \mathbf{DB}^{-1}\mathbf{A})^{-1} \\ (\mathbf{B} - \mathbf{AC}^{-1}\mathbf{D})^{-1} & (\mathbf{D} - \mathbf{CA}^{-1}\mathbf{B})^{-1} \end{bmatrix}.$$

4.13. Si consideri la matrice in forma bordata

$$\mathbf{M} = \begin{bmatrix} \mathbf{A} & \mathbf{b} \\ \mathbf{c}^T & d \end{bmatrix}$$

con $\mathbf{A}$ quadrata invertibile. Si provi che $\det \mathbf{M} = d \cdot \det \mathbf{A} - \mathbf{c}^T (\operatorname{adj} \mathbf{A}) \mathbf{b}$.

Paragrafo 4

4.14. Scrivere esplicitamente la formula per il determinante di una matrice della forma

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ 0 & 0 & 1 \end{bmatrix}$$

e interpretarne l'invertibilità in termini di cambiamenti di coordinate cartesiane.

4.15. Siano $x_1, x_2, x_3 \in \mathbb{C}$ e si consideri la matrice

$$\mathbf{V}(x_1, x_2, x_3) = \begin{bmatrix} 1 & x_1^1 & x_1^2 \\ 1 & x_2^1 & x_2^2 \\ 1 & x_3^1 & x_3^2 \end{bmatrix},$$

Si dimostri che

$$\det \mathbf{V}(x_1, x_2, x_3) = (x_2 - x_1)(x_3 - x_1)(x_3 - x_2).$$

4.16. Si consideri la matrice

$$\mathbf{V}(x_1, x_2, \dots, x_n) = \begin{bmatrix} 1 & x_1^1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2^1 & x_2^2 & \dots & x_2^{n-1} \\ \dots \\ 1 & x_n^1 & x_n^2 & \dots & x_n^{n-1} \end{bmatrix},$$

dove $x_1, x_2, \dots, x_n \in \mathbb{C}$, detta *matrice di Vandermonde*. Si dimostri che

$$\det \mathbf{V}(x_1, x_2, \dots, x_n) = \prod_{1 \le i < j \le n} (x_j - x_i).$$

Suggerimento: induzione su n; si usi il fatto che il determinante non cambia postmoltiplicando per le matrici elementari $\mathbf{E}_{ij}(d)$, usando successivamente

$$\mathbf{E}_{n-1,n}(-x_n), \quad \mathbf{E}_{n-2,n-1}(-x_n), \quad \dots, \quad \mathbf{E}_{1,2}(-x_n).$$

4.17. Data la matrice $n \times n$ $\mathbf{A} = [a_{ij}]$, con $a_{ij} = (x_i + y_j)^{-1}$, dove $x_i + y_j \neq 0$ per ogni i e j, si provi per induzione su n che

$$\det \mathbf{A} = \frac{\prod_{i>j} (x_i - x_j)(y_i - y_j)}{\prod_{i,j} (x_i + y_j)}.$$

(Suggerimento: sottrarre l'ultima colonna da ciascuna delle precedenti; usare che, per $j \neq n$,

$$(x_i + y_j)^{-1} - (x_i + y_n)^{-1} = (y_n - y_j)(x_i + y_n)^{-1}(x_i + y_j)^{-1};$$

raccogliere i fattori comuni nelle righe e nelle colonne; si ottiene una matrice che differisce da quella originaria perché ha tutti 1 sull'ultima colonna. Sottrarre ora l'ultima riga dalla precedente, raccogliere i fattori comuni nelle righe e ridursi a una matrice dello stesso tipo e di ordine $n-1$.)

4.18. Dato il polinomio monico $f(X) = X^n + a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + \cdots + a_1 X + a_0$, si chiama *matrice compagna* di $f(X)$ la matrice $n \times n$

$$\mathbf{A} = \begin{bmatrix} 0 & 0 & \dots & 0 & 0 & -a_0 \\ 1 & 0 & \dots & 0 & 0 & -a_1 \\ 0 & 1 & \dots & 0 & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 & -a_{n-2} \\ 0 & 0 & \dots & 0 & 1 & -a_{n-1} \end{bmatrix}$$

Si provi che $\det(X\mathbf{I}_n - \mathbf{A}) = f(X)$.

4.19. Si consideri la matrice tri-diagonale

$$\mathbf{A} = \begin{bmatrix} a_1 & b_1 & 0 & \dots & 0 & 0 & 0 \\ c_1 & a_2 & b_2 & \dots & 0 & 0 & 0 \\ 0 & c_2 & a_3 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & a_{n-2} & b_{n-2} & 0 \\ 0 & 0 & 0 & \dots & c_{n-2} & a_{n-1} & b_{n-1} \\ 0 & 0 & 0 & \dots & 0 & c_{n-1} & a_n \end{bmatrix}.$$

Si provi per induzione su n che

$$\det \mathbf{A} = a_n \det \mathbf{A}_{n-1} - b_{n-1} c_{n-1} \det \mathbf{A}_{n-2},$$

dove $\mathbf{A}_{n-1}$ e $\mathbf{A}_{n-2}$ sono le sottomatrici principali $(n-1)$-esima e $(n-2)$-esima rispettivamente.

Capitolo 5

Autovalori e autovettori

Le nozioni di autovalore e autovettore di una matrice sono basilari sia in Algebra Lineare che nello studio delle equazioni differenziali. A ogni autovalore resta associato un autospazio; l'insieme degli autovalori di una matrice costituisce il suo *spettro* che, con l'insieme degli autovettori, forma l'*autosistema* della matrice.

In questo Capitolo forniremo i fatti fondamentali sugli autosistemi delle matrici e illustreremo le loro connessioni con i problemi di diagonalizzazione e triangolarizzazione. Quest'ultima decomposizione, che vale per ogni matrice quadrata, è un fondamentale teorema dovuto a Schur e sta alla base di molti risultati che vedremo nel prossimo Capitolo.

Questo Capitolo si chiude con due classici risultati sul polinomio caratteristico di una matrice (Teorema di Hamilton-Cayley) e sulla dislocazione nel piano complesso degli autovalori (Teorema di Gerschgorin).

Come preambolo al Capitolo, a motivazione dello studio degli autosistemi, viene illustrato il semplice modello discreto detto "preda-predatore".

1. Un esempio di modello discreto

Per introdurre il lettore alla teoria degli autovalori e autovettori, viene presentata in questo Paragrafo la versione linearizzata discreta del "modello preda-predatore", originariamente sviluppato da Lotka (biofisico americano, 1880–1949) e da Volterra (matematico italiano, 1860–1940) tramite due equazioni differenziali non lineari del primo ordine. Il modello discreto, che si differenzia notevolmente da quello di Lotka-Volterra, bene si presta per fare capire l'utilità e il significato di autovalori e autovettori; per la sua comprensione è sufficiente la conoscenza del prodotto "righe per colonne" tra matrici.

Vediamo allora un caso particolare di questo modello, che si ispira all'esempio di popolazioni in competizione presentato nel Capitolo 2 del libro di B. Noble e J. W. Daniel: "Applied Linear Algebra" (Prentice Hall, 1988).

A un certo istante iniziale t_0 sono presenti in un territorio un numero P_0 di animali predatori e un numero p_0 di prede. In assenza di prede, i predatori tenderebbero a estinguersi velocemente. Supponiamo che all'istante t_{i+1} il numero di predatori P_{i+1} sia una frazione del numero P_i all'istante t_i, per esempio

$$P_{i+1} = \frac{3}{5}P_i.$$

Ma in presenza di prede, il numero P_{i+1} aumenta proporzionalmente al numero di prede p_i presenti all'istante precedente; supponiamo per esempio che

$$P_{i+1} = \frac{3}{5}P_i + \frac{1}{2}p_i.$$

Simmetricamente, in assenza di predatori le prede tenderebbero ad aumentare nel tempo; supponiamo che all'istante t_{i+1} il numero di prede p_{i+1} sia aumentato rispetto al numero di prede all'istante precedente p_i secondo un certo fattore di proporzionalità; sia per esempio

$$p_{i+1} = \frac{6}{5}p_i.$$

Ma, in presenza di predatori, il numero p_{i+1} decresce esattamente del numero di prede uccise dai predatori nell'intervallo di tempo $[t_i, t_{i+1}]$. Se k denota il numero medio di prede uccise in un intervallo temporale da ciascun predatore, risulta

$$p_{i+1} = \frac{6}{5}p_i - kP_i.$$

Si suppone che il numero k sia costante nel tempo. Si chiama *vettore della popolazione* all'istante t_i la coppia ordinata di numeri

$$\mathbf{v}_i = \begin{bmatrix} P_i \\ p_i \end{bmatrix}.$$

Il modello preda-predatore è quindi completamente descritto dalle due equazioni

$$\begin{aligned} P_{i+1} &= \frac{3}{5}P_i + \frac{1}{2}p_i \\ p_{i+1} &= -kP_i + \frac{6}{5}p_i \end{aligned}$$

nonché dal vettore della popolazione iniziale $\mathbf{v}_0$. La matrice

$$\mathbf{A}(k) = \begin{bmatrix} 3/5 & 1/2 \\ -k & 6/5 \end{bmatrix}$$

permette di scrivere le equazioni del modello in forma matriciale

$$\mathbf{v}_{i+1} = \mathbf{A}(k)\mathbf{v}_i, \qquad (i = 0, 1, 2, \ldots).$$

Per ogni $i > 0$ si ha dunque

$$\mathbf{v}_i = \mathbf{A}(k)\mathbf{v}_{i-1} = \mathbf{A}(k)^2\mathbf{v}_{i-2} = \mathbf{A}(k)^3\mathbf{v}_{i-3} = \cdots = \mathbf{A}(k)^i\mathbf{v}_0,$$

quindi l'andamento del vettore della popolazione nel tempo dipende dalle potenze della matrice $\mathbf{A}(k)$. Scopo del modello è predire cosa avverrà nel tempo del vettore della popolazione.

Facciamo tre simulazioni per il parametro k, numero medio di prede uccise in un intervallo temporale da ciascun predatore, e vediamo cosa succede del vettore della popolazione, partendo da una situazione iniziale rappresentata dal vettore

$$\mathbf{v}_0 = \begin{bmatrix} 100 \\ 1000 \end{bmatrix}.$$

Verranno rappresentati in tre tabelle i numeri di predatori e prede in diversi istanti t_i. Naturalmente tali numeri saranno arrotondati all'unità.

SIMULAZIONE 1: $k = 10/100$

	t_0	t_1	t_2	t_3	t_4	t_{15}	t_{29}	t_{99}
P_i	100	560	931	1244	1523	5107	19409	15328199
p_i	1000	1190	1372	1553	1739	5111	19409	15328199

Come si vede, le due popolazioni tendono a crescere, quella dei predatori più velocemente di quella delle prede, diventando da un certo istante in poi uguali. Al tendere del tempo all'infinito le due popolazioni tendono a crescere indefinitamente.

Sinteticamente: i predatori predano troppo poco. Il parametro k deve aumentare perché le due popolazioni non si espandano troppo. Ritocchiamo allora in aumento il parametro k portandolo da 10/100 a 18/100.

SIMULAZIONE 2: $k = 18/100$

	t_0	t_1	t_2	t_3	t_4	t_{15}	t_{29}	t_{59}	t_{79}	t_{99}
P_i	100	560	927	1214	1434	1654	713	43	3	0
p_i	1000	1182	1317	1413	1477	1177	459	25	2	0

Si vede che, dopo una buona espansione iniziale, pari quasi a quella del caso precedente, le due popolazioni delle prede e dei predatori diminuiscono entrambi gradualmente fino ad azzerarsi.

Sinteticamente: i predatori predano troppo. Il parametro k deve diminuire perché le due popolazioni non si esauriscano. Ritocchiamo allora di molto poco in decremento il parametro k, passando da 18/100 a 16/100.

SIMULAZIONE 3: $k = 16/100$

	t_0	t_1	t_2	t_3	t_4	t_{32}	t_{64}	t_{99}
P_i	100	560	928	1222	1457	2408	2400	2400
p_i	1000	1184	1331	1448	1542	1912	1920	1920

Si vede che le due popolazioni all'inizio tendono a crescere in una misura che è a metà strada tra i due casi precedenti e che per valori grandi del tempo si stabilizzano sulle quantità $P = 2400$ e $p = 1920$. Si è così raggiunto l'equilibrio.

È naturale chiedersi da che cosa dipende essenzialmente il diverso comportamento del modello nei tre casi simulati, e se i valori dati al vettore della popolazione all'istante iniziale sono un fattore influente oppure no. La risposta, come mostreremo di seguito, è che il comportamento del modello dipende da due numeri individuati dalla matrice $\mathbf{A}(k)$, che si chiamano gli autovalori della matrice e, più precisamente, dal fatto che il più grande degli autovalori sia minore, uguale o maggiore di 1. Inoltre, il vettore della popolazione iniziale influenza il comportamento del modello nel tempo, contrariamente a quanto accade in altri modelli rappresentati da matrici a coefficienti non negativi. Per pervenire alla risposta occorre "diagonalizzare" la matrice $\mathbf{A}(k)$ o, se ciò non è possibile, "triangolarizzarla".

Diagonalizzazione e triangolarizzazione di $\mathbf{A}(k)$

La matrice $\mathbf{A}(k)$ può essere "trattata" in modo diverso nei tre casi considerati nelle simulazioni precedenti.

CASO 1: $k = 10/100$

Se $k = 10/100 = 1/10$ la matrice $\mathbf{A}(1/10)$ si può fattorizzare nel prodotto di tre matrici nel modo seguente

$$\mathbf{A}(1/10) = \begin{bmatrix} 1 & 5 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 11/10 & 0 \\ 0 & 7/10 \end{bmatrix} \begin{bmatrix} -1/4 & 5/4 \\ 1/4 & -1/4 \end{bmatrix}.$$

Si noti che il primo fattore, chiamiamolo $\mathbf{S}$, è la matrice inversa del terzo fattore, che denotiamo quindi con $\mathbf{S}^{-1}$. Il secondo fattore, chiamiamolo $\mathbf{D}$, è una matrice diagonale. Si dice che la matrice $\mathbf{A}(1/10)$ è stata diagonalizzata.

Posto $\mathbf{A} = \mathbf{A}(1/10)$, l'uguaglianza $\mathbf{A} = \mathbf{SDS}^{-1}$ è equivalente a $\mathbf{AS} = \mathbf{SD}$ che, letta sulle due colonne, porge:

$$\mathbf{A}\begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{11}{10}\begin{bmatrix} 1 \\ 1 \end{bmatrix}$$
$$\mathbf{A}\begin{bmatrix} 5 \\ 1 \end{bmatrix} = \frac{7}{10}\begin{bmatrix} 5 \\ 1 \end{bmatrix}.$$

Ciò si esprime dicendo che i due vettori

$$\mathbf{v}_1 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \quad \mathbf{v}_2 = \begin{bmatrix} 5 \\ 1 \end{bmatrix}$$

sono *autovettori* della matrice relativi rispettivamente agli *autovalori* $\lambda_1 = 11/10$ e $\lambda_2 = 7/10$, giacché valgono le uguaglianze $A\mathbf{v}_i = \lambda_i \mathbf{v}_i$ $(i = 1, 2)$.

A cosa serve tutto ciò? E da dove saltano fuori i numeri 11/10 e 7/10 che, come vedremo, risultano cruciali per il modello?

La diagonalizzazione di A è utile per calcolare facilmente le potenze della matrice A. Infatti è immediato verificare induttivamente che per ogni intero positivo n si ha

$$\mathbf{A}^n = \mathbf{SD}^n\mathbf{S}^{-1}$$

dove

$$\mathbf{D}^n = \begin{bmatrix} (11/10)^n & 0 \\ 0 & (7/10)^n \end{bmatrix}.$$

Si può allora concludere che, fissato il vettore della popolazione $[P_0, p_0]^T$ all'istante t_0, per ogni n risulta

$$\begin{aligned}
\begin{bmatrix} P_n \\ p_n \end{bmatrix} = \mathbf{A}^n \begin{bmatrix} P_0 \\ p_0 \end{bmatrix} &= \begin{bmatrix} 1 & 5 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} (11/10)^n & 0 \\ 0 & (7/10)^n \end{bmatrix} \begin{bmatrix} -1/4 & 5/4 \\ 1/4 & -1/4 \end{bmatrix} \begin{bmatrix} P_0 \\ p_0 \end{bmatrix} \\
&= \begin{bmatrix} (11/10)^n & 5(7/10)^n \\ (11/10)^n & (7/10)^n \end{bmatrix} \begin{bmatrix} -(1/4)P_0 + (5/4)p_0 \\ (1/4)P_0 - (1/4)p_0 \end{bmatrix} \\
&= \begin{bmatrix} (11/10)^n(-(1/4)P_0 + (5/4)p_0) + (7/10)^n((5/4)P_0 - (5/4)p_0) \\ (11/10)^n(-(1/4)P_0 + (5/4)p_0) + (7/10)^n(P_0 - (1/4)p_0) \end{bmatrix}.
\end{aligned}$$

Evidentemente sia P_n che p_n tendono all'infinito al tendere di n all'infinito se e solo se vale la seguente condizione

$$\frac{5}{4}p_0 - \frac{1}{4}P_0 > 0,$$

e ciò dipende dal fatto che $\lambda_1 = 11/10 > 1$. Se invece risulta

$$\frac{5}{4}p_0 - \frac{1}{4}P_0 \leq 0,$$

allora sia P_n che p_n si azzerano a un certo istante t_n. Il lettore può verificare che, posto per esempio $P_0 = 50$ e $p_0 = 10$, le prede si azzerano all'istante t_8 e i predatori all'istante t_{10}.

Nel caso della Simulazione 1, i valori $P_0 = 100$ e $p_0 = 1000$ comportano che

$$\frac{5}{4} \cdot 1000 - \frac{1}{4} \cdot 100 = 1225 > 0$$

e quindi la popolazione tende a espandersi indefinitamente.

CASO 2: $k = 18/100$

Se $k = 18/100 = 9/50$ la matrice $\mathbf{A}(9/50)$ si può fattorizzare nel prodotto di tre matrici nel modo seguente

$$\mathbf{A}(9/50) = \begin{bmatrix} 5/\sqrt{34} & -3/\sqrt{34} \\ 3/\sqrt{34} & 5/\sqrt{34} \end{bmatrix} \begin{bmatrix} 9/10 & 17/25 \\ 0 & 9/10 \end{bmatrix} \begin{bmatrix} 5/\sqrt{34} & 3/\sqrt{34} \\ -3/\sqrt{34} & 5/\sqrt{34} \end{bmatrix}.$$

Si noti che il primo fattore, chiamiamolo $\mathbf{Q}$, è la matrice inversa del terzo fattore, che denotiamo quindi con $\mathbf{Q}^{-1}$; ma, di più, risulta $\mathbf{Q}^{-1} = \mathbf{Q}^T$, quindi la matrice $\mathbf{Q}$ è una matrice ortogonale. Il secondo fattore, chiamiamolo $\mathbf{T}$, è una matrice triangolare superiore. Si dice che la matrice $\mathbf{A}(9/50)$ è stata triangolarizzata ortogonalmente. Sulla diagonale di $\mathbf{T}$ compaiono ancora gli autovalori di $\mathbf{A}$, quindi $\lambda_1 = \lambda_2 = 9/10$ è autovalore doppio di $\mathbf{A}$.

La triangolarizzazione di $\mathbf{A}$ è ancora utile per calcolare le potenze della matrice $\mathbf{A}$, anche se c'è qualche problema in più rispetto a quando la matrice è diagonalizzabile. Infatti è immediato verificare induttivamente che per ogni intero positivo n si ha

$$\mathbf{A}^n = \mathbf{Q}\mathbf{T}^n\mathbf{Q}^{-1}$$

dove

$$\mathbf{T}^n = \begin{bmatrix} (9/10)^n & n(9/10)^{n-1}(17/25) \\ 0 & (9/10)^n \end{bmatrix}.$$

Poiché $\mathbf{T}^n$ tende alla matrice nulla al tendere di n all'infinito (e questo perché l'unico autovalore $9/10$ è minore di 1), ne consegue che il vettore della popolazione $[P_n\ p_n]^T$ tende ad annullarsi qualunque sia il vettore della popolazione $[P_0\ p_0]^T$ all'istante iniziale.

CASO 3: $k = 16/100 = 4/25$

Se $k = 16/100$ la matrice $\mathbf{A}(4/25)$ si può fattorizzare nel prodotto di tre matrici nel modo seguente:

$$\mathbf{A}(4/25) = \begin{bmatrix} 5 & 5 \\ 4 & 2 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 4/5 \end{bmatrix} \begin{bmatrix} -1/5 & 1/2 \\ 2/5 & -1/2 \end{bmatrix}.$$

Si noti che il primo fattore, chiamiamolo $\mathbf{U}$, è la matrice inversa del terzo fattore, che denotiamo quindi con $\mathbf{U}^{-1}$. Il secondo fattore, chiamiamolo $\mathbf{\Lambda}$, è una matrice diagonale. Quindi la matrice $\mathbf{A}(4/25)$ è stata diagonalizzata e i suoi autovalori sono $\lambda_1 = 1$ e $\lambda_2 = 4/5$.

La diagonalizzazione di $\mathbf{A}$ ci permette, come nel Caso 1, di calcolare facilmente le potenze della matrice $\mathbf{A} = \mathbf{A}(4/25)$. Si ha quindi per ogni $n \geq 1$:

$$\mathbf{A}^n = \mathbf{U}\mathbf{\Lambda}^n\mathbf{U}^{-1}$$

dove

$$\mathbf{\Lambda}^n = \begin{bmatrix} 1 & 0 \\ 0 & (4/5)^n \end{bmatrix}.$$

Si può allora concludere che, fissato il vettore della popolazione $[P_0\ p_0]^T$ all'istante t_0, per ogni n risulta

$$\begin{aligned}
\begin{bmatrix} P_n \\ p_n \end{bmatrix} = \mathbf{A}^n \begin{bmatrix} P_0 \\ p_0 \end{bmatrix} &= \begin{bmatrix} 5 & 5 \\ 4 & 2 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & (4/5)^n \end{bmatrix} \begin{bmatrix} -1/5 & 1/2 \\ 2/5 & -1/2 \end{bmatrix} \begin{bmatrix} P_0 \\ p_0 \end{bmatrix} \\
&= \begin{bmatrix} 5 & 5(4/5)^n \\ 4 & 2(4/5)^n \end{bmatrix} \begin{bmatrix} -(1/5)P_0 + (1/2)p_0 \\ (2/5)P_0 - (1/2)p_0 \end{bmatrix} \\
&= \begin{bmatrix} -P_0 + (5/2)p_0 + (4/5)^n(2P_0 - (5/2)p_0) \\ -(4/5)P_0 + 2p_0 + (4/5)^n((4/5)P_0 - p_0) \end{bmatrix}.
\end{aligned}$$

Evidentemente per n che tende all'infinito il vettore della popolazione $[P_n\ p_n]^T$ tende al vettore

$$\begin{bmatrix} -P_0 + (5/2)p_0 \\ -(4/5)P_0 + 2p_0 \end{bmatrix}.$$

Perché ciò abbia significato occorre che $5p_0 > 2P_0$, perché in caso contrario la popolazione giunge ad azzerarsi per qualche valore del tempo t_n.

Nel caso della Simulazione 3, i valori $P_0 = 100$ e $p_0 = 1000$ comportano che $5 \cdot 1000 > 2 \cdot 100$ e quindi la popolazione tende al valore limite

$$\begin{bmatrix} -100 + (5/2) \cdot 1000 \\ -(4/5) \cdot 100 + 2 \cdot 1000 \end{bmatrix} = \begin{bmatrix} 2400 \\ 1920 \end{bmatrix}.$$

È naturale chiedersi a questo punto: come si trovano gli autovalori della matrice $\mathbf{A}(k)$? Diamo qui il procedimento in questo caso specifico, rinviando ai Paragrafi successivi per la spiegazione di come vi si perviene.

Per trovare gli autovalori di $\mathbf{A}(k)$ bisogna per prima cosa trovarne il polinomio caratteristisco, che si ottiene calcolando il determinante della matrice

$$\mathbf{A}(k) - X\mathbf{I} = \begin{bmatrix} 3/5 & 1/2 \\ -k & 6/5 \end{bmatrix} - \begin{bmatrix} X & 0 \\ 0 & X \end{bmatrix} = \begin{bmatrix} 3/5 - X & 1/2 \\ -k & 6/5 - X \end{bmatrix}.$$

Si ricava il polinomio

$$p(X) = X^2 - \frac{9}{5}X + \frac{18}{25} + \frac{1}{2}k.$$

Gli autovalori di $\mathbf{A}(k)$ non sono che le radici di questo polinomio, cioè

$$\lambda_1 = \frac{9 + (9 - 50k)^{1/2}}{10}, \quad \lambda_2 = \frac{9 - (9 - 50k)^{1/2}}{10}.$$

Noi ci limiteremo a considerare autovalori reali, perché con autovalori complessi la diagonalizzazione perde di significato concreto, pur restando utile per il calcolo delle potenze della matrice. Si hanno radici reali per $k \le 9/50$, e due radici coincidenti con $\lambda = 9/10$ per $k = 9/50$, cioè quanto previsto nella seconda simulazione. Sempre per $k \le 9/50$, il più grande autovalore λ_1 è maggiore, uguale o minore di 1 a seconda che risulta $k < 8/50$, $k = 8/50$ o $k > 8/50$; l'ipotesi $k = 8/50$ è quanto previsto nella terza simulazione.

Una volta trovati gli autovalori λ_i, si cercano i corrispondenti autovettori, cioè dei vettori non nulli $\mathbf{v}_i$ tali che

$$\mathbf{A}(k)\mathbf{v}_i = \lambda_i \mathbf{v}_i$$

o, equivalentemente,

$$\mathbf{v}_i \in \mathrm{N}(\mathbf{A}(k) - \lambda_i \mathbf{I}),$$

dove $\mathrm{N}(\mathbf{X})$ denota lo spazio nullo della matrice $\mathbf{X}$.

Le uguaglianze $\mathbf{A}(k)\mathbf{v}_i = \lambda_i \mathbf{v}_i$ $(i = 1, 2)$ sono equivalenti a

$$\mathbf{A}(k)\mathbf{S} = \mathbf{S} \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}$$

dove $\mathbf{S} = [\mathbf{v}_1 \ \mathbf{v}_2]$. $\mathbf{S}$ è una matrice invertibile se e solo se i due vettori $\mathbf{v}_1$ e $\mathbf{v}_2$ sono linearmente indipendenti, il che sicuramente accade se $\lambda_1 \ne \lambda_2$, per un risultato che vedremo nel Paragrafo 4. Se $\lambda_1 \neq \lambda_2$ si può quindi sempre diagonalizzare la matrice $\mathbf{A}(k)$, come si è fatto nel primo e nel terzo caso.

Se invece $\lambda_1 = \lambda_2$, la possibilità di diagonalizzare $\mathbf{A}(k)$ dipende dal fatto di poter trovare due autovettori $\mathbf{v}_1$ e $\mathbf{v}_2$ che siano linearmente indipendenti. Nel caso di $k = 8/50$ ciò non è possibile, quindi $\mathbf{A}(8/50)$ non si può diagonalizzare.

Interviene però a questo punto un altro risultato che vedremo nel Paragrafo 5, il Teorema di triangolarizzazione di Schur, che assicura che ogni matrice quadrata complessa è unitariamente triangolarizzabile; se poi la matrice è reale con autovalori reali, essa è triangolarizzabile con una matrice reale ortogonale.

2. Generalità su autovalori e autospazi

Siano $\mathbf{A}$ una matrice $n \times n$ a coefficienti in K, dove K denota un campo che per noi sarà sempre $\mathbb{R}$ o $\mathbb{C}$. Sia $f_\mathbf{A}\colon K^n \to K^n$ l'applicazione lineare indotta da $\mathbf{A}$: $f_\mathbf{A}(\mathbf{v}) = \mathbf{Av}$ per ogni $\mathbf{v} \in K^n$.

È chiaro che maggiore è il numero dei coefficienti nulli di $\mathbf{A}$, minore è la difficoltà di calcolo di $f_\mathbf{A}(\mathbf{v}) = \mathbf{Av}$ per un generico vettore $\mathbf{v} \in K^n$. In particolare, come abbiamo già osservato nel Capitolo 1, se $\mathbf{A} = \mathbf{D} = \mathbf{Diag}(d_1, \dots, d_n)$ allora

$$f_\mathbf{D}\left(\begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}\right) = \begin{bmatrix} d_1 v_1 \\ \vdots \\ d_n v_n \end{bmatrix}$$

per ogni $[v_1 \ \dots \ v_n]^T \in K^n$ e se $\mathbf{A} = \lambda \mathbf{I}_n$ allora $f_\mathbf{A}(\mathbf{v}) = \lambda \mathbf{v}$.

Vedremo ora che anche nel caso in cui $\mathbf{A}$ non sia una matrice scalare, oltre al vettore nullo possono esistere (ed esistono certamente quando $K = \mathbb{C}$) vettori non nulli di K^n tali che la loro pre-moltiplicazione per $\mathbf{A}$ equivale alla moltiplicazione per un opportuno scalare.

Svilupperemo una teoria che ci permetterà di trovare condizioni necessarie e sufficienti su $\mathbf{A}$ affinché esista una base $\mathscr{B}$ di K^n costituita da vettori di tale tipo. Nel caso in cui ciò avvenga, la matrice associata a $f_\mathbf{A}$ rispetto a $\mathscr{B}$ è una matrice diagonale $\mathbf{D}$, per cui $f_\mathbf{A}$ ammette una fattorizzazione del tipo $f_\mathbf{A} = g f_\mathbf{D} g^{-1}$, per un opportuno isomorfismo g di K^n in sé, e la matrice $\mathbf{A}$ ammette corrispondentemente una fattorizzazione del tipo $\mathbf{A} = \mathbf{SDS}^{-1}$ dove $\mathbf{S}$ è una matrice invertibile.

Cominciamo con il risolvere i due seguenti problemi:

(i) stabilire per quali $\lambda \in K$ esistono sottospazi non nulli U di K^n tali che la restrizione di $f_\mathbf{A}$ a U coincide con la moltiplicazione per λ;

(ii) in corrispondenza di ciascuno di tali $\lambda \in K$ trovare il massimo sottospazio di K^n su cui $f_\mathbf{A}$ coincide con la moltiplicazione per λ.

Osserviamo innanzitutto che se U è un sottospazio di K^n su cui la restrizione di $f_\mathbf{A}$ coincide con la moltiplicazione per $\lambda \in K$, allora $\mathbf{Au} = \lambda \mathbf{u}$ appartiene a U, per ogni $\mathbf{u} \in U$. Più in generale si pone la seguente

Definizione. Siano $\mathbf{A}$ una matrice $n \times n$ a coefficienti in K e U un sottospazio di K^n. Il sottospazio U si dice $\mathbf{A}$-*invariante* (o anche $f_\mathbf{A}$-*invariante*) se $f_\mathbf{A}(\mathbf{u}) = \mathbf{A}\mathbf{u} \in U$ per ogni $\mathbf{u} \in U$.

Esempio 2.1. (a) $\{\mathbf{0}\}$ e K^n sono sottospazi $\mathbf{A}$-invarianti.

(b) Lo spazio nullo $\mathrm{N}(\mathbf{A})$ e lo spazio delle colonne $\mathrm{C}(\mathbf{A})$ di $\mathbf{A}$ sono sottospazi $\mathbf{A}$-invarianti.

Lasciamo da verificare come esercizio (si veda l'Esercizio 2.1) che la somma e l'intersezione di sottospazi $\mathbf{A}$-invarianti di K^n sono sottospazi $\mathbf{A}$-invarianti. □

Si osservi che uno scalare $\lambda \in K$ è soluzione del problema (i) se e solo se esiste un sottospazio unidimensionale U di K^n tale che la restrizione di $f_\mathbf{A}$ a U coincida con la moltiplicazione per λ, e quindi se e solo se esiste $\mathbf{0} \neq \mathbf{u} \in K^n$ tale che $\mathbf{A}\mathbf{u} = \lambda\mathbf{u}$.

Si pone allora la seguente definizione.

Definizione. Uno scalare $\lambda \in K$ tale che esista $\mathbf{0} \neq \mathbf{v} \in K^n$ per cui $\mathbf{A}\mathbf{v} = \lambda\mathbf{v}$ si dice un *autovalore* della matrice $\mathbf{A}$. L'insieme degli autovalori distinti di $\mathbf{A}$ si dice lo *spettro* di $\mathbf{A}$.

Dunque gli autovalori della matrice $\mathbf{A}$ sono le soluzioni del problema (i). È fondamentale ricordare che il vettore $\mathbf{v}$ di cui si richiede l'esistenza nella precedente definizione deve essere non nullo: infatti l'uguaglianza $\mathbf{A}\mathbf{0} = \lambda\mathbf{0}$ è verificata per ogni $\lambda \in K$.

Esempio 2.2. Sia $\mathbf{P}$ una matrice di proiezione complessa (per cui $K = \mathbb{C}$) di ordine n. Abbiamo visto (Capitolo 3, Paragrafo 6) che $\mathbb{C}^n = \mathrm{N}(\mathbf{P}) \oplus \mathrm{C}(\mathbf{P})$ e che la restrizione di $f_\mathbf{P}$ a $\mathrm{C}(\mathbf{P})$ è l'identità.

Se $\mathbf{P} = \mathbb{O}$ allora $\mathbb{C}^n = \mathrm{N}(\mathbf{P})$ e l'unico autovalore di $\mathbf{P}$ è $\lambda = 0$ (e quindi lo spettro di $\mathbf{P}$ è $\{0\}$); se $\mathbf{P}$ è invertibile allora $\mathbb{C}^n = \mathrm{C}(\mathbf{P})$ e l'unico autovalore di $\mathbf{P}$ è $\lambda = 1$ (e quindi lo spettro di $\mathbf{P}$ è $\{1\}$); infine se $\mathrm{N}(\mathbf{P}) \neq \{\mathbf{0}\} \neq \mathrm{C}(\mathbf{P})$, sia 0 che 1 sono autovalori di $\mathbf{P}$. Mostriamo che $\mathbf{P}$ non ha altri autovalori, ossia che lo spettro di $\mathbf{P}$ è $\{0, 1\}$. Siano dunque $\lambda \in \mathbb{C}$ un autovalore di $\mathbf{P}$ e $\mathbf{0} \neq \mathbf{v} \in \mathbb{C}^n$ tale che $\mathbf{P}\mathbf{v} = \lambda\mathbf{v}$. Da $\mathbf{P} = \mathbf{P}^2$ segue che $\lambda\mathbf{v} = \mathbf{P}\mathbf{v} = \mathbf{P}^2\mathbf{v} = \mathbf{P}(\lambda\mathbf{v}) = \lambda\mathbf{P}\mathbf{v} = \lambda^2\mathbf{v}$, per cui $(\lambda - \lambda^2)\mathbf{v} = \mathbf{0}$. Da $\mathbf{v} \neq \mathbf{0}$ si ottiene allora $\lambda - \lambda^2 = 0$, e quindi $\lambda \in \{0, 1\}$. □

Il seguente esempio mostra che il problema (i) può non avere soluzione se $K = \mathbb{R}$.

Esempio 2.3. Si consideri la matrice *reale* 2×2

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

e si osservi che $\mathbf{A}^2 = -\mathbf{I}_2$. Se $\mathbf{A}$ avesse un autovalore *reale* λ, esisterebbe un vettore $\mathbf{0} \neq \mathbf{v} \in \mathbb{R}^2$ tale che $\mathbf{A}\mathbf{v} = \lambda\mathbf{v}$. Premoltiplicando per $\mathbf{A}$ si otterrebbe

$$-\mathbf{v} = -\mathbf{I}_2\mathbf{v} = \mathbf{A}^2\mathbf{v} = \mathbf{A}(\mathbf{A}\mathbf{v}) = \mathbf{A}\lambda\mathbf{v} = \lambda\mathbf{A}\mathbf{v} = \lambda^2\mathbf{v},$$

e quindi, essendo $\mathbf{v} \neq \mathbf{0}$, $\lambda^2 = -1$, che non è possibile per alcun numero $\lambda \in \mathbb{R}$. □

Si usa la seguente terminologia relativamente ai sottospazi di K^n minimali e massimali (rispetto all'inclusione) su cui la pre-moltiplicazione per $\mathbf{A}$ coincide con la moltiplicazione per lo scalare λ.

Definizione. (1) Se $\lambda \in K$ è un autovalore di $\mathbf{A}$, ogni vettore $\mathbf{0} \neq \mathbf{v} \in K^n$ per cui si ha $\mathbf{A}\mathbf{v} = \lambda\mathbf{v}$ si dice un *autovettore di* $\mathbf{A}$ *relativo a* λ.

(2) Se $\lambda \in K$ è un autovalore di $\mathbf{A}$, il massimo sottospazio di K^n su cui $f_{\mathbf{A}}$ equivale alla moltiplicazione per λ si dice l'*autospazio di* $\mathbf{A}$ *relativo a* λ e si indica con il simbolo $\mathrm{E}_{\mathbf{A}}(\lambda)$. Risulta pertanto:

$$\mathrm{E}_{\mathbf{A}}(\lambda) = \{\mathbf{v} \in K^n \mid \mathbf{A}\mathbf{v} = \lambda\mathbf{v}\}.$$

La dimensione dello spazio vettoriale $\mathrm{E}_{\mathbf{A}}(\lambda)$ si chiama *molteplicità geometrica* di λ e si indica con il simbolo $d(\lambda)$. L'insieme degli autovalori di $\mathbf{A}$ e dei corrispondenti autospazi si chiama l'*autosistema di* $\mathbf{A}$.

Pertanto gli autospazi della matrice $\mathbf{A}$ sono le soluzioni del problema (ii); inoltre per ogni autovalore λ di $\mathbf{A}$, l'autospazio $\mathrm{E}_{\mathbf{A}}(\lambda)$ è costituito dal vettore nullo e da tutti gli autovettori di $\mathbf{A}$ relativi a λ. Osserviamo che $\mathrm{E}_{\mathbf{A}}(\lambda) = \{\mathbf{v} \in K^n \mid (\mathbf{A} - \lambda\mathbf{I})\mathbf{v} = \mathbf{0}\} = \mathrm{N}(\mathbf{A} - \lambda\mathbf{I})$, pertanto $d(\lambda)$ coincide con la nullità della matrice $\mathbf{A} - \lambda\mathbf{I}$.

Esempio 2.4. Tornando all'Esempio 2.2 si ha che se $\mathbf{P} = \mathbb{O}$ ogni vettore di $\mathbb{C}^n \setminus \{\mathbf{0}\}$ è un autovettore di $\mathbf{P}$ relativo all'autovalore 0 ed $\mathrm{E}_{\mathbf{P}}(0) = \mathrm{N}(\mathbf{P}) = \mathbb{C}^n$. Se $\mathbf{P}$ è invertibile ogni vettore di $\mathbb{C}^n \setminus \{\mathbf{0}\}$ è un autovettore di $\mathbf{P}$ relativo all'autovalore 1 ed $\mathrm{E}_{\mathbf{P}}(1) = \mathbb{C}^n$. Se infine $\mathrm{N}(\mathbf{P}) \neq \{\mathbf{0}\} \neq \mathrm{C}(\mathbf{P})$, ogni vettore di $\mathrm{N}(\mathbf{P}) \setminus \{\mathbf{0}\}$ è un autovettore di $\mathbf{P}$ relativo all'autovalore 0 e ogni vettore di $\mathrm{C}(\mathbf{P}) \setminus \{\mathbf{0}\}$ è un autovettore di $\mathbf{P}$ relativo all'autovalore 1.

Mostriamo che $\mathrm{E}_{\mathbf{P}}(1)$, l'autospazio di $\mathbf{P}$ relativo all'autovalore 1, coincide con $\mathrm{C}(\mathbf{P})$.

Se $U \gneq \mathrm{C}(\mathbf{P})$ è un sottospazio $\mathbf{P}$-invariante di $\mathbb{C}^n$, da $\mathbb{C}^n = \mathrm{N}(\mathbf{P}) \oplus \mathrm{C}(\mathbf{P})$ segue che $U = (U \cap \mathrm{N}(\mathbf{P})) \oplus \mathrm{C}(\mathbf{P})$ e $U \cap \mathrm{N}(\mathbf{P}) \neq \{\mathbf{0}\}$, per cui la restrizione di $f_{\mathbf{P}}$ a U non può coincidere con la moltiplicazione per 1. In modo analogo si prova che $\mathrm{E}_{\mathbf{P}}(0) = \mathrm{N}(\mathbf{P})$.

Si osservi che se 1 è autovalore di $\mathbf{P}$, la sua molteplicità geometrica è $\operatorname{rk}\mathbf{P}$. □

Abbiamo visto che se $\mathbf{P}$ è una matrice idempotente ed hermitiana di ordine n allora $\mathbb{C}^n$ si decompone in somma diretta di autospazi di $\mathbf{P}$. Il seguente esempio mostra che esistono matrici $n \times n$ per cui $\mathbb{C}^n$ non è somma diretta di loro autospazi.

Esempio 2.5. Siano

$$\mathbf{B} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix},$$

λ un autovalore di $\mathbf{B}$ e $[x\ y]^T$ un autovettore di $\mathbf{B}$ relativo a λ. Allora

$$\begin{bmatrix} x \\ y \end{bmatrix} \neq \begin{bmatrix} 0 \\ 0 \end{bmatrix} \quad \text{e} \quad \begin{bmatrix} x+y \\ y \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \lambda \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} \lambda x \\ \lambda y \end{bmatrix}.$$

Ne segue che l'unico autovalore di $\mathbf{B}$ è $\lambda = 1$ ed $\mathrm{E}_{\mathbf{B}}(\lambda) = \langle \mathbf{e}_1 \rangle$, per cui $\mathbb{C}^2$ non è somma di autospazi di $\mathbf{B}$. □

Vedremo che il fatto che una matrice $n \times n$ sia hermitiana è già una condizione sufficiente affinché $\mathbb{C}^n$ sia somma diretta di suoi autospazi, ma, come mostra il seguente esempio, non necessaria.

Esempio 2.6. Sia

$$\mathbf{C} = \begin{bmatrix} \lambda & 0 \\ \lambda & 0 \end{bmatrix}$$

con $\lambda \in \mathbb{C} \setminus \{0\}$. Da $\mathbf{Ce}_2 = \mathbf{0}$ e $\mathbf{C}(\mathbf{e}_1 + \mathbf{e}_2) = \mathbf{Ce}_1 + \mathbf{Ce}_2 = \lambda(\mathbf{e}_1 + \mathbf{e}_2) + \mathbf{0} = \lambda(\mathbf{e}_1 + \mathbf{e}_2)$ segue che $\mathbb{C}^n = \mathrm{E}_{\mathbf{C}}(0) \oplus \mathrm{E}_{\mathbf{C}}(\lambda)$ dove $\mathrm{E}_{\mathbf{C}}(0) = \langle \mathbf{e}_2 \rangle$ ed $\mathrm{E}_{\mathbf{C}}(\lambda) = \langle \mathbf{e}_1 + \mathbf{e}_2 \rangle$. Dunque $\mathbb{C}^2$ è somma diretta di autospazi di $\mathbf{C}$ pur non essendo $\mathbf{C}$ hermitiana. □

Fissato $\lambda \in \mathbb{C}$ si può sempre definire il sottospazio $\mathrm{E}_{\mathbf{A}}(\lambda)$ di $\mathbb{C}^n$, anche se λ non è un autovalore di $\mathbf{A}$. Per la definizione di autovalore si ha che

$$\lambda \text{ è un autovalore} \iff \{\mathbf{0}\} \neq \mathrm{E}_{\mathbf{A}}(\lambda) = \mathrm{N}(\mathbf{A} - \lambda \mathbf{I}_n). \tag{*}$$

Poiché

$$\mathrm{N}(\mathbf{A} - \lambda \mathbf{I}_n) \neq \{\mathbf{0}\} \iff \mathbf{A} - \lambda \mathbf{I}_n \text{ non è invertibile} \iff \det(\mathbf{A} - \lambda \mathbf{I}_n) = 0,$$

gli autovalori di una matrice $\mathbf{A}$ sono tutte e sole le soluzioni dell'equazione

$$\det(\mathbf{A} - X\mathbf{I}_n) = 0 \tag{**}$$

nell'incognita X, o, equivalentemente, tutte le radici del polinomio $p_{\mathbf{A}}(X) = \det(\mathbf{A} - X\mathbf{I}_n)$ nell'indeterminata X. L'equazione (**) e il polinomio $p_{\mathbf{A}}(X)$ si chiamano rispettivamente l'*equazione caratteristica di* $\mathbf{A}$ e il *polinomio caratteristico di* $\mathbf{A}$. Abbiamo provato allora il seguente risultato.

Proposizione 2.7. *Uno scalare $\lambda \in K$ è un autovalore di* $\mathbf{A}$ *se e solo se λ è soluzione dell'equazione caratteristica di* $\mathbf{A}$*; inoltre se λ è una autovalore di* $\mathbf{A}$ *allora l'autospazio di* $\mathbf{A}$ *relativo a λ risulta*

$$\mathrm{E}_{\mathbf{A}}(\lambda) = \mathrm{N}(\mathbf{A} - \lambda \mathbf{I}_n) \neq \{\mathbf{0}\}.$$

Esempio 2.8. Riprendiamo in considerazione gli Esempi 2.5, 2.6 e 2.3.

Il polinomio caratteristico della matrice

$$\mathbf{B} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

dell'Esempio 2.5 è

$$\begin{aligned} p_{\mathbf{B}}(X) &= \det\left(\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} - X\mathbf{I}_2\right) = \det\left(\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} - \begin{bmatrix} X & 0 \\ 0 & X \end{bmatrix}\right) \\ &= \det \begin{bmatrix} 1-X & 1 \\ 0 & 1-X \end{bmatrix} = (1-X)^2, \end{aligned}$$

la sua equazione caratteristica è $(1-X)^2 = 0$, e quindi, come avevamo già osservato, la matrice $\mathbf{B}$ ha come unico autovalore 1 (contato due volte, dal momento che l'equazione $(1-X)^2 = 0$ è di secondo grado). Inoltre l'autospazio di $\mathbf{B}$ relativo a 1 è

$$\mathrm{E}_{\mathbf{B}}(1) = \mathrm{N}\left(\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} - 1 \cdot \mathbf{I}_2\right) = \mathrm{N}\left(\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\right) = \langle \mathbf{e}_1 \rangle.$$

Il polinomio caratteristico della matrice

$$\mathbf{C} = \begin{bmatrix} \lambda & 0 \\ \lambda & 0 \end{bmatrix}$$

dell'Esempio 2.6, dove $\lambda \in \mathbb{C} \setminus \{0\}$, è

$$\begin{aligned} p_{\mathbf{C}}(X) &= \det\left(\begin{bmatrix} \lambda & 0 \\ \lambda & 0 \end{bmatrix} - X\mathbf{I}_2\right) = \det\left(\begin{bmatrix} \lambda & 0 \\ \lambda & 0 \end{bmatrix} - \begin{bmatrix} X & 0 \\ 0 & X \end{bmatrix}\right) \\ &= \det \begin{bmatrix} \lambda - X & 0 \\ \lambda & -X \end{bmatrix} = -X(\lambda - X), \end{aligned}$$

la sua equazione caratteristica è $-X(\lambda - X) = 0$, e quindi, come avevamo già osservato, la matrice $\mathbf{C}$ ha come autovalori i numeri 0 e λ. Gli autospazi di $\mathbf{C}$ relativi a 0 e λ sono

$$\begin{aligned} \mathrm{E}_{\mathbf{C}}(0) &= \mathrm{N}(\mathbf{C}) = \mathrm{N}\left(\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\right) = \langle \mathbf{e}_2 \rangle \\ \mathrm{E}_{\mathbf{C}}(\lambda) &= \mathrm{N}(\mathbf{C} - \lambda\mathbf{I}_2) = \mathrm{N}\left(\begin{bmatrix} 0 & 0 \\ \lambda & -\lambda \end{bmatrix}\right) = \mathrm{N}\left(\begin{bmatrix} 1 & -1 \\ 0 & 0 \end{bmatrix}\right) = \langle \mathbf{e}_1 + \mathbf{e}_2 \rangle. \end{aligned}$$

Il polinomio caratteristico della matrice

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

considerata nell'Esempio 2.3 è

$$p_{\mathbf{A}}(X) = \det\left(\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\right) - X\mathbf{I}_2) = \det \begin{bmatrix} -X & -1 \\ 1 & -X \end{bmatrix} = X^2 + 1.$$

Poiché $X^2 + 1$ non ha radici reali, $\mathbf{A}$ non ha autovalori reali. Ha però due autovalori complessi distinti: $\lambda_1 = i$ e $\lambda_2 = -i$. Si lascia al lettore come esercizio determinare $\mathrm{E}_{\mathbf{A}}(i)$ e $\mathrm{E}_{\mathbf{A}}(-i)$. □

3. Proprietà del polinomio caratteristico

Dal punto di vista teorico la Proposizione 2.7 risolve entrambi i problemi posti all'inizio del paragrafo. Ma dal punto di vista computazionale, anche quando si ha un'espressione esplicita del polinomio caratteristico di una matrice, il calcolo delle sue radici può presentare problemi, dal momento che non sappiamo risolvere una generica equazione polinomiale di grado qualsiasi.

Osservazione 3.1. La ricerca degli autovalori può risultare più accessibile se si individuano delle proprietà della matrice esprimibili tramite "equazioni" coinvolgenti somme di sue potenze e loro prodotti per scalari. In tal caso, infatti, da esse si ottengono corrispondenti equazioni di cui ogni autovalore deve essere soluzione, e che in generale hanno grado inferiore dell'equazione caratteristica e quindi sono più facilmente trattabili.

Un'illustrazione di questo è nell'Esempio 2.2, dove abbiamo espresso il fatto che una matrice $\mathbf{A}$ sia idempotente tramite "l'equazione" $\mathbf{A}^2 - \mathbf{A} = \mathbb{O}$, e trovato che gli autovalori di $\mathbf{A}$ devono essere soluzioni della corrispondente equazione $X^2 - X = 0$, che è un'equazione facilmente risolvibile, avendo grado 2. Vedremo più avanti che, invece, l'equazione caratteristica di una matrice di ordine n, in particolare di una matrice idempotente di ordine n, ha grado n.

Inversamente, dimostreremo nel Paragrafo 6 il teorema di Hamilton-Cayley che, partendo dal polinomio caratteristico di una generica matrice $\mathbf{A}$, e quindi da una particolare equazione soddisfatta dagli autovalori di $\mathbf{A}$, fornisce una "equazione" che deve essere soddisfatta da $\mathbf{A}$.

C'è una sostanziale differenza tra la fattorizzazione di polinomi a coefficienti reali e quella di polinomi a coefficienti complessi, in particolare di polinomi caratteristici di matrici. Tale differenza è espressa dal seguente risultato.

Teorema Fondamentale dell'Algebra. *Ogni polinomio a coefficienti complessi si fattorizza in fattori di grado* 1 *a coefficienti complessi.*

Per una dimostrazione del Teorema Fondamentale dell'Algebra che fa uso di risultati elementari sui polinomi e di risultati di Algebra Lineare rimandiamo all'Appendice D. Osserviamo anche che, pur mantenendo il nome tradizionale, questo teorema non è più così centrale nell'Algebra moderna.

Nell'Esempio 2.3 abbiamo visto che esistono matrici reali senza autovalori reali. Invece, per il Teorema Fondamentale dell'Algebra, le matrici complesse (o quelle reali pensate come complesse) hanno sempre autovalori complessi. Più precisamente, gli autovalori complessi di una matrice complessa sono, contati con la loro molteplicità, tanti quant'è il suo ordine.

Trovarli tutti dipende esclusivamente dalla nostra abilità tecnica nel fattorizzare in fattori lineari il suo polinomio caratteristico. In particolare, come abbiamo preannunciato all'inizio del paragrafo, per una matrice complessa $\mathbf{A}$ di ordine n esistono sempre vettori non nulli di $\mathbb{C}^n$ la cui pre-moltiplicazione per $\mathbf{A}$ equivale alla moltiplicazione per un opportuno scalare.

Per questo motivo quando si tratta la teoria degli autovalori si preferisce impiegare matrici complesse, piuttosto che quelle reali.

Vogliamo evidenziare alcune proprietà del polinomio caratteristico di una matrice. Si ricordi che per convenzione si assume che il polinomio nullo abbia grado $-\infty$, ossia minore di qualsiasi numero, in particolare di qualsiasi intero non negativo.

Cominciamo con il fare la seguente osservazione.

Osservazione 3.2. Se $\mathbf{B}(X)$ è una matrice quadrata di ordine m i cui elementi sono polinomi di grado ≤ 1, allora il grado del polinomio $\det(\mathbf{B}(X))$ è al più m. La dimostrazione di questo fatto, per induzione su m, è lasciata come esercizio (si veda l'Esercizio 5.8). Come conseguenza di ciò si ottiene in particolare che se tutti gli elementi di una colonna di $\mathbf{B}(X)$ sono elementi di K, allora il grado del polinomio $\det(\mathbf{B}(X))$ è al più $m-1$.

Lemma 3.3. *Sia $\mathbf{A} = [a_{ij}]$ una matrice $n \times n$ con $n \geq 2$. Allora esiste un polinomio $f(X)$ di grado al più $n-2$ tale che*

$$p_{\mathbf{A}}(X) = f(X) + \prod_{1\leq i\leq n} (a_{ii} - X).$$

Dimostrazione. Procediamo per induzione su $n \geq 2$.

Se $n = 2$ (primo passo dell'induzione) allora

$$p_{\mathbf{A}}(X) = \det(\mathbf{A} - X\mathbf{I}_2) = \det \begin{bmatrix} a_{11} - X & a_{12} \\ a_{21} & a_{22} - X \end{bmatrix} = (a_{11} - X)(a_{22} - X) + f(X)$$

dove $f(X) = -a_{12}a_{21}$. Il grado di $f(X)$ è minore o uguale a $0 = n-2$.

Sia $n > 2$ e si supponga (ipotesi induttiva) la proposizione vera per matrici $(n-1) \times (n-1)$. Sia $\mathbf{A} = [a_{ij}]$ una matrice $n \times n$. Sviluppando

$$p_{\mathbf{A}}(X) = \det(\mathbf{A} - X\mathbf{I}_n) = \det \begin{bmatrix} a_{11} - X & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} - X & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} - X \end{bmatrix}$$

rispetto alla prima riga si ottiene

$$p_{\mathbf{A}}(X) = (a_{11} - X) \det \begin{bmatrix} a_{22} - X & \dots & a_{2n} \\ \vdots & \ddots & \vdots \\ a_{n2} & \dots & a_{nn} - X \end{bmatrix} + \sum_{j\geq 2} (-1)^{1+j} a_{1j} \det(\mathbf{A}_{1j}(X))$$

dove $\mathbf{A}_{1j}(X)$, per $j \geq 2$, è la matrice $(n-1) \times (n-1)$ che si ottiene da $\mathbf{A} - X\mathbf{I}_n$ sopprimendo la prima riga e la j-esima colonna. Poiché i suoi elementi sono polinomi di grado ≤ 1, e inoltre tutti gli elementi della sua prima colonna sono elementi di K, dall'Osservazione 3.2 si ottiene che $\det(\mathbf{A}_{1j}(X))$ ha grado al più $n-2$, e quindi anche $g(X) = \sum_{j\geq 2}(-1)^{1+j} a_{1j} \det(\mathbf{A}_{1j}(X))$ ha grado al più $n-2$. Per ipotesi induttiva

$$\det \begin{bmatrix} a_{22} - X & \dots & a_{2n} \\ \vdots & \ddots & \vdots \\ a_{n2} & \dots & a_{nn} - X \end{bmatrix} = h(X) + \prod_{2\leq i\leq n} (a_{ii} - X),$$

dove $h(X)$ ha grado al più $n-3$. Allora $f(X) = (a_{11} - X)h(X) + g(X)$ ha grado al più $n-2$ e

$$p_{\mathbf{A}}(X) = f(X) + \prod_{1\leq i\leq n} (a_{ii} - X). \qquad \square$$

Possiamo ora agevolmente descrivere le principali proprietà cui soddisfa il polinomio caratteristico di una matrice quadrata. Ricordiamo (si veda l'Esercizio 1.17 del Capitolo 1) che se $\mathbf{A} = [a_{ij}]$ è una matrice $n \times n$, la traccia di $\mathbf{A}$ è il numero $\mathrm{Tr}(\mathbf{A}) = \sum_{1 \le i \le n} a_{ii}$.

Proposizione 3.4. *Sia* $\mathbf{A} = [a_{ij}]$ *una matrice* $n \times n$*. Allora*

(1) $p_{\mathbf{A}}(X)$ *ha grado* n*;*

(2) *il coefficiente di* X^n *in* $p_{\mathbf{A}}(X)$ *è* $(-1)^n$*;*

(3) *il coefficiente di* X^{n-1} *in* $p_{\mathbf{A}}(X)$ *è* $(-1)^{n-1}\mathrm{Tr}(\mathbf{A}) = (-1)^{n-1}\sum_{1 \le i \le n} a_{ii}$*;*

(4) *il termine noto di* $p_{\mathbf{A}}(X)$ *è* $\det(\mathbf{A})$.

Dimostrazione. Se $\mathbf{A} = [a_{11}]$, allora $p_{\mathbf{A}}(X) = a_{11} - X$ ha grado 1, coefficiente di X uguale a -1 e termine noto $a_{11} = \det(\mathbf{A})$.

Si supponga quindi $n \ge 2$. Poiché $\prod_{1 \le i \le n}(a_{ii} - X)$ ha grado n, dal Lemma 3.3 si ottiene (1), e inoltre che il coefficiente di X^n e il coefficiente di X^{n-1} di $p_{\mathbf{A}}(X)$ coincidono con il coefficiente di X^n e il coefficiente di X^{n-1} di $\prod_{1 \le i \le n}(a_{ii} - X)$ rispettivamente.

Sviluppando $\prod_{1 \le i \le n}(a_{ii} - X)$ si ottiene che il coefficiente di X^n è $(-1)^n$. Ciò prova (2).

Il coefficiente di X^{n-1} coincide con il coefficiente di X^{n-1} di $\sum_{1 \le i \le n} a_{ii} \prod_{j \ne i}(a_{jj} - X)$. Poiché per ogni $i = 1, \dots, n$ si ha che il coefficiente di X^{n-1} di $\prod_{j \ne i}(a_{jj} - X)$ è $(-1)^{n-1}$, allora il coefficiente di X^{n-1} di $\sum_{1 \le i \le n} a_{ii} \prod_{j \ne i}(a_{jj} - X)$ è $(-1)^{n-1}\sum_{1 \le i \le n} a_{ii} = (-1)^{n-1}\mathrm{Tr}(\mathbf{A})$, e anche (3) è provato.

Per provare (4) si osservi che attribuendo il valore 0 all'indeterminata X si ottiene che il termine noto di $p_{\mathbf{A}}(X)$ è

$$p_{\mathbf{A}}(0) = \det(\mathbf{A} - 0 \cdot \mathbf{I}) = \det(\mathbf{A}). \qquad \square$$

Siano $\mathbf{A}$ una matrice quadrata complessa di ordine n e $p_{\mathbf{A}}(X)$ il suo polinomio caratteristico. Per il Teorema Fondamentale dell'Algebra $p_{\mathbf{A}}(X)$ si fattorizza in fattori di grado 1, per cui esistono numeri complessi distinti $\lambda_1, \dots, \lambda_r$, gli autovalori di $\mathbf{A}$, e numeri naturali $m_1, \dots, m_r$ tali che

$$p_{\mathbf{A}}(X) = c(X - \lambda_1)^{m_1}(X - \lambda_2)^{m_2} \dots (X - \lambda_r)^{m_r}$$

per un opportuno numero complesso c. Il numero naturale m_i è detto la *molteplicità algebrica dell'autovalore* λ_i, per ogni $i = 1, \dots, r$.

Essa può non coincidere con la molteplicità geometrica. Per esempio, l'autovalore 1 della matrice $\mathbf{B}$ nell'Esempio 2.8 ha molteplicità algebrica uguale a 2 e molteplicità geometrica uguale a 1.

Per il punto (1) della Proposizione 3.4 $p_{\mathbf{A}}(X)$ ha grado n, per cui si ha

$$n = m_1 + m_2 + \dots + m_r.$$

Abbiamo quindi provato il seguente risultato.

Proposizione 3.5. *La somma delle molteplicità algebriche degli autovalori di una matrice quadrata è uguale all'ordine della matrice.* □

Inoltre per il punto (2) della Proposizione 3.4 il coefficiente di X^n di $p_{\mathbf{A}}(X)$ è $(-1)^n$, quindi $c = (-1)^n$ e si ha:

$$p_{\mathbf{A}}(X) = (\lambda_1 - X)^{m_1}(\lambda_2 - X)^{m_2} \dots (\lambda_r - X)^{m_r}.$$

In particolare $p_{\mathbf{A}}(X) = p_{\mathbf{D}}(X)$, dove $\mathbf{D}$ è la matrice diagonale di ordine n i cui elementi diagonali sono gli autovalori di $\mathbf{A}$ ciascuno contato con la sua molteplicità algebrica. Applicando la Proposizione 3.4 a $\mathbf{D}$ e $\mathbf{A}$ si ottiene allora il seguente risultato.

Proposizione 3.6. *Sia* $\mathbf{A}$ *una matrice complessa.*

(1) *La traccia di* $\mathbf{A}$ *coincide con la somma degli autovalori di* $\mathbf{A}$ *ciascuno contato con la sua molteplicità algebrica.*
(2) *Il determinante di* $\mathbf{A}$ *coincide con il prodotto degli autovalori di* $\mathbf{A}$ *ciascuno contato con la sua molteplicità algebrica.*

4. Proprietà degli autospazi

Sia $\mathbf{A}$ una matrice complessa $n \times n$. Abbiamo già accennato nel paragrafo precedente al fatto che l'idea di fondo per lo studio dell'applicazione lineare $f_{\mathbf{A}} \colon \mathbb{C}^n \to \mathbb{C}^n$ è quella di cercare, ed eventualmente costruire effettivamente, un'opportuna base $\mathscr{B}$ di $\mathbb{C}^n$ rispetto alla quale la matrice $\mathbf{B}$ associata a $f_{\mathbf{A}}$ abbia molti coefficienti nulli. In tal caso, come abbiamo già osservato, il calcolo di $f_{\mathbf{B}}$ è meno problematico ed $f_{\mathbf{A}}$ ammette una fattorizzazione del tipo $f_{\mathbf{A}} = g f_{\mathbf{B}} g^{-1}$ con g isomorfismo di $\mathbb{C}^n$. Dal punto di vista matriciale, se $\mathbf{S}$ è la matrice che ha come colonne i vettori della base $\mathscr{B}$, la relazione che intercorre tra $\mathbf{A}$ e $\mathbf{B}$ è $\mathbf{A} = \mathbf{SBS}^{-1}$ (si veda il Capitolo 2).

Definizione. Due matrici quadrate $\mathbf{A}$ e $\mathbf{B}$ si dicono *simili* se esiste una matrice invertibile $\mathbf{S}$ tale che $\mathbf{A} = \mathbf{SBS}^{-1}$.

La relazione di similitudine è una relazione riflessiva, simmetrica e transitiva (si veda l'Esercizio 5.11), ossia è una relazione di equivalenza, e, come proviamo nella prossima proposizione, conserva i polinomi caratteristici e le molteplicità algebriche e geometriche degli autovalori.

Proposizione 4.1. *Due matrici simili hanno lo stesso polinomio caratteristico e gli stessi autovalori con le stesse molteplicità algebriche e geometriche.*

Dimostrazione. Siano $\mathbf{A}$ e $\mathbf{B}$ due matrici simili di ordine n ed $\mathbf{S}$ una matrice invertibile tale che $\mathbf{A} = \mathbf{SBS}^{-1}$. Allora

$$\begin{aligned} p_{\mathbf{A}}(X) &= \det(\mathbf{A} - X\mathbf{I}_n) = \det(\mathbf{SBS}^{-1} - X\mathbf{I}_n) = \det(\mathbf{S}(\mathbf{B} - X\mathbf{I}_n)\mathbf{S}^{-1}) \\ &= \det\mathbf{S}\det(\mathbf{B} - X\mathbf{I}_n)(\det\mathbf{S})^{-1} = \det(\mathbf{B} - X\mathbf{I}_n) = p_{\mathbf{B}}(X) \end{aligned}$$

per cui $\mathbf{A}$ e $\mathbf{B}$ hanno lo stesso polinomio caratteristico, e quindi anche gli stessi autovalori con le stesse molteplicità algebriche.

Sia ora λ un autovalore di $\mathbf{A}$ e $\mathbf{B}$. Da

$$\mathbf{v} \in \mathrm{E}_{\mathbf{B}}(\lambda) \iff \mathbf{Bv} = \lambda\mathbf{v} \iff \mathbf{S}^{-1}\mathbf{ASv} = \lambda\mathbf{v} \iff \mathbf{ASv} = \lambda\mathbf{Sv} \iff \mathbf{Sv} \in \mathrm{E}_{\mathbf{A}}(\lambda),$$

segue che la restrizione a $\mathrm{E}_{\mathbf{B}}(\lambda)$ della pre-moltiplicazione per $\mathbf{S}$ è un'applicazione lineare da $\mathrm{E}_{\mathbf{B}}(\lambda)$ a $\mathrm{E}_{\mathbf{A}}(\lambda)$. Tale applicazione lineare è un isomorfismo: la sua inversa è la restrizione a $\mathrm{E}_{\mathbf{A}}(\lambda)$ della pre-moltiplicazione per $\mathbf{S}^{-1}$. In particolare gli spazi vettoriali $\mathrm{E}_{\mathbf{A}}(\lambda)$ ed $\mathrm{E}_{\mathbf{B}}(\lambda)$ hanno la stessa dimensione, ossia la molteplicità geometrica di λ in quanto autovalore di $\mathbf{A}$ coincide con la molteplicità geometrica di λ in quanto autovalore di $\mathbf{B}$. □

Nel teorema che segue, impiegando la relazione di similitudine tra matrici, proviamo che la molteplicità geometrica di un autovalore è minore o uguale a quella algebrica. Questo fatto ci permetterà nel prossimo paragrafo di caratterizzare in modo soddisfacente le matrici diagonalizzabili.

Teorema 4.2. *Siano* $\mathbf{A}$ *una matrice* $n \times n$ *e* λ *un autovalore di* $\mathbf{A}$ *con molteplicità geometrica e algebrica* d *ed* m *rispettivamente. Allora* $d \le m$.

Dimostrazione. Si estenda una base $\{\mathbf{v}_1;\mathbf{v}_2;\dots;\mathbf{v}_d\}$ dell'autospazio $\mathrm{E}_{\mathbf{A}}(\lambda)$ a una base $\mathscr{B} = \{\mathbf{v}_1;\mathbf{v}_2;\dots;\mathbf{v}_d;\mathbf{v}_{d+1};\dots;\mathbf{v}_n\}$ di $\mathbb{C}^n$, e si consideri la matrice $\mathbf{B}$ associata all'applicazione lineare $f_{\mathbf{A}}\colon \mathbb{C}^n \to \mathbb{C}^n$ rispetto alla base $\mathscr{B}$ (su dominio e codominio). Per ogni $i = 1,\dots,d$ si ha, per il Teorema 6.3 del Capitolo 2,

$$\mathbf{Be}_i = \mathrm{C}_{\mathscr{B}}(\mathbf{Av}_i) = \mathrm{C}_{\mathscr{B}}(\lambda\mathbf{v}_i) = \lambda\mathbf{e}_i,$$

dove $\mathbf{e}_1,\dots,\mathbf{e}_d$ sono le prime d colonne della matrice identica $\mathbf{I}_n$. Pertanto $\mathbf{B}$ è una matrice triangolare superiore a blocchi del tipo

$$\mathbf{B} = \begin{bmatrix} \lambda\mathbf{I}_d & \mathbf{C} \\ \mathbb{O} & \mathbf{D} \end{bmatrix}$$

con $\mathbf{D}$ matrice quadrata. Quindi $p_{\mathbf{B}}(X) = (\lambda - X)^d p_{\mathbf{D}}(X)$.

Poiché $\mathbf{A}$ è la matrice associata all'applicazione lineare $f_{\mathbf{A}}$ rispetto alla base canonica di $\mathbb{C}^n$ (su dominio e codominio), $\mathbf{B}$ è simile ad $\mathbf{A}$, e dalla Proposizione 4.1 segue che $p_{\mathbf{B}}(X) = p_{\mathbf{A}}(X)$. Dunque il polinomio $(\lambda - X)^d$ divide il polinomio caratteristico di $\mathbf{A}$, per cui la molteplicità geometrica d di λ è minore o uguale a quella algebrica m. □

Ricordiamo (si veda il Paragrafo 3 del Capitolo 2) che se U e Z sono due sottospazi vettoriali dello spazio vettoriale V, la somma di U e Z

$$U + Z = \{\mathbf{u} + \mathbf{z} \mid \mathbf{u} \in U, \mathbf{z} \in Z\}$$

è il più piccolo sottospazio di V contenente U e Z. Inoltre, se ogni elemento di $U + Z$ si scrive in modo unico come somma di un vettore di U e un vettore di Z, allora la somma di U e Z si chiama somma diretta e si indica con il simbolo $U \oplus Z$. Quanto detto si può estendere a un numero finito di sottospazi di V, come già accennato nella Proposizione 3.19 del Capitolo 2.

Definizione. Siano $U_1, \dots, U_n$ sottospazi vettoriali dello spazio vettoriale V. La *somma*

$$\sum_{1 \le i \le n} U_i = \{\mathbf{u}_1 + \cdots + \mathbf{u}_n \mid \mathbf{u}_i \in U_i, i = 1, \dots, n\}$$

è il più piccolo sottospazio di V contenente $U_1, \dots, U_n$. Se ogni elemento di $\sum_{1 \le i \le n} U_i$ si scrive in modo unico come somma di vettori di $U_1, \dots, U_n$, la somma $\sum_{1 \le i \le n} U_i$ si chiama *diretta* e si indica con il simbolo $\bigoplus_{1 \le i \le n} U_i$.

Si osservi che per verificare che $\sum_{1 \le i \le n} U_i = \bigoplus_{1 \le i \le n} U_i$, è sufficiente verificare che i sottospazi $U_1, \dots, U_n$ sono *indipendenti*, secondo la definizione data alla fine del Paragrafo 3 del Capitolo 2:

$$\sum_{1 \le i \le n} \mathbf{u}_i = \mathbf{0}, \quad \mathbf{u}_i \in U_i \quad \text{per ogni } i = 1, \dots, n \implies \mathbf{u}_i = \mathbf{0} \quad \text{per ogni } i = 1, \dots, n.$$

Si osservi inoltre che se $\sum_{1 \le i \le n} U_i = \bigoplus_{1 \le i \le n} U_i$, e $\mathscr{B}_i$ è una base di U_i per ogni $i = 1, \dots, n$, allora $\mathscr{B} = \mathscr{B}_1 \cup \cdots \cup \mathscr{B}_n$ è una base di $\bigoplus_{1 \le i \le n} U_i$ (si veda l'Esercizio 5.17).

Teorema 4.3. *Siano* $\mathbf{A}$ *una matrice* $n \times n$ *e* $\lambda_1, \dots, \lambda_k$ *autovalori distinti di* $\mathbf{A}$. *Allora si ha* $\sum_{1 \le i \le k} \mathrm{E}_{\mathbf{A}}(\lambda_i) = \bigoplus_{1 \le i \le k} \mathrm{E}_{\mathbf{A}}(\lambda_i)$.

Dimostrazione. Abbiamo osservato che è sufficiente provare che se $\mathbf{v}_i \in \mathrm{E}_{\mathbf{A}}(\lambda_i)$ allora

$$\sum_{1 \le i \le k} \mathbf{v}_i = \mathbf{0} \implies \mathbf{v}_i = \mathbf{0} \quad \text{per ogni } i = 1, \dots, k.$$

Procediamo per induzione su k. Per $k = 1$ non c'è nulla da dimostrare. Sia allora $k > 1$ e si supponga che la somma degli autospazi relativi a $k - 1$ autovalori distinti di $\mathbf{A}$ sia diretta.

Premoltiplicando ambo i membri dell'uguaglianza $\sum_{1 \le i \le k} \mathbf{v}_i = \mathbf{0}$ per λ_1 si ottiene

$$\sum_{1 \le i \le k} \lambda_1 \mathbf{v}_i = \mathbf{0}, \tag{*}$$

mentre pre-moltiplicandoli per $\mathbf{A}$ si ottiene

$$\mathbf{0} = \mathbf{A}\mathbf{0} = \mathbf{A} \sum_{1 \le i \le k} \mathbf{v}_i = \sum_{1 \le i \le k} \mathbf{A}\mathbf{v}_i = \sum_{1 \le i \le k} \lambda_i \mathbf{v}_i. \tag{**}$$

Sottraendo ora membro a membro (**) da (*), si ricava che

$$\sum_{2 \le i \le k} (\lambda_i - \lambda_1)\mathbf{v}_i = \mathbf{0},$$

da cui, per ipotesi induttiva, $(\lambda_i - \lambda_1)\mathbf{v}_i = \mathbf{0}$ per ogni $i \ge 2$. Poiché gli autovalori sono distinti, $\lambda_i - \lambda_1 \ne 0$ per ogni $i \ge 2$, per cui $\mathbf{v}_i = \mathbf{0}$ per ogni $i \ge 2$. Da ciò segue che anche $\mathbf{v}_1 = \mathbf{0}$, essendo $\sum_{1 \le i \le k} \mathbf{v}_i = \mathbf{0}$. La dimostrazione è così completata. □

Come conseguenza del Teorema 4.3 si ha il seguente risultato.

Corollario 4.4. *Autovettori relativi ad autovalori distinti sono linearmente indipendenti.*

Dimostrazione. Siano $\mathbf{A}$ una matrice quadrata, $\lambda_1,\dots,\lambda_k$ suoi autovalori distinti, con $\mathbf{v}_1,\dots,\mathbf{v}_k$ autovettori a essi corrispondenti, e $\alpha_1\mathbf{v}_1+\cdots+\alpha_k\mathbf{v}_k=\mathbf{0}$ una loro combinazione lineare nulla. Poiché $\mathrm{E}_{\mathbf{A}}(\lambda_i)$ è uno spazio vettoriale per ogni $i=1,\dots,k$, allora $\alpha_i\mathbf{v}_i\in\mathrm{E}_{\mathbf{A}}(\lambda_i)$, per cui dal Teorema 4.3 si ottiene che $\alpha_i\mathbf{v}_i=\mathbf{0}$ per ogni $i=1,\dots,k$. Dal fatto che ciascun $\mathbf{v}_i$, in quanto autovettore di $\mathbf{A}$, è non nullo, segue che $\alpha_i=0$ per ogni $i=1,\dots,k$, ossia che i vettori $\mathbf{v}_1,\dots,\mathbf{v}_k$ sono linearmente indipendenti. □

5. Matrici diagonalizzabili e matrici triangolarizzabili

Nel Paragrafo 2 abbiamo già espresso il concetto di matrice diagonalizzabile in relazione all'applicazione lineare da essa indotta. Riprendiamo ora quel concetto.

Definizione. Si dice che una matrice $\mathbf{A}$ è *diagonalizzabile* se è simile a una matrice diagonale, ossia se esistono una matrice diagonale $\mathbf{D}$ e una matrice invertibile $\mathbf{S}$ tali che $\mathbf{A}=\mathbf{SDS}^{-1}$. In tal caso si dice che $\mathbf{S}$ diagonalizza $\mathbf{A}$.

Oltre che per lo studio dell'applicazione lineare indotta, una situazione in cui risulta conveniente sapere se una matrice è diagonalizzabile, è quando si vogliono calcolare le sue potenze (si veda il Paragrafo 1), dal momento che se $\mathbf{A}=\mathbf{SDS}^{-1}$, allora per ogni numero naturale k si ha che $\mathbf{A}^k=\mathbf{SD}^k\mathbf{S}^{-1}$, e se $\mathbf{D}=\mathbf{Diag}(d_1,\dots,d_n)$, allora

$$\mathbf{D}^k=\mathbf{Diag}(d_1^k,\dots,d_n^k).$$

Il problema del calcolo delle potenze di una matrice è trattabile più facilmente non solo nel caso di matrici diagonali o diagonalizzabili, ma anche nel caso di matrici triangolari: sappiamo infatti che se $\mathbf{T}$ è una matrice triangolare, per ogni numero naturale k anche $\mathbf{T}^k$ è triangolare e i coefficienti diagonali di $\mathbf{T}^k$ sono le potenze k-esime dei coefficienti diagonali di $\mathbf{T}$.

Possiamo allora dare una definizione analoga.

Definizione. Si dice che una matrice $\mathbf{A}$ è *triangolarizzabile* se è simile a una matrice triangolare, ossia se esistono una matrice triangolare $\mathbf{T}$ e una matrice invertibile $\mathbf{S}$ tali che $\mathbf{A}=\mathbf{STS}^{-1}$. In tal caso si dice che $\mathbf{S}$ triangolarizza $\mathbf{A}$.

Abbiamo ora tutti gli strumenti per caratterizzare le matrici diagonalizzabili.

Teorema 5.1. *Siano* $\mathbf{A}$ *una matrice complessa* $n\times n$ *e* $\lambda_1,\dots,\lambda_k$ *i suoi autovalori distinti. Sono equivalenti i seguenti fatti:*

(1) $\mathbf{A}$ *è diagonalizzabile;*

(2) $\mathbb{C}^n$ *ha una base costituita da autovettori di* $\mathbf{A}$*;*

(3) $\mathbb{C}^n = \bigoplus_{1\le i\le k} \mathrm{E}_{\mathbf{A}}(\lambda_i)$;

(4) *la molteplicità geometrica di ciascun autovalore λ_i coincide con la sua molteplicità algebrica.*

Dimostrazione. (1) $\Longleftrightarrow$ (2) Poiché

$$\mathbf{A} = \mathbf{SDS}^{-1} \iff \mathbf{AS} = \mathbf{SD} \iff \mathbf{ASe}_i = \mathbf{SDe}_i = d_i\mathbf{Se}_i \quad \text{per ogni } i = 1,\dots,n,$$

l'insieme $\{\mathbf{Se}_1;\dots;\mathbf{Se}_n\}$ delle colonne di $\mathbf{S}$, che essendo $\mathbf{S}$ invertibile è una base di $\mathbb{C}^n$, è costituito da autovettori di $\mathbf{A}$. Si osservi che in tal caso gli elementi diagonali di $\mathbf{D}$ sono gli autovalori di $\mathbf{A}$, ripetuti tante volte quanto è la loro molteplicità algebrica.

(2) $\Longrightarrow$ (4) Sia $\mathscr{B}$ una base di $\mathbb{C}^n$ costituita da autovettori di $\mathbf{A}$. Per ogni $i = 1,\dots,k$ sia s_i il numero degli elementi di $\mathscr{B}$ appartenenti a $\mathrm{E}_{\mathbf{A}}(\lambda_i)$. Allora $s_i \le d_i$ e, per il Teorema 4.2, $d_i \le m_i$ per ogni $i = 1,\dots,k$. Poiché $\mathscr{B}$ ha n elementi, allora $\sum_{1\le i\le k} s_i = n$. D'altra parte per la Proposizione 3.5 si ha anche che $\sum_{1\le i\le k} m_i = n$, per cui $s_i = d_i = m_i$ per ogni $i = 1,\dots,k$.

(4) $\Longrightarrow$ (3) Se ogni autovalore λ_i ha molteplicità geometrica d_i e algebrica m_i uguali, allora $\sum_{1\le i\le k} m_i = \sum_{1\le i\le k} d_i$, per cui dalla Proposizione 3.5 si ottiene

$$\dim \mathbb{C}^n = n = \sum_{1\le i\le k} m_i = \sum_{1\le i\le k} d_i = \dim\Big(\bigoplus_{1\le i\le k} \mathrm{E}_{\mathbf{A}}(\lambda_i)\Big)$$

e quindi $\mathbb{C}^n = \bigoplus_{1\le i\le k} \mathrm{E}_{\mathbf{A}}(\lambda_i)$.

(3) $\Longrightarrow$ (2) Sia $\mathscr{B}_i$ una base di $\mathrm{E}_{\mathbf{A}}(\lambda_i)$ per ogni $i = 1,\dots,k$. Allora $\mathscr{B} = \mathscr{B}_1 \sqcup \dots \sqcup \mathscr{B}_k$ è una base di $\bigoplus_{1\le i\le k} \mathrm{E}_{\mathbf{A}}(\lambda_i) = \mathbb{C}^n$ costituita da autovettori di $\mathbf{A}$ per la Proposizione 3.19 del Capitolo 2 (si veda l'Esercizio 5.17). □

Dal Teorema precedente si deduce che le matrici di proiezione sono matrici diagonalizzabili (si veda l'Esempio 2.2), così come la matrice dell'Esempio 2.6. Non è invece diagonalizzabile la matrice dell'Esempio 2.5.

Osservando che se $\mathbf{A}$ è reale un autovalore λ di $\mathbf{A}$ è reale se e solo se gli autovettori di $\mathbf{A}$ relativi a λ possono essere scelti a coordinate reali, si ottiene il caso reale del teorema precedente.

Teorema 5.2. *Siano $\mathbf{A}$ una matrice reale $n \times n$ e $\lambda_1,\dots,\lambda_k$ i suoi autovalori complessi distinti. Sono equivalenti i seguenti fatti:*

(1) *$\mathbf{A}$ è diagonalizzabile con una matrice reale;*

(2) *$\lambda_1,\dots,\lambda_k \in \mathbb{R}$ e $\mathbb{R}^n$ ha una base costituita da autovettori di $\mathbf{A}$;*

(3) *$\lambda_1,\dots,\lambda_k \in \mathbb{R}$ e $\mathbb{R}^n = \bigoplus_{1\le i\le k}(\mathrm{E}_{\mathbf{A}}(\lambda_i) \cap \mathbb{R}^n)$;*

(4) *$\lambda_1,\dots,\lambda_k \in \mathbb{R}$ e per ogni $i = 1,\dots,k$ la dimensione del sottospazio $\mathrm{E}_{\mathbf{A}}(\lambda_i) \cap \mathbb{R}^n$ di $\mathbb{R}^n$ coincide con la molteplicità algebrica m_i di λ_i.*

Abbiamo inoltre un'immediata conseguenza dei Teoremi 4.2 e 5.1.

Corollario 5.3. *Una matrice $n \times n$ con n autovalori distinti è diagonalizzabile.* □

Naturalmente le matrici diagonali, e quindi in particolare le matrici scalari, sono diagonalizzabili, per cui esistono matrici diagonalizzabili che non hanno autovalori distinti.

Esempio 5.4. La matrice dell'Esempio 2.3 è una matrice reale con autovalori complessi distinti e per il Corollario 5.3 è diagonalizzabile come matrice complessa. Dal momento però che i suoi autovalori, i e $-i$, non sono reali, essa non è diagonalizzabile con una matrice reale. □

Per passare da una matrice a una a essa simile, occorre calcolare l'inversa della matrice $\mathbf{S}$ che realizza la similitudine. In alcuni casi questo calcolo può essere particolarmente semplice, come quando, per esempio, si riduce a una trasposizione o a una H-trasposizione.

Definizione. Una matrice $\mathbf{A}$ si dice *ortogonale* se $\mathbf{A}^{-1} = \mathbf{A}^T$; si dice *unitaria* se $\mathbf{A}^{-1} = \mathbf{A}^H$.

Le matrici reali ortogonali vengono chiamate in questo modo perché, come anche le matrici complesse unitarie, sono caratterizzate dal fatto che l'insieme delle loro colonne è un insieme ortonormale di vettori di $\mathbb{R}^n$, rispettivamente di $\mathbb{C}^n$ (vedremo queste cose più in dettaglio nel Capitolo 6).

Ovviamente una matrice reale è ortogonale se e solo se è unitaria, ma in generale esistono matrici ortogonali che non sono unitarie ed esistono matrici unitarie che non sono ortogonali.

Definizione. Se due matrici $\mathbf{A}$ e $\mathbf{B}$ sono simili e la matrice $\mathbf{S}$ che realizza la similitudine è ortogonale (rispettivamente unitaria), allora $\mathbf{A}$ e $\mathbf{B}$ si dicono *ortogonalmente simili* (rispettivamente *unitariamente simili*). Si parla anche di *similitudini ortogonali* e di *similitudini unitarie.*

Abbiamo già osservato che se $\mathbf{A}$ e $\mathbf{B}$ sono simili e $\mathbf{S}$ è la matrice che realizza la similitudine (ossia se $\mathbf{A} = \mathbf{SBS}^{-1}$), allora $\mathbf{B}$ è la matrice associata a $f_{\mathbf{A}}$ rispetto alla base ordinata $\mathscr{B}$ di $\mathbb{C}^n$ che ha come i-esimo vettore la i-esima colonna di $\mathbf{S}$. Se $\mathbf{A}$ e $\mathbf{B}$ sono matrici reali e $\mathbf{S}$ è una matrice reale ortogonale, ossia se $\mathbf{A}$ e $\mathbf{B}$ sono matrici reali ortogonalmente simili (e analogamente se $\mathbf{S}$ è una matrice unitaria, ossia se $\mathbf{A}$ e $\mathbf{B}$ sono unitariamente simili), allora la base $\mathscr{B}$ di $\mathbb{R}^n$ (rispettivamente di $\mathbb{C}^n$) è una base ortonormale.

Diamo ora una caratterizzazione delle matrici unitariamente simili a matrici triangolari, ottenendo in particolare che ogni matrice complessa è unitariamente simile a una matrice triangolare. Questo fatto verrà usato nel Capitolo 6 per caratterizzare le matrici che sono unitariamente diagonalizzabili, ossia unitariamente simili a una matrice diagonale.

Non è invece vero che ogni matrice reale è ortogonalmente simile a una matrice triangolare. Tale diversità dipende dal fatto che per il Teorema Fondamentale dell'Algebra ogni polinomio complesso si fattorizza in fattori lineari, e quindi ogni matrice complessa di ordine n ha n autovalori, se contati con la loro molteplicità, mentre le matrici reali di ordine n non necessariamente hanno n autovalori reali, anzi possono addirittura non averne alcuno (si veda l'Esempio 2.3). Nel seguito, come già in precedenza, K denota il campo $\mathbb{R}$ oppure il campo $\mathbb{C}$.

Teorema 5.5 (Schur)**.** *Sia* $\mathbf{A}$ *una matrice in* $\mathrm{M}_n(K)$*;* $\mathbf{A}$ *è unitariamente simile in* $\mathrm{M}_n(K)$ *a una matrice triangolare superiore se e solo se tutti gli n autovalori di* $\mathbf{A}$ *sono elementi di* K*.*

Dimostrazione. Sia $\mathbf{A} = \mathbf{UTU}^H$ con $\mathbf{U}$ unitaria e $\mathbf{T} = [t_{ij}] \in \mathrm{M}_n(K)$ triangolare. Allora per la Proposizione 4.1 si ha

$$p_{\mathbf{A}}(X) = p_{\mathbf{T}}(X) = (t_{11} - X)(t_{22} - X)\dots(t_{nn} - X)$$

per cui gli autovalori di $\mathbf{A}$ sono i coefficienti diagonali di $\mathbf{T}$, e pertanto elementi di K.

Viceversa si supponga che tutti gli n autovalori di $\mathbf{A} \in \mathrm{M}_n(K)$ siano elementi di K.

Procediamo per induzione su n per provare che $\mathbf{A}$ è unitariamente simile a una matrice triangolare superiore. Se $n = 1$ non c'è nulla da dimostrare. Supponiamo allora $n > 1$ e che ogni matrice $(n-1) \times (n-1)$ a coefficienti in K soddisfacente all'ipotesi sia unitariamente simile in $\mathrm{M}_{n-1}(K)$ a una matrice triangolare superiore.

Siano λ_1 un autovalore di $\mathbf{A}$ e $\mathbf{v}_1$ un autovettore di $\mathbf{A}$ relativo a λ_1 con $\|\mathbf{v}_1\|_2 = 1$. Completando $\mathbf{v}_1$ a una base ortonormale $\{\mathbf{v}_1;\dots;\mathbf{v}_n\}$ di K^n si ha che $\mathbf{U}_1 = [\mathbf{v}_1 \ \dots \ \mathbf{v}_n]$ è una matrice unitaria e che

$$\mathbf{U}_1^{-1}\mathbf{A}\mathbf{U}_1\mathbf{e}_1 = \mathbf{U}_1^{-1}\mathbf{A}\mathbf{v}_1 = \mathbf{U}_1^{-1}\lambda_1\mathbf{v}_1 = \lambda_1\mathbf{U}_1^{-1}\mathbf{v}_1 = \lambda_1\mathbf{e}_1,$$

per cui

$$\mathbf{A}' = \mathbf{U}_1^{-1}\mathbf{A}\mathbf{U}_1 = \begin{bmatrix} \lambda_1 & \mathbf{w}^T \\ \mathbf{0} & \mathbf{C} \end{bmatrix}$$

per opportune matrici $\mathbf{w}$ e $\mathbf{C}$. Ne segue che

$$p_{\mathbf{A}}(X) = p_{\mathbf{A}'}(X) = (\lambda_1 - X)p_{\mathbf{C}}(X),$$

per cui gli autovalori di $\mathbf{C}$ sono autovalori di $\mathbf{A}$ e quindi, per ipotesi, elementi di K.

Dall'ipotesi induttiva segue che esistono una matrice unitaria $\mathbf{V} \in \mathrm{M}_{n-1}(K)$ e una matrice triangolare superiore $\mathbf{T}_1 \in \mathrm{M}_{n-1}(K)$ tali che

$$\mathbf{C} = \mathbf{V}\mathbf{T}_1\mathbf{V}^H.$$

Posto $\mathbf{U}_2 = \mathbf{Diag}(1, \mathbf{V})$ e $\mathbf{U} = \mathbf{U}_1\mathbf{U}_2$, si ha che $\mathbf{U}_2$ è unitaria essendolo $\mathbf{V}$ e $\mathbf{U}$ è unitaria in quanto prodotto di due matrici unitarie (si veda la Proposizione 1.2 del Capitolo 6). Inoltre

$$\begin{aligned}\mathbf{U}^{-1}\mathbf{A}\mathbf{U} &= \mathbf{U}_2^{-1}\mathbf{U}_1^{-1}\mathbf{A}\mathbf{U}_1\mathbf{U}_2 = \mathbf{U}_2^{-1}\mathbf{A}'\mathbf{U}_2 = \mathbf{U}_2^{-1}\begin{bmatrix} \lambda_1 & \mathbf{w}^T \\ \mathbf{0} & \mathbf{C} \end{bmatrix}\mathbf{U}_2 \\ &= \begin{bmatrix} 1 & \mathbf{0}^T \\ \mathbf{0} & \mathbf{V}^H \end{bmatrix}\begin{bmatrix} \lambda_1 & \mathbf{w}^T \\ \mathbf{0} & \mathbf{C} \end{bmatrix}\begin{bmatrix} 1 & \mathbf{0}^T \\ \mathbf{0} & \mathbf{V} \end{bmatrix} = \begin{bmatrix} \lambda_1 & \mathbf{w}^T\mathbf{V} \\ \mathbf{0} & \mathbf{V}^H\mathbf{C}\mathbf{V} \end{bmatrix} = \begin{bmatrix} \lambda_1 & \mathbf{w}^T\mathbf{V} \\ \mathbf{0} & \mathbf{T}_1 \end{bmatrix}\end{aligned}$$

è triangolare superiore essendolo $\mathbf{T}_1$. Ciò completa la dimostrazione. □

Osserviamo che $\mathbf{A}$ è anche unitariamente simile a una matrice triangolare inferiore. Infatti, per quanto appena dimostrato, esistono una matrice triangolare superiore $\mathbf{T}_1$ e una matrice unitaria $\mathbf{U}$ tali che $\mathbf{A}^H = \mathbf{U}\mathbf{T}_1\mathbf{U}^H$. Passando alla H-trasposta, dall'uguaglianza precedente si ottiene $\mathbf{A} = \mathbf{U}\mathbf{T}_1^H\mathbf{U}^H$ con $\mathbf{T}_1^H$ triangolare inferiore.

Dal teorema precedente segue un corollario.

Corollario 5.6. *Ogni matrice complessa è unitariamente simile a una matrice triangolare.* □

Data una matrice $\mathbf{A}$ con polinomio caratteristico che si fattorizza in fattori lineari, la dimostrazione del teorema di Schur fornisce un procedimento effettivo per costruire una matrice triangolare $\mathbf{T}$ e una matrice unitaria $\mathbf{U}$ tali che $\mathbf{A} = \mathbf{U}\mathbf{T}\mathbf{U}^H$.

Dal punto di vista computazionale, però, tale costruzione dipende dalla possibilità di calcolare gli autovalori di $\mathbf{A}$, e tale calcolo, come abbiamo già sottolineato, può essere estremamente problematico, se non impossibile.

Ma dal punto di vista teorico il teorema di Schur ha applicazioni notevoli, permettendo di ricondursi al caso di matrici triangolari ogniqualvolta si vogliano studiare delle proprietà delle matrici che siano invarianti rispetto alla relazione di similitudine.

Il corollario che segue è un esempio di applicazione teorica del teorema di Schur.

Corollario 5.7. *Sia $\mathbf{A}$ una matrice $n \times n$ con n autovalori (ripetuti con le loro molteplicità) $\lambda_1, \dots, \lambda_n$. Per ogni intero positivo k gli autovalori di $\mathbf{A}^k$ sono i numeri $\lambda_1^k, \dots, \lambda_n^k$.*

Dimostrazione. Per il teorema di Schur esistono una matrice triangolare $\mathbf{T}$ e una matrice unitaria $\mathbf{U}$ tali che $\mathbf{A} = \mathbf{U}\mathbf{T}\mathbf{U}^{-1}$, per cui si ha anche $\mathbf{A}^k = \mathbf{U}\mathbf{T}^k\mathbf{U}^{-1}$. Dalla Proposizione 4.1 segue allora che gli autovalori di $\mathbf{A}$ coincidono con quelli di $\mathbf{T}$, e gli autovalori di $\mathbf{A}^k$ coincidono con quelli di $\mathbf{T}^k$. Poiché anche $\mathbf{T}^k$ è triangolare, essendolo $\mathbf{T}$, e gli autovalori di una matrice triangolare sono i suoi coefficienti diagonali, allora $\lambda_1, \dots, \lambda_n$ sono i coefficienti diagonali di $\mathbf{T}$, e gli autovalori di $\mathbf{A}^k$ sono i coefficienti diagonali di $\mathbf{T}^k$. La conclusione segue quindi dal fatto che i coefficienti diagonali di $\mathbf{T}^k$ sono le potenze k-esime dei coefficienti diagonali di $\mathbf{T}$, essendo $\mathbf{T}$ triangolare. □

6. I teoremi di Hamilton-Cayley e di Gerschgorin

Dei molti risultati sul polinomio caratteristico di una matrice quadrata e sui suoi autovalori, due sono di basilare importanza: il Teorema di Hamilton-Cayley e il Teorema "dei cerchi" di Gerschgorin.

Il primo teorema venne dimostrato per la prima volta per una particolare classe di matrici nel 1853 da W. R. Hamilton, matematico di Dublino famoso anche per la scoperta dei quaternioni (numeri che generalizzano i numeri complessi, si veda l'Appendice A) e per i suoi studi in dinamica fisica. Il matematico di Cambridge A. Cayley dimostrò il teorema in tutta generalità cinque anni dopo.

Del Teorema di Hamilton-Cayley esistono svariate dimostrazioni, la cui difficoltà decresce con l'aumentare della portata degli strumenti teorici a disposizione. La dimostrazione che viene qui presentata usa il Teorema di Schur 5.5; una dimostrazione più semplice fa uso della forma di Jordan (si veda l'Esercizio 5.25), da noi non trattata in questi Appunti.

Teorema 6.1 (Hamilton-Cayley)**.** *Sia* $\mathbf{A}$ *una matrice* $n \times n$ *con polinomio caratteristico* $p_{\mathbf{A}}(X) = (-1)^n X^n + a_{n-1}X^{n-1} + \dots + a_1 X + a_0$. *Allora* $p_{\mathbf{A}}(\mathbf{A}) = \mathbb{O}$, *cioè*

$$(-1)^n \mathbf{A}^n + a_{n-1}\mathbf{A}^{n-1} + \dots + a_1\mathbf{A} + a_0\mathbf{I}$$

è la matrice nulla.

Dimostrazione. Per il Teorema di Schur, la matrice $\mathbf{A}$ è unitariamente simile a una matrice triangolare superiore $\mathbf{T} = [t_{ij}]$:

$$\mathbf{A} = \mathbf{U}\mathbf{T}\mathbf{U}^{-1},$$

dove $\mathbf{U}$ è una matrice unitaria ($\mathbf{U}^{-1} = \mathbf{U}^H$). Per la Proposizione 4.1, $p_{\mathbf{A}}(X) = p_{\mathbf{T}}(X)$, perciò basta provare che $p_{\mathbf{T}}(\mathbf{A}) = \mathbb{O}$. Osserviamo che:

$$\begin{aligned} p_{\mathbf{A}}(\mathbf{A}) &= (-1)^n \mathbf{A}^n + a_{n-1}\mathbf{A}^{n-1} + \dots + a_1\mathbf{A} + a_0\mathbf{I} \\ &= (-1)^n (\mathbf{U}\mathbf{T}\mathbf{U}^{-1})^n + a_{n-1}(\mathbf{U}\mathbf{T}\mathbf{U}^{-1})^{n-1} + \dots + a_1(\mathbf{U}\mathbf{T}\mathbf{U}^{-1}) + a_0\mathbf{I} \\ &= (-1)^n \mathbf{U}\mathbf{T}^n\mathbf{U}^{-1} + a_{n-1}\mathbf{U}\mathbf{T}^{n-1}\mathbf{U}^{-1} + \dots + a_1(\mathbf{U}\mathbf{T}\mathbf{U}^{-1}) + a_0\mathbf{U}\mathbf{U}^{-1} \\ &= \mathbf{U}((-1)^n\mathbf{T}^n + a_{n-1}\mathbf{T}^{n-1} + \dots + a_1\mathbf{T} + a_0\mathbf{I})\mathbf{U}^{-1}, \end{aligned}$$

quindi $p_{\mathbf{T}}(\mathbf{A}) = \mathbf{U}p_{\mathbf{T}}(\mathbf{T})\mathbf{U}^{-1}$; pertanto è sufficiente provare che $p_{\mathbf{T}}(\mathbf{T}) = \mathbb{O}$, ovvero, basta provare il Teorema per la matrice triangolare $\mathbf{T}$. Essendo gli autovalori di $\mathbf{T}$ i suoi elementi diagonali, si ha:

$$p_{\mathbf{T}}(X) = (t_{11} - X)(t_{22} - X)\dots(t_{nn} - X),$$

quindi siamo ricondotti a provare l'uguaglianza:

$$(\mathbf{T} - t_{11}\mathbf{I})(\mathbf{T} - t_{22}\mathbf{I})\dots(\mathbf{T} - t_{nn}\mathbf{I}) = \mathbb{O}.$$

A tal fine, dimostriamo che la generica colonna j-esima della matrice $(\mathbf{T} - t_{11}\mathbf{I})\dots(\mathbf{T} - t_{nn}\mathbf{I})$ coincide con il vettore nullo. Tenuto conto del fatto che gli n fattori di tale matrice commutano tra di loro, basta provare che, per ogni $j \leq n$, si ha:

$$(\mathbf{T} - t_{11}\mathbf{I})(\mathbf{T} - t_{22}\mathbf{I})\dots(\mathbf{T} - t_{jj}\mathbf{I})\mathbf{e}_j = \mathbf{0} \tag{1}$$

Per $j = 1$ l'uguaglianza in (1) è banale, perché la prima colonna della matrice $\mathbf{T} - t_{11}\mathbf{I}$ è ovviamente nulla. Sia allora (1) vera per $j = 1, 2, \dots, k-1$, e proviamo che è vera per k. Si ha infatti:

$$(\mathbf{T} - t_{kk}\mathbf{I})\mathbf{e}_k = \mathbf{T}\mathbf{e}_k - t_{kk}\mathbf{e}_k = t_{1k}\mathbf{e}_1 + t_{2k}\mathbf{e}_2 + \dots + t_{k-1,k}\mathbf{e}_{k-1}.$$

Da ciò si ricava, usando il fatto che $(\mathbf{T} - t_{ii}\mathbf{I})(\mathbf{T} - t_{jj}\mathbf{I}) = (\mathbf{T} - t_{jj}\mathbf{I})(\mathbf{T} - t_{ii}\mathbf{I})$ per ogni i e j:

$$\begin{aligned} &(\mathbf{T} - t_{11}\mathbf{I})\dots(\mathbf{T} - t_{k-1,k-1}\mathbf{I})(\mathbf{T} - t_{kk}\mathbf{I})\mathbf{e}_k \\ &\qquad = (\mathbf{T} - t_{11}\mathbf{I})\dots(\mathbf{T} - t_{k-1,k-1}\mathbf{I})(t_{1k}\mathbf{e}_1 + t_{2k}\mathbf{e}_2 + \dots + t_{k-1,k}\mathbf{e}_{k-1}) = \mathbf{0}, \end{aligned}$$

giacché $(\mathbf{T} - t_{11}\mathbf{I})\dots(\mathbf{T} - t_{jj}\mathbf{I})\mathbf{e}_j = \mathbf{0}$ per $j = 1, 2, \dots, k-1$. □

Una immediata applicazione del Teorema di Hamilton-Cayley si dà al calcolo delle potenze di una matrice quadrata e al calcolo della sua inversa, nel caso esista (si vedano gli Esercizi 5.26 e 5.27).

Il secondo Teorema di questo paragrafo, dimostrato circa 80 anni dopo di quello di Hamilton-Cayley, è dovuto al matematico russo Gerschgorin (il cui nome trascritto dal cirillico ha spesso forme diverse). Si chiama anche Teorema "dei cerchi", perché localizza gli autovalori di una matrice $n \times n$ in una regione del piano complesso racchiusa in n cerchi, con centri e raggi immediatamente deducibili dai coefficienti della matrice. Questo fatto costituisce la prima parte del Teorema; la seconda parte dice qualcosa di più preciso nel caso in cui i cerchi siano disposti in modo opportuno.

Premettiamo una definizione e una notazione.

Data la matrice $\mathbf{A} = [a_{ij}] \in \mathrm{M}_n(\mathbb{C})$, si chiama *$i$-esimo cerchio di Gerschgorin* di $\mathbf{A}$ la regione del piano complesso:

$$C_i(\mathbf{A}) = \{z \in \mathbb{C} \mid |z - a_{ii}| \leq R_i\},$$

dove

$$R_i = \sum_{j \neq i} |a_{ij}|.$$

Pertanto $C_i(\mathbf{A})$ è costituito esattamente dai numeri complessi che stanno nel cerchio che ha centro nell'i-esimo elemento diagonale di $\mathbf{A}$, e ha come raggio R_i la somma dei moduli degli elementi nella i-esima riga di $\mathbf{A}$ diversi da a_{ii}.

Teorema 6.2 (Gerschgorin)**.** *Sia* $\mathbf{A} \in \mathrm{M}_n(\mathbb{C})$. *Allora:*

(i) *ogni autovalore di* $\mathbf{A}$ *appartiene ad almeno un cerchio di Gerschgorin,*

(ii) *se l'unione di $k \leq n$ cerchi di Gerschgorin forma una regione connessa e disgiunta dall'unione dei restanti $n - k$ cerchi, essa contiene esattamente k autovalori di* $\mathbf{A}$ *(contati con la loro molteplicità algebrica).*

Dimostrazione. (i) Sia $\mathbf{Av} = \lambda\mathbf{v}$ per un vettore $\mathbf{v} \neq \mathbf{0}$. Se $\mathbf{v} = [v_1\ v_2\ \dots\ v_n]^T$, per ogni $i \leq n$ risulta:

$$\sum_j a_{ij} v_j = \lambda v_i$$

da cui si ricava

$$(\lambda - a_{ii}) v_i = \sum_{j \neq i} a_{ij} v_j$$

e, passando ai moduli,

$$|\lambda - a_{ii}||v_i| \leq \sum_{j \neq i} |a_{ij}||v_j|. \tag{2}$$

Si scelga una coordinata v_k di $\mathbf{v}$ di modulo massimo, tale cioè che $|v_k| \geq |v_j|$ per ogni j. Risulta $|v_k| > 0$, perché $\mathbf{v} \neq \mathbf{0}$. Dividendo ambo i membri della disuguaglianza in (2) dove $i = k$, si ha:

$$|\lambda - a_{kk}| \leq \sum_{j \neq k} |a_{kj}| \left|\frac{v_j}{v_k}\right| \leq \sum_{j \neq k} |a_{kj}| = R_k,$$

il che dice appunto che $\lambda \in C_k(\mathbf{A})$.

(ii) Per una traccia di dimostrazione si vedano gli Esercizi 5.28–5.30. □

Un'utile applicazione del Teorema 6.2 si ha per le *matrici strettamente diagonalmente dominanti*, che sono quelle matrici $\mathbf{A} = [a_{ij}] \in \mathrm{M}_n(\mathbb{C})$ tali che, per ogni $i \leq n$, risulta:

$$|a_{ii}| > \sum_{j \neq i} |a_{ij}|.$$

Corollario 6.3. *Una matrice $\mathbf{A} \in \mathrm{M}_n(\mathbb{C})$ strettamente diagonalmente dominante è invertibile.*

Dimostrazione. Nessuno dei cerchi di Gerschgorin di $\mathbf{A}$ contiene l'origine del piano complesso, perché i centri a_{ii} hanno distanza dall'origine maggiore del raggio R_i. Allora 0 non è un autovalore di $\mathbf{A}$, cioè l'equazione $\mathbf{A}\mathbf{x} = \mathbf{0}$ ha solo la soluzione nulla. Per il Teorema 4.15 del Capitolo 1, $\mathbf{A}$ risulta invertibile. □

Esercizi

Paragrafo 2

5.1. Sia $\mathbf{A}$ una matrice $n \times n$ a coefficienti in K (dove $K = \mathbb{C}$ oppure $K = \mathbb{R}$). Si provi che la somma e l'intersezione di sottospazi $\mathbf{A}$-invarianti di K^n sono sottospazi $\mathbf{A}$-invarianti di K^n.

5.2. Sia $\mathbf{T}$ una matrice triangolare. Si provi che gli autovalori di $\mathbf{T}$ sono i suoi elementi diagonali.

5.3. Siano $\mathbf{A}$ una matrice invertibile e λ un autovalore di $\mathbf{A}$. Si provi che λ^{-1} è un autovalore di $\mathbf{A}^{-1}$ e che $\mathrm{E}_{\mathbf{A}}(\lambda) = \mathrm{E}_{\mathbf{A}^{-1}}(\lambda^{-1})$.

5.4. Siano $\mathbf{A}$ una matrice $n \times n$ e λ un autovalore di $\mathbf{A}$. Per ogni $k > 1$, si provi che λ^k è un autovalore di $\mathbf{A}^k$ e che $\mathrm{E}_{\mathbf{A}}(\lambda) \subseteq \mathrm{E}_{\mathbf{A}^k}(\lambda^k)$.

5.5. Siano $\mathbf{A}$ e $\mathbf{B}$ due matrici $n \times n$. Si provi che se esistono λ e μ autovalori di $\mathbf{A}$ e $\mathbf{B}$ rispettivamente con $\mathrm{E}_{\mathbf{A}}(\lambda) \cap \mathrm{E}_{\mathbf{B}}(\mu) \neq \{\mathbf{0}\}$, allora $\mathbf{AB} - \mathbf{BA}$ è non invertibile.

Paragrafo 3

5.6. Sia $\mathbf{A}$ una matrice nilpotente, tale cioè che $\mathbf{A}^k = \mathbb{O}$ per un $k > 0$. Si provi che l'unico autovalore di $\mathbf{A}$ è lo 0.

5.7. Sia $\mathbf{A}$ una matrice idempotente, tale cioè che $\mathbf{A}^{k+1} = \mathbf{A}^k$ per un $k > 0$. Si provi che se $\mathbf{A} \neq \mathbb{O}$ e $\mathbf{A} \neq \mathbf{I}$ allora lo spettro di $\mathbf{A}$ è $\{0, 1\}$.

5.8. Si provi l'Osservazione 3.2.

5.9. Si provi che se λ è un autovalore della matrice quadrata $\mathbf{A}$, allora $\overline{\lambda}$ è un autovalore della coniugata $\overline{\mathbf{A}}$ di $\mathbf{A}$. Si deduca che se $\mathbf{A}$ è reale e λ è un suo autovalore complesso, allora anche $\overline{\lambda}$ è un autovalore di $\mathbf{A}$.

5.10. Si deduca dall'esercizio precedente che una matrice quadrata reale di ordine dispari ha sempre un autovalore reale.

Paragrafo 4

5.11. Si provi che la relazione di similitudine è riflessiva, simmetrica e transitiva.

5.12. Siano $\mathbf{A}$ e $\mathbf{B}$ due matrici simili ed $\mathbf{S}$ tale che $\mathbf{A} = \mathbf{SBS}^{-1}$. Si supponga che $\mathbf{A}$ e $\mathbf{B}$ abbiano un autovalore λ in comune e, relativamente a λ, un autovettore $\mathbf{v}$ in comune, ossia che esistano uno scalare λ ed un vettore $\mathbf{v}$ tali che $\mathbf{0} \neq \mathbf{v} \in \mathrm{E}_{\mathbf{A}}(\lambda) \cap \mathrm{E}_{\mathbf{B}}(\lambda)$.

Si provi che sussiste uno dei seguenti fatti:

(a) $\langle \mathbf{v} \rangle \neq \mathrm{E}_{\mathbf{A}}(\lambda)$;

(b) $\mathbf{v}$ è un autovettore di $\mathbf{S}$.

5.13. Siano $\mathbf{A}$ e $\mathbf{B}$ due matrici simili e λ un autovalore della trasposta $\mathbf{A}^T$ di $\mathbf{A}$. Si provi che λ è un autovalore della trasposta $\mathbf{B}^T$ di $\mathbf{B}$ e che gli autospazi $\mathrm{E}_{\mathbf{A}^T}(\lambda)$ e $\mathrm{E}_{\mathbf{B}^T}(\lambda)$ hanno la stessa dimensione.

5.14. Si trovi una matrice 2×2 con un autovalore di molteplicità geometrica 1 e molteplicità algebrica 2.

5.15. Siano λ e μ due autovalori distinti della matrice quadrata $\mathbf{A}$. Si provi che se $\mathbf{v}$ e $\mathbf{w}$ sono due autovettori di $\mathbf{A}$ relativi a λ e μ rispettivamente, allora $\mathbf{v} + \mathbf{w}$ non è un autovettore di $\mathbf{A}$.

5.16. Si provi che una matrice complessa $n \times n$ $\mathbf{A}$ è simile ad una matrice triangolare superiore se e solo se esiste una successione crescente di sottospazi $\mathbf{A}$-invarianti di $\mathbb{C}^n$, $\{\mathbf{0}\} \subset V_1 \subset V_2 \subset \cdots \subset V_{n-1} \subset V_n = \mathbb{C}^n$, dove V_i ha dimensione i per ogni $i = 1, 2, \dots, n$.

5.17. Siano $U_1, U_2, \dots, U_n$ sottospazi indipendenti dello spazio vettoriale V. Sia $\mathscr{B}_i$ una base di U_i per ogni $i \leq n$. Si provi che $\bigcup_{i \leq n} \mathscr{B}_i$ è una base di $\bigoplus_{i \leq n} U_i$.

Paragrafo 5

5.18. Si provi che se $\mathbf{A}$ è una matrice diagonalizzabile, allora anche la trasposta $\mathbf{A}^T$ di $\mathbf{A}$ è diagonalizzabile.

5.19. Si trovino due matrici diagonalizzabili 2×2 $\mathbf{A}$ e $\mathbf{B}$ tali che $\mathbf{AB}$ non è diagonalizzabile.

5.20. Sia $\mathbf{P} = \mathbf{P}^2$ una matrice idempotente $n \times n$. Si provi che gli unici autovalori possibili di $\mathbf{P}$ sono 0 e 1 e che $\mathbb{C}^n = \mathrm{C}(\mathbf{P}) \oplus \mathrm{N}(\mathbf{P})$, con $\mathrm{C}(\mathbf{P}) = \mathrm{E}_{\mathbf{P}}(1)$. Si deduca che $\mathbf{P}$ è simile a $\mathbf{Diag}(\mathbf{I}_k, \mathbb{O})$, con $k = \mathrm{rk}\,\mathbf{P}$, e che $\mathrm{Tr}(\mathbf{P}) = k$.

5.21. Nelle ipotesi dell'esercizio precedente, si provi che $\mathrm{C}(\mathbf{P}) = \mathrm{N}(\mathbf{P})^{\perp}$ se e solo se $\mathbf{P}$ è normale, se e solo se $\mathbf{P}$ è una matrice di proiezione.

5.22. Siano **A** una matrice complessa $n \times n$ ed $\alpha \in \mathbb{C}$ tali che $(\mathbf{A} - \alpha\mathbf{I})^m = \mathbb{O}$, per un $m > 0$. Sia $\mathbf{A} = \mathbf{U}\mathbf{T}\mathbf{U}^H$ una decomposizione di Schur di **A**. Si provi che $(\mathbf{T} - \alpha\mathbf{I})^m = \mathbb{O}$. Si deduca che, se λ è un autovalore di **A**, allora $\lambda = \alpha$.

Paragrafo 6

5.23. Si provi il Teorema di Hamilton-Cayley per una matrice diagonale.

5.24. Sia $\mathbf{A} = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ una generica matrice 2×2. Si calcoli espressamente la matrice

$$\mathbf{A}^2 + (a+d)\mathbf{A} + (ad - bc)\mathbf{I}_2.$$

5.25. Si provi il Teorema di Hamilton-Cayley per una matrice **J** che è un λ-blocco di Jordan, cioè con elementi diagonali uguali a λ, elementi di posto $(i, i+1)$ uguali ad 1, e nulla altrove.

5.26. Sia $\mathbf{A} \in \mathrm{M}_n(\mathbb{C})$ una matrice invertibile. Si provi che $\mathbf{A}^{-1}$ si scrive come polinomio in **A** di grado $\leq n-1$.

5.27. Sia $\mathbf{A} \in \mathrm{M}_n(\mathbb{C})$. Si provi che per ogni intero $k \geq 1$, $\mathbf{A}^k$ si scrive come polinomio in **A** di grado minore o uguale a $n-1$.

5.28. Sia $\mathbf{A} = [a_{ij}] \in \mathrm{M}_n(\mathbb{C})$ e si ponga $\mathbf{A} = \mathbf{D} + \mathbf{B}$, dove $\mathbf{D} = \mathbf{Diag}(a_{11}, \dots, a_{nn})$. Per ogni numero reale ε nell'intervallo $[0,1]$, sia $\mathbf{A}_\varepsilon = \mathbf{D} + \varepsilon\mathbf{B}$; si provi che l'$i$-esimo cerchio di Gerschgorin di $\mathbf{A}_\varepsilon$ è contenuto nell'i-esimo cerchio di **A**.

5.29. Usando l'Esercizio 5.28 e il fatto che gli autovalori di una matrice sono funzioni continue dei coefficienti, si provi che ogni autovalore di **A** è l'estremo di una curva continua avente l'altro estremo in un elemento diagonale a_{ii} e contenuta nell'unione dei cerchi di Gerschgorin di **A**.

5.30. Si usi l'Esercizio 5.29 per provare che l'unione dei k cerchi considerati nel Teorema 6.2 (ii) contiene al più k autovalori di **A**. Si ragioni sui cerchi rimanenti per provare che la suddetta unione dei k cerchi contiene esattamente k autovalori.

5.31. Sia $\mathbf{A} \in \mathrm{M}_n(\mathbb{R})$ una matrice reale che ha i cerchi di Gerschgorin a due a due disgiunti. Si provi che **A** ha n autovalori distinti reali (si usino il Teorema 6.2 (ii) e il fatto che, se λ è un autovalore di **A**, anche $\overline{\lambda}$ lo è).

5.32. Si usi il Teorema di Gerschgorin per provare che gli autovalori di una matrice stocastica hanno modulo ≤ 1 (per la definizione di matrice stocastica si veda il Paragrafo 8 del Capitolo 6).

Capitolo 6

Matrici normali

In questo Capitolo vengono studiate le matrici che ammettono una diagonalizzazione tramite matrici unitarie. Viene provato il risultato che asserisce che esse coincidono con le matrici normali, già incontrate nel Capitolo 1; tale risultato costituisce il cosiddetto Teorema spettrale. Di particolare interesse all'interno della classe delle matrici normali sono le tre sottoclassi delle matrici unitarie, hermitiane e anti-hermitiane, che vengono studiate più in dettaglio. Tra le matrici hermitiane meritano un trattamento speciale le matrici definite e semidefinite positive, che intervengono in molteplici applicazioni. Una conveniente applicazione del Teorema spettrale alle matrici $\mathbf{A}\mathbf{A}^H$ e $\mathbf{A}^H\mathbf{A}$ produce una decomposizione in valori singolari di una generica matrice $\mathbf{A}$. Vengono illustrati alcuni risultati sugli autovalori delle matrici hermitiane, noti come "principi variazionali". Il capitolo viene chiuso dalla dimostrazione della famosa Legge d'inerzia di Sylvester che riguarda la relazione di congruenza tra matrici hermitiane.

1. Matrici unitarie e similitudini unitarie

Tra le matrici complesse invertibili sono di particolare interesse le matrici $\mathbf{A}$ la cui inversa coincide con la propria hermitiana: $\mathbf{A}^{-1} = \mathbf{A}^H$; nel caso reale esse sono le matrici la cui inversa coincide con la propria trasposta: $\mathbf{A}^{-1} = \mathbf{A}^T$. Si è già visto che queste matrici prendono il nome di matrici *unitarie* e di matrici reali *ortogonali*, rispettivamente. Il loro interesse consiste nel fatto che per calcolarne l'inversa non occorre eseguire l'algoritmo di Gauss-Jordan, ma semplicemente trasporre e coniugare la matrice.

Parimenti, una similitudine tra matrici è particolarmente interessante quando la matrice invertibile che produce la similitudine è una matrice unitaria (o ortogonale, nel caso reale). In tal caso le due matrici si diranno *unitariamente simili* (risp., *ortogonalmente simili*) e la relazione tra di esse una *similitudine unitaria* (risp., *similitudine ortogonale*), si veda il Paragrafo 5 del Capitolo precedente.

Per poter studiare le similitudini unitarie è utile sapere qualcosa di più sulle matrici unitarie e ortogonali reali. Raccogliamo perciò nel seguente teorema le principali proprietà delle matrici unitarie (per le matrici reali, basta sostituire la parola "unitaria" con la parola "ortogonale", $\mathbb{C}^n$ con $\mathbb{R}^n$ e l'operatore ^{H} con l'operatore ^{T}). Si faccia bene attenzione che una matrice complessa $\mathbf{A}$ non reale può essere ortogonale (cioè $\mathbf{A}^{-1} = \mathbf{A}^T$), ma in tal caso è di minore interesse rispetto alle matrici unitarie.

Teorema 1.1. *Per una matrice complessa $n \times n$ $\mathbf{U}$ le proprietà seguenti sono equivalenti:*

(i) $\mathbf{U}$ *è unitaria;*

(ii) $\mathbf{U}\mathbf{U}^H = \mathbf{I}_n = \mathbf{U}^H\mathbf{U}$*;*

(iii) $\mathbf{U}^H$ *è unitaria;*

(iv) *le colonne di* $\mathbf{U}$ *formano una base ortonormale di* $\mathbb{C}^n$*;*

(v) *le righe di* $\mathbf{U}$ *formano una base ortonormale di* $\mathbb{C}_n$*;*

(vi) *per ogni coppia di vettori* $\mathbf{u}, \mathbf{v} \in \mathbb{C}^n$*, il loro prodotto interno* $\mathbf{u}^H\mathbf{v}$ *coincide con quello dei vettori trasformati:* $(\mathbf{U}\mathbf{u})^H(\mathbf{U}\mathbf{v})$*;*

(vii) *per ogni vettore* $\mathbf{v} \in \mathbb{C}^n$*, la norma euclidea di* $\mathbf{v}$ *coincide con quella di* $\mathbf{U}\mathbf{v}$.

Dimostrazione. Lasciamo al lettore la facile dimostrazione della equivalenza di (i), (ii) e (iii).

(ii) $\Leftrightarrow$ (iv) Dire che le colonne di $\mathbf{U} = [\mathbf{u}_1 \ \dots \ \mathbf{u}_n]$ formano una base ortonormale di $\mathbb{C}^n$ equivale a dire che $\mathbf{u}_i^H\mathbf{u}_j = \delta_{ij}$ (simbolo di Kronecker). Ciò equivale a dire che $\mathbf{U}^H\mathbf{U} = \mathbf{I}_n$.

(iii) $\Leftrightarrow$ (v) Si applichi la precedente dimostrazione a $\mathbf{U}^H$.

(ii) $\Rightarrow$ (vi) $(\mathbf{U}\mathbf{u})^H(\mathbf{U}\mathbf{v}) = \mathbf{u}^H\mathbf{U}^H\mathbf{U}\mathbf{v} = \mathbf{u}^H\mathbf{I}_n\mathbf{v} = \mathbf{u}^H\mathbf{v}$.

(vi) $\Rightarrow$ (vii) È ovvio, giacché $\|\mathbf{v}\|_2^2 = \mathbf{v}^H\mathbf{v} = \mathbf{v}^H\mathbf{U}^H\mathbf{U}\mathbf{v} = \|\mathbf{U}\mathbf{v}\|_2^2$.

(vii) $\Rightarrow$ (ii) Data una generica matrice $\mathbf{A} = (a_{ij})$, discende immediatamente dalla Proposizione 2.14 del Capitolo 1 che $a_{ij} = \mathbf{e}_i^T\mathbf{A}\mathbf{e}_j$. Poiché $\mathbf{e}_i^T\mathbf{U}^H$ è la i-esima riga di $\mathbf{U}^H$ e $\mathbf{U}\mathbf{e}_j$ è la j-esima colonna di $\mathbf{U}$, dall'ipotesi si ha che:

$$\mathbf{e}_i^H\mathbf{U}^H\mathbf{U}\mathbf{e}_i = \|\mathbf{U}\mathbf{e}_i\|_2^2 = \|\mathbf{e}_i\|_2^2 = 1$$

quindi la matrice $\mathbf{A} = \mathbf{U}^H\mathbf{U}$ ha gli elementi diagonali uguali a 1. Se poi $i \neq j$, si ha:

$$(\mathbf{e}_i^H + \mathbf{e}_j^H)\mathbf{U}^H\mathbf{U}(\mathbf{e}_i + \mathbf{e}_j) = \|\mathbf{U}(\mathbf{e}_i + \mathbf{e}_j)\|_2^2 = \|\mathbf{e}_i + \mathbf{e}_j\|_2^2 = 2;$$

d'altra parte si ha:

$$\begin{aligned}(\mathbf{e}_i^H + \mathbf{e}_j^H)\mathbf{U}^H\mathbf{U}(\mathbf{e}_i + \mathbf{e}_j) &= \mathbf{e}_i^H\mathbf{A}\mathbf{e}_i + \mathbf{e}_j^H\mathbf{A}\mathbf{e}_j + \mathbf{e}_i^H\mathbf{A}\mathbf{e}_j + \mathbf{e}_j^H\mathbf{A}\mathbf{e}_i = \\ &= 1 + 1 + \mathbf{e}_i^H\mathbf{A}\mathbf{e}_j + \mathbf{e}_j^H\mathbf{A}\mathbf{e}_i.\end{aligned}$$

Pertanto, tenuto conto che $\mathbf{A}^H = \mathbf{A}$, risulta $a_{ij} + \bar{a}_{ij} = 0$. Similmente, considerando al posto del vettore $\mathbf{e}_i + \mathbf{e}_j$, il vettore $\mathbf{e}_i + i\mathbf{e}_j$ si ricava con un calcolo analogo $a_{ij} - \bar{a}_{ij} = 0$. Da ciò segue che $a_{ij} = 0$, quindi $\mathbf{U}^H\mathbf{U} = \mathbf{A}$ coincide con la matrice identica. □

Una trasformazione lineare $f : \mathbb{C}^m \to \mathbb{C}^n$ è detta una *isometria* se conserva le norme euclidee dei vettori, cioè se $\|\mathbf{v}\|_2 = \|f(\mathbf{v})\|_2$ per ogni $\mathbf{v} \in \mathbb{C}^m$. Il Teorema 1.1 dice che la trasformazione lineare di $\mathbb{C}^n$ in sé indotta da una matrice è una isometria se e solo se la matrice è unitaria.

Proposizione 1.2. *L'insieme delle matrici unitarie $n \times n$ è chiuso rispetto al passaggio alle inverse e al prodotto, e contiene la matrice identica.*

Dimostrazione. Se $\mathbf{U}$ è unitaria, tale è $\mathbf{U}^H = \mathbf{U}^{-1}$, per il Teorema 1.1; se anche $\mathbf{V}$ è unitaria, si ha

$$(\mathbf{UV})^H = \mathbf{V}^H\mathbf{U}^H = \mathbf{V}^{-1}\mathbf{U}^{-1} = (\mathbf{UV})^{-1}$$

da cui il secondo asserto. Il fatto che $\mathbf{I}_n$ è unitaria è ovvio. □

Con terminologia algebrica, la Proposizione 1.2 dice che le matrici unitarie di ordine n formano un gruppo, che è chiamato *gruppo unitario* $n \times n$; analogamente, le matrici reali ortogonali di ordine n formano un gruppo, che è chiamato *gruppo ortogonale* $n \times n$.

Dato un numero complesso $z \neq 0$, il suo coniugato $\bar{z}$ coincide con l'inverso z^{-1} se e solo se $|z| = 1$. Ciò si può esprimere dicendo (in modo un po' artefatto) che per una matrice complessa invertibile 1×1 la sua H-trasposta coincide con la inversa se e solo se il suo autovalore ha modulo 1. Questo fatto si estende alle matrici unitarie $n \times n$. Nella seguente proposizione dimostriamo la necessità; la sufficienza può essere dimostrata solo nell'ambito delle matrici normali e sarà provata nel Paragrafo successivo.

Proposizione 1.3. *Se λ è un autovalore di una matrice unitaria $\mathbf{U}$, allora $|\lambda| = 1$.*

Dimostrazione. Sia $\mathbf{Uv} = \lambda\mathbf{v}$ per un opportuno vettore non nullo $\mathbf{v}$. Si ha allora:

$$\mathbf{v}^H\mathbf{v} = \mathbf{v}^H\mathbf{U}^H\mathbf{Uv} = \bar{\lambda}\lambda\mathbf{v}^H\mathbf{v}$$

da cui, essendo $\|\mathbf{v}\| \neq 0$, si ricava che $1 = \bar{\lambda}\lambda = |\lambda|^2$. □

Passiamo ora a considerare le diagonalizzazioni unitarie. Il loro significato geometrico è chiarito dal seguente risultato.

Teorema 1.4. *Per una matrice complessa $n \times n$ $\mathbf{A}$, i fatti seguenti sono equivalenti:*

(a) $\mathbf{A}$ *è unitariamente diagonalizzabile;*

(b) $\mathbb{C}^n$ *ha una base ortonormale costituita da autovettori di* $\mathbf{A}$*;*

(c) $\mathbf{A}$ *è diagonalizzabile e autospazi relativi ad autovettori distinti sono tra di loro ortogonali.*

Dimostrazione. (a) $\Rightarrow$ (b) La dimostrazione è in tutto simile a quella del Teorema 5 del Capitolo 5, salvo che, essendo le colonne della matrice diagonalizzante un sistema ortonormale, la base di $\mathbb{C}^n$ che se ne ricava risulta ortonormale.

(b) $\Rightarrow$ (c) Il fatto che $\mathbf{A}$ sia diagonalizzabile consegue ancora dal Teorema 5 del Capitolo 5. Gli autovettori della base relativi a un medesimo autovalore λ formano una base dell'autospazio $\mathrm{E}_\mathbf{A}(\lambda)$; ne consegue che, se μ è un autovalore diverso da λ, $\mathrm{E}_\mathbf{A}(\lambda)$ ed $\mathrm{E}_\mathbf{A}(\mu)$ sono generati da vettori a due a due ortogonali, perciò ogni vettore in $\mathrm{E}_\mathbf{A}(\lambda)$ è ortogonale a ogni vettore in $\mathrm{E}_\mathbf{A}(\mu)$.

(c) $\Rightarrow$ (a) Scegliendo in ogni autospazio una base ortonormale, l'ipotesi assicura che l'insieme che si ottiene dall'unione di tali basi costituisce una base ortonormale di

$\mathbb{C}^n$, quindi la matrice che ha come colonne tale base e che diagonalizza la matrice $\mathbf{A}$ è unitaria. □

Osservazione 1.5. Non è detto che, scelta comunque una base di autovettori di una matrice unitariamente diagonalizzabile $\mathbf{A}$, essa risulti una base ortonormale, e quindi la matrice che se ne ricava non è detto risulti unitaria. Infatti il Teorema 1.4 assicura che risultano tra di loro ortogonali solo autovettori appartenenti ad autospazi distinti. Perché la base di autovettori risulti ortonormale occorre scegliere ogni singola base di ciascun autospazio ortonormale.

Per esempio, la matrice diagonale $\mathbf{D} = \mathbf{Diag}(-1,-1,2)$ è banalmente unitariamente diagonalizzabile. I suoi autovalori sono $\lambda_1 = -1$ con autospazio $\mathrm{E}_{\mathbf{A}}(\lambda_1)$ generato dai vettori $\mathbf{e}_1$ ed $\mathbf{e}_2$, e $\lambda_2 = 2$ con autospazio $\mathrm{E}_{\mathbf{A}}(\lambda_2)$ generato dal vettore $\mathbf{e}_3$. Se scegliamo come base di $\mathrm{E}_{\mathbf{A}}(\lambda_1)$ i vettori $[1\ 2\ 0]^T$ e $[2\ 1\ 0]^T$, e come base di $\mathrm{E}_{\mathbf{A}}(\lambda_2)$ il vettore $[0\ 0\ 3]^T$, abbiamo la diagonalizzazione di $\mathbf{D}$:

$$\mathbf{D} = \begin{bmatrix} 1 & 2 & 0 \\ 2 & 1 & 0 \\ 0 & 0 & 3 \end{bmatrix} \cdot \begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 2 \end{bmatrix} \cdot \begin{bmatrix} -1/3 & 2/3 & 0 \\ 2/3 & -1/3 & \\ 0 & 0 & 1/3 \end{bmatrix}.$$

Esempio 1.6. La matrice

$$\mathbf{A} = \begin{bmatrix} 1+i & 1 \\ 2 & 1-i \end{bmatrix}$$

ha polinomio caratteristico $p_{\mathbf{A}}(X) = X^2 - 2X$, quindi ha autovalori $\lambda_1 = 0$ con autospazio generato dal vettore $\mathbf{u}_1 = [-1\ 1+i]^T$, e $\lambda_2 = 2$ con autospazio generato dal vettore $\mathbf{u}_2 = [1\ 1-i]^T$. Poiché $\mathbf{u}_1^H\mathbf{u}_2 = -1-2i \neq 0$, i due autospazi non sono ortogonali, quindi la matrice $\mathbf{A}$ non è unitariamente diagonalizzabile. Ciò è in accordo col Teorema spettrale che proveremo nel prossimo Paragrafo, giacché $\mathbf{A}\mathbf{A}^H \neq \mathbf{A}^H\mathbf{A}$ (verificare). □

Il risultato analogo al Teorema 1.4 in ambiente reale, di cui omettiamo la semplice dimostrazione che il lettore può svolgere imitando quella del Teorema 1.4, è il seguente.

Teorema 1.7. *Per una matrice reale $n \times n$ $\mathbf{A}$, i fatti seguenti sono equivalenti:*

(a) $\mathbf{A}$ *è simile tramite una matrice reale ortogonale a una matrice reale diagonale;*

(b) $\mathbf{A}$ *ha tutti i suoi autovalori reali e $\mathbb{R}^n$ ha una base ortonormale costituita da autovettori di* $\mathbf{A}$*;*

(c) $\mathbf{A}$ *è diagonalizzabile, ha tutti i suoi autovalori reali, e autospazi relativi ad autovettori distinti sono tra di loro ortogonali.*

Esempi di matrici ortogonali e unitarie

Esempio 1.8 (Matrici di permutazione)**.** I più semplici esempi di matrici ortogonali sono offerti dalle matrici di permutazione, che abbiamo già incontrato nel Paragrafo 6 del Capitolo 1, nell'ambito dell'eliminazione di Gauss; esse intervengono infatti quando bisogna scambiare le righe di una matrice per avere dei *pivot* non nulli. Una matrice di permutazione $\mathbf{P}$ può essere definita come una matrice che ha in ogni riga e in ogni colonna un unico 1 e tutti gli altri coefficienti uguali a 0; equivalentemente, $\mathbf{P}$ è definita come un prodotto di matrici di trasposizione. Da questa seconda definizione segue facilmente che $\mathbf{P}^{-1} = \mathbf{P}^T$ (si veda l'Esercizio 1.46 del Capitolo 1); quindi le matrici di permutazione sono matrici reali ortogonali.

Data una matrice di permutazione $\mathbf{P}$ e una qualunque matrice del medesimo ordine $\mathbf{A}$, l'operazione che trasforma la matrice $\mathbf{A}$ nella matrice $\mathbf{PAP}^T$ si chiama *cogredienza* (si vedano gli Esercizi 1.48 e 1.49 del Capitolo 1). Ricordiamo che l'operazione che tramite una matrice invertibile $\mathbf{S}$ trasforma la matrice $\mathbf{A}$ nella matrice $\mathbf{SAS}^T$ si chiama invece *congruenza*. Una cogredienza è sia una similitudine che una congruenza.

Vale la pena di ricordare un importante ambito di applicazione delle matrici di permutazione. Una matrice quadrata si dice *doppiamente stocastica* se i suoi coefficienti sono numeri reali non negativi tali che la somma di ogni riga e di ogni colonna è uguale a 1. Le matrici di permutazione sono ovviamente doppiamente stocastiche; un famoso teorema di Birkhoff asserisce che le matrici doppiamente stocastiche sono esattamente le combinazioni convesse delle matrici di permutazione (si veda il Teorema 8.5). □

Esempio 1.9 (Matrici di rotazione)**.** Una *matrice di rotazione* è una matrice 2×2 del tipo

$$\mathbf{R}_\alpha = \begin{bmatrix} \cos\alpha & -\operatorname{sen}\alpha \\ \operatorname{sen}\alpha & \cos\alpha \end{bmatrix}$$

dove $0 \le \alpha < 2\pi$. Dalla relazione trigonometrica $(\cos\alpha)^2 + (\operatorname{sen}\alpha)^2 = 1$ segue che $\mathbf{R}_\alpha$ è una matrice ortogonale. È un facile esercizio di geometria elementare (si veda l'Esercizio 6.2) provare che la pre-moltiplicazione per la matrice $\mathbf{R}_\alpha$ in $\mathbb{R}^2$ ha l'effetto di ruotare i vettori di α radianti in senso anti-orario.

Una *matrice di rotazione generalizzata* è una matrice $n \times n$ $(n > 2)$ contenente come sottomatrice principale una matrice di rotazione e che al di fuori di tale sottomatrice coincide con la matrice identica. Pertanto una matrice di questo tipo ha nei posti i e j $(i \neq j)$ della diagonale coefficienti uguali a $\cos\alpha$, nel posto (i, j) coefficiente uguale a $-\operatorname{sen}\alpha$, nel posto (j, i) coefficiente uguale a $\operatorname{sen}\alpha$, e nei restanti posti coincide con $\mathbf{I}_n$. Da quanto detto sopra si ricava che la pre-moltiplicazione per una tale matrice in $\mathbb{R}^n$ ha l'effetto di ruotare la proiezione di un vettore sul sottospazio $\langle \mathbf{e}_i; \mathbf{e}_j \rangle$ di α radianti in senso anti-orario e di lasciare fissa la proiezione sul sottospazio complemento ortogonale di $\langle \mathbf{e}_i; \mathbf{e}_j \rangle$. Le matrici di rotazione generalizzate sono ovviamente matrici ortogonali. □

Esempio 1.10 (Matrici di Householder)**.** Sia $\mathbf{w} \in \mathbb{C}^n$ un vettore di norma euclidea 1: $\mathbf{w}^H\mathbf{w} = 1$. Si consideri la matrice

$$\mathbf{H}_\mathbf{w} = \mathbf{I}_n - 2\mathbf{w}\mathbf{w}^H$$

che si chiama *matrice di Householder* associata a $\mathbf{w}$; $\mathbf{H}_\mathbf{w}$ è una matrice $n \times n$ complessa e, se $\mathbf{w} \in \mathbb{R}^n$, è una matrice reale.

Si può anche partire da un vettore non nullo $\mathbf{w} \in \mathbb{C}^n$ di norma arbitraria e definire $\mathbf{H_w}$ come la matrice $\mathbf{I}_n - (2/\mathbf{w}^H\mathbf{w})\mathbf{w}\mathbf{w}^H$, ma useremo sempre la definizione precedente.

Vediamo alcune semplici proprietà delle matrici di Householder.

(I) $\mathbf{H_w}$ *è una matrice hermitiana e unitaria.*

La verifica che $\mathbf{H_w}$ è hermitiana è banale; verifichiamo che è unitaria:

$$\mathbf{H_w}\mathbf{H_w}^H = \mathbf{H_w}^2 = \mathbf{I}_n - 4\mathbf{w}\mathbf{w}^H\mathbf{w}\mathbf{w}^H + 4\mathbf{w}\mathbf{w}^H\mathbf{w}\mathbf{w}^H = \mathbf{I}_n.$$

(II) $\det(\mathbf{H_w}) = -1$.

Sia $\mathbf{A} = [\mathbf{w}\mathbf{v}_2 \ldots \mathbf{v}_n]$ la matrice con prima colonna il vettore $\mathbf{w}$ e successive colonne i vettori di una base ortonormale dello spazio $\langle \mathbf{w} \rangle^\perp$. Calcoliamo le colonne della matrice $\mathbf{H_w}\mathbf{A}$:

$$\begin{aligned}\mathbf{H_w}\mathbf{A} &= (\mathbf{I}_n - 2\mathbf{w}\mathbf{w}^H)\mathbf{A} \\ &= \mathbf{A} - 2\mathbf{w}\mathbf{w}^H\mathbf{A} \\ &= [-\mathbf{w}\,\mathbf{v}_2\ \ldots\ \mathbf{v}_n]\end{aligned}$$

dove si è tenuto conto che $\mathbf{w}^H\mathbf{w} = 1$ e $\mathbf{w}^H\mathbf{v}_i = 0$. Ne consegue che

$$\det(\mathbf{H_w})\det(\mathbf{A}) = \det(\mathbf{H_w}\mathbf{A}) = -\det(\mathbf{A})$$

e poiché $\det(\mathbf{A}) \neq 0$ si conclude che $\det(\mathbf{H_w}) = -1$.

Dal fatto che una matrice di Householder $\mathbf{H_w}$ è unitaria e dal Teorema 1.1 (vii) si ricava che, dato un vettore $\mathbf{u} \in \mathbb{C}^n$, la norma euclidea di $\mathbf{u}$ coincide con quella di $\mathbf{H_w}\mathbf{u}$; inoltre si ha che $\mathbf{u}^H\mathbf{H_w}\mathbf{u}$ è un numero reale, perché la matrice $\mathbf{H_w}$ è hermitiana. La proprietà seguente dà in un certo senso l'inverso di questo fatto.

(III) *Dati due vettori* $\mathbf{u} \neq \mathbf{v} \in \mathbb{C}^n$ *di uguale norma euclidea e tali che* $\mathbf{u}^H\mathbf{v} \in \mathbb{R}$*, esiste una matrice di Householder* $\mathbf{H_w}$ *tale che* $\mathbf{H_w}\mathbf{u} = \mathbf{v}$.

Si ponga $\mathbf{w} = (\mathbf{u}-\mathbf{v})/\|\mathbf{u}-\mathbf{v}\|_2$. Si lascia al lettore la facile verifica del fatto che $\mathbf{H_w}\mathbf{u} = \mathbf{v}$, tenuto conto che $\mathbf{u}^H\mathbf{v} = \mathbf{v}^H\mathbf{u}$ (si veda l'Esercizio 6.4).

Diamo ora un'interpretazione geometrica dell'azione svolta dalla pre-moltiplicazione in $\mathbb{C}^n$ per una matrice di Householder $\mathbf{H_w}$. Denoteremo con V lo spazio vettoriale complemento ortogonale del vettore $\mathbf{w}$, cioè $V = \{\mathbf{v} \in \mathbb{C}^n \mid \mathbf{v}^H\mathbf{w} = 0\} = \langle \mathbf{w} \rangle^\perp$, e con $\mathbf{P}_V$ la matrice di proiezione di $\mathbb{C}^n$ su V; naturalmente la matrice di proiezione su $\langle \mathbf{w} \rangle$ è data da $\mathbf{I}_n - \mathbf{P}_V = \mathbf{w}\mathbf{w}^H$. Osserviamo che, se $\mathbf{u} \in \mathbb{C}^n$, la riflessione $\mathbf{u}'$ di $\mathbf{u}$ rispetto al sottospazio V è caratterizzata dalle due proprietà:

$$\mathbf{P}_V\mathbf{u}' = \mathbf{P}_V\mathbf{u}, \qquad (\mathbf{I}_n - \mathbf{P}_V)\mathbf{u}' = -(\mathbf{I}_n - \mathbf{P}_V)\mathbf{u}$$

perciò $\mathbf{u}' = -\mathbf{u} + 2\mathbf{P}_V\mathbf{u}$. Ne deduciamo la seguente proprietà.

(IV) *La pre-moltiplicazione in* $\mathbb{C}^n$ *per la matrice di Householder* $\mathbf{H_w}$ *opera come la riflessione rispetto al sottospazio* $V = \langle \mathbf{w} \rangle^\perp$.

Se $\mathbf{u} \in \mathbb{C}^n$, $\mathbf{H_w}\mathbf{u} = \mathbf{u} - 2\mathbf{w}\mathbf{w}^H\mathbf{u} = \mathbf{u} - 2(\mathbf{I}_n - \mathbf{P}_V)\mathbf{u} = -\mathbf{u} + 2\mathbf{P}_V\mathbf{u} = \mathbf{u}'$. □

Esempio 1.11 (Matrici di Householder generalizzate)**.** Le matrici di Householder possono essere generalizzate considerando, anziché un vettore $\mathbf{w}$ di norma 1 e il sottospazio suo complemento ortogonale $V = \langle \mathbf{w} \rangle^{\perp}$, un sottospazio W di dimensione > 1 e il suo complemento ortogonale $V = W^{\perp}$.

Se denotiamo ancora con $\mathbf{P}_W$ e $\mathbf{P}_V = \mathbf{I}_n - \mathbf{P}_W$ le due matrici di proiezione su tali sottospazi, definiamo come *matrice di Householder generalizzata* associata al sottospazio W di $\mathbb{C}^n$ la matrice

$$\mathbf{H}_W = \mathbf{I}_n - 2\mathbf{P}_W.$$

Poiché le matrici di proiezione sono hermitiane e idempotenti, segue facilmente come in (I) che $\mathbf{H}_W$ è hermitiana e unitaria. Con ragionamento analogo a quello fatto in (II) si prova che $\det(\mathbf{H}_W) = (-1)^d$, dove $d = \dim W$. Infine, analogamente a quanto fatto in (IV), si vede che la pre-moltiplicazione in $\mathbb{C}^n$ per la matrice $\mathbf{H}_W$ opera sui vettori $\mathbf{u} \in \mathbb{C}^n$ come la riflessione rispetto al sottospazio $V = W^{\perp}$, cioè, posto $\mathbf{u}' = \mathbf{H}_W \mathbf{u}$, risulta:

$$\mathbf{P}_V \mathbf{u} = \mathbf{P}_V \mathbf{u}', \qquad \mathbf{P}_W \mathbf{u} = -\mathbf{P}_W \mathbf{u}'. \qquad \square$$

2. Matrici normali e teorema spettrale

Abbiamo già incontrato le matrici normali nella Proposizione 2.6 del Capitolo 1, dove abbiamo provato che la parte hermitiana e quella anti-hermitiana di una matrice commutano se e solo se la matrice è normale, cioè commuta con la sua H-trasposta.

Il termine “normale” per una matrice $n \times n$ con $n > 1$ non va inteso nel senso di matrice che si incontra usualmente; infatti la condizione di normalità è una condizione forte, raramente verificata nell’ambito di tutte le matrici $n \times n$ (si veda l’Esercizio 6.9). Pur tuttavia, c’è abbondanza di esempi di matrici normali.

Esempio 2.1. Le matrici diagonali sono banalmente matrici normali. È immediato inoltre verificare che tali sono le matrici unitarie $\mathbf{U}$ ($\mathbf{U}^H\mathbf{U} = \mathbf{I} = \mathbf{U}\mathbf{U}^H$), le matrici hermitiane $\mathbf{A}$ ($\mathbf{A}^H\mathbf{A} = \mathbf{A}^2 = \mathbf{A}\mathbf{A}^H$), e quelle anti-hermitiane $\mathbf{B}$ ($\mathbf{B}^H\mathbf{B} = -\mathbf{B}^2 = \mathbf{B}\mathbf{B}^H$). $\square$

I tre tipi di matrici elencate nel precedente Esempio possono essere caratterizzate, all’interno della classe delle matrici normali, tramite proprietà dei loro autovalori. La dimostrazione della sufficienza nei tre casi fa uso del Teorema spettrale, che sarà provato subito dopo.

Teorema 2.2. *Sia* $\mathbf{A}$ *una matrice normale.*
(a) $\mathbf{A}$ *è unitaria se e solo se i suoi autovalori hanno modulo* 1*;*
(b) $\mathbf{A}$ *è hermitiana se e solo se i suoi autovalori sono numeri reali;*
(c) $\mathbf{A}$ *è anti-hermitiana se e solo se i suoi autovalori sono numeri immaginari.*

Dimostrazione. (a) La necessità è già stata provata nella Proposizione 1.3.

Viceversa, per il Teorema spettrale si ha: $\mathbf{A} = \mathbf{U}\mathbf{D}\mathbf{U}^H$, con $\mathbf{U}$ unitaria e $\mathbf{D}$ diagonale; gli elementi diagonali d_i di $\mathbf{D}$, essendo gli autovalori di $\mathbf{A}$, hanno modulo 1. Risulta allora:

$$\mathbf{A}^H\mathbf{A} = \mathbf{U}\overline{\mathbf{D}}\mathbf{U}^H\mathbf{U}\mathbf{D}\mathbf{U}^H = \mathbf{U}\overline{\mathbf{D}}\mathbf{D}\mathbf{U}^H.$$

Ma $\overline{\mathbf{D}}\mathbf{D} = \mathbf{Diag}(|d_1|^2, \ldots, |d_n|^2) = \mathbf{I}$, da cui segue che $\mathbf{A}^H\mathbf{A} = \mathbf{I}$.

(b) Sia $\mathbf{A}$ hermitiana e sia $\mathbf{Av} = \lambda\mathbf{v}$ per un vettore $\mathbf{v} \neq \mathbf{0}$. Pre-moltiplicando ambo i membri per $\mathbf{v}^H$ si ricava:

$$\mathbf{v}^H\mathbf{Av} = \lambda\|\mathbf{v}\|_2^2.$$

Tenuto conto che $\mathbf{A} = \mathbf{A}^H$, il numero complesso $z = \mathbf{v}^H\mathbf{Av}$ coincide col proprio coniugato, quindi è un numero reale; ne consegue che $\lambda = z/\|\mathbf{v}\|_2^2$ è pure reale. Viceversa, per il Teorema spettrale si ha: $\mathbf{A} = \mathbf{UDU}^H$, con $\mathbf{U}$ unitaria e $\mathbf{D}$ diagonale; gli elementi diagonali di $\mathbf{D}$, essendo gli autovalori di $\mathbf{A}$, sono numeri reali. Ne consegue che $\mathbf{D} = \overline{\mathbf{D}}$ e quindi $\mathbf{A} = \mathbf{UDU}^H = \mathbf{U}\overline{\mathbf{D}}\mathbf{U}^H = \mathbf{A}^H$.

(c) La dimostrazione, in tutto simile a quella del punto (b), è lasciata al lettore come esercizio. □

Alcune proprietà delle matrici unitarie sono state studiate nel Paragrafo precedente; le matrici hermitiane saranno oggetto di studio del prossimo Paragrafo; quelle anti-hermitiane sono in parte riconducibili a quelle hermitiane, giacché è immediato verificare che una matrice $\mathbf{A}$ è anti-hermitiana se e solo se la matrice $i\mathbf{A}$ è hermitiana (si veda l'Esercizio 6.12).

Passiamo ora al risultato centrale di questo Paragrafo, uno dei più importanti teoremi della trattazione di autovalori e autovettori.

Teorema spettrale 2.3. *Una matrice complessa* $\mathbf{A}$ *è unitariamente diagonalizzabile se e solo se è normale.*

Dimostrazione. Per la necessità basta una semplice verifica: se $\mathbf{A} = \mathbf{UDU}^H$, con $\mathbf{U}$ unitaria e $\mathbf{D}$ diagonale, risulta

$$\begin{aligned}
\mathbf{AA}^H &= \mathbf{UDU}^H\mathbf{UD}^H\mathbf{U}^H \\
&= \mathbf{UDD}^H\mathbf{U}^H \\
&= \mathbf{UD}^H\mathbf{DU}^H \\
&= \mathbf{UD}^H\mathbf{U}^H\mathbf{UDU}^H \\
&= \mathbf{A}^H\mathbf{A}
\end{aligned}$$

dove si è usato il fatto che $\mathbf{DD}^H = \mathbf{D}^H\mathbf{D}$.

Per la sufficienza si parte dal risultato assicurato dal Teorema di Schur: $\mathbf{A} = \mathbf{UTU}^H$, con $\mathbf{U}$ unitaria e $\mathbf{T}$ triangolare superiore. Si prova da prima che anche $\mathbf{T}$ è normale, poi si prova che una matrice triangolare e normale deve essere diagonale.

La verifica che $\mathbf{T}$ è normale è immediata:

$$\begin{aligned}
\mathbf{TT}^H &= \mathbf{U}^{-1}\mathbf{AUU}^{-1}\mathbf{A}^H\mathbf{U} \\
&= \mathbf{U}^{-1}\mathbf{AA}^H\mathbf{U} \\
&= \mathbf{U}^{-1}\mathbf{A}^H\mathbf{AU} \\
&= \mathbf{U}^{-1}\mathbf{A}^H\mathbf{UU}^{-1}\mathbf{AU} \\
&= \mathbf{T}^H\mathbf{T}.
\end{aligned}$$

Proviamo ora che $\mathbf{T}$ è diagonale per induzione sull'ordine n di $\mathbf{T}$. Se $n = 1$ l'asserto è banale. Sia allora $n > 1$ e l'asserto vero per le matrici triangolari normali di ordine $n-1$. Scriviamo $\mathbf{T}$ in forma bordata:

$$\mathbf{T} = \begin{bmatrix} t & \mathbf{x}^H \\ \mathbf{0} & \mathbf{S} \end{bmatrix}$$

dove $\mathbf{S}$ è una matrice triangolare di ordine $n-1$. Proviamo che $\mathbf{S}$ è normale, di modo che potremo applicare a $\mathbf{S}$ l'ipotesi induttiva. Si ha infatti:

$$\mathbf{T}\mathbf{T}^H = \begin{bmatrix} |t|^2 + \mathbf{x}^H\mathbf{x} & \mathbf{x}^H\mathbf{S}^H \\ \mathbf{S}\mathbf{x} & \mathbf{S}\mathbf{S}^H \end{bmatrix}$$
$$\mathbf{T}^H\mathbf{T} = \begin{bmatrix} |t|^2 & \bar{t}\mathbf{x}^H \\ t\mathbf{x} & \mathbf{x}\mathbf{x}^H + \mathbf{S}^H\mathbf{S} \end{bmatrix}.$$

Dal fatto che $\mathbf{T}$ è normale si deduce, confrontando i blocchi di posto $(1,1)$, che $\mathbf{x}^H\mathbf{x} = 0$, e quindi $\mathbf{x} = \mathbf{0}$; confrontando i blocchi di posto $(2,2)$, si ricava $\mathbf{S}\mathbf{S}^H = \mathbf{S}^H\mathbf{S}$, cioè $\mathbf{S}$ è normale.

Per l'ipotesi induttiva $\mathbf{S}$ è diagonale quindi, ricordandoci che $\mathbf{x} = \mathbf{0}$, si deduce che $\mathbf{T}$ è pure diagonale. □

Ricordiamo che, dato un sottospazio vettoriale V di $\mathbb{C}^n$, si denota con $P_V : \mathbb{C}^n \to \mathbb{C}^n$ la trasformazione lineare proiezione ortogonale su V. Essa si può realizzare come la moltiplicazione per una matrice di proiezione $\mathbf{P}_V$, che si ottiene da una qualunque base ortonormale $\{\mathbf{v}_1; \dots; \mathbf{v}_r\}$ di V come somma di matrici di proiezione di rango 1 nel modo seguente:

$$\mathbf{P}_V = \mathbf{v}_1\mathbf{v}_1^H + \cdots + \mathbf{v}_r\mathbf{v}_r^H.$$

Sappiamo che le matrici di proiezione sono hermitiane e idempotenti e sono indipendenti dalla base ortonormale scelta per ottenerle.

Vedremo ora la versione additiva del teorema spettrale, che dice in sostanza che la moltiplicazione in $\mathbb{C}^n$ per una matrice normale agisce come la somma delle matrici di proiezione sui diversi autospazi ciascuna moltiplicata per il corrispondente autovalore (questo vale per ogni matrice diagonalizzabile, si veda la successiva Osservazione 2.5) e tali matrici di proiezione hanno due a due prodotto nullo.

Teorema spettrale 2.4 (versione additiva)**.** *Una matrice complessa* $\mathbf{A}$ *è unitariamente diagonalizzabile se e solo se è del tipo*

$$\lambda_1\mathbf{P}_1 + \cdots + \lambda_r\mathbf{P}_r$$

dove gli scalari λ_i *sono i suoi distinti autovalori e le matrici* $\mathbf{P}_i$ *sono le matrici di proiezione sui relativi autospazi e soddisfano alle condizioni* $\mathbf{P}_i\mathbf{P}_j = \mathbb{O}$ *per* $i \neq j$.

Dimostrazione. Siano $\lambda_1, \dots, \lambda_r$ gli autovalori distinti di $\mathbf{A}$, con rispettive molteplicità algebriche $m_1, \dots, m_r$. Se $\mathbf{A} = \mathbf{U}\mathbf{D}\mathbf{U}^H$, con $\mathbf{U} = [\mathbf{u}_1 \ \dots \ \mathbf{u}_n]$ matrice unitaria e $\mathbf{D} =$

$\mathbf{Diag}(d_1, \dots, d_n)$ matrice diagonale, non è restrittivo supporre che gli autovalori coincidenti compaiano consecutivamente sulla diagonale di $\mathbf{D}$:

$$\lambda_1 = d_1 = \cdots = d_{m_1}, \dots, \lambda_r = d_{n-m_r+1} = \cdots = d_n.$$

Di conseguenza, l'insieme $\{\mathbf{u}_1; \dots; \mathbf{u}_{m_1}\}$ è una base ortonormale dell'autospazio $\mathrm{E}_{\mathbf{A}}(\lambda_1)$, l'insieme $\{\mathbf{u}_{m_1+1}; \dots; \mathbf{u}_{m_1+m_2}\}$ è una base ortonormale dell'autospazio $\mathrm{E}_{\mathbf{A}}(\lambda_2)$, eccetera. Un calcolo diretto del prodotto (righe per colonne) $\mathbf{A} = \mathbf{UDU}^H$ mostra che risulta

$$\mathbf{A} = \sum_{i \le n} d_i \mathbf{u}_i \mathbf{u}_i^H.$$

Raggruppando gli scalari d_i coincidenti si ha (avendo posto $m_0 = 0$ e $k_i = m_0 + m_1 + \ldots + m_i$):

$$\mathbf{A} = \sum_{i \le r} \lambda_i \sum_{k_{i-1} < j \le k_i} \mathbf{u}_j \mathbf{u}_j^H.$$

Ma, come si è ricordato sopra,

$$\mathbf{P}_i = \sum_{k_{i-1} < j \le k_i} \mathbf{u}_j \mathbf{u}_j^H$$

non è altro che la matrice di proiezione sull'autospazio $\mathrm{E}_{\mathbf{A}}(\lambda_i)$. Poiché, se $i \neq j$, ogni colonna di $\mathbf{P}_i$ è ortogonale a ogni colonna di $\mathbf{P}_j$, ne consegue immediatamente che $\mathbf{P}_i \mathbf{P}_j = \mathbf{P}_i^H \mathbf{P}_j = \mathbb{O}$, come desiderato.

Viceversa, sia $\mathbf{A} = \lambda_1 \mathbf{P}_1 + \ldots + \lambda_r \mathbf{P}_r$ con $\mathbf{P}_i \mathbf{P}_j = \mathbb{O}$ per $i \neq j$. Un calcolo diretto, tenuto conto che le matrici $\mathbf{P}_i$ sono hermitiane e idempotenti, mostra che $\mathbf{AA}^H = \mathbf{A}^H\mathbf{A}$, quindi l'asserto segue dal Teorema 2.3. □

Osservazione 2.5. Come già accennato, il ragionamento fornito nella precedente dimostrazione si applica a ogni matrice diagonalizzabile $\mathbf{A}$, tranne che per il fatto che non è vero che $\mathbf{P}_i \mathbf{P}_j = \mathbb{O}$ per $i \neq j$. Infatti, per una matrice non normale $\mathbf{A}$ non è vero che gli autospazi di autovettori distinti sono ortogonali. Si possono però ancora scegliere le basi di ciascun autospazio ortonormali, pervenendo a una diagonalizzazione $\mathbf{A} = \mathbf{SDS}^{-1}$ con $\mathbf{S} = [\mathbf{S}_1 \ \dots \ \mathbf{S}_r]$ avente r blocchi $\mathbf{S}_i$ formati ciascuno da colonne ortonormali (le basi degli r autospazi), soddisfacenti quindi alle uguaglianze $\mathbf{S}_i^H \mathbf{S}_i = \mathbf{I}_{m_i}$, dove m_i è la molteplicità algebrica e geometrica dell'autovalore λ_i.

Esempio 2.6. Si consideri la matrice simmetrica reale

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

La matrice $\mathbf{A}$ è normale con autovalori reali, quindi ortogonalmente diagonalizzabile. Una sua diagonalizzazione con matrice ortogonale $\mathbf{Q} = [\mathbf{u}_1 \ \mathbf{u}_2 \ \mathbf{u}_3]$ è data da:

$$\begin{aligned} \mathbf{A} &= \mathbf{Q\Lambda Q}^T \\ &= \frac{1}{\sqrt{6}} \begin{bmatrix} -\sqrt{3} & 1 & \sqrt{2} \\ \sqrt{3} & 1 & \sqrt{2} \\ 0 & -2 & \sqrt{2} \end{bmatrix} \begin{bmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & -3 \end{bmatrix} \frac{1}{\sqrt{6}} \begin{bmatrix} -\sqrt{3} & \sqrt{3} & 0 \\ 1 & 1 & -2 \\ \sqrt{2} & \sqrt{2} & \sqrt{2} \end{bmatrix}. \end{aligned}$$

La versione additiva del Teorema spettrale porge la decomposizione

$$\mathbf{A} = 3\mathbf{P}_1 - 3\mathbf{P}_2 = 3 \cdot \frac{1}{3}\begin{bmatrix} 2 & -1 & -1 \\ -1 & 2 & -1 \\ -1 & -1 & 2 \end{bmatrix} - 3 \cdot \frac{1}{3}\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

dove $\mathbf{P}_1 = \mathbf{u}_1\mathbf{u}_1^H + \mathbf{u}_2\mathbf{u}_2^H$ è la matrice di proiezione sull'autospazio $\mathrm{E}_{\mathbf{A}}(3)$ e $\mathbf{P}_2 = \mathbf{u}_3\mathbf{u}_3^H$ è la matrice di proiezione sull'autospazio $\mathrm{E}_{\mathbf{A}}(-3)$. □

Se $\mathbf{A} = [a_{ij}]$ è una matrice qualunque, risulta

$$\mathrm{Tr}(\mathbf{A}\mathbf{A}^H) = \mathrm{Tr}(\mathbf{A}^H\mathbf{A}) = \sum_{i,j} |a_{ij}|^2$$

(si veda l'Esercizio 6.16). Per le matrici normali si ha una caratterizzazione tramite questa quantità confrontata con una quantità derivata dagli autovalori (queste quantità si esprimono tecnicamente in termini di opportune norme matriciali).

Proposizione 2.7. *Una matrice complessa* $\mathbf{A} = [a_{ij}]$*, con autovalori* $d_1, \dots, d_n$ *(ripetuti con le loro molteplicità algebriche), è normale se e solo se* $\mathrm{Tr}(\mathbf{A}\mathbf{A}^H) = \sum_i |d_i|^2$.

Dimostrazione. Se $\mathbf{A} = \mathbf{U}\mathbf{D}\mathbf{U}^H$ è normale (le notazioni sono quelle della dimostrazione del Teorema 2.4), allora, ricordando che $\mathrm{Tr}(\mathbf{XY}) = \mathrm{Tr}(\mathbf{YX})$ per ogni coppia di matrici $\mathbf{X}$ e $\mathbf{Y}$ e moltiplicabili nei due sensi, si ha

$$\mathrm{Tr}(\mathbf{A}\mathbf{A}^H) = \mathrm{Tr}(\mathbf{U}\mathbf{D}\mathbf{U}^H\mathbf{U}\mathbf{D}^H\mathbf{U}^H) = \mathrm{Tr}(\mathbf{U}^H\mathbf{U}\mathbf{D}\mathbf{D}^H) = \mathrm{Tr}(\mathbf{D}\mathbf{D}^H) = \sum_i |d_i|^2.$$

Viceversa, sia $\mathrm{Tr}(\mathbf{A}\mathbf{A}^H) = \sum_i |d_i|^2$. Da una fattorizzazione $\mathbf{A} = \mathbf{U}\mathbf{T}\mathbf{U}^H$ ottenuta dal Teorema di Schur, con $\mathbf{T} = (t_{ij})$ matrice triangolare e $\mathbf{U}$ matrice unitaria, si ricava che gli elementi t_{ii} coincidono (a meno dell'ordine) con gli autovalori d_i e che $\mathbf{A}\mathbf{A}^H = \mathbf{U}\mathbf{T}\mathbf{T}^H\mathbf{U}^H$. Di conseguenza

$$\sum_i |d_i|^2 = \mathrm{Tr}(\mathbf{A}\mathbf{A}^H) = \mathrm{Tr}(\mathbf{U}\mathbf{T}\mathbf{T}^H\mathbf{U}^H) = \mathrm{Tr}(\mathbf{U}^H\mathbf{U}\mathbf{T}\mathbf{T}^H) = \mathrm{Tr}(\mathbf{T}\mathbf{T}^H) = \sum_{i,j} |t_{ij}|^2$$

da cui, in virtù del fatto che $\sum_i |d_i|^2 = \sum_i |t_{ii}|^2$, si ricava che $t_{ij} = 0$ per $i \neq j$, ovvero, $\mathbf{T}$ è diagonale e $\mathbf{A}$ è unitariamente diagonalizzabile. La conclusione segue dal Teorema spettrale. □

3. Matrici simmetriche e hermitiane

In questo Paragrafo daremo alcune informazioni di base sulle matrici simmetriche reali e sulle matrici complesse hermitiane. Esse sono tra le matrici più studiate, fin dal XIX secolo, anche perché intimamente legate alle forme quadratiche complesse e reali: vediamo come.

A ogni matrice $\mathbf{A} = [a_{ij}] \in \mathrm{M}_n(\mathbb{C})$ si può associare la forma quadratica complessa n-dimensionale $Q\colon \mathbb{C}^n \to \mathbb{C}$ tale che, per ogni vettore $\mathbf{x} \in \mathbb{C}^n$,

$$Q(\mathbf{x}) = \mathbf{x}^H\mathbf{A}\mathbf{x} = \sum_{i,j} a_{ij}\bar{x}_i x_j.$$

La matrice $\mathbf{A} = [a_{ij}] \in \mathrm{M}_n(\mathbb{C})$ è detta la matrice *generatrice* di Q. Le matrici hermitiane intervengono quando si considerano le forme quadratiche complesse che assumono solo valori reali, come prova il seguente risultato (nella dimostrazione la lettera "i" è usata sia come indice che come numero complesso; riteniamo che il lettore sia sufficientemente formato per non restarne confuso).

Proposizione 3.1. *La forma quadratica complessa $Q(\mathbf{x}) = \mathbf{x}^H\mathbf{A}\mathbf{x}$, con $\mathbf{A} = [a_{ij}] \in \mathrm{M}_n(\mathbb{C})$, assume solo valori reali se e solo se la matrice $\mathbf{A}$ è hermitiana.*

Dimostrazione. Dato un arbitrario vettore $\mathbf{x} \in \mathbb{C}^n$, si ha:

$$\mathbf{x}^H\mathbf{A}\mathbf{x} \in \mathbb{R} \iff \mathbf{x}^H\mathbf{A}\mathbf{x} = (\mathbf{x}^H\mathbf{A}\mathbf{x})^H = \mathbf{x}^H\mathbf{A}^H\mathbf{x}$$

e ne segue subito la sufficienza. Viceversa, prendendo $\mathbf{x} = \mathbf{e}_i$ si vede che $a_{ii} = \mathbf{e}_i^T\mathbf{A}\mathbf{e}_i = \mathbf{e}_i^T\mathbf{A}^H\mathbf{e}_i = \bar{a}_{ii}$, quindi gli elementi diagonali di $\mathbf{A}$ sono reali. Prendendo poi $i \neq j$ e $\mathbf{x} = \mathbf{e}_i + \mathbf{e}_j$, il fatto che $\mathbf{x}^H\mathbf{A}\mathbf{x} \in \mathbb{R}$ equivale a dire che $a_{ii} + a_{jj} + a_{ij} + a_{ji} \in \mathbb{R}$, quindi, per quanto appena visto, $a_{ij} + a_{ji} \in \mathbb{R}$. Analogamente, prendendo $i \neq j$ e $\mathbf{y} = \mathbf{e}_i + i\mathbf{e}_j$, il fatto che $\mathbf{y}^H\mathbf{A}\mathbf{y} \in \mathbb{R}$ equivale a dire che $a_{ii} + a_{jj} + ia_{ij} - ia_{ji} \in \mathbb{R}$, quindi $i(a_{ij} - a_{ji}) \in \mathbb{R}$. Scrivendo a_{ij} e a_{ji} in forma algebrica si vede con un facile calcolo (si veda l'Esercizio 6.18) che ciò implica che $a_{ij} = \bar{a}_{ji}$, quindi la matrice $\mathbf{A}$ è hermitiana. □

Se la matrice $\mathbf{A}$ è reale, definiamo forma quadratica n-dimensionale una funzione $Q\colon \mathbb{R}^n \to \mathbb{R}$ tale che, per ogni vettore $\mathbf{x} \in \mathbb{R}^n$,

$$Q(\mathbf{x}) = \mathbf{x}^T\mathbf{A}\mathbf{x} = \sum_{i,j} a_{ij}x_i x_j$$

dove $\mathbf{A} = [a_{ij}] \in \mathrm{M}_n(\mathbb{R})$. Quindi Q è una funzione polinomiale omogenea di secondo grado in n variabili. La matrice generatrice di una tale forma può essere una qualunque matrice reale di ordine n, però anche in questo caso le matrici simmetriche giocano un ruolo privilegiato, come mostra il seguente risultato.

Proposizione 3.2. *Data la forma quadratica reale $Q\colon \mathbb{R}^n \to \mathbb{R}$ generata dalla matrice $\mathbf{A}_1$, esiste una e una sola matrice simmetrica $\mathbf{A} \in \mathrm{M}_n(\mathbb{R})$ tale che $Q(\mathbf{x}) = \mathbf{x}^T\mathbf{A}\mathbf{x}$.*

Dimostrazione. Se $\mathbf{A} = (\mathbf{A}_1 + \mathbf{A}_1^T)/2$ è la parte simmetrica di $\mathbf{A}_1$, si ha, per ogni $\mathbf{x} \in \mathbb{R}^n$:

$$\mathbf{x}^T\mathbf{A}\mathbf{x} = (\mathbf{x}^T\mathbf{A}_1\mathbf{x} + \mathbf{x}^T\mathbf{A}_1^T\mathbf{x})/2 = \mathbf{x}^T\mathbf{A}_1\mathbf{x}$$

dove si è usato il fatto che $\mathbf{x}^T\mathbf{A}_1^T\mathbf{x} = (\mathbf{x}^T\mathbf{A}_1^T\mathbf{x})^T = \mathbf{x}^T\mathbf{A}_1\mathbf{x}$. Quindi anche $\mathbf{A}$ è matrice generatrice di Q. Quanto all'unicità, $Q(\mathbf{e}_i) = \mathbf{e}_i^T\mathbf{A}\mathbf{e}_i = a_{ii}$ individua univocamente l'elemento diagonale a_{ii} per ogni indice i, e assieme a $Q(\mathbf{e}_i + \mathbf{e}_j) = a_{ii} + a_{jj} + a_{ij} + a_{ji}$ individua $a_{ij} + a_{ji}$; essendo $\mathbf{A}$ simmetrica, a_{ij} e a_{ji} restano pure univocamente individuati. □

Esempio 3.3. La forma quadratica reale 2-dimensionale

$$Q([x_1, x_2]) = ax_1^2 + bx_1x_2 + cx_2x_1 + dx_2^2, \quad (a, b, c, d \in \mathbb{R})$$

è generata dalla matrice

$$\mathbf{A}_1 = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

e dall'unica matrice simmetrica

$$\mathbf{A} = \begin{bmatrix} a & (b+c)/2 \\ (b+c)/2 & d \end{bmatrix}. \qquad \square$$

L'importanza delle matrici reali simmetriche deriva oltre che da quanto asserito nella Proposizione 3.2, soprattutto dal fatto che molti fenomeni che possono essere modellizzati in modo discreto tramite matrici e che presentano delle simmetrie danno luogo a matrici simmetriche. Quindi tali matrici si incontrano spesso nelle applicazioni.

Raggruppiamo di seguito alcune elementari proprietà delle matrici hermitiane e anti-hermitiane, simmetriche e anti-simmetriche (ricordando che per questi ultimi due tipi di matrici ci limitiamo a matrici reali).

(i) *Gli elementi diagonali di una matrice hermitiana* $\mathbf{A} = [a_{ij}]$*, la sua traccia e il suo determinante sono numeri reali.*

Infatti a_{ii} deve coincidere con $\bar{a}_{ii}$ per ogni i, quindi $a_{ii} \in \mathbb{R}$. La traccia, essendo la somma degli elementi diagonali, è essa pure reale. È stato poi provato nel Teorema 2.2 che gli autovalori di una matrice hermitiana sono reali. Il determinante, essendo il prodotto degli autovalori, è esso pure reale. Faremo uso di questo fatto nei Teoremi 3.5 e 3.6.

(ii) *Gli elementi diagonali di una matrice anti-hermitiana* $\mathbf{A} = [a_{ij}]$ *sono numeri immaginari e gli elementi diagonali di una matrice anti-simmetrica reale* $\mathbf{A} = [a_{ij}]$ *sono nulli.*

Infatti nel primo caso a_{ii} deve coincidere con $-\bar{a}_{ii}$ per ogni i, quindi a_{ii} ha parte reale nulla. Nel secondo caso a_{ii} deve coincidere con $-a_{ii}$, quindi $a_{ii} = 0$.

(iii) *Il determinante di una matrice anti-simmetrica reale* $n \times n$ $\mathbf{A}$ *è nullo per* n *dispari, ed è un numero reale non negativo per* n *pari.*

Poiché il polinomio caratteristico di $\mathbf{A}$ ha coefficienti reali, se λ è una sua radice lo è anche $\bar{\lambda}$; ma λ ha parte reale nulla, per il Teorema 2.2, quindi gli autovalori di $\mathbf{A}$, se non sono nulli, vanno a coppie: ir, $-ir$, con $r \in \mathbb{R}$. Poiché il determinante è il prodotto degli autovalori e $-ir \cdot ir = r^2$, segue l'asserto.

Ci concentreremo d'ora in avanti sulle matrici hermitiane, tenendo presente che tutti i risultati che proveremo sono validi anche per le matrici simmetriche reali, con le ovvie modifiche per adattarli al caso reale. La trattazione delle matrici hermitiane non reca nessuna aggravio rispetto a quella delle matrici simmetriche reali.

Poiché una matrice hermitiana $\mathbf{A}$ di ordine n ha tutti i suoi n autovalori reali, possiamo disporre tali autovalori, ripetuti con la loro molteplicità, in ordine non decrescente:

$$\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_{n-1} \leq \lambda_n.$$

Questa notazione resterà fissata e sottintesa per tutto il resto del Capitolo. Nostro prossimo scopo è caratterizzare gli autovalori λ_i come massimi o minimi di una certa funzione a valori reali definita su $\mathbb{C}^n$, assunti su opportuni sottospazi di $\mathbb{C}^n$.

La funzione impiegata a tal fine prende il nome dai due fisici inglesi Rayleigh e Ritz; data la matrice hermitiana $\mathbf{A}$ di ordine n, si chiama *funzione di Rayleigh-Ritz* associata ad $\mathbf{A}$ la funzione

$$\rho_{\mathbf{A}}\colon \mathbb{C}^n \setminus \{\mathbf{0}\} \to \mathbb{R}, \qquad \rho_{\mathbf{A}}(\mathbf{x}) = \frac{\mathbf{x}^H\mathbf{A}\mathbf{x}}{\mathbf{x}^H\mathbf{x}} \quad \text{per ogni } \mathbf{0} \neq \mathbf{x} \in \mathbb{C}^n.$$

Denotando con $\mathrm{S}_n = \{\mathbf{x} \in \mathbb{C}^n \mid \|\mathbf{x}\|_2 = 1\}$ la superficie sferica n-dimensionale costituita dai vettori di norma euclidea 1, si può equivalentemente definire la funzione di Rayleigh-Ritz come:

$$\rho_{\mathbf{A}}\colon \mathrm{S}_n \to \mathbb{R}, \qquad \rho_{\mathbf{A}}(\mathbf{y}) = \mathbf{y}^H\mathbf{A}\mathbf{y} \quad \text{per ogni } \mathbf{y} \in \mathrm{S}_n;$$

è infatti immediato verificare che, se $\mathbf{0} \neq \mathbf{x} \in \mathbb{C}^n$, allora $\rho_{\mathbf{A}}(\mathbf{x}) = \rho_{\mathbf{A}}(\mathbf{x}/\|\mathbf{x}\|_2)$. Noi useremo indifferentemente le due differenti definizioni. Si noti che il fatto che la funzione di Rayleigh-Ritz ha come codominio $\mathbb{R}$ dipende dalla proprietà della matrice $\mathbf{A}$ di essere hermitiana.

La caratterizzazione degli autovalori di $\mathbf{A}$ in termini della funzione di Rayleigh-Ritz a essa associata avviene in due passi: prima si caratterizzano il minimo autovalore λ_1 e il massimo autovalore λ_n (qui non si vincola la funzione $\rho_{\mathbf{A}}$ ad alcun sottospazio proprio); poi si caratterizzano gli autovalori intermedi, vincolando la funzione $\rho_{\mathbf{A}}$ a opportuni sottospazi di $\mathbb{C}^n$. È necessario perciò introdurre i sottospazi vettoriali di $\mathbb{C}^n$ a cui vincolare la funzione di Rayleigh-Ritz.

Se $\mathbf{A} = \mathbf{U}\mathbf{\Lambda}\mathbf{U}^H$ è una diagonalizzazione unitaria di $\mathbf{A}$, possiamo supporre che $\mathbf{\Lambda} = \mathbf{Diag}(\lambda_1, \dots, \lambda_n)$ e $\mathbf{U} = [\mathbf{u}_1 \ \dots \ \mathbf{u}_n]$, dove $\{\mathbf{u}_1; \dots; \mathbf{u}_n\}$ è una base ortonormale di $\mathbb{C}^n$. Per ogni k compreso tra 1 ed n, poniamo:

$$V_k = \langle \mathbf{u}_k; \dots; \mathbf{u}_n \rangle, \qquad V^k = \langle \mathbf{u}_1; \dots; \mathbf{u}_k \rangle.$$

Si noti che $V_1 = \mathbb{C}^n = V^n$.

In queste notazioni si ha il seguente risultato.

Teorema 3.4 (Principio di Rayleigh-Ritz). *Data la matrice hermitiana* $\mathbf{A}$ *di ordine* n*, si ha:*

(1) $\lambda_1 \leq \rho_{\mathbf{A}}(\mathbf{x}) \leq \lambda_n$, *per ogni* $\mathbf{0} \neq \mathbf{x} \in \mathbb{C}^n$;

(2) $\lambda_1 = \min_{\mathbf{0}\neq\mathbf{x}} \rho_{\mathbf{A}}(\mathbf{x})$;

(3) $\lambda_n = \max_{\mathbf{0}\neq\mathbf{x}} \rho_{\mathbf{A}}(\mathbf{x})$;

(4) *se* $2 \leq k \leq n-1$ *si ha:*

$$\lambda_k = \min_{\mathbf{0}\neq\mathbf{x}\in V_k} \rho_{\mathbf{A}}(\mathbf{x}) = \max_{\mathbf{0}\neq\mathbf{x}\in V^k} \rho_{\mathbf{A}}(\mathbf{x}).$$

Dimostrazione. (1) Se $\mathbf{x} \in \mathbb{C}^n$ e $\|\mathbf{x}\|_2 = 1$, posto $\mathbf{U}^H\mathbf{x} = \mathbf{z} = [z_1 \dots z_n]^T$, si ha:

$$\mathbf{x}^H\mathbf{A}\mathbf{x} = \mathbf{x}^H\mathbf{U}\mathbf{\Lambda}\mathbf{U}^H\mathbf{x} = \mathbf{z}^H\mathbf{\Lambda}\mathbf{z} = \sum_{i=1}^{n} \lambda_i |z_i|^2$$

dove $\|\mathbf{z}\|_2 = 1$ per il Teorema 1.1 (vii). Dal fatto che $\lambda_1 \le \lambda_i \le \lambda_n$ per ogni i segue:

$$\lambda_1 = \lambda_1 \sum_{i=1}^{n} |z_i|^2 \le \sum_{i=1}^{n} \lambda_i |z_i|^2 \le \lambda_n \sum_{i=1}^{n} |z_i|^2 = \lambda_n$$

da cui l'asserto.

(2) L'asserto segue da (1) e da

$$\lambda_1 = \lambda_1 \|\mathbf{u}_1\|_2^2 = \lambda_1 \mathbf{u}_1^H \mathbf{u}_1 = \mathbf{u}_1^H \mathbf{A} \mathbf{u}_1 = \rho_{\mathbf{A}}(\mathbf{u}_1),$$

(3) L'asserto segue da (1) e da

$$\lambda_n = \lambda_n \|\mathbf{u}_n\|_2^2 = \lambda_n \mathbf{u}_n^H \mathbf{u}_n = \mathbf{u}_n^H \mathbf{A} \mathbf{u}_n = \rho_{\mathbf{A}}(\mathbf{u}_n).$$

(4) Dimostriamo la prima uguaglianza e lasciamo al lettore come esercizio l'analoga verifica della seconda. Se $\|\mathbf{x}\|_2 = 1$ e $\mathbf{x} \in V_k = \langle \mathbf{u}_k; \ldots; \mathbf{u}_n \rangle = \langle \mathbf{u}_1; \ldots; \mathbf{u}_{k-1} \rangle^{\perp}$, allora il vettore $\mathbf{U}^H \mathbf{x} = \mathbf{z}$ ha le prime $k-1$ coordinate nulle. Pertanto si ha:

$$\lambda_k = \lambda_k \sum_{i=1}^{n} |z_i|^2 = \lambda_k \sum_{i=k}^{n} |z_i|^2 \le \sum_{i=k}^{n} \lambda_i |z_i|^2 = \sum_{i=1}^{n} \lambda_i |z_i|^2 = \rho_{\mathbf{A}}(\mathbf{x}).$$

Si ha infine $\lambda_k = \lambda_k \|\mathbf{u}_k\|_2^2 = \lambda_k \mathbf{u}_k^H \mathbf{u}_k = \mathbf{u}_k^H \mathbf{A} \mathbf{u}_k$, quindi $\lambda_k = \min_{\mathbf{0} \ne \mathbf{x} \in V_k} \rho_{\mathbf{A}}(\mathbf{x})$, come desiderato. □

Il Principio di Rayleigh-Ritz costituisce il punto di partenza per provare svariati principi variazionali sugli autovalori delle matrici hermitiane, che vedremo nel Paragrafo 5.

L'ultima parte di questo Paragrafo studia le matrici hermitiane (e simmetriche reali) i cui autovalori reali sono positivi oppure non-negativi; nel primo caso le matrici sono dette *definite positive*, nel secondo caso *semi-definite positive*. I due teoremi che seguono caratterizzano queste matrici in vari modi, senza ricorrere agli autovalori, che in generale non si possono conoscere in modo esatto, ma solo approssimato. Il primo teorema usa, tra l'altro, le sottomatrici principali k-esime, introdotte nell'Esempio 2.10 del Capitolo 1.

Teorema 3.5. *Data la matrice hermitiana* $\mathbf{A}$ *di ordine* n*, i fatti seguenti sono equivalenti:*

(1) *gli autovalori di* $\mathbf{A}$ *sono positivi;*

(2) *la funzione di Rayleigh assume valori solo positivi:* $\rho_{\mathbf{A}}(\mathbf{x}) > 0$ *per ogni vettore* $\mathbf{x} \ne \mathbf{0}$*;*

(3) *ogni sottomatrice principale* k*-esima di* $\mathbf{A}$ *ha determinante positivo;*

(4) *l'eliminazione di Gauss su* $\mathbf{A}$ *produce senza permutazioni una decomposizione del tipo* $\mathbf{A} = \mathbf{L}_0 \mathbf{D} \mathbf{L}_0^H$*, con* $\mathbf{L}_0$ *matrice uni-triangolare inferiore e* $\mathbf{D}$ *matrice diagonale con elementi diagonali reali positivi;*

(5) *esiste una matrice invertibile* $\mathbf{W}$ *tale che* $\mathbf{A} = \mathbf{W}\mathbf{W}^H$*;*

(6) *esiste una matrice definita positiva* $\mathbf{B}$ *tale che* $\mathbf{A} = \mathbf{B}^2$*;*

(7) *se* $\mathbf{A}$ *è in forma bordata:*

$$\mathbf{A} = \begin{bmatrix} \mathbf{A}_1 & \mathbf{x} \\ \mathbf{x}^H & a \end{bmatrix},$$

allora $\mathbf{A}_1$ *è definita positiva e* $a > \mathbf{x}^H \mathbf{A}_1^{-1} \mathbf{x}$.

Dimostrazione. (1) $\iff$ (2) È immediata conseguenza del Teorema 3.4, (1) e (2).

(1) $\implies$ (3) Osserviamo innanzi tutto che $\det(\mathbf{A}) > 0$, perché il determinante è il prodotto degli autovalori. È sufficiente allora provare che, se $\mathbf{A}_k$ denota la sottomatrice principale k-esima (ottenuta intersecando le prime k righe e colonne di $\mathbf{A}$), anche $\mathbf{A}_k$ è definita positiva. Ovviamente $\mathbf{A}_k$ è hermitiana. Attesa l'equivalenza già provata dei punti (1) e (2), è sufficiente dimostrare che $\mathbf{y}^H \mathbf{A}_k \mathbf{y} > 0$ per ogni vettore non nullo $\mathbf{y} \in \mathbb{C}^k$. Posto $\mathbf{z}^H = [\mathbf{y}^H \ \mathbf{0}^H] \in \mathbb{C}^n$, si ha:

$$\mathbf{y}^H \mathbf{A}_k \mathbf{y} = \sum_{i,j \le k} a_{ij} \bar{y}_i y_j = \sum_{i,j \le n} a_{ij} \bar{z}_i z_j = \mathbf{z}^H \mathbf{A} \mathbf{z} > 0$$

dove naturalmente i numeri y_i sono le coordinate di $\mathbf{y}$ e i numeri z_i sono le coordinate di $\mathbf{z}$.

(3) $\implies$ (4) Proviamo per induzione su k che il k-esimo pivot d_k incontrato nel corso della EG è reale positivo, purché si esegua la EG impiegando solo le matrici elementari del tipo $\mathbf{E}_{ij}(\alpha)$ e pervenendo a una forma a scalini di $\mathbf{A}$, denotata con $\mathbf{U}_0$, contenente sulla diagonale i pivot d_k.

Per $k = 1$ si ha $d_1 = a_{11} > 0$, perché a_{11} è il determinante di $\mathbf{A}_1$. Sia $k > 1$ e $d_i > 0$ per $i \le k-1$. Le matrici elementari $\mathbf{E}_{ij}(\alpha)$ impiegate non modificano tramite premoltiplicazione il determinante della matrice $\mathbf{A}$. Le corrispondenti operazioni elementari trasformano $\mathbf{A}_k$ nella sottomatrice principale k-esima di $\mathbf{U}_0$. Pertanto $\det(\mathbf{A}_k)$ coincide con il determinante di tale sottomatrice che, essendo triangolare superiore con elementi diagonali $d_1, d_2, \dots, d_k$, ha come determinante il prodotto $d_1 \cdot \dots \cdot d_k$. Pertanto $\det(\mathbf{A}_k) = d_1 \cdot \dots \cdot d_k$. Ne consegue che $d_k = \det(\mathbf{A}_k) / \det(\mathbf{A}_{k-1}) > 0$. A questo punto osserviamo che

$$\mathbf{U}_0 = \mathbf{Diag}(d_1, \dots, d_n)\mathbf{U}$$

dove $\mathbf{U}$ è forma ridotta di Gauss di $\mathbf{A}$. Si ha quindi

$$\mathbf{A} = \mathbf{L}_0 \mathbf{U}_0 = \mathbf{L}_0 \mathbf{D} \mathbf{U}$$

dove $\mathbf{L}_0$ è uni-triangolare inferiore, $\mathbf{U}$ è uni-triangolare superiore e $\mathbf{D} = \mathbf{Diag}(d_1, \dots, d_n)$ con elementi diagonali reali positivi. Infine, da $\mathbf{A} = \mathbf{A}^H$ segue facilmente che $\mathbf{U} = \mathbf{L}_0^H$ (si veda l'Esercizio 6.19).

(4) $\implies$ (5) Basta porre $\mathbf{W} = \mathbf{L}_0 \mathbf{D}^{1/2}$, dove $\mathbf{D}^{1/2} = \mathbf{Diag}(d_1^{1/2}, \dots, d_n^{1/2})$ (la fattorizzazione $\mathbf{A} = (\mathbf{L}_0 \mathbf{D}^{1/2})(\mathbf{L}_0 \mathbf{D}^{1/2})^H$ si chiama *decomposizione di Choleski* di $\mathbf{A}$).

(5) $\implies$ (2) Per ogni vettore $\mathbf{x}$ di norma euclidea 1 risulta

$$\rho_{\mathbf{A}}(\mathbf{x}) = \mathbf{x}^H \mathbf{W} \mathbf{W}^H \mathbf{x} = \|\mathbf{W}^H \mathbf{x}\|_2^2.$$

Tale norma risulta positiva, perché la matrice $\mathbf{W}$ è invertibile e quindi $\mathbf{W}^H \mathbf{x} \ne \mathbf{0}$.

(1) $\iff$ (6) Se $\mathbf{A} = \mathbf{U}\boldsymbol{\Lambda}\mathbf{U}^H$ è una diagonalizzazione unitaria di $\mathbf{A}$, essendo gli autovalori λ_i positivi possiamo porre: $\boldsymbol{\Lambda}^{1/2} = \mathbf{Diag}(\lambda_1^{1/2},\dots,\lambda_n^{1/2})$. Si ha allora che $\mathbf{A} = \mathbf{B}^2$, dove $\mathbf{B} = \mathbf{U}\boldsymbol{\Lambda}^{1/2}\mathbf{U}^H$ è evidentemente una matrice definita positiva. Viceversa, se $\mathbf{A} = \mathbf{B}^2$ con $\mathbf{B}$ matrice definita positiva, poiché gli autovalori di $\mathbf{B}$ sono reali non nulli e quelli di $\mathbf{B}^2$ sono i quadrati degli autovalori di $\mathbf{B}$, si deduce che gli autovalori di $\mathbf{A}$ sono positivi.

(3) $\iff$ (7) Se ogni sottomatrice principale k-esima di $\mathbf{A}$ ha determinante positivo, in particolare si ha che $\det(\mathbf{A}_1) > 0$, quindi $\mathbf{A}_1$ è invertibile. La formula del determinante a blocchi (si veda l'Esercizio 4.11) porge

$$\det(\mathbf{A}) = (a - \mathbf{x}^H\mathbf{A}_1^{-1}\mathbf{x})\det(\mathbf{A}_1)$$

da cui, sapendo che $\det(\mathbf{A}) > 0$ si ricava che $a > \mathbf{x}^H\mathbf{A}^{-1}\mathbf{x}$. Le sottomatrici principali k-esime di $\mathbf{A}_1$ sono le sottomatrici principali k-esime di $\mathbf{A}$ per $k \le n-1$. Pertanto esse hanno determinante positivo. Sapendo già che (3) $\Rightarrow$ (1) si deduce che $\mathbf{A}_1$ è definita positiva. Viceversa, sapendo che $\mathbf{A}_1$ è definita positiva, da (1) $\Rightarrow$ (3) si deduce che le sottomatrici principali k-esime di $\mathbf{A}$ hanno determinante positivo per $k \le n-1$ e resta da provare che $\det(\mathbf{A}) > 0$. Ciò segue dalla ricordata formula del determinante a blocchi e dall'ipotesi che $a > \mathbf{x}^H\mathbf{A}_1^{-1}\mathbf{x}$. □

Il risultato analogo al Teorema 3.5 per le matrici semi-definite positive si differenzia di poco dal suddetto teorema. Vale la pena di osservare che nell'enunciato del Teorema 3.6 si richiede nel punto (3) che abbiano determinante non negativo *tutte* le sottomatrici principali di $\mathbf{A}$ e non solo le sottomatrici principali k-esime; non si richiede nei punti (5) e (6) che le matrici che fattorizzano $\mathbf{A}$ siano invertibili; infine che il punto (7), su cui torneremo dopo la dimostrazione, è quello che più si allontana dal medesimo punto del Teorema 3.5.

Teorema 3.6. *Data la matrice hermitiana* $\mathbf{A}$ *di ordine* n*, i fatti seguenti sono equivalenti:*

(1) *gli autovalori di* $\mathbf{A}$ *sono non negativi;*

(2) *la funzione di Rayleigh assume valori non negativi:* $\rho_{\mathbf{A}}(\mathbf{x}) \ge 0$ *per ogni vettore* $\mathbf{x}$*;*

(3) *ogni sottomatrice principale di* $\mathbf{A}$ *ha determinante non negativo;*

(4) $\mathbf{A} = \mathbf{L}_0\mathbf{D}\mathbf{L}_0^H$*, con* $\mathbf{L}_0$ *matrice uni-triangolare inferiore e* $\mathbf{D}$ *matrice diagonale con elementi diagonali reali non negativi;*

(5) *esiste una matrice* $\mathbf{W}$ *tale che* $\mathbf{A} = \mathbf{W}\mathbf{W}^H$*;*

(6) *esiste una matrice semi-definita positiva* $\mathbf{B}$ *tale che* $\mathbf{A} = \mathbf{B}^2$*;*

(7) *se* $\mathbf{A}$ *è in forma bordata:*

$$\mathbf{A} = \begin{bmatrix} \mathbf{A}_1 & \mathbf{x} \\ \mathbf{x}^H & a \end{bmatrix},$$

allora $\mathbf{A}_1$ *è semi-definita positiva,* $a \ge \mathbf{x}^H\mathbf{A}_1^{+}\mathbf{x}$ *e il vettore* $\mathbf{x}$ *appartiene allo spazio delle colonne di* $\mathbf{A}_1$.

Dimostrazione. Lasciamo al lettore come facile esercizio l'adattamento delle dimostrazioni fatte nel Teorema 3.5 delle implicazioni: (1) $\Leftrightarrow$ (2) $\Rightarrow$ (3), (4) $\Rightarrow$ (5) $\Rightarrow$ (2), (1) $\Leftrightarrow$ (6), e proviamo le restanti implicazioni.

(3) $\Rightarrow$ (4) Per induzione sull'ordine n della matrice. Il caso $n = 1$ è banale; sia $n > 1$ e l'asserto vero per $n - 1$. Decomponiamo la matrice $\mathbf{A}$ a blocchi nel modo seguente:

$$\mathbf{A} = \begin{bmatrix} a & \mathbf{x}^H \\ \mathbf{x} & \mathbf{A}_1 \end{bmatrix}.$$

Per l'ipotesi induttiva, $\mathbf{A}_1 = \mathbf{L}_1\mathbf{D}_1\mathbf{L}_1^H$, con $\mathbf{L}_1$ matrice uni-triangolare inferiore e $\mathbf{D}_1$ matrice diagonale con elementi diagonali reali non negativi. Se $\mathbf{x} = \mathbf{0}$ basta porre $\mathbf{L}_0 = \mathbf{Diag}(1, \mathbf{L}_1)$ e $\mathbf{D} = \mathbf{Diag}(a, \mathbf{D}_1)$. Se invece $\mathbf{x} \neq \mathbf{0}$, allora necessariamente $a > 0$ (si veda l'Esercizio 6.21). Si esegua dunque l'eliminazione simmetrica su prima riga e colonna, pre-moltiplicando e post-moltiplicando successivamente per le matrici elementari $\mathbf{E}_{i1}(-a^{-1}a_{i1})$ e $\mathbf{E}_{1i}(-a^{-1}a_{1i})$, rispettivamente. Si osservi che

$$\mathbf{E}_{i1}(-a^{-1}a_{i1})^H = \mathbf{E}_{1i}(-a^{-1}\bar{a}_{i1}) = \mathbf{E}_{1i}(-a^{-1}a_{1i}).$$

Se $\mathbf{E}$ denota il prodotto delle matrici elementari che pre-moltiplicano $\mathbf{A}$, si ha:

$$\mathbf{EAE}^H = \begin{bmatrix} a & \mathbf{0}^H \\ \mathbf{0} & \mathbf{C} \end{bmatrix}.$$

Per quanto già visto nel caso in cui $\mathbf{x} = \mathbf{0}$, risulta $\mathbf{EAE}^H = \mathbf{LDL}^H$, con $\mathbf{L}$ matrice uni-triangolare inferiore e $\mathbf{D}$ matrice diagonale con elementi diagonali reali non negativi. Basta allora porre $\mathbf{L}_0 = \mathbf{E}^{-1}\mathbf{L}$, ricordando che prodotti e inverse di matrici uni-triangolari inferiori sono ancora tali.

(5) $\Rightarrow$ (7) Posto $\mathbf{W}^H = [\mathbf{Y}^H\ \mathbf{w}]$, dal prodotto a blocchi $\mathbf{WW}^H$ uguagliato ad $\mathbf{A}$ si ricavano le uguaglianze:

$$\mathbf{YY}^H = \mathbf{A}_1, \qquad \mathbf{Yw} = \mathbf{x}, \qquad \mathbf{w}^H\mathbf{w} = a.$$

Dalla prima uguaglianza segue che $\mathbf{A}_1$ è semi-definita positiva, perché già sappiamo che (5) $\Rightarrow$ (1); dalla seconda segue che $\mathbf{x} \in C(\mathbf{Y})$ ed è facile provare (si veda l'Esercizio 22) che $C(\mathbf{Y}) = C(\mathbf{YY}^H) = C(\mathbf{A}_1)$. Infine, attesa la terza uguaglianza, si tratta di provare che $\|\mathbf{w}\|_2^2 \geq \mathbf{x}^H\mathbf{A}_1^+\mathbf{x}$. Tenuto conto dell'Esercizio 32 del Capitolo 1, risulta

$$\mathbf{x}^H\mathbf{A}_1^+\mathbf{x} = \mathbf{x}^H(\mathbf{YY}^H)^+\mathbf{x} = \mathbf{x}^H(\mathbf{Y}^+)^H\mathbf{Y}^+\mathbf{x} = \|\mathbf{Y}^+\mathbf{x}\|_2^2 = \|\mathbf{Y}^+\mathbf{Yw}\|_2,$$

perciò dobbiamo provare che $\|\mathbf{w}\|_2 \geq \|\mathbf{Y}^+\mathbf{Yw}\|_2$. Ma $\mathbf{Y}^+\mathbf{Yw}$ coincide con la proiezione di $\mathbf{w}$ sul sottospazio $C(\mathbf{Y}^H)$ di $\mathbb{C}^n$, perché la matrice $\mathbf{Y}^+\mathbf{Y}$ risulta essere la matrice di proiezione su $C(\mathbf{Y}^H)$ (si veda il Corollario 7.4 del Capitolo 3), da cui l'asserto segue in modo ovvio.

(7) $\Rightarrow$ (1) Sapendo che (5) $\Leftrightarrow$ (1), $\mathbf{A}_1 = \mathbf{YY}^H$ per una opportuna matrice $\mathbf{Y}$. Proviamo che risulta semi-definita positiva la matrice

$$\mathbf{B} = \begin{bmatrix} \mathbf{A}_1 & \mathbf{x} \\ \mathbf{x}^H & \|\mathbf{Y}^+\mathbf{x}\|_2^2 \end{bmatrix}.$$

Ciò deriva dal fatto che

$$\mathbf{B} = \begin{bmatrix} \mathbf{Y} \\ (\mathbf{Y}^+\mathbf{x})^H \end{bmatrix} \begin{bmatrix} \mathbf{Y}^H & \mathbf{Y}^+\mathbf{x} \end{bmatrix}$$

come prova un calcolo diretto, tenuto conto che $\mathbf{Y}\mathbf{Y}^+\mathbf{x} = \mathbf{x}$ (questa uguaglianza segue dal fatto che, se $\mathbf{x} \in C(\mathbf{Y})$, allora $\mathbf{x} = \mathbf{Y}\mathbf{w}$ per un certo vettore $\mathbf{w}$ e $\mathbf{Y}\mathbf{Y}^+\mathbf{Y}\mathbf{w} = \mathbf{Y}\mathbf{w}$ perché $\mathbf{Y}\mathbf{Y}^+\mathbf{Y} = \mathbf{Y}$). Quindi $\mathbf{B}$ è semi-definita positiva perché (5) $\Leftrightarrow$ (1). Ricordiamo che al punto precedente abbiamo visto che $\mathbf{x}^H\mathbf{A}_1^+\mathbf{x} = \|\mathbf{Y}^+\mathbf{x}\|_2^2$. Poniamo

$$\mathbf{C} = \begin{bmatrix} \mathbb{O} & \mathbf{0} \\ \mathbf{0}^H & a - \mathbf{x}^H\mathbf{A}_1^+\mathbf{x} \end{bmatrix}.$$

È evidente che $\mathbf{A} = \mathbf{B} + \mathbf{C}$, e poiché sia $\mathbf{B}$ che $\mathbf{C}$ sono semi-definite positive, segue banalmente da (2) che pure $\mathbf{A}$ è semi-definita positiva. □

Si osservi che i punti (7) dei due precedenti teoremi danno un criterio induttivo per verificare se una matrice hermitiana è definita o semi-definita positiva. Si noti che nel Teorema 3.6 la matrice pseudo-inversa $\mathbf{A}_1^+$ sostituisce la matrice inversa $\mathbf{A}_1^{-1}$ usata nel Teorema 3.5, e che la condizione aggiuntiva: $\mathbf{x} \in C(\mathbf{A})$, è automaticamente verificata quando $\mathbf{A}_1$ è invertibile.

Una matrice semi-definita positiva $\mathbf{B}$ tale che $\mathbf{A} = \mathbf{B}^2$, di cui il Teorema 3.6 (6) assicura l'esistenza, si chiama *radice quadrata* della matrice semi-definita positiva $\mathbf{A}$; essa è unica, come prova il seguente risultato.

Proposizione 3.7. *La radice quadrata di una matrice hermitiana semi-definita positiva* $\mathbf{A}$ *è unica.*

Dimostrazione. Supponiamo che $\mathbf{A} = \mathbf{B}^2 = \mathbf{C}^2$, con $\mathbf{B}$ e $\mathbf{C}$ matrici hermitiane semi-definite positive. Le matrici $\mathbf{B}$ e $\mathbf{C}$ hanno gli stessi autovalori con le stesse molteplicità, perché i loro quadrati sono gli autovalori di $\mathbf{A}$. Siano allora $\lambda_1, \dots, \lambda_r$ i distinti autovalori e siano

$$\mathbf{B} = \lambda_1\mathbf{P}_1 + \ldots + \lambda_r\mathbf{P}_r, \qquad \mathbf{C} = \lambda_1\mathbf{Q}_1 + \ldots + \lambda_r\mathbf{Q}_r$$

due decomposizioni spettrali (additive) di $\mathbf{B}$ e $\mathbf{C}$, rispettivamente. Usando il fatto che per $i \neq j$ risulta $\mathbf{P}_i\mathbf{P}_j = \mathbb{O} = \mathbf{Q}_i\mathbf{Q}_j$, da $\mathbf{A} = \mathbf{B}^2 = \mathbf{C}^2$ si ricava:

$$\lambda_1^2\mathbf{P}_1 + \ldots + \lambda_r^2\mathbf{P}_r = \mathbf{A} = \lambda_1^2\mathbf{Q}_1 + \ldots + \lambda_r^2\mathbf{Q}_r.$$

Se $i \neq j$, moltiplicando primo e ultimo membro a sinistra per $\mathbf{P}_i$ e a destra per $\mathbf{Q}_j$ si ricava:

$$\lambda_i^2\mathbf{P}_i\mathbf{Q}_j = \lambda_j^2\mathbf{P}_i\mathbf{Q}_j$$

da cui si ottiene che $\mathbf{P}_i\mathbf{Q}_j = \mathbb{O}$. Invertendo i ruoli di $\mathbf{P}_i$ e $\mathbf{Q}_j$ si ricava anche $\mathbf{Q}_j\mathbf{P}_i = \mathbb{O}$. Dalle uguaglianze $\mathbf{P}_1 + \cdots + \mathbf{P}_r = \mathbf{I} = \mathbf{Q}_1 + \ldots + \mathbf{Q}_r$, moltiplicando prima per $\mathbf{P}_i$ e poi per $\mathbf{Q}_i$, si ricava, per ogni indice i:

$$\mathbf{P}_i = \mathbf{P}_i\mathbf{Q}_i = \mathbf{Q}_i\mathbf{P}_i = \mathbf{Q}_i.$$

Si può allora concludere che $\mathbf{B} = \mathbf{C}$. □

4. Decomposizione in valori singolari

Data una arbitraria matrice complessa $m \times n$ $\mathbf{A}$, abbiamo già avuto modo di considerare nel Capitolo 1, Proposizione 2.5, una matrice hermitiana associata naturalmente ad $\mathbf{A}$, la cosiddetta *parte hermitiana* di $\mathbf{A}$: $(\mathbf{A}+\mathbf{A}^H)/2$.

Esistono altre due matrici hermitiane naturalmente associate ad $\mathbf{A}$ che, a differenza della sua parte hermitiana che ha le stesse dimensioni di $\mathbf{A}$, sono matrici quadrate; esse sono

$$\mathbf{A}\mathbf{A}^H \quad \text{e} \quad \mathbf{A}^H\mathbf{A}.$$

Per il Teorema spettrale queste due matrici sono unitariamente diagonalizzabili; una opportuna combinazione delle loro diagonalizzazioni unitarie produce una nuova fattorizzazione della matrice $\mathbf{A}$ che si chiama *decomposizione in valori singolari* di $\mathbf{A}$.

Tale decomposizione venne provata per matrici quadrate reali nel 1889 da Sylvester, ma la prova per arbitrarie matrici complesse venne fornita solo 50 anni più tardi da Eckart e Young. La decomposizione in valori singolari rappresenta uno dei risultati più utili e sfruttati di tutta l'Algebra Lineare.

Lo studio delle matrici $\mathbf{A}\mathbf{A}^H$ e $\mathbf{A}^H\mathbf{A}$ inizia con un esame dei loro autovalori e delle relative molteplicità. Un primo risultato riguarda più genericamente una coppia di matrici $\mathbf{A}$ e $\mathbf{B}$ di dimensioni rispettivamente $m \times n$ e $n \times m$, per le quali sono eseguibili quindi i due prodotti $\mathbf{AB}$ e $\mathbf{BA}$.

Proposizione 4.1. *Date due matrici complesse* $\mathbf{A}$ *e* $\mathbf{B}$ *di dimensioni rispettivamente* $m \times n$ *e* $n \times m$, *le due matrici* $\mathbf{AB}$ *e* $\mathbf{BA}$ *hanno gli stessi autovalori non nulli con le stesse molteplicità algebriche e geometriche.*

Dimostrazione. Siano $0 \neq \lambda \in \mathbb{C}$ e $\sigma \in \mathbb{C}$ tali che $\sigma^2 = \lambda$. Dimostriamo che le due trasformazioni lineari così definite

$$\varphi_\lambda\colon \mathrm{E}_{\mathbf{AB}}(\lambda) \to \mathrm{E}_{\mathbf{BA}}(\lambda), \quad \varphi_\lambda(\mathbf{u}) = \frac{1}{\sigma}\mathbf{Bu},$$
$$\psi_\lambda\colon \mathrm{E}_{\mathbf{BA}}(\lambda) \to \mathrm{E}_{\mathbf{AB}}(\lambda), \quad \psi_\lambda(\mathbf{v}) = \frac{1}{\sigma}\mathbf{Av}$$

sono ben definite e una l'inversa dell'altra. Da ciò si deduce che λ è un autovalore di $\mathbf{AB}$ con una certa molteplicità geometrica se e solo se è anche autovalore di $\mathbf{BA}$ con la stessa molteplicità geometrica. Sia $\mathbf{u} \in \mathrm{E}_{\mathbf{AB}}(\lambda)$; allora $\mathbf{ABu} = \lambda\mathbf{u}$, quindi

$$\mathbf{BA}\varphi_\lambda(\mathbf{u}) = \frac{1}{\sigma}\mathbf{BABu} = \frac{1}{\sigma}\mathbf{B}\lambda\mathbf{u} = \lambda\varphi_\lambda(\mathbf{u}).$$

Ne consegue che $\varphi_\lambda(\mathbf{u}) \in \mathrm{E}_{\mathbf{AB}}(\lambda)$ e φ_λ è ben definita. Analoga è la dimostrazione per ψ_λ. Proviamo ora che $\psi_\lambda \cdot \varphi_\lambda$ coincide con l'identità. Se $\mathbf{u} \in \mathrm{E}_{\mathbf{AB}}(\lambda)$ risulta:

$$(\psi_\lambda\varphi_\lambda)(\mathbf{u}) = \psi_\lambda\Big(\frac{1}{\sigma}\mathbf{Bu}\Big) = \frac{1}{\sigma}\frac{1}{\sigma}\mathbf{ABu} = \frac{1}{\lambda}\lambda\mathbf{u} = \mathbf{u}.$$

Analogamente si prova che $\varphi_\lambda \cdot \psi_\lambda$ coincide con l'identità. Resta da provare che le molteplicità algebriche coincidono. Ciò è lasciato come esercizio per il lettore (si veda l'Esercizio 6.25). $\square$

Se nella Proposizione 4.1 la matrice $\mathbf{B}$ coincide con la matrice $\mathbf{A}^H$, allora i due prodotti $\mathbf{AB}$ e $\mathbf{BA}$ sono entrambi matrici semi-definite positive, quindi con autovalori reali non negativi, per il Teorema 3.6. Inoltre alla Proposizione 4.1 si aggiunge la seguente integrazione riguardante le due applicazioni $\varphi_\lambda\colon \mathrm{E}_{\mathbf{AA}^H}(\lambda) \to \mathrm{E}_{\mathbf{A}^H\mathbf{A}}(\lambda)$ e $\psi_\lambda\colon \mathrm{E}_{\mathbf{A}^H\mathbf{A}}(\lambda) \to \mathrm{E}_{\mathbf{AA}^H}(\lambda)$.

Proposizione 4.2. *Data la matrice complessa $m \times n$ $\mathbf{A}$ e detto λ un suo autovalore non nullo, le due applicazioni φ_λ e ψ_λ, definite nella dimostrazione della Proposizione 4.1 sostituendo $\mathbf{A}^H$ a $\mathbf{B}$, conservano i prodotti interni dei vettori, quindi sono due isometrie.*

Dimostrazione. Verifichiamo che φ_λ conserva i prodotti interni; analoga dimostrazione si ha per ψ_λ. Siano $\mathbf{u}, \mathbf{w} \in \mathrm{E}_{\mathbf{AA}^H}$; si ha:

$$\varphi_\lambda(\mathbf{u})^H \varphi_\lambda(\mathbf{w}) = \left(\frac{1}{\sigma}\mathbf{A}^H\mathbf{u}\right)^H \frac{1}{\sigma}\mathbf{A}^H\mathbf{w} = \frac{1}{\lambda}\mathbf{u}^H\mathbf{AA}^H\mathbf{w} = \frac{1}{\lambda}\mathbf{u}^H\lambda\mathbf{w} = \mathbf{u}^H\mathbf{w},$$

dove si è tenuto conto che $\mathbf{AA}^H\mathbf{w} = \lambda\mathbf{w}$. □

La conseguenza rilevante della Proposizione 4.2 consiste nel fatto che le due applicazioni φ_λ e ψ_λ scambiano basi ortonormali degli autospazi $\mathrm{E}_{\mathbf{AA}^H}(\lambda)$ e $\mathrm{E}_{\mathbf{A}^H\mathbf{A}}(\lambda)$. Si osservi che le due precedenti Proposizioni non dicono nulla sugli spazi nulli delle matrici coinvolte, che infatti non hanno nessuna relazione tra di loro.

Data una arbitraria matrice complessa $m \times n$ di rango k $\mathbf{A}$, si chiama *decomposizione in valori singolari* di $\mathbf{A}$ una sua fattorizzazione del tipo

$$\mathbf{A} = \mathbf{U\Sigma V}^H$$

dove $\mathbf{U}$ e $\mathbf{V}$ sono matrici unitarie di ordini rispettivi m ed n, e $\mathbf{\Sigma}$ è una matrice $m \times n$ pseudo-diagonale (cioè con elementi non diagonali nulli) i cui elementi diagonali σ_i sono reali non negativi (qui chiamiamo elementi diagonali di una matrice rettangolare gli elementi di posto (i,i), estendendo la definizione del caso quadrato). Per comodità si richiede usualmente che $\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_k > 0$ e $\sigma_{k+1} = \cdots = \sigma_n = 0$.

Gli elementi positivi $\sigma_1, \dots, \sigma_k$ sulla diagonale di $\mathbf{\Sigma}$, che sono tanti quanto è il rango di $\mathbf{\Sigma}$ e quindi di $\mathbf{A}$, si chiamano i *valori singolari* di $\mathbf{A}$. Si osservi che in queste notazioni vale il seguente fatto.

Lemma 4.3. *I valori singolari di $\mathbf{A}$ sono univocamente individuati dalla matrice $\mathbf{A}$.*

Dimostrazione. La matrice $\mathbf{A}$ individua $\mathbf{AA}^H$ e

$$\mathbf{AA}^H = \mathbf{U\Sigma V}^H\mathbf{V\Sigma}^H\mathbf{U}^H = \mathbf{U\Sigma\Sigma}^H\mathbf{U}^H,$$

quindi $\mathbf{AA}^H$ individua univocamente, a meno dell'ordine, gli elementi σ_i^2 che sono i suoi autovalori. Essendo $\mathbf{\Sigma\Sigma}^H$ una matrice diagonale con elementi diagonali reali non negativi, resta univocamente determinata la matrice $\mathbf{\Sigma}$, per l'ipotesi di non negatività dei suoi elementi diagonali. □

Naturalmente si pone il problema dell'esistenza di una decomposizione in valori singolari di una generica matrice $\mathbf{A}$. Ciò è assicurato dal seguente risultato.

Teorema 4.4. *Ogni matrice complessa* $\mathbf{A}$ *ha una decomposizione in valori singolari.*

Dimostrazione. Sia $\mathbf{A}\mathbf{A}^H = \mathbf{U}\boldsymbol{\Lambda}\mathbf{U}^H$ una diagonalizzazione unitaria di $\mathbf{A}\mathbf{A}^H$, esistente per il Teorema spettrale. Possiamo supporre che

$$\boldsymbol{\Lambda} = \mathbf{Diag}(\lambda_1, \dots, \lambda_k, 0, \dots, 0)$$

con k uguale al rango di $\mathbf{A}\mathbf{A}^H$, coincidente con il rango di $\mathbf{A}$, e i λ_i numeri reali positivi (usualmente si scelgono i λ_i in ordine non crescente); ciò in virtù del fatto che la matrice $\mathbf{A}\mathbf{A}^H$ è semi-definita positiva, per il Teorema 3.6. Sia $\mathbf{U} = [\mathbf{u}_1 \ \dots \ \mathbf{u}_m]$. Allora una base ortonormale dello spazio nullo $\mathrm{N}(\mathbf{A}\mathbf{A}^H)$, coincidente con l'autospazio di $\mathbf{A}\mathbf{A}^H$ relativo all'autovalore 0, è data da

$$\{\mathbf{u}_{k+1}; \dots; \mathbf{u}_m\}.$$

La Proposizione 4.2 e il Teorema 1.4 (c) assicurano che, se $\sigma_i^2 = \lambda_i$ per ogni $i \le k$, posto:

$$\mathbf{v}_i = \frac{1}{\sigma_i}\mathbf{A}^H\mathbf{u}_i,$$

i vettori $\mathbf{v}_1, \dots, \mathbf{v}_k$ formano una base ortonormale del complemento ortogonale dello spazio nullo $\mathrm{N}(\mathbf{A}^H\mathbf{A})$ di $\mathbf{A}^H\mathbf{A}$. Qualora risulti $k < n$, fissiamo una base ortonormale $\{\mathbf{v}_{k+1}; \dots; \mathbf{v}_n\}$ di $\mathrm{N}(\mathbf{A}^H\mathbf{A})$, per cui $\{\mathbf{v}_1; \dots; \mathbf{v}_n\}$ costituisce una base ortonormale di $\mathbb{C}^n$ formata da autovettori di $\mathbf{A}^H\mathbf{A}$. Ma allora, posto $\mathbf{V} = [\mathbf{v}_1 \ \dots \ \mathbf{v}_n]$, risulta $\mathbf{A}^H\mathbf{A} = \mathbf{V}\boldsymbol{\Lambda}'\mathbf{V}^H$, dove la matrice diagonale degli autovalori $\boldsymbol{\Lambda}'$ ha come primi elementi diagonali diversi da zero ordinatamente gli elementi $\lambda_1, \dots, \lambda_k$. Infatti per $i \le k$ risulta

$$\mathbf{A}^H\mathbf{A}\mathbf{v}_i = \mathbf{A}^H\mathbf{A}\frac{1}{\sigma_i}\mathbf{A}^H\mathbf{u}_i = \frac{1}{\sigma_i}\mathbf{A}^H\lambda_i\mathbf{u}_i = \lambda_i\mathbf{v}_i.$$

Sia $\boldsymbol{\Sigma}$ la matrice pseudo-diagonale $m \times n$ i cui primi k elementi diagonali sono ordinatamente $\sigma_1, \dots, \sigma_k$ e con gli altri elementi diagonali nulli. Proviamo che risulta $\mathbf{A} = \mathbf{U}\boldsymbol{\Sigma}\mathbf{V}^H$. Ciò è equivalente a provare che $\mathbf{A}\mathbf{V} = \mathbf{U}\boldsymbol{\Sigma}$, ovvero che

$$\mathbf{A}\mathbf{v}_i = \sigma_i\mathbf{u}_i \quad \text{per } i \le k, \qquad \mathbf{A}\mathbf{v}_i = \mathbf{0} \quad \text{per } i > k.$$

Verifichiamo le uguaglianze per $i \le k$:

$$\mathbf{A}\mathbf{v}_i = \mathbf{A}\frac{1}{\sigma_i}\mathbf{A}^H\mathbf{u}_i = \frac{1}{\sigma_i}\lambda_i\mathbf{u}_i = \sigma_i\mathbf{u}_i$$

come si voleva dimostrare.

La verifica delle uguaglianze per $i > k$ è banale, perché i vettori $\mathbf{v}_{k+1}, \dots, \mathbf{v}_n$ sono una base di $\mathrm{N}(\mathbf{A}^H\mathbf{A})$, e $\mathrm{N}(\mathbf{A}^H\mathbf{A})$ coincide con $\mathrm{N}(\mathbf{A})$ (si veda l'Esercizio 6.22). □

Osservazione 4.5. (1) La strategia usata nel Teorema 4.4 per trovare una decomposizione in valori singolari $\mathbf{U\Sigma V}^H$ della matrice $\mathbf{A}$ è consistita nel diagonalizzare unitariamente la matrice $\mathbf{AA}^H$, determinando in tal modo la matrice unitaria $\mathbf{U}$, gli autovalori reali positivi di $\mathbf{AA}^H$ e quindi i valori singolari di $\mathbf{A}$, che sono le loro radici quadrate positive. Si è così determinata anche la matrice $\mathbf{\Sigma}$. La parte centrale della dimostrazione è consistita nel definire opportunamente la matrice unitaria $\mathbf{V}$ a partire dalla matrice $\mathbf{U}$. Si poteva però partire da una diagonalizzazione unitaria della matrice $\mathbf{A}^H\mathbf{A}$, determinando prima $\mathbf{V}$ e poi definendo di conseguenza $\mathbf{U}$. Di fatto, usualmente si sceglie la strada che comporta minor fatica, quindi si sceglie la prima via se $m \le n$, la seconda in caso contrario.

(2) Se la matrice $\mathbf{A}$ è reale, le matrici $\mathbf{AA}^H$ e $\mathbf{A}^H\mathbf{A}$ sono simmetriche reali e possono quindi essere ortogonalmente diagonalizzate in ambito reale. Ne consegue che $\mathbf{A}$ ha una decomposizione in valori singolari $\mathbf{U\Sigma V}^H$ con entrambi le matrici $\mathbf{U}$ e $\mathbf{V}$ ortogonali reali.

Delle molteplici applicazioni della decomposizione in valori singolari, di cui ricordiamo sono particolarmente importanti quelle alle norme matriciali (che non rientrano tra i nostri obiettivi), vedremo ora il legame con la decomposizione polare e una prova dell'esistenza della matrice pseudo-inversa alternativa a quella fornita dalla Proposizione 4.19 e dal Teorema 4.20 del Capitolo 1.

Forma polare

Ogni numero complesso z si può scrivere in forma trigonometrica:

$$z = \rho(\cos\alpha + i \operatorname{sen}\alpha)$$

dove ρ è un numero reale non negativo e coincide con $|z|$, il modulo di z, mentre α è l'argomento; ρ e α sono le coordinate polari (il polo è l'origine), e per questo la forma trigonometrica è detta anche *forma polare*. È naturale chiedersi se per matrici complesse $n \times n$ esiste una decomposizione analoga. La risposta è positiva e vale più generalmente per matrici $m \times n$ con $m \le n$.

La generalizzazione alle matrici della forma polare di un numero è fornita dalla seguente definizione: si chiama *forma polare* di una matrice complessa $m \times n$ $\mathbf{A}$, con $m \le n$, una fattorizzazione del tipo

$$\mathbf{A} = \mathbf{PQ}$$

dove $\mathbf{P}$ è hermitiana semi-definita positiva e $\mathbf{Q}$ è $m \times n$ a righe ortonormali, cioè $\mathbf{QQ}^H = \mathbf{I}_m$.

Teorema 4.6. *Ogni matrice complessa $m \times n$ $\mathbf{A}$, con $m \le n$, ha una decomposizione polare $\mathbf{A} = \mathbf{PQ}$, con $\mathbf{P}$ univocamente individuata, e $\mathbf{Q}$ univocamente individuata se $\mathbf{A}$ ha rango m.*

Dimostrazione. Sia $\mathbf{A} = \mathbf{U\Sigma V}^H$ una decomposizione in valori singolari di $\mathbf{A}$. Sia $\mathbf{\Sigma}_0$ la matrice diagonale $m \times m$ avente la stessa diagonale di $\mathbf{\Sigma}$. Posto $\mathbf{J} = [\mathbf{I}_m \ \mathbb{O}]$, dove il blocco nullo di $\mathbf{J}$ ha dimensioni $m \times (n-m)$, è immediato verificare che $\mathbf{\Sigma} = \mathbf{\Sigma}_0\mathbf{J}$ e che $\mathbf{J}\mathbf{J}^H = \mathbf{I}_m$. Si ha di conseguenza:

$$\mathbf{A} = \mathbf{U}\mathbf{\Sigma}_0\mathbf{J}\mathbf{V}^H = \mathbf{U}\mathbf{\Sigma}_0\mathbf{U}^H\mathbf{U}\mathbf{J}\mathbf{V}^H.$$

Si ponga $\mathbf{P} = \mathbf{U}\mathbf{\Sigma}_0\mathbf{U}^H$ e $\mathbf{Q} = \mathbf{U}\mathbf{J}\mathbf{V}^H$. È chiaro che $\mathbf{P}$ è semi-definita positiva, per il Teorema 3.6; si ha inoltre

$$\mathbf{Q}\mathbf{Q}^H = \mathbf{U}\mathbf{J}\mathbf{V}^H\mathbf{V}\mathbf{J}^H\mathbf{U}^H = \mathbf{U}\mathbf{J}\mathbf{J}^H\mathbf{U}^H = \mathbf{U}\mathbf{U}^H = \mathbf{I}_m.$$

Quanto all'unicità di $\mathbf{P}$, essa segue dalla Proposizione 3.7, in quanto $\mathbf{P}^2 = \mathbf{A}\mathbf{A}^H$. Infine, se $\mathbf{A}$ ha rango m, allora $\mathbf{P}$ ha pure rango m, quindi è invertibile e risulta $\mathbf{Q} = \mathbf{P}^{-1}\mathbf{A}$. □

Si osservi che nella costruzione eseguita nel Teorema 4.6 la matrice $\mathbf{P}$ ha il medesimo rango di $\mathbf{A}$; inoltre, se $\mathbf{A}$ è reale, la decomposizione in valori singolari $\mathbf{U}\mathbf{\Sigma}\mathbf{V}^H$ può essere scelta, per la Osservazione 4.5 (2), con entrambe le matrici $\mathbf{U}$ e $\mathbf{V}$ ortogonali reali. Ne consegue che $\mathbf{A}$ ha una decomposizione polare $\mathbf{A} = \mathbf{P}\mathbf{Q}$ con $\mathbf{P}$ e $\mathbf{Q}$ entrambe matrici reali.

Esempio 4.7. Si consideri la matrice già incontrata nell'Esempio 4.21 del Capitolo 1:

$$\mathbf{A} = \begin{bmatrix} 4 & 0 & 2 & 6 \\ 2 & 0 & 1 & 3 \end{bmatrix}.$$

Risulta

$$\mathbf{A}\mathbf{A}^H = \begin{bmatrix} 56 & 28 \\ 28 & 14 \end{bmatrix}$$

e un facile calcolo mostra che gli autovalori di $\mathbf{A}\mathbf{A}^H$ sono $\lambda_1 = 70$ e $\lambda_2 = 0$. Sono autovettori di norma 1 di λ_1 e λ_2, rispettivamente:

$$\mathbf{u}_1 = \begin{bmatrix} 2/\sqrt{5} & 1/\sqrt{5} \end{bmatrix}^T, \quad \mathbf{u}_2 = \begin{bmatrix} 1/\sqrt{5} & -2/\sqrt{5} \end{bmatrix}^T.$$

Perciò una diagonalizzazione unitaria di $\mathbf{A}\mathbf{A}^H$ è data da:

$$\mathbf{A}\mathbf{A}^H = \begin{bmatrix} 2/\sqrt{5} & 1/\sqrt{5} \\ 1/\sqrt{5} & -2/\sqrt{5} \end{bmatrix} \begin{bmatrix} 70 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 2/\sqrt{5} & 1/\sqrt{5} \\ 1/\sqrt{5} & -2/\sqrt{5} \end{bmatrix} = \mathbf{U}\mathbf{\Lambda}\mathbf{U}^H.$$

La matrice $\mathbf{U}$ è quindi individuata e la matrice $\mathbf{\Sigma}$ si ricava dal valore singolare $\sigma_1 = \lambda_1^{1/2} = \sqrt{70}$:

$$\mathbf{\Sigma} = \begin{bmatrix} \sqrt{70} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

In accordo con la dimostrazione del Teorema 4.4, la prima colonna della matrice unitaria $\mathbf{V}$ che diagonalizza $\mathbf{A}^H\mathbf{A}$ è data da:

$$\mathbf{v}_1 = \frac{1}{\sigma_1}\mathbf{A}^H\mathbf{u}_1 = \sqrt{\frac{1}{14}} \begin{bmatrix} 2 \\ 0 \\ 1 \\ 3 \end{bmatrix}.$$

Una base ortonormale dello spazio nullo di $\mathbf{A}^H\mathbf{A}$, che è il complemento ortogonale di $\langle \mathbf{v}_1 \rangle$, è data da:

$$\left\{ \mathbf{v}_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}; \mathbf{v}_3 = \begin{bmatrix} 0 \\ 0 \\ 3/\sqrt{10} \\ -1/\sqrt{10} \end{bmatrix}; \mathbf{v}_4 = \begin{bmatrix} 5/\sqrt{35} \\ 0 \\ -1/\sqrt{35} \\ -3/\sqrt{35} \end{bmatrix} \right\}.$$

I quattro vettori $\mathbf{v}_i$ sono le colonne della matrice unitaria $\mathbf{V}$ che diagonalizza $\mathbf{A}^H\mathbf{A}$:

$$\mathbf{V} = \begin{bmatrix} 2\sqrt{1/14} & 0 & 0 & 5/\sqrt{35} \\ 0 & 1 & 0 & 0 \\ \sqrt{1/14} & 0 & 3/\sqrt{10} & -1/\sqrt{35} \\ 3\sqrt{1/14} & 0 & -1/\sqrt{10} & -3/\sqrt{35} \end{bmatrix}.$$

Una decomposizione in valori singolari di $\mathbf{A}$ è data quindi da:

$$\begin{aligned} \mathbf{A} &= \mathbf{U}\boldsymbol{\Sigma}\mathbf{V}^H \\ &= \begin{bmatrix} 2/\sqrt{5} & 1/\sqrt{5} \\ 1/\sqrt{5} & -2/\sqrt{5} \end{bmatrix} \begin{bmatrix} \sqrt{70} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 2\sqrt{1/14} & 0 & \sqrt{1/14} & 3\sqrt{1/14} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 3/\sqrt{10} & -1/\sqrt{10} \\ 5/\sqrt{35} & 0 & -1/\sqrt{35} & -3/\sqrt{35} \end{bmatrix}. \end{aligned}$$

Per avere una dcomposizione polare a partire dalla decomposizione in valori singolari ottenuta, in accordo con la dimostrazione del Teorema 4.6 si ricava:

$$\mathbf{A} = \mathbf{U}\boldsymbol{\Sigma}\mathbf{V}^H = (\mathbf{U}\boldsymbol{\Sigma}_0\mathbf{U}^H)(\mathbf{U}\mathbf{J}\mathbf{V}^H) = \mathbf{P}\mathbf{Q}$$

dove

$$\mathbf{P} = \begin{bmatrix} 2/\sqrt{5} & 1/\sqrt{5} \\ 1/\sqrt{5} & -2/\sqrt{5} \end{bmatrix} \begin{bmatrix} \sqrt{70} & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 2/\sqrt{5} & 1/\sqrt{5} \\ 1/\sqrt{5} & -2/\sqrt{5} \end{bmatrix} = \frac{\sqrt{70}}{5} \begin{bmatrix} 4 & 2 \\ 2 & 1 \end{bmatrix}$$

$$\begin{aligned} \mathbf{Q} &= \begin{bmatrix} 2/\sqrt{5} & 1/\sqrt{5} \\ 1/\sqrt{5} & -2/\sqrt{5} \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 2\sqrt{1/14} & 0 & \sqrt{1/14} & 3\sqrt{1/14} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 3/\sqrt{10} & -1/\sqrt{10} \\ 5/\sqrt{35} & 0 & -1/\sqrt{35} & -3/\sqrt{35} \end{bmatrix} \\ &= \frac{1}{\sqrt{70}} \begin{bmatrix} 4 & \sqrt{14} & 2 & 6 \\ 2 & -2\sqrt{14} & 1 & 3 \end{bmatrix}. \end{aligned}$$

□

Decomposizione in valori singolari e pseudo-inversa

Ricordiamo che l'esistenza della matrice pseudo-inversa di una generica matrice complessa $m \times n$ $\mathbf{A}$ di rango k è stata ricavata nel Paragrafo 4 del Capitolo 1 tramite una decomposizione a rango pieno di $\mathbf{A}$, cioè una fattorizzazione del tipo $\mathbf{A} = \mathbf{B}\mathbf{C}$, con $\mathbf{B}$ $m \times k$ e $\mathbf{C}$ $k \times n$.

Vedremo ora come l'esistenza di decomposizioni in valori singolari di $\mathbf{A}$ produce una dimostrazione alternativa dell'esistenza della matrice pseudo-inversa.

Proposizione 4.8. *Data una decomposizione in valori singolari* $\mathbf{A} = \mathbf{U\Sigma V}^H$ *della matrice* $m \times n$ $\mathbf{A}$ *con valori singolari* $\sigma_1, \dots, \sigma_k$, *si ha che* $\mathbf{A}^+ = \mathbf{V\Sigma}^+\mathbf{U}^H$, *dove* $\mathbf{\Sigma}^+$ *è la matrice pseudo-diagonale* $n \times m$ *con sulla diagonale ordinatamente gli elementi* $\sigma_1^{-1}, \dots, \sigma_k^{-1}$, $0, \dots, 0$.

Dimostrazione. Lasciamo al lettore la facile verifica che la matrice $\mathbf{V\Sigma}^+\mathbf{U}^H$ sopra definita soddisfa alle quattro condizioni richieste per essere la pseudo-inversa $\mathbf{A}^+$. È poi altrettanto facile verificare che la matrice pseudo-diagonale con elementi diagonali $\sigma_1^{-1}, \dots, \sigma_k^{-1}, 0, \dots, 0$ è la pseudo-inversa di $\mathbf{\Sigma}$. □

Un terzo modo per ottenere la pseudo-inversa della matrice $\mathbf{A}$ è quello di fare uso di una decomposizione polare $\mathbf{A} = \mathbf{PQ}$; è facile controllare (si veda l'Esercizio 6.27) che $\mathbf{A}^+ = \mathbf{Q}^H\mathbf{P}^+$, dove $\mathbf{P}^+$ si ricava da una diagonalizzazione unitaria $\mathbf{U\Lambda U}^H$ di $\mathbf{P}$ con $\mathbf{\Lambda} = \mathbf{Diag}(\lambda_1, \dots, \lambda_k, 0, \dots, 0)$ e i numeri λ_i reali positivi:

$$\mathbf{P}^+ = \mathbf{U\Lambda}^+\mathbf{U}^H, \quad \mathbf{\Lambda}^+ = \mathbf{Diag}(\lambda_1^{-1}, \dots, \lambda_k^{-1}, 0, \dots, 0).$$

Esempio 4.9. Si consideri la matrice

$$\mathbf{A} = \begin{bmatrix} 4 & 0 & 2 & 6 \\ 2 & 0 & 1 & 3 \end{bmatrix};$$

si è visto nell'Esempio 4.21 del Capitolo 1 che la sua pseudo-inversa è

$$\mathbf{A}^+ = \frac{1}{70}\mathbf{A}^T.$$

Calcoliamo $\mathbf{A}^+$ tramite la Proposizione 4.8. Una decomposizione in valori singolari $\mathbf{A} = \mathbf{U\Sigma V}^H$ è stata calcolata nell'Esempio 4.7; dalla Proposizione 4.8 sappiamo che $\mathbf{A}^+ = \mathbf{V\Sigma}^+\mathbf{U}^H$, quindi risulta:

$$\begin{aligned}
\mathbf{A}^+ &= \begin{bmatrix} 2/\sqrt{14} & 0 & 0 & 5/\sqrt{35} \\ 0 & 1 & 0 & 0 \\ 1/\sqrt{14} & 0 & 3\sqrt{10} & -1/\sqrt{35} \\ 3/\sqrt{14} & 0 & -1/\sqrt{10} & -3/\sqrt{35} \end{bmatrix} \begin{bmatrix} 1/\sqrt{70} & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 2/\sqrt{5} & 1/\sqrt{5} \\ 1/\sqrt{5} & -2/\sqrt{5} \end{bmatrix} \\
&= \begin{bmatrix} 2/\sqrt{14\cdot 70} & 0 \\ 0 & 0 \\ 1/\sqrt{14\cdot 70} & 0 \\ 3/\sqrt{14\cdot 70} & 0 \end{bmatrix} \begin{bmatrix} 2/\sqrt{5} & 1/\sqrt{5} \\ 1/\sqrt{5} & -2/\sqrt{5} \end{bmatrix} = \begin{bmatrix} 4/70 & 2/70 \\ 0 & 0 \\ 2/70 & 1/70 \\ 6/70 & 3/70 \end{bmatrix}
\end{aligned}$$

in accordo con il risultato dell'Esempio 4.21 del Capitolo 1. □

5. Principi variazionali per autovalori di matrici hermitiane

Nell'ambito della classe delle matrici normali, le matrici hermitiane costituiscono una sottoclasse privilegiata, per il fatto che esistono una serie di importanti risultati sui loro autovalori, che sono usualmente designati col termine di “principi variazionali”. I risultati più importanti riguardano

— la caratterizzazione degli autovalori in termini di minimi e massimi vincolati, quindi come soluzioni di problemi di ottimizzazione (Teorema “min-max” di Courant-Fischer), che costituisce un raffinamento del Principio di Rayleigh-Ritz (Teorema 3.4);

— il confronto tra gli autovalori di una matrice hermitiana con quelli delle sue sottomatrici principali (Principio di inclusione, o Teorema dell’intreccio), da cui segue come caso particolare il Teorema di separazione di Poincaré;

— il confronto tra gli autovalori di due matrici hermitiane dello stesso ordine con quelli della loro somma (Teorema di monotonicità di Weyl).

Ciascuno di questi risultati ha un suo analogo riguardante i valori singolari di matrici arbitrarie; ciò non sorprende se si ricorda che i valori singolari di una matrice $\mathbf{A}$ sono le radici quadrate degli autovalori positivi della matrice hermitiana semi-definita positiva $\mathbf{A}\mathbf{A}^H$. In questo Paragrafo vedremo i principi variazionali per gli autovalori di matrici hermitiane. I corrispondenti risultati per i valori singolari non rientrano invece tra gli scopi di questo libro; il lettore a essi interessato può per esempio consultare il Capitolo X del testo “Matrix Algebra and its Applications to Statistics and Econometrics”, di C. R. Rao e M. B. Rao, World Scientific (1998).

Nel seguito $\rho_{\mathbf{A}}$ denota la funzione di Rayleigh-Ritz introdotta nel Paragrafo 3; se $1 \le k \le n$, denoteremo con $\mathcal{V}_k$ l’insieme dei sottospazi vettoriali di $\mathbb{C}^n$ di dimensione k; porremo poi $\mathcal{V}_0 = \{\mathbf{0}\}$.

Teorema min-max 5.1 (Courant-Fischer). *Data una matrice hermitiana* $\mathbf{A}$ *con autovalori* $\lambda_1 \le \lambda_2 \le \cdots \le \lambda_n$, *per ogni* $k \le n$ *risulta*

$$\begin{aligned}\lambda_k &= \max_{V \in \mathcal{V}_{k-1}} \min_{\mathbf{0} \neq \mathbf{x} \in V^\perp} \rho_{\mathbf{A}}(\mathbf{x})\\ &= \min_{V \in \mathcal{V}_{n-k}} \max_{\mathbf{0} \neq \mathbf{x} \in V^\perp} \rho_{\mathbf{A}}(\mathbf{x}).\end{aligned}$$

Dimostrazione. Nel caso in cui $k = n$, nella caratterizzazione di λ_n come min-max la minimizzazione viene fatta sul solo sottospazio nullo, il cui ortogonale è tutto $\mathbb{C}^n$; invece nella caratterizzazione di λ_n come max-min, la massimizzazione viene fatta sui sottospazi $(n-1)$-dimensionali, i cui complementi ortogonali hanno dimensione 1, perciò equivale a massimizzare su tutto $\mathbb{C}^n \setminus \mathbf{0}$. Se invece $k = 1$, nella caratterizzazione di λ_1 come max-min la massimizzazione viene fatta sul solo sottospazio nullo, e nella caratterizzazione come min-max la minimizzazione viene fatta sui sottospazi $n-1$-dimensionali, per cui si ragiona come prima. In questi due casi estremi quindi il risultato si riduce al Teorema 3.4, perciò supporremo $1 < k < n$.

Nel Teorema 3.4 si è visto che, per ogni k compreso tra 2 ed $n-1$, posto $V_k = \langle \mathbf{u}_k, \dots, \mathbf{u}_n \rangle$, risulta

$$\lambda_k = \min_{\mathbf{0} \neq \mathbf{x} \in V_k} \rho_{\mathbf{A}}(\mathbf{x}).$$

Poiché $V_k = \langle \mathbf{u}_1, \dots, \mathbf{u}_{k-1} \rangle^\perp$, risulta

$$\lambda_k = \min_{\mathbf{0} \neq \mathbf{x} \in (V^{k-1})^\perp} \rho_{\mathbf{A}}(\mathbf{x})$$

dove $V^{k-1} = \langle \mathbf{u}_1, \dots, \mathbf{u}_{k-1} \rangle \in \mathcal{V}_{k-1}$. Quindi per dimostrare la prima uguaglianza è sufficiente provare che

$$\lambda_k \geq \inf_{\mathbf{0} \neq \mathbf{x} \in V^\perp} \rho_{\mathbf{A}}(\mathbf{x})$$

per ogni scelta di $V \in \mathcal{V}_{k-1}$. Osserviamo che l'inf nella disuguaglianza precedente è in realtà un minimo, perché la funzione di Rayleigh-Ritz è continua sull'intersezione della sfera n-dimensionale unitaria col sottospazio $V^\perp$, che è un sottoinsieme chiuso e limitato, quindi compatto, di $\mathbb{C}^n$.

Posto $\mathbf{U}^H \mathbf{x} = \mathbf{y}$ e $\mathbf{U}^H V = \{\mathbf{U}^H \mathbf{v} \mid \mathbf{v} \in V\}$, e ricordando che $\mathbf{A} = \mathbf{U}\boldsymbol{\Lambda}\mathbf{U}^H$ con $\boldsymbol{\Lambda} = \mathbf{Diag}(\lambda_i)$, si ha:

$$\begin{aligned}
\inf_{\mathbf{0} \neq \mathbf{x} \in V^\perp} \rho_{\mathbf{A}}(\mathbf{x}) &= \inf_{\mathbf{0} \neq \mathbf{x} \in V^\perp} \frac{\mathbf{x}^H \mathbf{U}\boldsymbol{\Lambda}\mathbf{U}^H \mathbf{x}}{\mathbf{x}^H \mathbf{x}} = \inf_{\mathbf{0} \neq \mathbf{y} \in (\mathbf{U}^H V)^\perp} \frac{\mathbf{y}^H \boldsymbol{\Lambda} \mathbf{y}}{\mathbf{y}^H \mathbf{y}} \\
&= \inf\{\sum_i \lambda_i |y_i|^2 \mid \sum_i |y_i|^2 = 1, \mathbf{y} \in (\mathbf{U}^H V)^\perp\} \\
&\leq \inf\{\sum_i \lambda_i |y_i|^2 \mid \sum_i |y_i|^2 = 1, \mathbf{y} \in (\mathbf{U}^H V)^\perp, y_i = 0 \text{ per } k+1 \leq i \leq n\}.
\end{aligned}$$

L'ultimo inf ha senso, perché il sottospazio $(\mathbf{U}^H V)^\perp$ ha dimensione $n-(k-1)$ e il sottospazio $W = \{\mathbf{y} \mid y_i = 0 \text{ per } k+1 \leq i \leq n\}$ ha dimensione k, perciò la loro intersezione è non nulla, quindi contiene un vettore $\mathbf{y}$ di norma euclidea 1. Per concludere basta osservare che, se $\sum_i |y_i|^2 = 1$ e $0 = y_{k+1} = \ldots = y_n$, risulta

$$\lambda_k = \sum_{1 \leq i \leq n} \lambda_k |y_i|^2 = \sum_{1 \leq i \leq k} \lambda_k |y_i|^2 \geq \sum_{1 \leq i \leq k} \lambda_i |y_i|^2.$$

La caratterizzazione di λ_k come min-max è simile ed è lasciata al lettore come esercizio. □

Osserviamo che la formulazione più complicata del Teorema min-max rispetto al Principio di Rayleigh-Ritz è compensata dal fatto che esso si svincola dalla conoscenza degli autovalori.

Il risultato seguente si può derivare dal Teorema min-max; ne forniamo qui una dimostrazione diretta che fa uso solo del Teorema spettrale.

Teorema 5.2 (Principio di inclusione)**.** *Date una matrice hermitiana* $\mathbf{A}$ *e una sua sottomatrice principale* $\mathbf{B}$ *di ordine* r*, con rispettivi autovalori* $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n$*,* $\mu_1 \leq \mu_2 \leq \cdots \leq \mu_r$*, si ha per ogni* $k \leq r$*:*

$$\lambda_k \leq \mu_k \leq \lambda_{k+n-r}.$$

Dimostrazione. Con una cogredienza, possiamo portare le righe e le colonne che formano la sottomatrice principale $\mathbf{B}$ ai primi r posti; poiché le cogredienze sono similitudini e non cambiano gli autovalori delle matrici, non è restrittivo supporre che $\mathbf{B} = \mathbf{A}_r$.

Consideriamo diagonalizzazioni unitarie delle due matrici:

$$\mathbf{A} = \mathbf{U\Lambda U}^H, \qquad \mathbf{A}_r = \mathbf{VMV}^H$$

e siano $\mathbf{u}_i$ e $\mathbf{v}_j$ ($1 \le i \le n$, $1 \le j \le r$) le colonne rispettivamente delle matrici unitarie $\mathbf{U}$ e $\mathbf{V}$. Per ogni $j \le r$ consideriamo il vettore n-dimensionale $\mathbf{w}_j = [\mathbf{v}_j^T \ \mathbf{0}^T]^T$; i vettori $\mathbf{w}_1, \dots, \mathbf{w}_r$ formano un sistema ortonormale in $\mathbb{C}^n$.

Fissato l'indice k, consideriamo i due sottospazi di $\mathbb{C}^n$:

$$U = \langle \mathbf{u}_k, \mathbf{u}_{k+1}, \dots, \mathbf{u}_n \rangle, \qquad W = \langle \mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_k \rangle.$$

Le loro dimensioni sono rispettivamente $n-k+1$ e k, perciò esiste un vettore $\mathbf{x} \in U \cap W$ tale che $\|\mathbf{x}\|_2 = 1$.

Risulta $\mathbf{x} = \sum_{k \le i \le n} \alpha_i \mathbf{u}_i$ per opportuni α_i tali che $\sum_{k \le i \le n} |\alpha_i|^2 = 1$, e similmente $\mathbf{x} = \sum_{1 \le i \le k} \beta_i \mathbf{w}_i$ per opportuni β_i tali che $\sum_{1 \le i \le k} |\beta_i|^2 = 1$. Posto $\mathbf{y} = \sum_{1 \le i \le k} \beta_i \mathbf{v}_i$, si ha che $\mathbf{x} = [\mathbf{y}^T \ \mathbf{0}^T]^T$, da cui consegue che

$$\mathbf{x}^H \mathbf{A} \mathbf{x} = [\mathbf{y}^H \ \mathbf{0}^H] \mathbf{A} \begin{bmatrix} \mathbf{y} \\ \mathbf{0} \end{bmatrix} = \mathbf{y}^H \mathbf{A}_r \mathbf{y}.$$

Osservando che, per ogni $i \le n$, $\mathbf{U}^H \mathbf{u}_i = \mathbf{e}_i$, i-esimo vettore coordinato di $\mathbb{C}^n$, risulta:

$$\begin{aligned} \mathbf{x}^H \mathbf{A} \mathbf{x} &= \Big(\sum_{k \le i \le n} \bar{\alpha}_i \mathbf{u}_i^H \Big) \mathbf{U\Lambda U}^H \Big(\sum_{k \le i \le n} \alpha_i \mathbf{u}_i \Big) \\ &= \sum_{k \le i \le n} |\alpha_i|^2 \lambda_i \ge \sum_{k \le i \le n} |\alpha_i|^2 \lambda_k = \lambda_k. \end{aligned}$$

Analogamente, osservando che, per ogni $j \le r$, $\mathbf{V}^H \mathbf{v}_j = \mathbf{e}'_j$, j-esimo vettore coordinato di $\mathbb{C}^r$, risulta:

$$\begin{aligned} \mathbf{y}^H \mathbf{A}_r \mathbf{y} &= \Big(\sum_{1 \le j \le k} \bar{\beta}_j \mathbf{v}_j^H \Big) \mathbf{VMV}^H \Big(\sum_{1 \le j \le k} \beta_j \mathbf{v}_j \Big) \\ &= \sum_{1 \le j \le k} |\beta_j|^2 \mu_j \le \sum_{1 \le j \le k} |\beta_j|^2 \mu_k = \mu_k. \end{aligned}$$

Dalle disuguaglianze precedenti si ricava pertanto che $\lambda_k \le \mu_k$.

Applichiamo il risultato appena ottenuto alla matrice $-\mathbf{A}$ e alla sua sottomatrice principale r-esima $-\mathbf{A}_r$; i loro autovalori ordinati in modo non decrescente sono rispettivamente $-\lambda_n, \dots, -\lambda_1$ e $-\mu_r, \dots, -\mu_1$. Fissato $j \le r$, per la coppia dei j-esimi autovalori si ha la disuguaglianza appena provata

$$-\lambda_{n-j+1} \le -\mu_{r-j+1}$$

che equivale a $\lambda_{n-j+1} \geq \mu_{r-j+1}$. Posto $k = r - j + 1$, risulta $n - j + 1 = n - r + r - j + 1 = n - r + k$, quindi la disuguaglianza precedente coincide con la disuguaglianza cercata $\lambda_{n-k+1} \geq \mu_k$. □

Il Principio di inclusione, nel caso di sottomatrici principali di ordine $n-1$, viene anche detto Teorema dell'intreccio, perché le disuguaglianze del Teorema 5.2 diventano le seguenti:

$$\lambda_1 \leq \mu_1 \leq \lambda_2 \leq \cdots \leq \lambda_k \leq \mu_k \leq \lambda_{k+1} \leq \cdots \leq \mu_{n-1} \leq \lambda_n,$$

ovvero, gli $n-1$ autovalori della sottomatrice si "intrecciano" con gli n autovalori della matrice di partenza.

Nel caso invece in cui $r = 1$, le disuguaglianze del Teorema 5.2 dicono semplicemente che $\lambda_1 \leq a_{ii} \leq \lambda_n$ per ogni $i \leq n$.

Una conseguenza immediata del Principio di inclusione è il risultato seguente.

Teorema di separazione 5.3 (Poincaré)**.** *Data una matrice hermitiana $n \times n$ $\mathbf{A}$ con autovalori $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n$ e una matrice $n \times r$ a colonne ortonormali $\mathbf{Q}$ (quindi $\mathbf{Q}^H\mathbf{Q} = \mathbf{I}_r$), sia $\mathbf{B} = \mathbf{Q}^H\mathbf{A}\mathbf{Q}$ e siano $\mu_1 \leq \mu_2 \leq \cdots \leq \mu_r$ i suoi autovalori. Allora valgono le disuguaglianze per ogni $k \leq r$:*

$$\lambda_k \leq \mu_k \leq \lambda_{k+n-r}.$$

Dimostrazione. Si completi la matrice $\mathbf{Q}$ aggiungendole $n-r$ colonne in modo che la nuova matrice $\mathbf{U} = [\mathbf{Q}\ \mathbf{Q}_1]$ così ottenuta risulti una matrice unitaria. Le matrici $\mathbf{A}$ e $\mathbf{U}^H\mathbf{A}\mathbf{U}$ hanno gli stessi autovalori e la matrice $\mathbf{B}$ coincide con la sottomatrice principale r-esima di $\mathbf{U}^H\mathbf{A}\mathbf{U}$:

$$\mathbf{U}^H\mathbf{A}\mathbf{U} = \begin{bmatrix} \mathbf{Q}^H \\ \mathbf{Q}_1^H \end{bmatrix} \mathbf{A}[\mathbf{Q}\ \mathbf{Q}_1] = \begin{bmatrix} \mathbf{Q}^H\mathbf{A}\mathbf{Q} & \mathbf{Q}^H\mathbf{A}\mathbf{Q}_1 \\ \mathbf{Q}_1^H\mathbf{A}\mathbf{Q} & \mathbf{Q}_1^H\mathbf{A}\mathbf{Q}_1 \end{bmatrix}.$$

Basta ora applicare il Teorema 5.2. □

Si osservi che il Principio di inclusione non è che il caso particolare del Teorema 5.3, quando si sceglie come matrice $\mathbf{Q}$ la matrice avente come r colonne i vettori coordinati con gli indici delle colonne che formano la matrice B.

Passiamo ora al terzo e ultimo dei principi variazionali presentati in questo Paragrafo.

Teorema di monotonicità 5.4 (H. Weyl)**.** *Date due matrici hermitiane $n \times n$ $\mathbf{A}$ e $\mathbf{B}$ con rispettivi autovalori $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n$, $\mu_1 \leq \mu_2 \leq \cdots \leq \mu_n$, detti $\gamma_1 \leq \gamma_2 \leq \cdots \leq \gamma_n$ gli autovalori di $\mathbf{A}+\mathbf{B}$, si ha per ogni $k \leq n$ e per $1 \leq j \leq k \leq i \leq n$:*

$$\lambda_j + \mu_{k-j+1} \leq \gamma_k \leq \lambda_i + \mu_{n-i+k}.$$

Dimostrazione. Consideriamo diagonalizzazioni unitarie delle tre matrici:

$$\mathbf{A} = \mathbf{U}\boldsymbol{\Lambda}\mathbf{U}^H, \qquad \mathbf{B} = \mathbf{V}\mathbf{M}\mathbf{V}^H, \qquad \mathbf{A}+\mathbf{B} = \mathbf{W}\boldsymbol{\Gamma}\mathbf{W}^H$$

e siano $\mathbf{u}_i$, $\mathbf{v}_i$, $\mathbf{w}_i$ $(1 \le i \le n)$ le colonne rispettivamente delle matrici unitarie $\mathbf{U}$, $\mathbf{V}$, $\mathbf{W}$. Fissati gli indici $j \le k \le i$, consideriamo i tre sottospazi di $\mathbb{C}^n$:

$$\begin{aligned} U &= \langle \mathbf{u}_j, \mathbf{u}_{j+1}, \dots, \mathbf{u}_n \rangle, \\ V &= \langle \mathbf{v}_{k-j+1}, \mathbf{v}_{k-j+2}, \dots, \mathbf{v}_n \rangle, \\ W &= \langle \mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_k \rangle. \end{aligned}$$

Le loro dimensioni sono rispettivamente $n-j+1$, $n-k+j$, k. Applicando due volte la formula che dice che, dati due sottospazi X e Y di uno spazio vettoriale di dimensione finita, risulta $\dim(X \cap Y) = \dim X + \dim Y - \dim(X+Y)$, si ricava:

$$\begin{aligned} \dim(U \cap V \cap W) &= \dim U + \dim(V \cap W) - \dim(U + (V \cap W)) \\ &= \dim U + \dim V + \dim W - \dim(V+W) - \dim(U + (V \cap W)) \\ &\ge \dim U + \dim V + \dim W - n - n \\ &= n - j + 1 + n - k + j + k - 2n = 1. \end{aligned}$$

Di conseguenza esiste un vettore $\mathbf{z} \in U \cap V \cap W$ di norma euclidea 1. Il fatto che $\mathbf{z} \in U$ assicura che si può scrivere

$$\mathbf{z} = \alpha_j \mathbf{u}_j + \alpha_{j+1} \mathbf{u}_{j+1} + \dots + \alpha_n \mathbf{u}_n$$

per opportuni coefficienti complessi α_l. L'ipotesi che $\|\mathbf{z}\|_2 = 1$ e il fatto che i vettori $\mathbf{u}_l$ sono un sistema ortonormale assicurano che $\sum_{j \le l \le n} |\alpha_l|^2 = 1$. Inoltre si ha:

$$\begin{aligned} \mathbf{z}^H \mathbf{A} \mathbf{z} &= \Big(\sum_j^n \bar{\alpha}_l \mathbf{u}_l^H \Big) \mathbf{U} \boldsymbol{\Lambda} \mathbf{U}^H \Big(\sum_j^n \alpha_l \mathbf{u}_l \Big) \\ &= \sum_j^n |\alpha_l|^2 \lambda_l \ge \lambda_j \sum_j^n |\alpha_l|^2 = \lambda_j \end{aligned}$$

dove si è usato il fatto che $\mathbf{U}$ è a colonne ortonormali. In modo analogo si prova che

$$\mathbf{z}^H \mathbf{B} \mathbf{z} \ge \mu_{k-j+1}, \qquad \mathbf{z}^H (\mathbf{A} + \mathbf{B}) \mathbf{z} \le \gamma_k.$$

Dalle tre disuguaglianze precedenti si ricava

$$\gamma_k \ge \mathbf{z}^H (\mathbf{A} + \mathbf{B}) \mathbf{z} = \mathbf{z}^H \mathbf{A} \mathbf{z} + \mathbf{z}^H \mathbf{B} \mathbf{z} \ge \lambda_j + \mu_{k-j+1}$$

il che dimostra la prima delle due disuguaglianze in enunciato. L'altra disuguaglianza si prova in modo analogo e la prova è lasciata al lettore come esercizio. Si può anche applicare quanto appena provato alle tre matrici $-\mathbf{A}$, $-\mathbf{B}$ e $-\mathbf{A} - \mathbf{B}$. □

È opportuno visualizzare la serie di disuguaglianze espresse in modo sintetico nell'enunciato del Teorema 5.4; con le notazioni ivi impiegate si ha:

$$\begin{gathered} \lambda_1 + \mu_1 \le \gamma_1 \le \lambda_1 + \mu_n,\ \lambda_2 + \mu_{n-1},\ \dots,\ \lambda_n + \mu_1 \\ \lambda_2 + \mu_1,\ \lambda_1 + \mu_2 \le \gamma_2 \le \lambda_2 + \mu_n,\ \lambda_3 + \mu_{n-1},\ \dots,\ \lambda_n + \mu_2 \\ \dots \\ \lambda_{n-1} + \mu_1,\ \dots,\ \lambda_2 + \mu_{n-2},\ \lambda_1 + \mu_{n-1} \le \gamma_{n-1} \le \lambda_{n-1} + \mu_n,\ \lambda_n + \mu_{n-1} \\ \lambda_n + \mu_1,\ \dots,\ \lambda_2 + \mu_{n-1},\ \lambda_1 + \mu_n \le \gamma_n \le \lambda_n + \mu_n. \end{gathered}$$

Per esempio, se $n = 3$, la lista completa delle disuguaglianze è la seguente:

$$\begin{gathered}
\lambda_1 + \mu_1 \le \gamma_1 \le \lambda_1 + \mu_3,\ \lambda_2 + \mu_2,\ \lambda_3 + \mu_1 \\
\lambda_2 + \mu_1,\ \lambda_1 + \mu_2 \le \gamma_2 \le \lambda_2 + \mu_3,\ \lambda_3 + \mu_2 \\
\lambda_3 + \mu_1,\ \lambda_2 + \mu_2,\ \lambda_1 + \mu_3 \le \gamma_3 \le \lambda_3 + \mu_3.
\end{gathered}$$

Esempio 5.5. Consideriamo le matrici hermitiane

$$\mathbf{A} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 4 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \qquad \mathbf{B} = \begin{bmatrix} 10 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}$$

che hanno come polinomi caratteristici rispettivamente $p_{\mathbf{A}}(X) = (4 - X)(X^2 - X - 1)$ e $p_{\mathbf{B}}(X) = (1 + X)(X^2 - 11X + 9)$. La matrice somma è

$$\mathbf{A} + \mathbf{B} = \begin{bmatrix} 11 & 1 & 1 \\ 1 & 5 & 0 \\ 1 & 0 & -1 \end{bmatrix}$$

che ha polinomio caratteristico $p_{\mathbf{A}+\mathbf{B}}(X) = -X^3 + 15X^2 - 37X - 59$. Quindi i loro autovalori, sistemati in ordine crescente, sono:

$$\begin{aligned}
&\text{per } \mathbf{A}\text{: } \lambda_1 = \frac{1 - \sqrt{5}}{2} < \lambda_2 = \frac{1 + \sqrt{5}}{2} < \lambda_3 = 4; \\
&\text{per } \mathbf{B}\text{: } \mu_1 = -1 < \mu_2 = \frac{11 - \sqrt{85}}{2} < \mu_3 = \frac{11 + \sqrt{85}}{2}.
\end{aligned}$$

Un esame del polinomio caratteristico di $\mathbf{A} + \mathbf{B}$ mostra che

$$\begin{aligned}
&p_{\mathbf{A}+\mathbf{B}}(-1.5) > 0,\ p_{\mathbf{A}+\mathbf{B}}(-1) < 0 \implies -1.5 < \gamma_1 < -1 \\
&p_{\mathbf{A}+\mathbf{B}}(4) < 0,\ p_{\mathbf{A}+\mathbf{B}}(4.85) > 0 \implies 4 < \gamma_2 < 4.85 \\
&p_{\mathbf{A}+\mathbf{B}}(11) > 0,\ p_{\mathbf{A}+\mathbf{B}}(12) < 0 \implies 11 < \gamma_3 < 12.
\end{aligned}$$

Si vede allora che le disuguaglianze del Teorema 5.4 sono verificate:

$$\begin{gathered}
\lambda_1 + \mu_1 = \frac{-1 - \sqrt{5}}{2} < -1.5 < \gamma_1 \\
\gamma_1 < -1 < \lambda_1 + \mu_3 = \frac{12 + \sqrt{85} - \sqrt{5}}{2},\ \lambda_2 + \mu_2 = \frac{12 + \sqrt{5} - \sqrt{85}}{2},\ \lambda_3 + \mu_1 = 3 \\
\lambda_2 + \mu_1 = \frac{\sqrt{5} - 1}{2},\ \lambda_1 + \mu_2 = \frac{12 - \sqrt{85} - \sqrt{5}}{2} < 4 < \gamma_2 \\
\gamma_2 < 4.85 < \lambda_2 + \mu_3 = \frac{12 + \sqrt{85} + \sqrt{5}}{2},\ \lambda_3 + \mu_2 = \frac{19 - \sqrt{85}}{2} \\
\lambda_3 + \mu_1 = 3,\ \lambda_2 + \mu_2 = \frac{12 + \sqrt{5} - \sqrt{85}}{2},\ \lambda_1 + \mu_3 = \frac{12 + \sqrt{85} - \sqrt{5}}{2} < 11 < \gamma_3 \\
\gamma_3 < 12 < \lambda_3 + \mu_3 = \frac{19 + \sqrt{85}}{2}.
\end{gathered}$$

□

6. Congruenze e Legge d'inerzia

La relazione di similitudine che intercorre tra matrici quadrate dello stesso ordine ha la sua origine dal confronto tra due matrici che rappresentano la stessa trasformazione lineare di uno spazio vettoriale in sé rispetto a due diverse basi.

Il confronto tra due matrici che rappresentano invece la stessa forma bilineare reale simmetrica (o sesquilineare hermitiana, nel caso complesso) rispetto a due diverse basi produce la relazione di congruenza. Una *forma sesquilineare hermitiana* di ordine n è una funzione $f\colon V \times V \to \mathbb{C}$, dove V è una spazio vettoriale complesso di dimensione n, che gode delle proprietà

(1) $f(\mathbf{v}, \alpha\mathbf{w} + \beta\mathbf{z}) = \alpha f(\mathbf{v}, \mathbf{w}) + \beta f(\mathbf{v}, \mathbf{z})$, per ogni $\mathbf{v}, \mathbf{w}, \mathbf{z} \in V$ e $\alpha, \beta \in \mathbb{C}$;

(2) $f(\mathbf{v}, \mathbf{w}) = \overline{f(\mathbf{w}, \mathbf{v})}$, per ogni $\mathbf{v}, \mathbf{w} \in V$.

Siano $\mathscr{B}$ e $\mathscr{B}'$ due basi dello spazio vettoriale n-dimensionale V e sia $\mathbf{M}$ la matrice di passaggio (invertibile) dalle coordinate rispetto a $\mathscr{B}'$ alle coordinate rispetto a B; come si è visto nel Paragrafo 5 del Capitolo 2, $\mathbf{M}$ soddisfa alla relazione:

$$C_{\mathscr{B}}(\mathbf{v}) = \mathbf{M}\, C_{\mathscr{B}'}(\mathbf{v}), \quad \text{per ogni } \mathbf{v} \in V.$$

Nel Teorema 2.5 del Capitolo 3 abbiamo visto, usando solo le proprietà cui soddisfa f che, per ogni $\mathbf{x}, \mathbf{y} \in \mathbb{C}^n$, risulta

$$C_{\mathscr{B}}(\mathbf{x})^H \mathbf{A}\, C_{\mathscr{B}}(\mathbf{y}) = f(\mathbf{x}, \mathbf{y}) = C_{\mathscr{B}'}(\mathbf{x})^H \mathbf{A}'\, C_{\mathscr{B}'}(\mathbf{y}),$$

dove $\mathbf{A}$ e $\mathbf{A}'$ sono le matrici di Gram associate a f rispetto alle due basi $\mathscr{B}$ e $\mathscr{B}'$, rispettivamente. Dalle due relazioni precedenti si ricava che

$$C_{\mathscr{B}'}(\mathbf{x})^H \mathbf{M}^H \mathbf{A}\mathbf{M}\, C_{\mathscr{B}'}(\mathbf{y}) = C_{\mathscr{B}'}(\mathbf{x})^H \mathbf{A}'\, C_{\mathscr{B}'}(\mathbf{y})$$

e quindi, vista l'arbitrarietà dei vettori $\mathbf{x}$ e $\mathbf{y}$, $\mathbf{M}^H\mathbf{A}\mathbf{M} = \mathbf{A}'$.

Questa uguaglianza motiva la seguente definizione.

Definizione. Date due matrici $\mathbf{A}$ e $\mathbf{B}$ di ordine n, si dice che $\mathbf{A}$ è *congrua* a $\mathbf{B}$ se esiste una matrice invertibile $\mathbf{S}$ tale che $\mathbf{A} = \mathbf{S}\mathbf{B}\mathbf{S}^H$.

Evidentemente la relazione di congruenza gode delle proprietà riflessiva, simmetrica e transitiva, quindi è una relazione di equivalenza. Noi siamo interessati a congruenze tra matrici hermitiane; si noti che, se $\mathbf{A}$ è hermitiana ed è congrua a $\mathbf{B}$, allora anche $\mathbf{B}$ è hermitiana.

Scopo principale di questo Paragrafo è dimostrare la Legge d'inerzia dovuta a Sylvester, la quale afferma che due matrici hermitiane sono tra di loro congrue se e solo se hanno lo stesso numero di autovalori positivi, negativi e nulli. È utile a tal fine definire come *inerzia* della matrice hermitiana $\mathbf{A}$ la terna ordinata di numeri interi non negativi

$$i(\mathbf{A}) = [i_+(\mathbf{A}), i_-(\mathbf{A}), i_0(\mathbf{A})]$$

dove $i_+(\mathbf{A})$ denota il numero di autovalori (reali) positivi di $\mathbf{A}$, $i_-(\mathbf{A})$ il numero di quelli negativi e $i_0(\mathbf{A})$ il numero di quelli nulli. Si osservi che, se k denota il rango di $\mathbf{A}$, allora $k = i_+(\mathbf{A}) + i_-(\mathbf{A})$.

Chiameremo poi *matrice d'inerzia* associata alla matrice hermitiana $\mathbf{A}$, e la denoteremo con $\mathbf{Z_A}$, la matrice $\mathbf{Diag}(1,\dots,1,-1,\dots,-1,0,\dots,0)$ contenente sulla diagonale $i_+(\mathbf{A})$ elementi uguali a 1, $i_-(\mathbf{A})$ elementi uguali a -1 e $i_0(\mathbf{A})$ elementi uguali a 0, ordinatamente.

Con tali notazioni possiamo enunciare in modo semplice il seguente risultato.

Teorema 6.1 (Legge d'inerzia)**.** *Due matrici hermitiane sono tra di loro congrue se e solo se hanno la stessa inerzia.*

Dimostrazione. Per dimostrare la sufficienza basta provare che ogni matrice hermitiana $\mathbf{A}$ è congrua alla matrice d'inerzia a essa associata $\mathbf{Z_A}$, col che la conclusione segue subito dalla proprietà transitiva della congruenza. Per il Teorema spettrale, $\mathbf{A} = \mathbf{U\Lambda U}^H$ è unitariamente simile alla matrice diagonale $\mathbf{\Lambda} = \mathbf{Diag}(\lambda_1,\dots,\lambda_n)$ dei suoi autovalori, che sono numeri reali, per il Teorema 2.2. Possiamo supporre che i primi $i_+(\mathbf{A})$ autovalori siano positivi, i successivi $i_-(\mathbf{A})$ autovalori siano negativi, e i restanti $i_0(\mathbf{A})$ autovalori siano nulli. Denotiamo con $\mathbf{D} = \mathbf{Diag}(d_1,\dots,d_n)$ la matrice diagonale invertibile così definita:

$$d_i = \begin{cases} \frac{1}{\sqrt{\lambda_i}} & \text{se } \lambda_i > 0, \\ \frac{1}{\sqrt{-\lambda_i}} & \text{se } \lambda_i < 0, \\ 1 & \text{se } \lambda_i = 0. \end{cases}$$

Un facile calcolo mostra che $\mathbf{D\Lambda D}^H = \mathbf{Z_A}$, perciò risulta

$$\mathbf{A} = \mathbf{U\Lambda U}^H = \mathbf{UD}^{-1}\mathbf{Z_A}(\mathbf{D}^H)^{-1}\mathbf{U}^H = \mathbf{UD}^{-1}\mathbf{Z_A}(\mathbf{UD}^{-1})^H$$

quindi $\mathbf{A}$ è congrua a $\mathbf{Z_A}$, come si voleva dimostrare.

La parte più difficile della dimostrazione è la necessità. Siano $\mathbf{A}$ e $\mathbf{B}$ due matrici hermitiane congrue tra di loro. Poiché esse hanno uguale rango, risulta $i_+(\mathbf{A}) + i_-(\mathbf{A}) = i_+(\mathbf{B}) + i_-(\mathbf{B})$, da cui segue che $i_0(\mathbf{A}) = i_0(\mathbf{B})$. Per dimostrare che $\mathbf{A}$ e $\mathbf{B}$ hanno la stessa inerzia, basta allora provare che $i_+(\mathbf{A}) = i_+(\mathbf{B})$. Supponiamo per assurdo che $i_+(\mathbf{A}) < i_+(\mathbf{B})$. Per quanto visto sopra, cioè che una matrice hermitiana è congrua alla matrice d'inerzia a essa associata, si ha che $\mathbf{Z_A}$ è congrua a $\mathbf{Z_B}$. Esiste pertanto una matrice invertibile $\mathbf{S}$ tale che $\mathbf{Z_B} = \mathbf{S}^H\mathbf{Z_A}\mathbf{S}$.

Supponiamo dapprima che $i_+(\mathbf{A}) > 0$. Sia $\mathbf{S}_0$ la sottomatrice di $\mathbf{S}$ formata dalle sue prime $i_+(\mathbf{A})$ righe. L'ipotesi che $i_+(\mathbf{A}) < i_+(\mathbf{B})$ assicura che esistono soluzioni non nulle del sistema omogeneo $\mathbf{S}_0\mathbf{x} = \mathbf{0}$ del tipo

$$\mathbf{v} = [v_1 \ \dots \ v_{i_+(\mathbf{B})} \ 0 \ \dots \ 0]^T.$$

Per un tale vettore $\mathbf{v}$, il vettore $\mathbf{w} = \mathbf{Sv}$ ha le prime $i_+(\mathbf{A})$ coordinate nulle, perché $\mathbf{S}_0\mathbf{v} = \mathbf{0}$; perciò, posto $\mathbf{w} = [w_1,\dots,w_n]^T$, risulta:

$$(\mathbf{Sv})^H\mathbf{Z_A}\mathbf{Sv} = -\sum_{i_+(\mathbf{A})+1}^{i_+(\mathbf{B})} |w_i|^2 \le 0.$$

D'altra parte si ha:

$$\mathbf{v}^H\mathbf{Z_B}\mathbf{v} = \sum_{1}^{i_+(\mathbf{B})} |v_i|^2 > 0$$

e dall'uguaglianza $(\mathbf{Sv})^H\mathbf{Z_A}\mathbf{Sv} = \mathbf{v}^H\mathbf{S}^H\mathbf{Z_A}\mathbf{Sv} = \mathbf{v}^H\mathbf{Z_B}\mathbf{v}$ si ricava l'assurdo. Nel caso $i_+(\mathbf{A}) = 0$, si scelga un qualunque vettore non nullo $\mathbf{v}$ del tipo $\mathbf{v} = [v_1 \ \dots \ v_{i_+(\mathbf{B})} \ 0 \ \dots \ 0]^T$ e si ragioni come sopra. Pertanto era assurdo supporre che $i_+(\mathbf{A}) < i_+(\mathbf{B})$. In modo analogo si ragiona se si suppone valida la disuguaglianza opposta, quindi si conclude che $i_+(\mathbf{A}) = i_+(\mathbf{B})$. □

Esempio 6.2. Le due matrici hermitiane

$$\mathbf{A} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 4 & 0 & 2 \\ 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 \end{bmatrix}, \quad \mathbf{B} = \begin{bmatrix} 10 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

hanno polinomi caratteristici rispettivamente $p_{\mathbf{A}}(X) = X(X-5)(X^2-X-1)$ e $p_{\mathbf{B}}(X) = X(X+1)(X^2-11X+9)$. Quindi i loro autovalori, sistemati in ordine crescente, sono:

- per **A**: $\lambda_1 = (1-\sqrt{5})/2 < \lambda_2 = 0 < \lambda_3 = (1+\sqrt{5})/2 < \lambda_4 = 5$;
- per **B**: $\mu_1 = -1 < \mu_2 = 0 < \mu_3 = (11-\sqrt{85})/2 < \mu_4 = (11+\sqrt{85})/2$.

La matrice d'inerzia comune ad **A** e **B** è quindi la matrice

$$\mathbf{Z} = \mathbf{Diag}(1, 1, -1, 0).$$

La Legge d'inerzia dice che **A** e **B** sono congrue tra di loro; in effetti risulta $\mathbf{A} = \mathbf{S}_1^H\mathbf{Z}\mathbf{S}_1$ con

$$\mathbf{S}_1 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix}$$

e $\mathbf{B} = \mathbf{S}_2^H\mathbf{Z}\mathbf{S}_2$ con

$$\mathbf{S}_2 = \begin{bmatrix} 3 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 3 \end{bmatrix}.$$

Perciò risulta

$$\mathbf{A} = \mathbf{S}_1^H\mathbf{Z}\mathbf{S}_1 = \mathbf{S}_1^H(\mathbf{S}_2^H)^{-1}\mathbf{B}\mathbf{S}_2^{-1}\mathbf{S}_1 = \mathbf{S}\mathbf{B}\mathbf{S}^H$$

dove si è posto $\mathbf{S} = (\mathbf{S}_2^{-1}\mathbf{S}_1)^H$. □

Date due matrici hermitiane **A** e **B** congrue tra di loro, con rispettivi autovalori (ripetuti con le loro molteplicità) ordinati in modo non decrescente

$$\lambda_1 \le \lambda_2 \le \dots \le \lambda_n, \quad \mu_1 \le \mu_2 \le \dots \le \mu_n,$$

la Legge d'inerzia assicura che λ_k è negativo, nullo o positivo se e solo se tale è μ_k, per ogni $k \le n$. È naturale chiedersi, qualora λ_k e μ_k siano non nulli, se la differenza tra le loro grandezze (uguali nel segno) possa essere arbitrariamente grande, oppure se tale differenza è controllata in qualche modo. A questa domanda risponde il seguente teorema, dovuto a Ostrowski (1959). Esso si deduce senza troppa difficoltà, come ora vedremo, dal Teorema di monotonicità di H. Weyl, e dà una formulazione quantitativa della Legge d'inerzia.

Teorema 6.3 (Ostrowski)**.** *Date due matrici hermitiane* **A** *e* **B** *tra di loro congrue:* $\mathbf{A} = \mathbf{SBS}^H$ *(***S** *matrice invertibile), con rispettivi autovalori* $\lambda_1 \le \lambda_2 \le \cdots \le \lambda_n$, $\mu_1 \le \mu_2 \le \cdots \le \mu_n$*, se* $\mu_k \ne 0$ *risulta*

$$\sigma_1^2 \ge \lambda_k/\mu_k \ge \sigma_n^2$$

dove σ_1 *e* σ_n *sono rispettivamente il massimo e il minimo valore singolare della matrice* **S**.

Dimostrazione. Si osservi preliminarmente che, essendo la matrice **S** invertibile, essa ha n valori singolari positivi i cui quadrati sono gli autovalori della matrice definita positiva $\mathbf{SS}^H$. È inoltre immediato verificare che, se $r \in \mathbb{R}$, gli autovalori di $\mathbf{B} - r\mathbf{I}$ sono $\mu_1 - r \le \mu_2 - r \le \cdots \le \mu_n - r$. Pertanto la matrice $\mathbf{B} - \mu_k\mathbf{I}$ ha come k-esimo autovalore (in ordine non decrescente) $\mu_k - \mu_k = 0$. Essendo $\mathbf{B} - \mu_k\mathbf{I}$ congrua ad $\mathbf{A} - \mu_k\mathbf{SS}^H$, per la Legge d'inerzia pure il k-esimo autovalore di tale matrice è nullo. Il Teorema di H. Weyl sopra ricordato assicura allora che, denotando rispettivamente con α_1 e α_n il massimo e il minimo autovalore della matrice hermitiana $-\mu_k\mathbf{SS}^H$, risulta

$$\lambda_k + \alpha_1 \ge 0 \ge \lambda_k + \alpha_n$$

o equivalentemente

$$-\alpha_n \ge \lambda_k \ge -\alpha_1.$$

Se $\mu_k > 0$, $-\alpha_1$ coincide con il minimo autovalore di $\mu_k\mathbf{SS}^H$, cioè con $\mu_k\sigma_n^2$, mentre $-\alpha_n$ coincide con il massimo autovalore di $\mu_k\mathbf{SS}^H$, cioè con $\mu_k\sigma_1^2$. Si deduce che

$$\mu_k\sigma_1^2 \ge \lambda_k \ge \mu_k\sigma_n^2.$$

Se invece $\mu_k < 0$, si deduce analogamente che

$$\mu_k\sigma_n^2 \ge \lambda_k \ge \mu_k\sigma_1^2.$$

In entrambi i casi si ricava quindi che $\sigma_1^2 \ge \lambda_k/\mu_k \ge \sigma_n^2$. □

Esempio 6.4. Consideriamo le matrici hermitiane

$$\mathbf{A} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 4 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \quad \mathbf{B} = \begin{bmatrix} 10 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}$$

già viste nell'Esempio 5.5, con autovalori sistemati in ordine crescente:

- per $\mathbf{A}$: $\lambda_1 = (1-\sqrt{5})/2 < \lambda_2 = (1+\sqrt{5})/2 < \lambda_3 = 4$;
- per $\mathbf{B}$: $\mu_1 = -1 < \mu_2 = (11-\sqrt{85})/2 < \mu_3 = (11+\sqrt{85})/2$.

La matrice d'inerzia comune ad $\mathbf{A}$ e $\mathbf{B}$ è quindi la matrice

$$\mathbf{Z} = \mathbf{Diag}(1, 1, -1).$$

La Legge d'inerzia dice che $\mathbf{A}$ e $\mathbf{B}$ sono congrue tra di loro; in effetti risulta $\mathbf{A} = \mathbf{S}_1^H \mathbf{Z} \mathbf{S}_1$ con

$$\mathbf{S}_1 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

e $\mathbf{B} = \mathbf{S}_2^H \mathbf{Z} \mathbf{S}_2$ con

$$\mathbf{S}_2 = \begin{bmatrix} 3 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Perciò risulta $\mathbf{A} = \mathbf{S}\mathbf{B}\mathbf{S}^H$ dove $\mathbf{S} = (\mathbf{S}_2^{-1}\mathbf{S}_1)^H$. Un facile calcolo porge:

$$\mathbf{S}_2^{-1} = \begin{bmatrix} 1/3 & 0 & 0 \\ -1/3 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

$$\mathbf{S}^H = \mathbf{S}_2^{-1}\mathbf{S}_1 = \begin{bmatrix} 1/3 & 0 & 1/3 \\ -1/3 & 2 & -1/3 \\ 0 & 0 & 1 \end{bmatrix},$$

$$\mathbf{S} = \begin{bmatrix} 1/3 & -1/3 & 0 \\ 0 & 2 & 0 \\ 1/3 & -1/3 & 1 \end{bmatrix}.$$

Per poter applicare il Teorema 6.3 bisogna calcolare i quadrati del minimo e del massimo valore singolare della matrice $\mathbf{S}$, ovvero, il minimo e il massimo autovalore della matrice hermitiana definita positiva $\mathbf{S}\mathbf{S}^H$. Risulta:

$$\mathbf{S}\mathbf{S}^H = \begin{bmatrix} 2/9 & -2/3 & 2/9 \\ -2/3 & 4 & -2/3 \\ 2/9 & -2/3 & 11/9 \end{bmatrix} = \frac{1}{9}\begin{bmatrix} 2 & -6 & 2 \\ -6 & 36 & -6 \\ 2 & -6 & 11 \end{bmatrix} = \frac{1}{9}\mathbf{C}.$$

Il polinomio caratteristico della matrice $\mathbf{C}$ è $p_{\mathbf{C}}(X) = -X^3 + 49X^2 - 414X + 324$. Dall'andamento del grafico di $p_{\mathbf{C}}(X)$ si vede che tale polinomio ha uno zero tra 0 e 1, un'altro tra 9 e 10 e un terzo zero tra 30 e 40. Corrispondentemente, la matrice $\mathbf{S}\mathbf{S}^H = (1/9)\mathbf{C}$ ha tre autovalori:

$$0 < \sigma_3^2 < \frac{1}{9}, \quad 1 < \sigma_2^2 < \frac{10}{9}, \quad \frac{30}{9} < \sigma_1^2 < \frac{40}{9}.$$

Deve risultare:

$$\sigma_3^2 \le \frac{\lambda_1}{\mu_1} = \frac{\sqrt{5}-1}{2}, \frac{\lambda_2}{\mu_2} = \frac{1+\sqrt{5}}{11-\sqrt{85}}, \frac{\lambda_3}{\mu_3} = \frac{8}{11+\sqrt{85}} \le \sigma_1^2.$$

Questi tre numeri valgono approssimativamente

$$\frac{\lambda_1}{\mu_1} = 0.62, \quad \frac{\lambda_2}{\mu_2} = 1.24, \quad \frac{\lambda_3}{\mu_3} = 0.39$$

che stanno infatti tra $1/9$ e $30/9$, quindi tra σ_1^2 e σ_3^2. □

7. Spettro e diagonale di matrici hermitiane

Il problema di confrontare gli elementi diagonali a_{ii} di una matrice hermitiana $\mathbf{A}$ $n \times n$ con i suoi autovalori $\lambda_1 \leq \cdots \leq \lambda_n$ si pone naturalmente non appena si ricordi che $\sum_{1 \leq i \leq n} a_{ii} = \sum_{1 \leq i \leq n} \lambda_i$ e che, come si deduce dal Principio di inclusione applicato al caso $r = 1$, $\lambda_1 \leq a_{ii} \leq \lambda_n$ per ogni $i \leq n$.

Denoteremo, per comodità, con $\mathbf{d}(\mathbf{A}) = [a_{11}\ a_{22}\ \ldots\ a_{nn}]^T$ il "vettore diagonale" di $\mathbf{A}$, e con $\mathbf{l}(\mathbf{A}) = [\lambda_1\ \lambda_2\ \ldots\ \lambda_n]^T$ il "vettore spettro" di $\mathbf{A}$. Non è restrittivo supporre che gli elementi diagonali siano in ordine crescente, cioè:

$$a_{11} \leq a_{22} \leq \ldots \leq a_{nn};$$

infatti, se gli elementi diagonali di $\mathbf{A}$ non soddisfano a tali disuguaglianze, si può eseguire una cogredienza su $\mathbf{A}$ in modo che gli elementi sulla diagonale della matrice ottenuta siano in ordine crescente; una cogredienza è una similitudine e quindi gli autovalori della nuova matrice coincidono con quelli di $\mathbf{A}$. D'ora in avanti supporremo sempre $a_{11} \leq a_{22} \leq \ldots \leq a_{nn}$.

Osserviamo che per una matrice 2×2 risulta:

$$a_{11} \geq \lambda_1, \quad a_{22} \leq \lambda_2, \quad a_{11} + a_{22} = \lambda_1 + \lambda_2.$$

Generalizzando tali relazioni, definiamo un opportuno pre-ordine in $\mathbb{R}^n$ nel modo seguente: dati due vettori $\mathbf{x} = [x_1\ x_2\ \ldots\ x_n]^T$, $\mathbf{y} = [y_1\ y_2\ \ldots\ y_n]^T \in \mathbb{R}^n$, poniamo

$$\mathbf{x} \succeq \mathbf{y}$$

se, supponendo di avere

$$x_{i_1} \leq x_{i_2} \leq \cdots \leq x_{i_n}, \quad y_{j_1} \leq y_{j_2} \leq \cdots \leq y_{j_n}$$

risulta

$$\begin{gathered} x_{i_1} \geq y_{j_1}, \\ x_{i_1} + x_{i_2} \geq y_{j_1} + y_{j_2} \\ \ldots x_{i_1} + x_{i_2} + \cdots + x_{i_{n-1}} \geq y_{j_1} + y_{j_2} + \cdots + y_{j_{n-1}} \\ x_{i_1} + x_{i_2} + \cdots + x_{i_n} = y_{j_1} + y_{j_2} + \cdots + y_{j_n}. \end{gathered}$$

Naturalmente le disuguaglianze precedenti assumono una veste più semplice se si suppone che le coordinate dei due vettori siano in ordine crescente.

La relazione $\mathbf{x} \geq \mathbf{y}$ in $\mathbb{R}^n$ è riflessiva e transitiva, ma non è anti-simmetrica, quindi dà luogo a un pre-ordine. Se in $\mathbb{R}^n$ si passa al quoziente modulo la relazione di equivalenza che raggruppa in una medesima classe vettori le cui coordinate cambiano solo per l'ordine (cioè, dato $\mathbf{x} \in \mathbb{R}^n$, $[\mathbf{x}] = \{\mathbf{Px} \mid \mathbf{P}$ matrice di permutazione$\}$), allora la relazione $\geq$ dà luogo a una relazione di ordine parziale sull'insieme quoziente.

Il pre-ordine appena definito, che appare a prima vista alquanto artificioso, è di fatto la relazione giusta in $\mathbb{R}^n$ per risolvere il problema del confronto tra diagonale e spettro di una matrice hermitiana, come mostra il seguente risultato.

Teorema 7.1 (Schur, 1923). *Per ogni matrice hermitiana* $\mathbf{A}$ *risulta:* $\mathbf{d}(\mathbf{A}) \geq \mathbf{l}(\mathbf{A})$.

Dimostrazione. Facciamo induzione sull'ordine n di $\mathbf{A}$, il caso $n = 1$ essendo banale. Sia quindi $n > 1$ e decomponiamo $\mathbf{A}$ in forma bordata:

$$\mathbf{A} = \begin{bmatrix} \mathbf{A}_{n-1} & \mathbf{x} \\ \mathbf{x}^H & a_{nn} \end{bmatrix}.$$

Per l'ipotesi induttiva, detti $\mu_1 \leq \mu_2 \leq \cdots \leq \mu_{n-1}$ gli autovalori di $\mathbf{A}_{n-1}$, si ha:

$$\begin{aligned} \mu_1 &\leq a_{11}, \\ \mu_1 + \mu_2 &\leq a_{11} + a_{22}, \\ \mu_1 + \mu_2 + \dots \mu_{n-1} &= a_{11} + a_{22} + \dots + a_{n-1}. \end{aligned}$$

Per il Teorema dell'intreccio, risulta $\lambda_1 \leq \mu_1 \leq \lambda_2 \leq \cdots \leq \mu_{n-1} \leq \lambda_n$, da cui la conclusione segue facilmente. □

Osservazione 7.2. Le disuguaglianze che definiscono la relazione $\mathbf{x} \geq \mathbf{y}$ sono equivalenti, in virtù del fatto che l'ultima è un'uguaglianza, alle disuguaglianze:

$$\begin{gathered} x_{i_n} \leq y_{j_n}, \\ x_{i_n} + x_{i_{n-1}} \leq y_{j_n} + y_{j_{n-1}}, \\ \dots \\ x_{i_n} + x_{i_{n-1}} + \cdots + x_{i_2} \leq y_{j_n} + y_{j_{n-1}} + \cdots + y_{j_2} \end{gathered}$$

oltre naturalmente a

$$x_{i_1} + x_{i_2} + \cdots + x_{i_n} = y_{j_1} + y_{j_2} + \cdots + y_{j_n}.$$

Si potrebbe quindi a buon motivo denotare la relazione $\mathbf{x} \geq \mathbf{y}$ con il simbolo opposto $\mathbf{x} \preceq \mathbf{y}$. In effetti, molti autori privilegiano questa seconda notazione. C'è però una ragione che induce a preferire la prima notazione, come abbiamo fatto noi; essa deriva dalla prima delle due seguenti disuguaglianze di Hadamard.

Disuguaglianze di Hadamard 7.3. (i) *Data una matrice hermitiana* $n \times n$ *semi-definita positiva* $\mathbf{A} = [a_{ij}]$, *risulta:* $\det(\mathbf{A}) \leq \prod_{i \leq n} a_{ii}$.

(ii) *Data una matrice* $n \times n$ $\mathbf{B}$, *risulta:* $|\det(\mathbf{B})|^2 \leq \prod_{j \leq n} \sum_{i \leq n} |b_{ij}|^2$.

Dimostrazione. (1) Per induzione su n, il caso $n = 1$ essendo banale. Sia $n > 1$ e decomponiamo $\mathbf{A}$ in forma bordata:

$$\mathbf{A} = \begin{bmatrix} \mathbf{A}_{n-1} & \mathbf{x} \\ \mathbf{x}^H & a_{nn} \end{bmatrix}.$$

Se $\mathbf{A}$ non è invertibile, l'asserto è banale, perciò supponiamo che $\det(\mathbf{A}) > 0$. Poiché $\mathbf{A}_{n-1}$ è definita positiva, per l'ipotesi induttiva risulta $\det(\mathbf{A}_{n-1}) \le \prod_{i \le n-1} a_{ii}$. D'altra parte la formula del determinante a blocchi dice che

$$\det(\mathbf{A}) = \det(\mathbf{A}_{n-1})(a_{nn} - \mathbf{x}^H \mathbf{A}_{n-1}^{-1} \mathbf{x})$$

da cui si deduce la conclusione non appena si osservi che $a_{nn} - \mathbf{x}^H \mathbf{A}_{n-1}^{-1} \mathbf{x} \le a_{nn}$ perché $\mathbf{x}^H \mathbf{A}_{n-1}^{-1} \mathbf{x} \ge 0$, essendo $\mathbf{A}_{n-1}^{-1}$ pure definita positiva.

(2) Basta porre $\mathbf{A} = \mathbf{B}^H \mathbf{B}$ e applicare la disuguaglianza in (1). □

La seconda disuguaglianza di Hadamard ha la seguente interpretazione geometrica: il volume del parallelepipedo n-dimensionale costruito con i vettori colonna della matrice $\mathbf{B}$ (che, come è ben noto, è rappresentato dal modulo del determinante di $\mathbf{B}$) è minore o al più uguale al volume del parallelepipedo n-dimensionale rettangolo avente come spigoli segmenti di lunghezza pari ai vettori colonna di $\mathbf{B}$.

Al Teorema 7.2 di Schur si affianca un teorema di esistenza: dati due vettori di $\mathbb{R}^n$ soddisfacenti alla relazione $\mathbf{x} \succeq \mathbf{y}$, esiste una matrice hermitiana $n \times n$ che ha il primo come vettore diagonale e il secondo come vettore spettro. Tale teorema venne provato da Horn, e si basa sul seguente risultato puramente combinatorio di cui non daremo la dimostrazione (per la quale rimandiamo a Horn-Johnson, "Matrix Analysis", Cambridge Univ. Press, Cambridge 1985, Lemma 4.3.28, pp. 194–196).

Lemma 7.4. *Dati due vettori* $\mathbf{d} = [d_1\ d_2\ \dots\ d_n]^T \succeq \mathbf{l} = [\lambda_1\ \lambda_2\ \dots\ \lambda_n]^T$ *in* $\mathbb{R}^n$, *con* $d_1 \le d_2 \le \dots \le d_n$ *e* $\lambda_1 \le \lambda_2 \le \dots \le \lambda_n$, *esiste un vettore* $\mathbf{m} = [\mu_1\ \mu_2\ \dots\ \mu_{n-1}]^T \in \mathbb{R}^{n-1}$ *tale che* $\lambda_1 \le \mu_1 \le \lambda_2 \le \mu_2 \le \cdots \le \mu_{n-1} \le \lambda_n$ *e* $\mathbf{d}' \succeq \mathbf{m}$, *dove* $\mathbf{d}'$ *è il vettore ottenuto da* $\mathbf{d}$ *sopprimendo l'ultima coordinata.* □

Teorema 7.5 (Horn)**.** *Dati due vettori* $\mathbf{d} \succeq \mathbf{l}$ *in* $\mathbb{R}^n$, *esiste una matrice reale simmetrica* $\mathbf{A}$ *di ordine n tale che* $\mathbf{d}(\mathbf{A}) = \mathbf{d}$ *e* $\mathbf{l}(\mathbf{A}) = \mathbf{l}$.

Il Teorema di Horn si ricava facilmente una volta che sia stato provato il seguente risultato, una cui traccia di dimostrazione è fornita negli esercizi 6.47–6.49.

Teorema inverso dell'intreccio 7.6. *Dati una matrice reale simmetrica* $\mathbf{A}'$ *di ordine* $n-1$ *con autovalori* $\mu_1 \le \mu_2 \le \cdots \le \mu_{n-1}$ *e un vettore* $\mathbf{l} = [\lambda_1\ \lambda_2\ \dots\ \lambda_n]^T \in \mathbb{R}^n$ *soddisfacente alle disuguaglianze*

$$\lambda_1 \le \mu_1 \le \lambda_2 \le \mu_2 \le \cdots \le \mu_{n-1} \le \lambda_n,$$

esistono uno scalare $a \in \mathbb{R}$ *e un vettore* $\mathbf{b} \in \mathbb{R}^{n-1}$ *tali che la matrice*

$$\mathbf{A} = \begin{bmatrix} a & \mathbf{b}^T \\ \mathbf{b} & \mathbf{A}' \end{bmatrix}$$

ha autovalori $\lambda_1 \le \lambda_2 \le \cdots \le \lambda_n$.

Dimostrazione del Teorema 7.5. Per il Lemma 7.4, esiste $\mathbf{m} = [\mu_1\ \mu_2\ \dots\ \mu_{n-1}]^T \in \mathbb{R}^{n-1}$ tale che $\lambda_1 \le \mu_1 \le \cdots \le \mu_{n-1} \le \lambda_n$ e $\mathbf{d}' \ge \mathbf{m}$. Per l'ipotesi induttiva, esiste una matrice hermitiana $\mathbf{A}'$ di ordine $n-1$ tale che $\mathbf{l}(\mathbf{A}') = \mathbf{m}$ e $\mathbf{d}(\mathbf{A}') = \mathbf{d}'$. Poiché sono soddisfatte le disuguaglianze $\lambda_1 \le \mu_1 \le \cdots \le \mu_{n-1} \le \lambda_n$, il Teorema 7.6 assicura l'esistenza di una matrice reale simmetrica

$$\mathbf{A} = \begin{bmatrix} a & \mathbf{b}^T \\ \mathbf{b} & \mathbf{A}' \end{bmatrix}$$

con $\mathbf{l}(\mathbf{A}) = \mathbf{l}$. Resta da provare che $\mathbf{d}(\mathbf{A}) = \mathbf{d}$. Poiché $\mathbf{d}(\mathbf{A}') = \mathbf{d}'$, basta provare che $a = d_n$; ma $\mathrm{Tr}(\mathbf{A}) = a + d_1 + \cdots + d_{n-1} = \lambda_1 + \cdots + \lambda_n = d_1 + \cdots + d_{n-1} + d_n$ (l'ultima uguaglianza segue dall'ipotesi $\mathbf{d} \ge \mathbf{l}$), per cui $a = d_n$, come desiderato. □

Controlliamo il Teorema di Horn nel semplice caso 2×2 in ambiente reale.

Esempio 7.7. Dato il vettore $\mathbf{v} = [a\ b]^T \in \mathbb{R}^2$ (supponiamo $a \le b$), è facile vedere che un vettore $\mathbf{u} = [u_1\ u_2]^T$ soddisfa alla disuguaglianza $\mathbf{u} \preceq \mathbf{v}$ se e solo se rappresenta un punto della retta di equazione $y = -x + a + b$ con ascissa non interna al segmento di estremi a e b. Il Teorema 7.5 assicura che esiste una matrice reale simmetrica 2×2

$$\mathbf{A} = \begin{bmatrix} a & z \\ z & b \end{bmatrix}$$

che ha come autovalori $\lambda_1 = u_1$, $\lambda_2 = u_2$ se $u_1 \le u_2$ (oppure $\lambda_1 = u_2$, $\lambda_2 = u_1$ se $u_2 \le u_1$). Ciò si può vedere direttamente. Infatti gli autovalori di $\mathbf{A}$ sono:

$$\lambda_1 = (a + b - \sqrt{\Delta})/2, \qquad \lambda_2 = (a + b + \sqrt{\Delta})/2$$

dove $\Delta = (a-b)^2 + 4z^2$; tenuto conto che $\lambda_1 + \lambda_2 = a + b$, esiste $z \in \mathbb{R}$ soddisfacente a queste eguaglianze se e solo se $4z^2 = (\lambda_1 - \lambda_2)^2 - (a-b)^2$; ovviamente ciò accade se e solo se $\lambda_2 - \lambda_1 \ge b - a$, equivalentemente, se $\lambda_2 - \lambda_1 + \lambda_1 + \lambda_2 \ge b - a + a + b$, cioè se $\lambda_2 \ge b$, il che vale sempre se $\mathbf{u} \preceq \mathbf{v}$. □

8. Matrici bistocastiche

Il pre-ordine definito in $\mathbb{R}^n$ nel Paragrafo precedente, che fornisce la relazione intercorrente tra diagonale e spettro di una matrice hermitiana, ha una notevole caratterizzazione tramite le matrici bistocastiche.

Ricordiamo che una matrice quadrata a coefficienti reali non negativi si dice *stocastica per colonne* se ogni colonna ha somma 1; si dice *stocastica!per righe* se ogni riga ha somma 1; si dice infine *bistocastica* se è stocastica sia per colonne che per righe.

Forniamo alcuni esempi di matrici bistocastiche.

Esempi 8.1. (1) Ogni matrice di permutazione è una matrice bistocastica.

(2) Fissato $n \ge 1$, la matrice $n \times n$ con tutti i coefficienti uguali a $1/n$ è una matrice bistocastica. Si lascia provare al lettore come esercizio che essa può essere scritta come somma di n matrici di permutazione moltiplicate ciascuna per $1/n$.

(3) Una combinazione convessa di matrici bistocastiche $n \times n$ è una matrice bistocastica. Si consideri infatti $\mathbf{S} = \sum_{h \le r} \alpha_h \mathbf{S}_h$, dove $\mathbf{S}_h$ è matrice bistocastica per ogni $h \le r$ e gli α_h sono numeri reali non negativi tali che $\sum_{h \le r} \alpha_h = 1$. Se $\mathbf{S} = [s_{ij}]$ e $\mathbf{S}_h = [s_{ij}^{(h)}]$, la somma della prima riga di $\mathbf{S}$ risulta:

$$\sum_{1 \le j \le n} s_{1j} = \sum_{1 \le j \le n} \Big(\sum_{h \le r} \alpha_h s_{1j}^{(h)} \Big) = \sum_{h \le r} \alpha_h \Big(\sum_{1 \le j \le n} s_{1j}^{(h)} \Big) = \sum_{h \le r} \alpha_h = 1.$$

Analogo conto vale per le altre righe e colonne.

(4) Data una matrice unitaria $\mathbf{U} = [\mathbf{u}_j]$ $(1 \le j \le n)$, si chiama matrice *ortostocastica* generata da $\mathbf{U}$ la matrice $\mathbf{S}(\mathbf{U}) = [s_{ij}]$ definita ponendo: $s_{ij} = |u_{ij}|^2$. È immediato verificare che una tale matrice è bistocastica. □

I precedenti esempi (1) e (3) permettono di dire che ogni combinazione convessa di matrici di permutazione dà luogo a una matrice bistocastica. Scopo principale di questo Paragrafo è dimostrare il celebre risultato dovuto a G. Birkhoff nel 1946, il quale afferma che ogni matrice bistocastica è di questo tipo.

Partiamo allora dalla caratterizzazione del pre-ordine in $\mathbb{R}^n$ tramite matrici bistocastiche cui abbiamo prima accennato.

Teorema 8.2. *Dati due vettori* $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$, *risulta* $\mathbf{x} \succeq \mathbf{y}$ *se e solo se esiste una matrice bistocastica* $\mathbf{S}$ *tale che* $\mathbf{x} = \mathbf{S}\mathbf{y}$.

Dimostrazione. Necessità. Per il Teorema 7.5 esiste una matrice simmetrica reale $\mathbf{A}$ tale che $\mathbf{d}(\mathbf{A}) = \mathbf{x}$ e $\mathbf{l}(\mathbf{A}) = \mathbf{y}$. Per il Teorema spettrale si ha una diagonalizzazione unitaria: $\mathbf{A} = \mathbf{U}\boldsymbol{\Lambda}\mathbf{U}^H$, dove i coefficienti sulla diagonale di $\boldsymbol{\Lambda}$ formano il vettore $\mathbf{l}(\mathbf{A})$. Sia $\mathbf{S}(\mathbf{U})$ la matrice ortostocastica generata da $\mathbf{U}$. Un facile calcolo mostra che

$$\mathbf{x} = \mathbf{d}(\mathbf{A}) = \mathbf{S}(\mathbf{U})\mathbf{l}(\mathbf{A}) = \mathbf{S}(\mathbf{U})\mathbf{y}$$

da cui l'asserto.

Sufficienza. Sia $\mathbf{x} = \mathbf{S}\mathbf{y}$ con $\mathbf{S} = [s_{ij}]$ matrice bistocastica. Mostriamo innanzi tutto che non è restrittivo supporre che

$$x_1 \le x_2 \le \cdots \le x_n, \quad y_1 \le y_2 \le \cdots \le y_n.$$

Se così non fosse, si pre-moltiplichino $\mathbf{x}$ per una matrice di permutazione $\mathbf{P}$ e $\mathbf{y}$ per una matrice di permutazione $\mathbf{P}_1$ in modo che $\mathbf{P}\mathbf{x}$ e $\mathbf{P}_1\mathbf{y}$ abbiano le coordinate soddisfacenti a tali disuguaglianze. Poiché

$$\mathbf{x} = \mathbf{S}\mathbf{y} \iff \mathbf{P}\mathbf{x} = \mathbf{P}\mathbf{S}\mathbf{P}_1^T\mathbf{P}_1\mathbf{y} = \mathbf{S}_1\mathbf{P}_1\mathbf{y}$$

dove $\mathbf{S}_1 = \mathbf{P}\mathbf{S}\mathbf{P}_1^T$ è ancora evidentemente bistocastica, e poiché $\mathbf{x} \succeq \mathbf{y}$ se e solo se $\mathbf{P}\mathbf{x} \succeq \mathbf{P}_1\mathbf{y}$, si deduce quanto volevamo mostrare.

Per ogni $k \le n$ e per ogni indice di colonna j, consideriamo la j-esima somma di colonna "troncata a k":

$$\sigma_j^{(k)} = \sum_{1 \le i \le k} s_{ij}.$$

Ovviamente $\sigma_j^{(n)} = 1$ per ogni j.

Dobbiamo provare che per ogni $k \le n$ vale: $\sum_{1\le i\le k} x_i - \sum_{1\le i\le k} y_i \ge 0$. Si ha infatti:

$$\begin{aligned}\sum_{1\le i\le k} x_i - \sum_{1\le i\le k} y_i &= \sum_{1\le i\le k}\Big(\sum_{1\le j\le n} s_{ij}y_j\Big) - \sum_{1\le i\le k} y_i\\ &= \sum_{1\le j\le n}\Big(\sum_{1\le i\le k} s_{ij}\Big)y_j - \sum_{1\le i\le k} y_i\\ &= \sum_{1\le j\le n}\sigma_j^{(k)}y_j - \sum_{1\le i\le k} y_i.\end{aligned}$$

Poiché $\sum_{1\le j\le n}\sigma_j^{(k)} = k$, trattandosi della somma di tutte le colonne troncate a k e avendo ogni riga somma 1, la precedente serie di uguaglianze continua così:

$$\begin{aligned}&= \sum_{1\le j\le n}\sigma_j^{(k)}y_j - \sum_{1\le i\le k} y_i + \Big(k - \sum_{1\le j\le n}\sigma_j^{(k)}\Big)y_k\\ &= \sum_{1\le j\le k}\sigma_j^{(k)}y_j + \sum_{k+1\le j\le n}\sigma_j^{(k)}y_j - \sum_{1\le j\le k} y_j\\ &\qquad + \sum_{1\le j\le k} 1\cdot y_k - \sum_{1\le j\le k}\sigma_j^{(k)}y_k - \sum_{k+1\le j\le n}\sigma_j^{(k)}y_k\\ &= \sum_{1\le j\le k}(1-\sigma_j^{(k)})(y_k - y_j) + \sum_{k+1\le j\le n}\sigma_j^{(k)}(y_j - y_k).\end{aligned}$$

Nell'ultima espressione tutti gli addendi sono non negativi, come desiderato. Resta da provare che $\sum_{1\le i\le n} x_i = \sum_{1\le i\le n} y_i$, il che si deduce da:

$$\sum_{1\le i\le n} x_i = \sum_{1\le i\le n}\Big(\sum_{1\le j\le n} s_{ij}y_j\Big) = \sum_{1\le j\le n}\sigma_j^{(n)}y_j = \sum_{1\le j\le n} y_j. \qquad \square$$

La dimostrazione originale della necessità nel Teorema 8.2, fornita da Hardy, Littlewood e Polya nel 1939, non faceva uso del Teorema 7.5 di Horn, che non era stato ancora dimostrato, ma di puri argomenti combinatori (si veda Minc, "Nonnegative matrices", Wiley, New York 1988, pp. 112–114).

Rivolgiamo ora la nostra attenzione al Teorema di Birkhoff; esso asserisce che i mattoni fondamentali con cui costruire tramite combinazioni convesse tutte le matrici bistocastiche sono le matrici di permutazione. Tali matrici sono caratterizzate dalla proprietà di avere tutti i coefficienti nulli tranne un "serpente" di coefficienti uguali a 1. Chiamiamo *serpente* di una matrice $n \times n$ $\mathbf{A}$ una n-pla di suoi coefficienti $a_{1\sigma_1}, a_{2\sigma_2}, \ldots, a_{n\sigma_n}$, dove $(\sigma_1, \sigma_2, \ldots, \sigma_n)$ è una permutazione di $(1, 2, \ldots, n)$. Il punto di partenza nella dimostrazione del Teorema di Birkhoff è il fatto che una matrice bistocastica ha un serpente positivo, cosa che si deduce facilmente dal seguente risultato, di cui l'Esempio 5 dell'Appendice B fornisce una versione puramente combinatoria.

Lemma 8.3 (Frobenius-König)**.** *Condizione necessaria e sufficiente affinché ogni serpente di una matrice $n \times n$ $\mathbf{A}$ contenga un coefficiente nullo è che $\mathbf{A}$ abbia una sottomatrice nulla $s \times t$, con $s + t = n + 1$.*

Dimostrazione. Si osservi innanzi tutto che permutando le righe di $\mathbf{A}$, oppure le colonne, sia la condizione necessaria che quella sufficiente continuano a valere.

Sufficienza. Per quanto appena osservato possiamo supporre che la sottomatrice nulla sia formata dalla intersezione delle prime s righe e delle prime t colonne. Un serpente senza coefficienti nulli ha tutti i t coefficienti delle prime t colonne nelle ultime $n-s$ righe; ma $n-s=t-1$, per cui un tale serpente non esiste.

Necessità. Ragioniamo per induzione su n, il caso $n=1$ essendo banale. Sia allora $n>1$ e supponiamo $\mathbf{A}\neq\mathbb{O}$, altrimenti l'asserto è ovvio; $\mathbf{A}$ ha quindi un coefficiente non nullo. Eseguendo permutazioni sulle righe e sulle colonne, non è restrittivo supporre che tale coefficiente sia a_{nn}. La sottomatrice principale $\mathbf{A}_{n-1}$ gode ancora della proprietà che ogni suo serpente contiene un coefficiente nullo, quindi per l'ipotesi induttiva $\mathbf{A}_{n-1}$ contiene una sottomatrice nulla $p\times q$, con $p+q=n$. Permutando ancora righe e colonne di $\mathbf{A}$ possiamo ottenere una matrice $\mathbf{A}'=\mathbf{PAP}'$ ($\mathbf{P}$ e $\mathbf{P}'$ matrici di permutazione) che ha come sottomatrice nulla l'intersezione delle prime p righe e delle ultime $q=n-p$ colonne di $\mathbf{A}'$. Si ha quindi una decomposizione a blocchi

$$\mathbf{A}'=\begin{bmatrix}\mathbf{X} & \mathbb{O}\\ \mathbf{Y} & \mathbf{Z}\end{bmatrix}$$

dove $\mathbf{X}$ è $p\times p$ e $\mathbf{Z}$ è $q\times q$. Applichiamo una seconda volta l'ipotesi induttiva: poiché uno dei due blocchi quadrati diagonali deve godere ancora della proprietà che ogni serpente contiene un coefficiente nullo, tale blocco (sia esso $\mathbf{X}$, ma analogamente si ragionerebbe se fosse $\mathbf{Z}$) contiene una sottomatrice nulla di dimensioni $h\times k$ con $h+k=p+1$. Con ulteriori permutazioni delle righe e delle colonne di $\mathbf{A}'$ si ottiene una matrice $\mathbf{A}''$ che ha una sottomatrice nulla nell'intersezione delle prime h righe e delle ultime $k+q$ colonne. Poiché $h+k+q=p+1+q=n+1$, si ha la conclusione per la matrice $\mathbf{A}''$ e quindi per $\mathbf{A}$. □

Corollario 8.4. *Ogni matrice bistocastica* $\mathbf{S}$ *ha un serpente di coefficienti tutti positivi.*

Dimostrazione. Se per assurdo ogni serpente di $\mathbf{S}$ contenesse un coefficiente nullo, dal Lemma 8.3 ricaveremmo una sottomatrice nulla $\mathbf{B}$ di $\mathbf{S}$ di dimensioni $s\times t$, con $s+t=n+1$. La somma di tutti i coefficienti di $\mathbf{S}$ situati sulle s righe e sulle t colonne le cui intersezioni formano $\mathbf{B}$ vale $s+t$, perché sulle loro intersezioni c'è sempre 0; ma $s+t=n+1$, il che produce un assurdo, perché la somma di tutti i coefficienti di $\mathbf{S}$ vale n. □

Siamo ora in grado di provare il risultato del 1946 di Birkhoff ("Tres observaciones sobre el álgebra lineal", Rev. Univ. Nac. Tucumán, ser. A, vol. 5, pp. 147–151), la cui dimostrazione è costruttiva, nel senso che produce un procedimento per ricavare le matrici di permutazione che compongono tramite combinazione convessa la matrice bistocastica considerata.

Teorema 8.5 (Birkhoff)**.** *Ogni matrice bistocastica è combinazione convessa di matrici di permutazione.*

Dimostrazione. Sia **S** matrice bistocastica $n \times n$. Sia k il numero dei suoi coeffcienti non nulli. Ovviamente $k \ge n$ e $k = n$ esattamente se **S** è matrice di permutazione. Facciamo pertanto induzione su k, partendo da $k = n$, e supponiamo $k > n$. Per il Corollario 8.4, **S** ha un serpente positivo, i cui coefficienti non possono coincidere tutti con 1, altrimenti sarebbe $k = n$. Sia a il valore minimo dei coefficienti del serpente; risulta $0 < a < 1$. Sia **P** la matrice di permutazione associata a tale serpente. Consideriamo la matrice

$$\mathbf{T} = \frac{1}{1-a}(\mathbf{S} - a\mathbf{P}).$$

Allora $\mathbf{T} = [t_{ij}]$ è bistocastica, giacché per ogni indice di riga i risulta

$$\sum_{1 \le j \le n} t_{ij} = \frac{1}{1-a}\Big(\sum_{1 \le j \le n} s_{ij}\Big) - \frac{a}{1-a} = \frac{1}{1-a} - \frac{a}{1-a} = 1$$

e analogamente per le colonne. Dunque **T** ha un numero di elementi positivi minore di **S**, quindi per l'ipotesi induttiva risulta

$$\mathbf{T} = \alpha_1\mathbf{P}_1 + \cdots + \alpha_r\mathbf{P}_r, \qquad \alpha_i > 0, \quad \sum_{i \le r} \alpha_i = 1.$$

Ma allora si ha:

$$\mathbf{S} = (1-a)\mathbf{T} + a\mathbf{P} = \sum_{i \le r} (1-a)\alpha_i\mathbf{P}_i + a\mathbf{P}$$

da cui si ha la conclusione, una volta osservato che $\sum_{i \le r}(1-a)\alpha_i + a = (1-a)\sum_{i \le r}\alpha_i + a = 1 - a + a = 1$. □

Applichiamo a un esempio molto semplice il procedimento usato nella dimostrazione del Teorema 8.5.

Esempio 8.6. Si consideri la matrice bistocastica

$$\mathbf{S} = \begin{bmatrix} 0 & 1/2 & 1/2 \\ 1/4 & 1/2 & 1/4 \\ 3/4 & 0 & 1/4 \end{bmatrix}.$$

Scegliamo come serpente positivo quello formato dai tre coefficienti di posto $(1,2)$, $(2,3)$ e $(3,1)$ e sia $\mathbf{P}_1$ la matrice di permutazione associata. Il minimo tra i tre coefficienti di **S** in questi tre posti è $a = 1/4$. Nella matrice bistocastica

$$\mathbf{T} = \frac{1}{1-a}(\mathbf{S} - a\mathbf{P}_1) = \begin{bmatrix} 0 & 1/3 & 2/3 \\ 1/3 & 2/3 & 0 \\ 2/3 & 0 & 1/3 \end{bmatrix}$$

scegliamo come serpente positivo quello formato dai tre coefficienti di posto $(1,2)$, $(2,1)$ e $(3,3)$ e sia $\mathbf{P}_2$ la matrice di permutazione associata. Ora il minimo tra i tre coefficienti di **T** in questi tre posti è $b = 1/3$. Un facile calcolo mostra che

$$\frac{1}{1-b}(\mathbf{T} - b\mathbf{P}_2) = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} = \mathbf{P}_3.$$

Si ricava pertanto:

$$\mathbf{S} = \frac{3}{4}\mathbf{T} + \frac{1}{4}\mathbf{P}_1 = \frac{3}{4}\left(\frac{2}{3}\mathbf{P}_3 + \frac{1}{3}\mathbf{P}_2\right) + \frac{1}{4}\mathbf{P}_1 = \frac{1}{2}\mathbf{P}_3 + \frac{1}{4}\mathbf{P}_2 + \frac{1}{4}\mathbf{P}_1. \qquad \square$$

Le matrici di permutazione di ordine n sono $n!$. C'è allora da chiedersi: quante di tali matrici occorrono per scrivere una generica matrice bistocastica come loro combinazione convessa? Usando il procedimento illustrato nella dimostrazione del Teorema 8.5, partendo da una matrice bistocastica $n \times n$ $\mathbf{S}$ con tutti i coefficienti positivi, occorrono $n^2 - n$ passaggi in cui ogni volta si "scorpora" una matrice di permutazione, per giungere a una matrice di permutazione finale, ottenendo $\mathbf{S}$ come combinazione convessa di $n^2 - n + 1$ matrici di permutazione. Di fatto ne bastano $n-1$ di meno, cioè $n^2 - 2n + 2$. Per dimostrarlo ci occorre il seguente risultato di Analisi convessa (per una traccia della dimostrazione si vedano gli Esercizi).

Teorema 8.7. *Siano $\mathbf{v}_1, \ldots, \mathbf{v}_r$ vettori di uno spazio vettoriale reale di dimensione k. Ogni combinazione convessa degli r vettori $\mathbf{v}_i$ è pure combinazione convessa di al più $k+1$ di tali vettori.* □

Possiamo ora stabilire il risultato annunciato.

Proposizione 8.8. *Una matrice bistocastica $\mathbf{S}$ di ordine n è combinazione convessa di al più $n^2 - 2n + 2$ matrici di permutazione.*

Dimostrazione. Per il Teorema 8.5 si ha che $\mathbf{S} = \sum_{i \le r} \alpha_i \mathbf{P}_i$, dove le matrici $\mathbf{P}_i$ sono di permutazione e la combinazione è convessa. Passando alle sottomatrici principali $(n-1)$-esime, si ricava che $\mathbf{S}_{n-1} = \sum_{i \le r} \alpha_i (\mathbf{P}_i)_{n-1}$. Ma tali sottomatrici principali appartengono a uno spazio vettoriale di dimensione $k = (n-1)^2$; dal Teorema 8.7 si deduce che esistono al più $k + 1 = n^2 - 2n + 2$ matrici $(\mathbf{P}_i)_{n-1}$ di cui $\mathbf{S}_{n-1}$ è combinazione convessa. Non è restrittivo supporre che $\mathbf{S}_{n-1} = \sum_{i \le k+1} \beta_i (\mathbf{P}_i)_{n-1}$ (combinazione convessa). Proviamo che allora risulta $\mathbf{S} = \sum_{i \le k+1} \beta_i \mathbf{P}_i$. Per il generico elemento s_{hn} dell'ultima colonna di $\mathbf{S}$, con $h < n$, detto $p_{hn}^{(i)}$ l'analogo elemento di $\mathbf{P}_i$, risulta:

$$\begin{aligned} s_{hn} &= 1 - \sum_{1 \le j \le n-1} s_{hj} = 1 - \sum_{1 \le j \le n-1} \Big(\sum_{i \le k+1} \beta_i p_{hj}^{(i)} \Big) \\ &= 1 - \sum_{i \le k+1} \Big(\sum_{1 \le j \le n-1} p_{hj}^{(i)} \Big) \beta_i = 1 - \sum_{i \le k+1} (1 - p_{hn}^{(i)}) \beta_i \\ &= 1 - \sum_{i \le k+1} \beta_i + \sum_{i \le k+1} p_{hn}^{(i)} \beta_i = \sum_{i \le k+1} \beta_i p_{hn}^{(i)}. \end{aligned}$$

Analogamente per il generico elemento dell'ultima riga di $\mathbf{S}$; perciò risulta, come voluto, $\mathbf{S} = \sum_{i \le k+1} \beta_i \mathbf{P}_i$. □

Esercizi

Paragrafo 1

6.1. Dimostrare direttamente nel Teorema 1.1 che (vi) implica (ii), considerando i prodotti interni dei diversi vettori $\mathbf{e}_i$.

6.2. Sia $\mathbf{v} \in \mathbb{R}^2$ e $\mathbf{R}_\alpha$ una matrice di rotazione. Provare che il vettore $\mathbf{R}_\alpha \mathbf{v}$ si ottiene da $\mathbf{v}$ ruotandolo di α radianti in senso anti-orario.

6.3. Si provi che una matrice di rotazione $\mathbf{R}_\alpha$ si realizza come prodotto di due opportune matrici di Householder: $\mathbf{R}_\alpha = \mathbf{H}_\mathbf{u}\mathbf{H}_\mathbf{v}$, dove $\mathbf{u} = \mathbf{e}_2 - \mathbf{r}$, $\mathbf{v} = \mathbf{e}_1 - \mathbf{e}_2$ ed $\mathbf{r}$ è la prima colonna di $\mathbf{R}_\alpha$. Darne una interpretazione geometrica.

6.4. Si verifichi che, se $\mathbf{u} \neq \mathbf{v} \in \mathbb{C}^n$ e se $\mathbf{u}^H\mathbf{v} \in \mathbb{R}$, posto $\mathbf{w} = (\mathbf{u}-\mathbf{v})/\|\mathbf{u}-\mathbf{v}\|_2$ risulta $\mathbf{H}_\mathbf{w}\mathbf{u} = \mathbf{v}$.

6.5. Si provi nei dettagli quanto asserito nell'Esempio 1.11 sulle matrici di Householder generalizzate.

6.6. Dato un vettore $\mathbf{v} \in \mathbb{C}^n$, provare che: (i) se la prima coordinata v_1 di $\mathbf{v}$ è reale, esiste un vettore $\mathbf{w} \in \mathbb{C}^n$ tale che $\mathbf{H}_\mathbf{w}\mathbf{v} = \|\mathbf{v}\|_2\mathbf{e}_1$; (ii) se v_1 non è reale, esiste un vettore $\mathbf{w} \in \mathbb{C}^n$ tale che $\mathbf{H}_\mathbf{w}\mathbf{v} = (\mathbf{v}_1/|\mathbf{v}_1|)\|\mathbf{v}\|_2\mathbf{e}_1$.

6.7. Si trovino gli autovettori di una matrice di Householder $\mathbf{H}_\mathbf{w}$, con relative basi ortonormali di autovettori.

6.8. Si provi che una matrice $\mathbf{A}$ è unitaria ed hermitiana se e solo se è una matrice di Householder generalizzata.

Paragrafo 2

6.9. Si provi che una matrice 2×2 simmetrica reale $\mathbf{A}$ è normale se e solo se è simmetrica, oppure $\mathbf{A} = r\mathbf{Q}$, con r numero reale e $\mathbf{Q}$ matrice ortogonale.

6.10. Si descrivano tramite proprietà dei loro coefficienti tutte le matrici complesse normali 2×2.

6.11. Si provi il punto (c) del Teorema 2.2.

6.12. Si provi che una matrice $\mathbf{A}$ è hermitiana se e solo se $i\mathbf{A}$ è anti-hermitiana e che in tal caso la matrice $(i\mathbf{I}-\mathbf{A})(i\mathbf{I}+\mathbf{A})^{-1}$ è una matrice unitaria che non ha -1 come autovalore.

6.13. Si provi che, data una matrice unitaria $\mathbf{U}$ che non ha -1 come autovalore, la matrice $(\mathbf{I}-\mathbf{U})(\mathbf{I}+\mathbf{U})^{-1}$ è una matrice anti-hermitiana.

6.14. Si trovino tutte le matrici complesse 2×2 che sono hermitiane e normali.

6.15. Si provi nei dettagli il "viceversa" nella versione additiva del Teorema spettrale.

6.16. Si provi che, se $\mathbf{A} = [a_{ij}]$ è una matrice qualunque, allora $\mathrm{Tr}(\mathbf{A}\mathbf{A}^H) = \mathrm{Tr}(\mathbf{A}^H\mathbf{A}) = \sum_{i,j}|a_{ij}|^2$.

Paragrafo 3

6.17. Si provi che la forma quadratica $Q(\mathbf{x}) = \mathbf{x}^H\mathbf{A}\mathbf{x}$, con $\mathbf{A} \in \mathrm{M}_n(\mathbb{C})$, assume valori reali sui vettori a coordinate reali se e solo se $\mathbf{A} = \mathbf{B} + \mathbf{C}$, con $\mathbf{B}$ matrice reale e $\mathbf{C}$ matrice hermitiana.

6.18. Dati due numeri complessi z_1 e z_2 tali che $z_1 + z_2 \in \mathbb{R}$ e $i(z_1 - z_2) \in \mathbb{R}$, si provi che $z_1 = \bar{z}_2$.

6.19. Sia $\mathbf{A}$ una matrice hermitiana tale che $\mathbf{A} = \mathbf{L}_0\mathbf{D}\mathbf{U}$, con $\mathbf{L}_0$ uni-triangolare inferiore, $\mathbf{D}$ diagonale con elementi diagonali non nulli e $\mathbf{U}$ uni-triangolare superiore. Si provi che $\mathbf{U} = \mathbf{L}_0^H$.

6.20. Si provi che l'insieme delle matrici reali semi-definite positive $n \times n$ forma un cono in $\mathrm{M}_n(\mathbb{R})$, cioè è chiuso rispetto alla somma e al prodotto per numeri reali ≥ 0.

6.21. Sia $\mathbf{A} = [a_{ij}]$ una matrice semi-definita positiva. Si provi che, se $a_{ii} = 0$, allora la i-esima riga e la i-esima colonna sono nulle. Suggerimento: usare il fatto che le sottomatrici 2×2 hanno determinante ≥ 0.

6.22. Data una matrice arbitraria $\mathbf{A}$, si provi che lo spazio delle colonne di $\mathbf{A}$ coincide con quello di $\mathbf{A}\mathbf{A}^H$. Suggerimento: si provi che gli spazi nulli di $\mathbf{A}^H$ e di $\mathbf{A}\mathbf{A}^H$ coincidono.

6.23. (A. Albert, 1969) Data la matrice hermitiana a blocchi, con $\mathbf{A}$ invertibile,

$$\mathbf{X} = \begin{bmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{B}^H & \mathbf{C} \end{bmatrix}$$

si provi che $\mathbf{X}$ è definita positiva se e solo se sono tali le tre matrici $\mathbf{A}$, $\mathbf{A} - \mathbf{B}\mathbf{C}^+\mathbf{B}^H$ e $\mathbf{C} - \mathbf{B}^H\mathbf{A}^{-1}\mathbf{B}$.

6.24. (A. Albert, 1969) Data la matrice hermitiana a blocchi

$$\mathbf{X} = \begin{bmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{B}^H & \mathbf{C} \end{bmatrix}$$

si provi che $\mathbf{X}$ è semi-definita positiva se e solo se sono tali le due matrici $\mathbf{A}$ e $\mathbf{C} - \mathbf{B}^H\mathbf{A}^+\mathbf{B}$ e inoltre $\mathbf{A}\mathbf{A}^+\mathbf{B} = \mathbf{B}$.

Paragrafo 4

6.25. Si dimostri che nella Proposizione 4.1 le molteplicità algebriche di un numero $\lambda \neq 0$ che sia autovalore di $\mathbf{AB}$ e di $\mathbf{BA}$ sono le stesse, usando le uguaglianze

$$\begin{aligned} \begin{bmatrix} \mathbf{AB} - X\mathbf{I}_m & \mathbb{O} \\ \mathbf{B} & -X\mathbf{I}_n \end{bmatrix} \begin{bmatrix} \mathbf{I}_m & \mathbf{A} \\ \mathbf{0} & \mathbf{I}_n \end{bmatrix} &= \begin{bmatrix} \mathbf{AB} - X\mathbf{I}_m & \mathbf{ABA} - X\mathbf{A} \\ \mathbf{B} & \mathbf{BA} - X\mathbf{I}_n \end{bmatrix} \\ &= \begin{bmatrix} \mathbf{I}_m & \mathbf{A} \\ \mathbf{0} & \mathbf{I}_n \end{bmatrix} \begin{bmatrix} -X\mathbf{I}_m & \mathbb{O} \\ \mathbf{B} & \mathbf{BA} - X\mathbf{I}_n \end{bmatrix}. \end{aligned}$$

6.26. Si verifichi che la matrice $\mathbf{V}\boldsymbol{\Sigma}^+\mathbf{U}^H$ definita nella Proposizione 4.8 soddisfa alle quattro condizioni richieste per essere la pseudo-inversa $\mathbf{A}^+$ di $\mathbf{A} = \mathbf{U}\boldsymbol{\Sigma}\mathbf{V}^H$, dopo avere provato che la matrice $\boldsymbol{\Sigma}^+$ coincide con quella ivi descritta.

6.27. Si verifiche quanto asserito dopo la Proposizione 4.8 per ottenere la pseudo-inversa di una matrice $\mathbf{A}$ a partire da una sua decomposizione polare.

6.28. Sia $\mathbf{A} = \mathbf{U}\boldsymbol{\Sigma}\mathbf{V}^H$ una decomposizione in valori singolari della matrice $m \times n$ $\mathbf{A}$ di rango k, con $\mathbf{U} = [\mathbf{u}_1 \ \dots \ \mathbf{u}_m]$, $\mathbf{V} = [\mathbf{v}_1 \ \dots \ \mathbf{v}_n]$, e valori singolari $\sigma_1, \dots, \sigma_k$. Si provi che:

(i) $\{\mathbf{u}_{k+1}; \dots; \mathbf{u}_m\}$ è una base ortonormale dello spazio nullo di $\mathbf{A}^H$;

(ii) $\{\mathbf{v}_{k+1}; \dots; \mathbf{v}_n\}$ è una base ortonormale dello spazio nullo di $\mathbf{A}$;

(iii) $\{\mathbf{u}_1; \dots; \mathbf{u}_k\}$ è una base ortonormale dello spazio delle colonne di $\mathbf{A}$;

(iv) $\{\mathbf{v}_1; \dots; \mathbf{v}_k\}$ è una base ortonormale dello spazio delle colonne di $\mathbf{A}^H$.

6.29. Dati il sistema lineare $\mathbf{A}\mathbf{x} = \mathbf{b}$ e una decomposizione in valori singolari della matrice $\mathbf{A} = \mathbf{U}\boldsymbol{\Sigma}\mathbf{V}^H$, si provi che il vettore $\mathbf{v}$ è una soluzione del sistema delle equazioni normali $\mathbf{A}^H\mathbf{A}\mathbf{x} = \mathbf{A}^H\mathbf{b}$ se e solo se $\mathbf{v} = \mathbf{V}\mathbf{y}$, dove le prime k coordinate di $\mathbf{y}$ coincidono con le prime k coordinate del vettore $\boldsymbol{\Sigma}^+\mathbf{U}^H\mathbf{b}$, mentre le ultime $n-k$ coordinate di $\mathbf{y}$ sono arbitrarie.

6.30. Nelle notazioni del precedente Esercizio, si provi che il vettore $\mathbf{v}$ è la soluzione ai minimi quadrati del sistema $\mathbf{A}\mathbf{x} = \mathbf{b}$ se e solo se $\mathbf{v} = \mathbf{V}\mathbf{y}$, dove $\mathbf{y} = \boldsymbol{\Sigma}^+\mathbf{U}^H\mathbf{b}$.

6.31. Si provi che i valori singolari di una matrice hermitiana coincidono con i moduli dei suoi autovalori.

6.32. Si provi che una matrice invertibile è unitaria se e solo se i suoi valori singolari sono tutti uguali a 1.

6.33. Data una decomposizione polare $\mathbf{A} = \mathbf{P}\mathbf{Q}$ della matrice $m \times n$ $\mathbf{A}$ $(m \le n)$, si ricavi da questa una decomposizione in valori singolari.

Paragrafo 5

6.34. Si dimostri la caratterizzazione di λ_k come min-max nel Teorema 5.1.

6.35. Si provi la seconda disuguaglianza nel Teorema 5.4.

6.36. (Dimostrazione di un caso speciale del Teorema dell'intreccio) È data la matrice hermitiana in forma bordata

$$\mathbf{A} = \begin{bmatrix} a & \mathbf{x}^H \\ \mathbf{x} & \mathbf{A}_1 \end{bmatrix}$$

con autovalori $\lambda_1 \le \dots \le \lambda_n$. Supponiamo che gli autovalori di $\mathbf{A}_1$ siano distinti, quindi, una volta ordinati, saranno $\mu_1 < \dots < \mu_{n-1}$. Se $\mathbf{U}$ è una matrice unitaria che diagonalizza $\mathbf{A}_1$ e $\mathbf{U}^H\mathbf{x} = \mathbf{z} = [z_1 \ \dots \ z_{n-1}]^T$, si provi che

(i) $p_{\mathbf{A}}(X) = (X-a)(X-\mu_1)\dots(X-\mu_{n-1}) - \sum_{1 \le i \le n-1} p_i(X)$, dove $p_i(X) = |z_i|^2 \prod_{j \ne i} X - \mu_j$;

(ii) se $z_i \neq 0$ per ogni i, allora $p_{\mathbf{A}}(X)$ assume valori di segno alterno sui successivi autoivalori μ_i;

(iii) dedurre il Teorema dell'intreccio dal teorema del valor medio.

6.37. Siano **A** e **B** matrici hermitiane con rispettivi autovalori $\lambda_1 \leq \cdots \leq \lambda_n$ e $\mu_1 \leq \cdots \leq \mu_n$. Siano $\gamma_1 \leq \cdots \leq \gamma_n$ gli autovalori di $\mathbf{A}+\mathbf{B}$. Si deduca dal Teorema 3.4 (2) e (3), che $\gamma_1 \geq \lambda_1 + \mu_1$ e $\gamma_n \leq \lambda_n + \mu_n$.

6.38. (Fan, 1949) Sia **A** una matrice hermitiana con autovalori $\lambda_1 \leq \cdots \leq \lambda_n$. Sia $1 \leq k \leq n$ e sia $\mathscr{O}_k$ l'insieme delle k-ple ortonormali di vettori di $\mathbb{C}^n$. Si provi che $\sum_{1\leq i\leq k} \lambda_i = \min_{I\in\mathscr{O}_k} \sum_{\mathbf{x}\in I} \mathbf{x}^H\mathbf{A}\mathbf{x}$. Suggerimento: per avere l'uguaglianza si consideri un sistema ortonormale di k autovettori relativi a $\lambda_1, \dots, \lambda_k$; per mostrare che fissato $I = \{\mathbf{x}_1; \dots; \mathbf{x}_1\}$ vale $\sum_{1\leq i\leq k} \lambda_i \geq \sum_i \mathbf{x}_i^H\mathbf{A}\mathbf{x}_i$, si completi I a una base ortonormale di $\mathbb{C}^n$ che produce una matrice unitaria **U** e si applichi l'Esercizio precedente alla matrice $\mathbf{U}^H\mathbf{A}\mathbf{U}$.

6.39. (Fan, 1949) Nelle ipotesi e notazioni dell'Esercizio 6.37, si provi che per ogni $k \leq n$ si ha: $\sum_{1\leq i\leq k} \gamma_i \geq \sum_{1\leq i\leq k} \lambda_i + \sum_{1\leq i\leq k} \mu_i$.

Paragrafo 6

6.40. Si provi che la relazione di congruenza è una relazione di equivalenza.

6.41. Data una matrice hermitiana (e invertibile) **A**, si provi che essa è congrua ad $\mathbf{A}^k$ per ogni intero positivo (e negativo) dispari.

6.42. Si provi che una matrice normale **A** è congrua a una matrice diagonale unitaria **D**.

6.43. Si provi che, se nell'Esercizio precedente la matrice **A** è anti-hermitiana, allora **D** può essere scelta immaginaria.

6.44. Che cosa dimostra il Teorema 6.3 applicato alla matrice hermitiana **A** e alla matrice $\mathbf{B} = \mathbf{Z}_{\mathbf{A}}$, usando come matrice **S** la matrice $\mathbf{U}\mathbf{D}^{-1}$ usata nella prima parte della dimostrazione del Teorema 6.1?

6.45. Siano **A** una matrice definita positiva e **B** una matrice hermitiana. Si provi, usando il Teorema 3.5 (6), che la matrice **AB** è diagonalizzabile con tutti i suoi autovalori reali, che sono positivi, negativi o nulli nello stesso numero degli autovalori di **B**.

6.46. Sia **C** una matrice diagonalizzabile con autovalori tutti reali. Si provi che $\mathbf{C} = \mathbf{A}\mathbf{B}$, con **A** matrice definita positiva e **B** matrice hermitiana.

Paragrafo 7

6.47. Mostrare che nel Teorema 7.6 ci si può ridurre al caso in cui la matrice $\mathbf{A}'$ è diagonale. Supposto che $\lambda_1 < \lambda_2 < \cdots < \lambda_n$, e posto $f(X) = \prod_{1\leq i\leq n}(X - \lambda_i)$ e $g(X) = \prod_{1\leq j\leq n-1}(X - \mu_j)$, provare che per dimostrare il Teorema 7.6 è sufficiente stabilire che

$$\frac{f(X)}{g(X)} = (X - a) - \sum_{1\leq j\leq n-1} \frac{b_j^2}{X - \mu_j}$$

per un $a \in \mathbb{R}$ e un $\mathbf{b} = [b_1 \ \dots \ b_n]^T \in \mathbb{R}^{n-1}$.

6.48. Nelle notazioni dell'esercizio precedente, provare che

$$\frac{f(X)}{g(X)} = (X-\gamma) + \sum_{1\le j\le n-1} \frac{f(\mu_j)}{g'(\mu_j)} \cdot \frac{1}{X-\mu_j}$$

dove $\gamma = \sum_{1\le i\le n} \lambda_i - \sum_{1\le j\le n-1} \mu_j$. Dedurre che $f(\mu_j)/g'(\mu_j) \le 0$ per ogni $j \le n-1$ e che $b_j^2 = -f(\mu_j)/g'(\mu_j)$ e $a = \gamma$ producono la matrice $\mathbf{A}$ cercata.

6.49. Provare il Teorema 7.6 nel caso generale in cui $\lambda_1 \le \lambda_2 \le \dots \le \lambda_n$, considerando prescritti autovalori $\lambda_1+\varepsilon_1 < \lambda_2+\varepsilon_2 < \dots < \lambda_n+\varepsilon_n$ e usando poi argomenti di passaggio al limite.

6.50. Si usi il Teorema di Courant-Fischer per provare che il j-esimo valore singolare di una matrice $m \times n$ $\mathbf{A}$ di rango k ($j \le k$) è dato da

$$\sigma_k = \min_{V\in\mathcal{V}_{k-1}} \max_{\substack{\mathbf{x}\in V^\perp \\ \|\mathbf{x}\|_2=1}} \|\mathbf{Ax}\|_2 = \max_{V\in\mathcal{V}_{n-k}} \min_{\substack{\mathbf{x}\in V^\perp \\ \|\mathbf{x}\|_2=1}} \|\mathbf{Ax}\|_2.$$

6.51. Dato $\mathbf{x} \in \mathbb{R}^n$, si provi che l'insieme

$$\{\mathbf{y} \in \mathbb{R}^n \mid \mathbf{y} \prec \mathbf{x}\}$$

è un sottoinsieme chiuso e limitato di $\mathbb{R}^n$.

6.52. Si provi che la disuguaglianza di Hadamard in 7.3 (i) è un'uguaglianza se e solo se la matrice hermitiana $\mathbf{A}$ è diagonale.

Paragrafo 8

6.53. Sia $\mathbf{e} = [1 \ 1 \ \dots \ 1]^T \in \mathbb{R}^n$ e sia $\mathbf{A} = \frac{1}{n}\mathbf{e}\mathbf{e}^T$. Si provi che $\mathbf{A}$ è bistocastica e che è combinazione convessa di n matrici di permutazione con coefficienti tutti uguali a $1/n$.

6.54. Si dimostri che una matrice $n \times n$ $\mathbf{S}$ è bistocastica se e solo se $\mathbf{Sx} \prec \mathbf{x}$ per ogni $\mathbf{x} \in \mathbb{R}^n$. (Suggerimento: per la necessità si usi il Teorema di Schur 7.1; per la sufficienza si impieghino prima i vettori coordinati $\mathbf{e}_i$ e poi il vettore $\mathbf{e} = [1 \ 1 \ \dots \ 1]^T$.)

6.55. Siano $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_r$ vettori di uno spazio vettoriale tali che $\dim\langle \mathbf{v}_1; \mathbf{v}_2; \dots; \mathbf{v}_r\rangle = k$. Si provi che, se $r \ge k+2$, esistono scalari $\alpha_1, \alpha_2, \dots, \alpha_r$ non tutti nulli tali che $\sum_{i\le r} \alpha_i \mathbf{v}_i = \mathbf{0}$ e $\sum_{i\le r} \alpha_i = 0$.

6.56. Siano $\lambda_1, \lambda_2, \dots, \lambda_r$ numeri reali positivi e $\alpha_1, \alpha_2, \dots, \alpha_r$ numeri reali non tutti nulli. Allora esiste $c \in \mathbb{R}$, $c \ne 0$, tale che $\lambda_{i_0} = c\alpha_{i_0}$ per un $i_0 \le r$ e $\lambda_i \ge c\alpha_i$ per $i \ne i_0$.

6.57. Si provi il Teorema 8.7 impiegando i due esercizi precedenti.

Appendici

Appendice A

I numeri complessi

Non dovrebbe essere considerata un'idea insolita quella di ampliare un insieme numerico per consentire di eseguire operazioni altrimenti impossibili: i numeri interi negativi vengono introdotti esattamente per rendere possibili tutte le sottrazioni e le frazioni per rendere possibili le divisioni (con divisore diverso da zero). I numeri reali rispondono all'esigenza di misurare segmenti incommensurabili rispetto all'unità di misura.

Rimane almeno un'operazione che non ha sempre senso nei numeri reali: non esistono numeri reali r tali che $r^2 = s$, se $s < 0$.

Ci accorgiamo che basterebbe trovare un "numero" che elevato al quadrato dia -1 per "risolvere" questo problema. Come abbiamo già fatto allora in situazioni simili, introduciamo un nuovo "numero" con questa proprietà. Seguendo l'esempio dei matematici del '500 (Cardano e Bombelli fra gli altri), chiameremo questo numero *unità immaginaria* e lo denoteremo con il simbolo i, secondo la notazione di Euler.

Ovviamente questo numero deve essere "come tutti gli altri" e quindi avrà senso moltiplicarlo e sommarlo con un altro numero reale. Dunque abbiamo un'intera famiglia di nuovi numeri: quelli della forma

$$a + bi$$

con $a, b \in \mathbb{R}$. Non abbiamo bisogno di altro, perché vogliamo che continuino a valere le usuali proprietà delle operazioni; quindi

$$(a + bi) + (c + di) = (a + c) + (b + d)i$$

per l'addizione (abbiamo usato le proprietà associativa e commutativa dell'addizione e quella distributiva della moltiplicazione). Per la moltiplicazione:

$$(a + bi)(c + di) = ac + bic + adi + bdi^2 = (ac - bd) + (ad + bc)i$$

(notiamo che si è usato il fatto che $i^2 = -1$). Dunque questi nuovi numeri si comportano esattamente come gli altri, basta usare le solite regole di calcolo con la regola aggiuntiva che $i^2 = -1$.

Abbiamo però alcuni problemi. Il primo è: può capitare che $a+bi = c+di$? Lo esaminiamo con calma. Intanto, se eseguiamo la somma

$$(a+bi)+(-a+(-b)i),$$

troviamo zero; scriveremo $-a-bi$, per brevità. Questo numero è l'*opposto* di $a+bi$. Domandarsi quando $a+bi = c+di$ equivale allora a chiedersi quando $x+yi = 0$ (basta scrivere $x = a-c$ e $y = b-d$). Osserviamo che risulta

$$(x+yi)(x-yi) = x^2 + yix - xyi + y(-y)i^2 = x^2 + xyi - xyi + (-y^2)(-1) = x^2 + y^2.$$

Se $x+yi = 0$, anche $(x+yi)(x-yi) = 0$ e quindi $x^2+y^2 = 0$. Ciò accade solo se $x = y = 0$.

Definizione. Un *numero complesso* è un'espressione del tipo $a+bi$, con $a, b \in \mathbb{R}$.

I numeri a e b sono univocamente determinati e si chiamano rispettivamente *parte reale* e *parte immaginaria* del numero complesso. Quando scriveremo espressioni del tipo $z = a+bi$, intenderemo che a e b siano reali.

Rimane un altro problema importante: siamo sicuri che per questi numeri le regole di calcolo usuali siano veramente applicabili? Non potrà succedere che si incontri una contraddizione nell'uso di questi nuovi “numeri”? Risolveremo il problema più avanti. Per ora continueremo a operare con questi numeri applicando le regole usuali.

Esempio. Ogni numero complesso diverso da zero ha esattamente due radici quadrate. Sia infatti $a+bi \neq 0$. Cerchiamo allora i numeri complessi $x+yi$ (con $x, y \in \mathbb{R}$) tali che

$$(x+yi)^2 = a+bi.$$

Svolgendo i calcoli, dobbiamo avere $(x^2-y^2)+2xyi = a+bi$ e quindi

$$\begin{cases} x^2 - y^2 = a, \\ 2xy = b. \end{cases}$$

Se $b = 0$ il numero complesso è di fatto reale e sappiamo già risolvere il problema: se $a > 0$ prendiamo $x = \sqrt{a}$ oppure $x = -\sqrt{a}$ e $y = 0$; se $a < 0$ prendiamo $x = 0$ e $y = i\sqrt{-a}$ oppure $y = -i\sqrt{-a}$.

Se $b \neq 0$, possiamo ricavare $y = b/(2x)$ e sostituire, ottenendo l'equazione biquadratica

$$4x^4 - 4ax^2 - b^2 = 0$$

che porge

$$x^2 = \frac{4a + \sqrt{16a^2 + 16b^2}}{8} = \frac{a + \sqrt{a^2+b^2}}{2}.$$

L'altra radice è negativa, quindi inaccettabile come valore di x^2. Otteniamo due valori opposti per x e, in corrispondenza, due valori opposti per y. Con calcoli analoghi ai precedenti avremo $x = b/2y$, da cui $4y^4 + 4ay^2 - b^2 = 0$ e

$$y^2 = \frac{-4a + \sqrt{16a^2 + 16b^2}}{8} = \frac{-a + \sqrt{a^2+b^2}}{2}.$$

I segni delle soluzioni in x e y vanno scelti in modo che $2xy = b$. □

Un prodotto di numeri complessi può essere reale (cioè avere parte immaginaria nulla): abbiamo già visto un caso calcolando $(a + bi)(a - bi) = a^2 + b^2$.

Definizione. Se $z = a + bi$ è un numero complesso, il numero complesso $\bar{z} = a - bi$ si dice il *coniugato* di z.

Questa operazione di passaggio al coniugato ha proprietà interessanti:

(C_1) $\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2$;

(C_2) $\overline{z_1 z_2} = \bar{z}_1 \bar{z}_2$;

(C_3) $\bar{\bar{z}} = z$;

(C_4) z è reale se e solo se $z = \bar{z}$.

Le dimostrazioni sono semplici applicazioni delle regole di calcolo. Con il coniugato si possono anche calcolare la parte reale e la parte immaginaria di un numero complesso:

$$z = \frac{z + \bar{z}}{2} + \frac{z - \bar{z}}{2i} i.$$

Si noti l'analogia di questa scrittura con quella di una matrice come somma di una matrice simmetrica e di una anti-simmetrica.

Avendo osservato che, per $z = a + bi$, $z\bar{z} = a^2 + b^2$ è un numero reale non negativo, possiamo dare questa definizione.

Definizione. Se $z = a + bi$ è un numero complesso, il *modulo* di z è

$$|z| = \sqrt{a^2 + b^2}.$$

La seconda proprietà del coniugio dice allora che

$$|z_1 z_2| = |z_1||z_2|.$$

Infatti

$$|z_1 z_2|^2 = (z_1 z_2)\overline{(z_1 z_2)} = (z_1 z_2)(\bar{z}_1 \bar{z}_2) = (z_1 \bar{z}_1)(z_2 \bar{z}_2) = |z_1|^2 |z_2|^2,$$

da cui la tesi.

In particolare, se $|z| = 1$, abbiamo che $z\bar{z} = 1$, cioè $\bar{z}$ è l'inverso di z rispetto alla moltiplicazione. Possiamo generalizzare questo fatto per trovare l'inverso di ogni numero complesso diverso da zero. Supponiamo dunque che $z = a + bi$ sia diverso da zero e cerchiamo un numero complesso $w = x + yi$ tale che $zw = 1$. Se z è reale, cioè $b \neq 0$, il suo inverso è quello già noto. Quindi, anche se z non è reale, possiamo usare l'inverso di $|z|$. Siccome

$$z\bar{z} = |z|^2,$$

avremo anche

$$z(|z|^{-2}\bar{z}) = 1$$

e quindi

$$z^{-1} = \frac{1}{|z|^2}\bar{z}.$$

In realtà, il calcolo si fa più facilmente *razionalizzando*:

$$\frac{1}{a+bi} = \frac{a-bi}{(a+bi)(a-bi)} = \frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}i.$$

Un modo per rendere accettabili i numeri complessi, fino ad allora considerati con sospetto come numeri “fittizi”, fu proposto da Gauss e perfezionato da Argand. Il numero complesso $z = a+bi$ è determinato dalla sua parte reale e dalla parte immaginaria e quindi determina le coordinate di un punto nel piano cartesiano. Si può anche considerare l'insieme $\mathbb{C}$ dei numeri complessi come uno spazio vettoriale reale di dimensione due: una base è data da $\{1;i\}$. In effetti ogni numero complesso si scrive in uno e un solo modo come combinazione lineare a coefficienti reali di 1 e i. L'applicazione delle coordinate rispetto a questa base fornisce proprio il vettore che ha come prima componente la parte reale e come seconda componente la parte immaginaria.

L'interpretazione geometrica di Argand e Gauss dà anche un metodo per giustificare l'uso algebrico dei numeri complessi, trovandone un modello proprio nelle matrici. Ciò che segue può essere omesso in prima lettura e ripreso quando si siano studiati gli spazi vettoriali e le applicazioni lineari.

Se consideriamo un numero $z = a+bi \in \mathbb{C}$ fissato, l'applicazione $\mu_z : \mathbb{C} \to \mathbb{C}$ definita da $\mu_z(w) = zw$ è lineare, considerando $\mathbb{C}$ come spazio vettoriale sui reali, visto che supponiamo valide le regole di calcolo usuali. La sua matrice associata rispetto alla base $\{1;i\}$ è allora

$$\begin{bmatrix} a & -b \\ b & a \end{bmatrix}.$$

Infatti $\mu_z(1) = z \cdot 1 = z = a+bi$ e $\mu_z(i) = (a+bi)i = -b+ai$. Ora, dati $z_1 = a+bi$ e $z_2 = c+di$, abbiamo

$$\mu_{z_1}(w) + \mu_{z_2}(w) = z_1 w + z_2 w = (z_1+z_2)w = \mu_{z_1+z_2}(w)$$
$$\mu_{z_1}(\mu_{z_2}(w)) = z_1(z_2 w) = (z_1 z_2)w = \mu_{z_1 z_2}(w)$$

che in forma matriciale diventano

$$\begin{bmatrix} a & -b \\ b & a \end{bmatrix} + \begin{bmatrix} c & -d \\ d & c \end{bmatrix} = \begin{bmatrix} a+c & -(b+d) \\ b+d & a+c \end{bmatrix}$$
$$\begin{bmatrix} a & -b \\ b & a \end{bmatrix} \begin{bmatrix} c & -d \\ d & c \end{bmatrix} = \begin{bmatrix} ac-bd & -(ad+bc) \\ ad+bc & ac-bd \end{bmatrix}$$

che sono esattamente la somma e il prodotto di matrici. Perciò abbiamo il risultato che cercavamo: il calcolo con i numeri complessi non può portare a contraddizioni, perché altrimenti otterremmo corrispondenti contraddizioni nel calcolo delle matrici a coefficienti reali.

Questa rappresentazione matriciale dei numeri complessi ha anche un'altra conseguenza. Supponiamo che $z = a + bi$ abbia modulo 1. Allora la matrice associata è ortogonale: infatti

$$\begin{bmatrix} a & -b \\ b & a \end{bmatrix} \begin{bmatrix} a & -b \\ b & a \end{bmatrix}^T = \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \begin{bmatrix} a^2 + b^2 & ab - ba \\ ba - ab & b^2 + a^2 \end{bmatrix} = \mathbf{I}_2.$$

Inoltre

$$\det \begin{bmatrix} a & -b \\ b & a \end{bmatrix} = a^2 + b^2 = 1$$

e quindi è la matrice associata a una rotazione del piano (si veda il Capitolo 3 e l'Appendice C). Eseguire la moltiplicazione zw di numeri complessi, con $|z| = 1$, equivale a ruotare il punto del piano corrispondente a w di un certo angolo. Quale angolo? Il numero complesso z corrisponde a uno e un solo punto della circonferenza di centro nell'origine e raggio 1, quindi definisce in modo univoco un angolo α tale che $0 \le \alpha < 2\pi$.

Con semplici considerazioni di trigonometria si trova allora

$$a = \cos\alpha, \qquad b = \operatorname{sen}\alpha.$$

Se poi ci ricordiamo che ogni numero complesso z diverso da zero si può scrivere come $z = |z|w$ e che $|w| = 1$, abbiamo la *forma trigonometrica* dei numeri complessi

$$z = |z|(\cos\alpha + i \operatorname{sen}\alpha)$$

dove α è determinato a meno di multipli interi di 2π (come vedremo è utile considerare angoli qualsiasi). Il numero reale α si chiama *argomento* di z. La forma trigonometrica è particolarmente utile quando si devono eseguire moltiplicazioni di numeri complessi. Infatti, rinforzando l'intuizione che una moltiplicazione corrisponda a una rotazione, si ha, per $z_1 = |z_1|(\cos\alpha + i \operatorname{sen}\alpha)$ e $z_2 = |z_2|(\cos\beta + i \operatorname{sen}\beta)$,

$$\begin{aligned} z_1 z_2 &= |z_1||z_2|(\cos\alpha + i \operatorname{sen}\alpha)(\cos\beta + i \operatorname{sen}\beta) \\ &= |z_1 z_2|(\cos\alpha\cos\beta - \operatorname{sen}\alpha\operatorname{sen}\beta) + i(\cos\alpha\operatorname{sen}\beta + \operatorname{sen}\alpha\cos\beta) \\ &= |z_1 z_2|\bigl(\cos(\alpha+\beta) + i \operatorname{sen}(\alpha+\beta)\bigr) \end{aligned}$$

Per giungere alla conclusione abbiamo usato le note formule della trigonometria. Il prodotto di due numeri complessi non nulli ha come modulo il prodotto dei moduli e come argomento la somma degli argomenti. In effetti la conoscenza di questo permette di usare i numeri complessi per ricordare le formule di addizione!

A corollario di questa discussione, menzioniamo la *formula di de Moivre*: se $z = |z|(\cos\alpha + i \operatorname{sen}\alpha) \neq 0$

$$z^n = |z|^n(\cos n\alpha + i \operatorname{sen} n\alpha)$$

valida per ogni esponente n intero (per $n = -1$ ritroviamo l'espressione già nota per l'inverso). Come esempio di applicazione, possiamo ricavare le formule di triplicazione di seno e coseno:

$$\begin{aligned}(\cos 3\alpha + i \operatorname{sen} 3\alpha)^3 &= (\cos\alpha + i \operatorname{sen}\alpha)^3 \\ &= (\cos\alpha)^3 + 3i(\cos\alpha)^2 \operatorname{sen}\alpha + 3i^2 \cos\alpha(\operatorname{sen}\alpha)^2 + i^3(\operatorname{sen}\alpha)^3 \\ &= (\cos^3\alpha - 3\cos\alpha \operatorname{sen}^2\alpha) + i(3\cos^2\alpha \operatorname{sen}\alpha - \operatorname{sen}^3\alpha)\end{aligned}$$

e perciò

$$\begin{aligned}\cos 3\alpha &= \cos^3\alpha - 3\cos\alpha \operatorname{sen}^2\alpha, \\ \operatorname{sen} 3\alpha &= 3\cos^2\alpha \operatorname{sen}\alpha - \operatorname{sen}^3\alpha.\end{aligned}$$

Un classico problema che si risolve in questo modo è quello di trovare le *radici n-esime* dei numeri complessi. Consideriamo $z \neq 0$ e cerchiamo tutti i numeri complessi w tali che $w^n = z$, con n intero positivo. Scrivendo z e w in forma trigonometrica

$$\begin{aligned}z &= |z|(\cos\alpha + i \operatorname{sen}\alpha) \\ w &= |w|(\cos\beta + i \operatorname{sen}\beta)\end{aligned}$$

dobbiamo porre

$$w^n = |w|^n(\cos n\beta + i \operatorname{sen} n\beta) = |z|(\cos\alpha + i \operatorname{sen}\alpha)$$

e quindi, per cominciare, $|w| = \sqrt[n]{|z|}$ (radice n-esima calcolata nei reali). La seconda uguaglianza da soddisfare è

$$\cos n\beta + i \operatorname{sen} n\beta = \cos\alpha + i \operatorname{sen}\alpha.$$

Due angoli che abbiano uguali coseno e seno devono differire per un multiplo intero di 2π, quindi avremo

$$n\beta = \alpha + 2k\pi \qquad (k \text{ intero}),$$

cioè

$$\beta = \frac{\alpha + 2k\pi}{n} \qquad (k \text{ intero}).$$

Due soluzioni sono lo stesso numero complesso quando differiscono per multipli interi di 2π; ma da

$$\frac{\alpha + 2k\pi}{n} = \frac{\alpha + 2k'\pi}{n} + 2h\pi$$

ricaviamo

$$2k\pi = 2k'\pi + 2nh\pi$$

cioè $k - k' = nh$. Dunque esistono esattamente n soluzioni distinte, che si ottengono per i valori $k = 0, 1, 2, \dots, n-1$.

Per esempio, si vogliano calcolare le radici cubiche di $z = 8i$. Abbiamo $|z| = 8$ e $z = 8(\cos(\pi/2) + i\,\mathrm{sen}(\pi/2))$ e quindi le radici cubiche sono

$$w_0 = 2\left(\cos\frac{1}{3}\left(\frac{\pi}{2} + 0\cdot 2\pi\right) + i\,\mathrm{sen}\,\frac{1}{3}\left(\frac{\pi}{2} + 0\cdot 2\pi\right)\right),$$
$$w_1 = 2\left(\cos\frac{1}{3}\left(\frac{\pi}{2} + 1\cdot 2\pi\right) + i\,\mathrm{sen}\,\frac{1}{3}\left(\frac{\pi}{2} + 1\cdot 2\pi\right)\right),$$
$$w_2 = 2\left(\cos\frac{1}{3}\left(\frac{\pi}{2} + 2\cdot 2\pi\right) + i\,\mathrm{sen}\,\frac{1}{3}\left(\frac{\pi}{2} + 2\cdot 2\pi\right)\right),$$

che, scritte in altra forma, sono

$$w_0 = 2\left(\cos\frac{\pi}{6} + i\,\mathrm{sen}\,\frac{\pi}{6}\right) = 2\left(\frac{\sqrt{3}}{2} + \frac{1}{2}i\right) = \sqrt{3} + i,$$
$$w_1 = 2\left(\cos\frac{5}{6}\pi + i\,\mathrm{sen}\,\frac{5}{6}\pi\right) = 2\left(-\frac{\sqrt{3}}{2} + \frac{1}{2}i\right) = -\sqrt{3} + i,$$
$$w_1 = 2\left(\cos\frac{3}{2}\pi + i\,\mathrm{sen}\,\frac{3}{2}\pi\right) = 2(0 - i) = -2i.$$

È interessante allora notare che esistono in $\mathbb{C}$ esattamente n radici n-esime di 1; i punti corrispondenti nel piano di Argand-Gauss sono i vertici dell'n-agono regolare inscritto nella circonferenza di raggio 1 avente un vertice nel punto di coordinate $(1,0)$ che corrisponde al numero complesso 1.

Tuttavia la massima importanza dei numeri complessi risiede nel risultato dimostrato rigorosamente per la prima volta da Gauss nel 1799 come tesi di laurea (per una dimostrazione che fa uso degli strumenti dell'Algebra Lineare si veda l'Appendice D).

Teorema Fondamentale dell'Algebra. *Ogni polinomio di grado positivo a coefficienti complessi ammette una radice complessa.*

Da esso si deduce il corollario che ogni polinomio a coefficienti reali può essere decomposto in fattori irriducibili di primo o secondo grado.

Sia infatti $f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ un polinomio a coefficienti reali. La dimostrazione è per induzione sul grado.

Se $n = 1$ non c'è nulla da dimostrare.

Sia $n > 1$. Se c è una radice reale di f (cioè $f(c) = 0$) possiamo dividere f per $X - c$, riducendo il problema a un polinomio di grado inferiore. Se invece c è una radice complessa non reale, possiamo calcolare

$$\begin{aligned} f(\bar{c}) &= a_0 + a_1\bar{c} + a_2\bar{c}^2 + \cdots + a_n\bar{c}^n = \overline{a_0} + \overline{a_1}\,\bar{c} + \overline{a_2}\,\bar{c}^2 + \cdots + \overline{a_n}\,\bar{c}^n \\ &= \overline{a_0 + a_1c + a_2c^2 + \cdots + a_nc^n} \\ &= \overline{f(c)} = \overline{0} = 0. \end{aligned}$$

Dunque $\bar{c}$ è una radice di f *distinta* da c e perciò f è divisibile per

$$(X-c)(X-\bar{c}) = X^2-(c+\bar{c})X+c\bar{c}$$

che è un polinomio a coefficienti reali. Il quoziente ha allora coefficienti reali e anche in questo caso ci siamo ridotti a un polinomio di grado inferiore.

Naturalmente la stessa tecnica permette di affermare che ogni polinomio di grado positivo a coefficienti complessi si scrive come prodotto di n fattori di primo grado. Al Capitolo 5 si vede come sfruttare questo risultato nello studio degli autovalori di una matrice.

La funzione esponenziale complessa

Un altro modo di scrivere un numero complesso in forma trigonometrica si ottiene ponendo, secondo la definizione data da Euler,

$$\cos\alpha + i\,\mathrm{sen}\,\alpha = e^{i\alpha},$$

dove e è il numero di Napier, base dei logaritmi naturali. La notazione è giustificata dalla proprietà già dimostrata che

$$e^{i\alpha}e^{i\beta} = e^{i(\alpha+\beta)}.$$

In questo modo l'esponenziale viene esteso ai numeri complessi, definendo, per $z = a+bi$,

$$e^z = e^{a+bi} = e^a e^{ib} = e^a(\cos b + i\,\mathrm{sen}\,b).$$

Si verifica immediatamente che vale l'usuale proprietà dell'esponenziale:

$$e^z e^{z'} = e^{z+z'}.$$

Non dobbiamo pensare a una "potenza" nel senso usuale di moltiplicazione; del resto nemmeno $e^{\sqrt{2}}$ è ottenibile come moltiplicazione di fattori ripetuti. Stiamo solo usando una notazione comoda perché, quando z è intero, e^z coincide con la potenza di esponente z. Si pone anche

$$\cos z = \frac{e^{iz}+e^{-iz}}{2}, \qquad \mathrm{sen}\,z = \frac{e^{iz}-e^{-iz}}{2i}.$$

Quando z è reale, $\cos z$ e $\mathrm{sen}\,z$ sono gli usuali coseno e seno:

$$\frac{e^{iz}+e^{-iz}}{2} = \frac{\cos z + i\,\mathrm{sen}\,z + \cos(-z) + i\,\mathrm{sen}(-z)}{2} = \frac{2\cos z}{2} = \cos z,$$
$$\frac{e^{iz}-e^{-iz}}{2i} = \frac{\cos z + i\,\mathrm{sen}\,z - \cos(-z) - i\,\mathrm{sen}(-z)}{2i} = \frac{2i\,\mathrm{sen}\,z}{2i} = \mathrm{sen}\,z.$$

Queste estensioni ai complessi delle funzioni trigonometriche hanno le stesse proprietà che sui reali:

$$\begin{gathered}
\operatorname{sen}^2 z + \cos^2 z = 1, \\
\operatorname{sen}(z+2\pi) = \operatorname{sen} z, \quad \cos(z+2\pi) = \cos z, \\
\operatorname{sen}(z+z') = \operatorname{sen} z \cos z' + \cos z \operatorname{sen} z', \\
\cos(z+z') = \cos z \cos z' - \operatorname{sen} z \operatorname{sen} z',
\end{gathered}$$

come si verifica con un calcolo diretto.

Per esempio si vuole risolvere (nei complessi) l'equazione $\cos z = 2$ che sui reali non ha senso:

$$\frac{e^{iz} + e^{-iz}}{2} = 2$$

diventa

$$e^{2iz} - 4e^{iz} + 1 = 0$$

e, ponendo $w = e^{iz}$, troviamo $w^2 - 4w + 1 = 0$, da cui

$$w = 2 - \sqrt{3} \qquad \text{oppure} \qquad w = 2 + \sqrt{3}.$$

Scrivendo $z = x + yi$ si ha $iz = -y + xi$ e quindi $e^{iz} = e^{-y}(\cos x + i \operatorname{sen} x)$. La prima equazione allora è

$$e^{-y}(\cos x + i \operatorname{sen} x) = 2 - \sqrt{3},$$

cioè $y = -\log(2 - \sqrt{3})$ e $x = 2k\pi$ (k intero). Analogamente per la seconda.

La funzione esponenziale complessa ha molte proprietà che vengono sfruttate in elettrotecnica, oltre che a livello teorico.

I quaternioni

Le matrici in $M_2(\mathbb{C})$ della forma

$$\begin{bmatrix} z & -\bar{w} \\ w & \bar{z} \end{bmatrix}$$

sono tutte unitarie, a meno di un fattore reale: infatti

$$\begin{aligned}
\begin{bmatrix} z & -\bar{w} \\ w & \bar{z} \end{bmatrix} \begin{bmatrix} z & -\bar{w} \\ w & \bar{z} \end{bmatrix}^H &= \begin{bmatrix} z & -\bar{w} \\ w & \bar{z} \end{bmatrix} \begin{bmatrix} \bar{z} & \bar{w} \\ -w & z \end{bmatrix} \\
&= \begin{bmatrix} z\bar{z} + \bar{w}w & z\bar{w} - \bar{w}z \\ w\bar{z} - \bar{z}w & w\bar{w} + \bar{z}z \end{bmatrix} = (|z|^2 + |w|^2)\mathbf{I}_2.
\end{aligned}$$

C'è un'eccezione, naturalmente, quando $z = w = 0$.

Notiamo che, quando z e w sono reali, questa matrice è proprio quella associata al numero complesso $z + wi$. Si può facilmente verificare che la somma e il prodotto di matrici di questo tipo è ancora una matrice dello stesso tipo. Inoltre l'inversa di una matrice di questa forma ha ancora la stessa forma: infatti

$$\det\begin{bmatrix} z & -\bar{w} \\ w & \bar{z}\end{bmatrix} = |z|^2 + |w|^2$$

e, se la matrice è non nulla,

$$\begin{bmatrix} z & -\bar{w} \\ w & \bar{z}\end{bmatrix}^{-1} = \frac{1}{|z|^2 + |w|^2}\begin{bmatrix} \bar{z} & \bar{w} \\ -w & z\end{bmatrix}.$$

L'insieme di queste matrici ha quindi proprietà molto simili a quelle dei numeri reali e complessi, con l'eccezione della commutatività della moltiplicazione. In quanto spazio vettoriale sui reali, questo insieme che indichiamo con $\mathbb{H}$ ha dimensione 4: una base è data dalle matrici

$$\mathbb{1} = \begin{bmatrix} 1 & 0 \\ 0 & 1\end{bmatrix}; \quad \mathbb{i} = \begin{bmatrix} 0 & -1 \\ 1 & 0\end{bmatrix}; \quad \mathbb{j} = \begin{bmatrix} i & 0 \\ 0 & -i\end{bmatrix}; \quad \mathbb{k} = \begin{bmatrix} 0 & i \\ i & 0\end{bmatrix}.$$

Risulta

$$\begin{gathered} \mathbb{i}\,\mathbb{j} = \mathbb{k}, \quad \mathbb{j}\,\mathbb{k} = \mathbb{i}, \quad \mathbb{k}\,\mathbb{i} = \mathbb{j}, \\ \mathbb{j}\,\mathbb{i} = -\mathbb{k}, \quad \mathbb{k}\,\mathbb{j} = -\mathbb{i}, \quad \mathbb{i}\,\mathbb{k} = -\mathbb{j}, \\ \mathbb{i}^2 = \mathbb{j}^2 = \mathbb{k}^2 = \mathbb{i}\,\mathbb{j}\,\mathbb{k} = -\mathbb{1}. \end{gathered}$$

Se $z = a + ci$ e $w = b + di$, abbiamo

$$\begin{bmatrix} z & -\bar{w} \\ w & \bar{z}\end{bmatrix} = \begin{bmatrix} a+ci & -b+di \\ b+di & a-ci\end{bmatrix} = a\mathbb{1} + b\,\mathbb{i} + c\,\mathbb{j} + d\mathbb{k}$$

e da questa espressione possiamo, usando le regole di moltiplicazione viste sopra e quelle usuali, eseguire i calcoli. Queste matrici (o le espressioni equivalenti in termini di combinazioni lineari di $\mathbb{1}$, $\mathbb{i}$, $\mathbb{j}$ e $\mathbb{k}$) si chiamano *quaternioni* e furono scoperti da Hamilton nel 1810.

Il quaternione $\mathbb{1}$ ha la proprietà che $\mathbb{1}\mathbb{q} = \mathbb{q}\mathbb{1}$, per ogni $\mathbb{q} \in \mathbb{H}$. Inoltre tutte le proprietà usuali delle operazioni valgono, con l'eccezione della proprietà commutativa. Definiamo, per $\mathbb{q} = a\mathbb{1} + b\,\mathbb{i} + c\,\mathbb{j} + d\mathbb{k}$, il *coniugato* di $\mathbb{q}$ come

$$\bar{\mathbb{q}} = a\mathbb{1} - b\,\mathbb{i} - c\,\mathbb{j} - d\mathbb{k}.$$

Non si ha difficoltà a verificare che, scritto $\mathbb{q}$ come matrice

$$\mathbb{q} = \begin{bmatrix} a+ci & -b+di \\ b+di & a-ci\end{bmatrix}$$

si ha

$$\bar{\mathbb{q}} = \begin{bmatrix} a-ci & b-di \\ -b-di & a+ci\end{bmatrix} = \mathbb{q}^H$$

e quindi non c'è bisogno di calcoli per dedurre che

$$\overline{\mathbb{q}+\mathbb{r}} = \bar{\mathbb{q}} + \bar{\mathbb{r}}, \qquad \overline{\mathbb{q}\,\mathbb{r}} = \bar{\mathbb{r}}\,\bar{\mathbb{q}},$$

per ogni $\mathbb{q}, \mathbb{r} \in \mathbb{H}$. Si noti l'inversione dei fattori con la moltiplicazione. Abbiamo facilmente

$$\mathbb{q}\bar{\mathbb{q}} = (a^2 + b^2 + c^2 + d^2)\mathbb{1} = \bar{\mathbb{q}}\mathbb{q}.$$

Inoltre $\mathbb{q} = \bar{\mathbb{q}}$ se e solo se $b = c = d = 0$. In questo caso si parla di *quaternioni reali*, che sono *una copia* dei numeri reali all'interno di $\mathbb{H}$, cioè un sottoinsieme che ha le stesse proprietà algebriche dei numeri reali.

Il *modulo* di $\mathbb{q} = a\mathbb{1} + b\,\mathbb{i} + c\,\mathbb{j} + d\mathbb{k}$ è

$$|\mathbb{q}| = \sqrt{a^2 + b^2 + c^2 + d^2}$$

e valgono ancora le proprietà

$$|\mathbb{q}\,\mathbb{r}| = |\mathbb{q}|\,|\mathbb{r}|, \qquad |\mathbb{q} + \mathbb{r}| \le |\mathbb{q}| + |\mathbb{r}|.$$

Il coniugato e il modulo permettono di scrivere l'inverso di un quaternione esattamente come nel caso dei numeri complessi: se $\mathbb{q} \in \mathbb{H}$ e $\mathbb{q} \neq \mathbb{O}$, allora

$$\mathbb{q}^{-1} = \frac{1}{|\mathbb{q}|^2}\bar{\mathbb{q}}.$$

Infatti

$$\Big(\frac{1}{|\mathbb{q}|^2}\bar{\mathbb{q}}\Big)\mathbb{q} = \frac{1}{|\mathbb{q}|^2}|\mathbb{q}|^2\mathbb{1} = \mathbb{1} = \mathbb{q}\Big(\frac{1}{|\mathbb{q}|^2}\bar{\mathbb{q}}\Big).$$

Sembrerà paradossale che in $\mathbb{H}$ esistano almeno sei quaternioni il cui quadrato è $-\mathbb{1}$: $\mathbb{i}$, $-\mathbb{i}$, $\mathbb{j}$, $-\mathbb{j}$, $\mathbb{k}$ e $-\mathbb{k}$. Di fatto ne esistono infiniti. Se infatti calcoliamo a partire da $\mathbb{q} = a\mathbb{1} + b\,\mathbb{i} + c\,\mathbb{j} + d\mathbb{k}$, abbiamo

$$\begin{aligned}
\mathbb{q}^2 &= a\mathbb{1}a\mathbb{1} + a\mathbb{1}b\,\mathbb{i} + a\mathbb{1}c\,\mathbb{j} + a\mathbb{1}d\mathbb{k} + \\
&\quad\; b\,\mathbb{i}\,a\mathbb{1} + b\,\mathbb{i}\,b\,\mathbb{i} + b\,\mathbb{i}\,c\,\mathbb{j} + b\,\mathbb{i}\,d\mathbb{k} + \\
&\quad\; c\,\mathbb{j}\,a\mathbb{1} + c\,\mathbb{j}\,b\,\mathbb{i} + c\,\mathbb{j}\,c\,\mathbb{j} + c\,\mathbb{j}\,d\mathbb{k} + \\
&\quad\; d\mathbb{k}a\mathbb{1} + d\mathbb{k}b\,\mathbb{i} + d\mathbb{k}c\,\mathbb{j} + d\mathbb{k}d\mathbb{k} \\
&= a^2\mathbb{1} + ab\,\mathbb{i} + ac\,\mathbb{j} + ad\mathbb{k} + \\
&\quad\; ab\,\mathbb{i} - b^2\mathbb{1} + bc\mathbb{k} - bd\,\mathbb{j} + \\
&\quad\; ac\,\mathbb{j} - bc\mathbb{k} - c^2\mathbb{1} + cd\,\mathbb{i} + \\
&\quad\; ad\mathbb{k} + bd\,\mathbb{j} - cd\,\mathbb{i} - d^2\mathbb{1} \\
&= (a^2 - b^2 - c^2 - d^2)\mathbb{1} + 2ab\,\mathbb{i} + 2ac\,\mathbb{j} + 2ad\mathbb{k}.
\end{aligned}$$

Ponendo $\mathbb{q}^2 = -\mathbb{1}$, otteniamo il sistema

$$\begin{cases} a^2 - b^2 - c^2 - d^2 = -1 \\ ab = ac = ad = 0 \end{cases}$$

nel quale non si può avere $a \neq 0$; dunque $a = 0$ e quindi le soluzioni sono tutti i quaternioni $\mathbb{q} = b\,\mathbb{i} + c\,\mathbb{j} + d\,\mathbb{k}$ tali che
$$b^2 + c^2 + d^2 = 1,$$
cioè tutti i quaternioni con parte reale nulla e modulo 1. Non è una contraddizione che un'equazione "di secondo grado" abbia infinite soluzioni: siccome la moltiplicazione non è commutativa, alcuni fatti che valgono per i numeri reali o complessi non valgono per i quaternioni.

Moltiplichiamo fra loro due quaternioni con *parte reale* nulla:
$$\begin{aligned}(b\,\mathbb{i} + c\,\mathbb{j} + d\,\mathbb{k})&(b'\,\mathbb{i} + c'\,\mathbb{j} + d'\,\mathbb{k}) \\ &= -(bb' + cc' + dd')\mathbb{1} + (cd' - dc')\,\mathbb{i} + (db' - bd')\,\mathbb{j} + (bc' - cb')\,\mathbb{k}.\end{aligned}$$

Se identifichiamo il quaternione $b\,\mathbb{i} + c\,\mathbb{j} + d\,\mathbb{k}$ con il vettore dello spazio tridimensionale con la stessa espressione in termini dei tre vettori coordinati, abbiamo che il prodotto esprime nella parte reale l'opposto del prodotto scalare e, nella *parte vettoriale*, il prodotto esterno noto dalla fisica.

Questa proprietà permette di applicare il formalismo dei quaternioni allo studio dei campi elettromagnetici, ricavando formule compatte che sottolineano bene l'interazione fra potenziale elettrico, espresso da un quaternione reale, e vettore potenziale magnetico, espresso da un quaternione con parte reale nulla.

Un'altra interessante applicazione dei quaternioni è allo *spazio di Minkowski*, ambiente ideale per lo studio della relatività speciale: la parte reale rappresenta la coordinata temporale, la parte vettoriale le coordinate spaziali.

Dal punto di vista algebrico, i quaternioni permettono di dimostrare in modo molto elegante un teorema dovuto a Lagrange: *ogni intero positivo si può scrivere come somma di quattro quadrati di interi.*

Un risultato importante, dovuto a Hurwitz, mostra che i numeri complessi e i quaternioni sono le uniche strutture che estendono i numeri reali mantenendone le proprietà formali (esclusa la commutatività della moltiplicazione), a meno di isomorfismi. Esiste comunque un'altra estensione, gli *ottetti* di Cayley e Graves, dove però non vale più l'associatività della moltiplicazione.

Esempio. I quaternioni forniscono anche un gruppo dalle proprietà particolari: si prenda infatti
$$Q_8 = \{\mathbb{1}, -\mathbb{1}, \mathbb{i}, -\mathbb{i}, \mathbb{j}, -\mathbb{j}, \mathbb{k}, -\mathbb{k}\}.$$
È evidente dalle definizioni che il prodotto di due elementi di Q_8 appartiene a Q_8, che quindi è un sottogruppo di $\mathbb{H} \setminus \{0\}, \cdot$. L'ordine degli elementi è: 1 per $\mathbb{1}$, 2 per $-\mathbb{1}$, 4 per gli altri. Perciò i sottogruppi propri di Q_8 sono:
$$\begin{gathered}\{\mathbb{1}\}, \qquad \{\mathbb{1}, -\mathbb{1}\}, \\ \{\mathbb{1}, -\mathbb{1}, \mathbb{i}, -\mathbb{i}\}, \quad \{\mathbb{1}, -\mathbb{1}, \mathbb{j}, -\mathbb{j}\}, \quad \{\mathbb{1}, -\mathbb{1}, \mathbb{k}, -\mathbb{k}\}.\end{gathered}$$
Si verifica facilmente che $\{\mathbb{1}, -\mathbb{1}\}$ è normale in Q_8; $\{\mathbb{1}\}$ è normale; i sottogruppi di ordine 4 hanno indice 2, quindi sono normali. Dunque Q_8 è un gruppo non commutativo nel quale tutti i sottogruppi sono normali. □

Appendice B

Il Principio di induzione

Esistono proprietà riferite a numeri interi non negativi, cioè agli elementi di $\mathbb{N}$, che sono soddisfatte solo da alcuni numeri, altre che sono soddisfatte da tutti i numeri, altre da nessun numero. Consideriamo per esempio le seguenti proprietà:

(1) il numero n ha il quadrato che è uguale a 2;

(2) il cubo del numero n è compreso tra 50 e 100;

(3) la somma dei numeri $\leq n$ è uguale a $n(n+1)/2$.

È ben noto che la proprietà (1) non è soddisfatta da alcun numero intero, essendo la radice quadrata di 2 un numero irrazionale. La proprietà (2) è soddisfatta solo dal numero 4. La proprietà (3) è invece soddisfatta da ogni numero intero positivo. Ma come fare a provare quest'ultima affermazione?

Si potrebbe verificarla passo dopo passo partendo da $n = 0$, ma il tempo di una vita non basterebbe; si può avere un'idea brillante, come quella che ebbe Gauss bambino, quando il suo maestro diede come esercizio quello di calcolare la somma di 100 numeri interi. Proviamo con la somma dei primi cento interi: poiché $101 = 1+100 = 2+99 = 3+98 = \cdots$, e poiché ci sono 50 coppie di numeri la cui somma fa 101, il risultato è $101 \cdot 50 = 5050$. Si noti che $5050 = 100(100+1)/2$. Naturalmente questo ragionamento si può estendere a ogni intero pari e, con una leggera variante, si applica anche agli interi dispari.

A dire il vero, quel maestro assegnava problemi più difficili, del genere di calcolare $81297 + 81495 + 81693 + \cdots + 100899$ (questa è una progressione di 100 termini con differenza costante 198). L'idea per la soluzione veloce è la stessa; la si può modificare immaginando i numeri da sommare scritti due volte, ma in ordine inverso:

$$\begin{aligned} S &= 81297 + 81495 + 81693 + \cdots + 100701 + 100899, \\ S &= 100899 + 100701 + 100503 + \cdots + 81495 + 81297, \end{aligned}$$

osservando che la somma di ogni colonna è 182196 e che ci sono 100 colonne. Perciò $S = (182196 \cdot 100)/2 = 9109800$.

C'è però un altro modo per provare la proprietà (3), che funziona meglio di ogni altro per provare proprietà più complicate, come per esempio la seguente: la somma delle quarte potenze dei numeri $\le n$ è uguale a $n(n+1)(2n+1)(3n^2+3n-1)/30$.

Tale metodo si chiama *Principio di induzione* e ha due versioni.

Prima versione del Principio di induzione. *Sia* $\mathrm{P}(n)$ *una proprietà riferita al numero* $n \in \mathbb{N}$*. Se*
(a) $\mathrm{P}(0)$ *è vera (Base dell'induzione)*
e se
(b) *dato* $n \ge 0$*, da* $\mathrm{P}(n)$ *consegue* $\mathrm{P}(n+1)$ *(Passo induttivo)*
allora $\mathrm{P}(n)$ *è vera per tutti gli interi* $n \in \mathbb{N}$*.*

Dimostrazione. Se per assurdo $\mathrm{P}(n)$ non fosse vera per qualche intero positivo, sia n il minimo intero per cui $\mathrm{P}(n)$ non è vera. Risulta $n > 0$ per la Base dell'induzione, e $\mathrm{P}(n-1)$ è vera, per la minimalità di n; ma allora, per il Passo induttivo, anche $\mathrm{P}(n)$ è vera, da cui l'assurdo. □

Seconda versione del Principio di induzione. *Sia* $\mathrm{P}(n)$ *una proprietà riferita al numero* $n \in \mathbb{N}$*. Se*
(a) $\mathrm{P}(0)$ *è vera*
e se
(b) *dato* $n \ge 0$, $\mathrm{P}(k)$ *vera per ogni* $k \le n$ *implica che* $\mathrm{P}(n+1)$ *è vera,*
allora $\mathrm{P}(n)$ *è vera per tutti gli interi* $n \in \mathbb{N}$*.*

Evidentemente le due versioni del Principio di induzione sono equivalenti; esistono situazioni per le quali la seconda versione si presta meglio della prima per dimostrare certe proprietà (si veda l'Esempio 5).

Il Principio di induzione può essere formulato a partire da un minimo intero (anche negativo) n_0, nel qual caso la Base dell'induzione sarà:
(a) $\mathrm{P}(n_0)$ è vera
e il Passo induttivo sarà:
(b) dato $n \ge n_0$, da $\mathrm{P}(n)$ consegue $\mathrm{P}(n+1)$;
come risultato si ha che $\mathrm{P}(n)$ è vera per ogni $n \ge n_0$ (si veda l'Esempio 3).

Mostriamo su alcuni esempi come funziona il Principio di induzione, e invitiamo il lettore a cimentarsi su vari Esercizi forniti al termine di questa Appendice, che sono tra i più comuni delle centinaia di esercizi disponibili.

Esempio 1. Proviamo la proprietà (3) vista all'inizio di questa Appendice: la somma dei numeri $\le n$ è uguale a $n(n+1)/2$.

Per $n = 0$ è banalmente vera. Supponiamo sia vera per n: $\sum_{k\le n} k = n(n+1)/2$; allora

$$\sum_{k\le n+1} k = \frac{n(n+1)}{2} + (n+1) = (n+1)\left(\frac{n}{2}+1\right) = \frac{(n+1)(n+2)}{2}.$$

Pertanto il passo induttivo è provato e la proprietà è vera per tutti gli interi non negativi. □

Esempio 2. Si provi che per ogni $n \geq 0$ risulta: $2^0 + 2^1 + 2^2 + \ldots + 2^n = 2^{n+1} - 1$.

Per $n = 0$ l'uguaglianza è banalmente vera. Supponiamo sia vero che $\sum_{0\leq k\leq n} 2^k = 2^{n+1} - 1$; allora $\sum_{0\leq k\leq n+1} 2^k = 2^{n+1} - 1 + 2^{n+1} = 2 \cdot 2^{n+1} - 1 = 2^{n+2} - 1$. Pertanto il passo induttivo è provato e l'uguaglianza è vera per tutti gli interi non negativi. □

Esempio 3. Si provi che $2^n \geq n^3$ $(n \geq 0)$ se e solo se $n = 0$, $n = 1$, oppure $n \geq 10$.

È facile verificare con calcoli diretti che la disuguaglianza vale per $n = 0$ e $n = 1$, e che non vale per $n = 2, 3, 4, 5, 6, 7, 8, 9$. Proviamo come Base dell'induzione che vale per $n = 10$; si ha infatti $2^{10} = 1.024 > 10^3$. Sia allora $n \geq 10$, la disuguaglianza vera per n e proviamola per $n + 1$. Si ha: $2^{n+1} = 2^n + 2^n \geq n^3 + n^3 > (n+1)^3$, come si voleva dimostrare. Si noti che l'ultima disuguaglianza stretta dipende dal fatto che $n^3 > 3n^2 + 3n + 1$ vale per ogni $n > 3$ (fatto che si può pure dimostrare per induzione). □

Esempio 4. Per ogni $n, k \geq 0$ si definiscono i coefficienti binomiali nel modo seguente:

$$\binom{n}{0} = 1, \qquad \binom{0}{k} = 0, \qquad \binom{n}{1} = n \text{ se } n \geq 1, \qquad \binom{n}{k} = 0 \text{ se } k \geq n+1,$$

e, se $1 \leq k \leq n$, si definisce induttivamente

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

Si provi per induzione su n che $\sum_{0\leq k\leq n} \binom{n}{k} = 2^n$. □

In questo libro il Principio di induzione è prevalentemente usato per provare che matrici di ordine arbitrario soddisfacenti a date condizioni verificano a certe proprietà. Poichè le matrici 1×1 sono assimilabili ai numeri, le proprietà considerate risultano spesso banali nel caso $n = 1$ (Base dell'induzione), per cui la parte centrale delle dimostrazioni consiste nel provare che se le matrici $n \times n$ soddisfacenti alle condizioni date godono delle proprietà richieste, ciò accade anche per le matrici $(n+1) \times (n+1)$ soddisfacenti alle stesse condizioni.

Come esempio che prelude a questa tecnica dimostrativa diamo un risultato provato da Frobenius e König per le matrici, che viene qui riformulato in modo più immediato.

Esempio 5. Un quadrato $\mathbf{Q}$ contiene n^2 tessere, disposte in n righe e in n colonne; le tessere sono o di colore bianco o di colore nero. Si chiama "serpente" un insieme di n tessere scelte in modo che ogni riga e ogni colonna ne contenga una. Si provi per induzione su n che, se ogni serpente contiene una tessera nera, allora esistono s righe e t colonne, con $s + t = n + 1$, tali che nelle loro intersezioni ci sono solo tessere nere (vale anche il viceversa).

L'asserto è banalmente vero per $n = 1$; assumiamolo vero per n e proviamo che è vero anche per $n + 1$. Se ci sono solo tessere nere l'asserto è ancora banalmente vero. Supponiamo quindi che all'incrocio della riga i_0-esima e della colonna j_0-esima ci sia una tessera bianca. Osserviamo preliminarmente che, se cambiamo l'ordine delle righe o l'ordine delle colonne, un insieme di n tessere che forma un serpente resta tale dopo questi cambiamenti. Se eliminiamo la riga i_0-esima e la colonna j_0-esima, nelle righe e colonne restanti, che formano un sottoquadrato $\mathbf{Q}_1$, ogni serpente ha ancora necessariamente una tessera nera. Per l'Ipotesi induttiva esistono s_0 righe e t_0 colonne del sottoquadrato $\mathbf{Q}_1$, con $s_0 + t_0 = (n-1)+1 = n$, nelle cui intersezioni ci sono solo tessere nere. Possiamo a questo punto cambiare l'ordine delle righe e delle colonne del quadrato originario $\mathbf{Q}$ in modo che le tessere nere individuate stiano tutte nell'angolo in alto a destra, formando un sottorettangolo tutto nero con s_0 righe e t_0 colonne. Chiamiamo $\mathbf{Q}^*$ il quadrato così ottenuto. Le prime s_0 righe e s_0 colonne di $\mathbf{Q}^*$ si intersecano in un quadrato $\mathbf{X}^*$, mentre le ultime t_0 righe e t_0 colonne di $\mathbf{Q}^*$ si intersecano in un secondo quadrato $\mathbf{Y}^*$. Dal fatto che il quadrato $\mathbf{Q}^*$ gode della proprietà che ogni serpente nel quadrato contiene una tessera nera discende che tale proprietà deve essere soddisfatta o dal quadrato $\mathbf{X}^*$ o dal quadrato $\mathbf{Y}^*$; supponiamo che sia $\mathbf{X}^*$ il quadrato in questione.

Usando la Seconda versione del Principio di induzione, supponiamo che, sotto le opportune ipotesi, l'asserto valga per i quadrati con k righe e colonne di tessere, per ogni $k \le n-1$, e quindi che anche nel quadrato $\mathbf{X}^*$ esistano s_1 righe e t_1 colonne, con $s_1 + t_1 = s_0 + 1$, nelle cui intersezioni ci sono solo tessere nere. Cambiamo nuovamente l'ordine delle prime s_0 righe e delle prime s_0 colonne di $\mathbf{Q}^*$, in modo da portare in alto a sinistra nel sottoquadrato $\mathbf{X}^*$ le tessere nere così individuate. Otteniamo un terzo quadrato $\mathbf{Q}^{**}$ con n^2 tessere, che ha un rettangolo tutto nero in alto a destra formato dalla intersezione delle prime s_1 righe e delle ultime $t_1 + t_0$ colonne. Ma $s_1 + t_1 + t_0 = s_0 + 1 + t_0 = n+1$, perciò abbiamo provato l'asserto per il quadrato $\mathbf{Q}^{**}$. Effettuando i cambiamenti d'ordine delle righe e delle colonne inversi di quelli che ci hanno portato prima da $\mathbf{Q}$ a $\mathbf{Q}^*$ e poi da $\mathbf{Q}^*$ a $\mathbf{Q}^{**}$, riotteniamo il quadrato $\mathbf{Q}$ in cui all'incrocio delle righe e delle colonne corrispondenti alle prime s_1 righe e alle ultime $t_1 + t_0$ colonne di $\mathbf{Q}^{**}$ ci sono tessere nere. □

Esercizi

1. Sia $\{X_i\}_{1\le i\le n}$ una famiglia di n sottoinsiemi di un insieme finito X. Denotando con $|X_i|$ il numero di elementi di ciascun insieme X_i, si provi per induzione su n che

$$\Big|\bigcup_{i\le n} X_i\Big| = \sum_{i\le n} |X_i| - \sum_{i<j\le n} |X_i \cap X_j| + \sum_{i<j<k\le n} |X_i \cap X_j \cap X_k| - \cdots + (-1)^n \Big|\bigcap_{i\le n} X_i\Big|.$$

2. Si provi per induzione su n che il numero di sottoinsiemi di un insieme con n elementi è uguale a 2^n.

3. Provare per induzione su n che la somma dei quadrati dei primi n interi positivi è uguale a

$$\frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n.$$

4. Provare per induzione su n che la somma dei cubi dei primi n interi positivi è uguale a

$$\frac{1}{4}n^4 + \frac{1}{2}n^3 + \frac{1}{4}n^2.$$

5. Provare per induzione su $n \geq 1$ la proprietà (4) enunciata all'inizio di questa Appendice: la somma delle quarte potenze dei numeri $\leq n$ è uguale a

$$\frac{n(n+1)(2n+1)(3n^2+3n-1)}{30} = \frac{1}{5}n^5 + \frac{1}{2}n^4 + \frac{1}{3}n^3 + \frac{1}{4}n^2 - \frac{1}{30}n.$$

6. Trovare il "baco" nel ragionamento seguente, che prova per induzione il fatto che, prese comunque n persone, esse hanno lo stesso nome.

L'asserto è banalmente vero per $n = 1$. Sia $n > 1$ e l'asserto vero per $n-1$. Prese n persone, mettiamole in ordine. Le prime $n-1$ hanno tutte lo stesso nome, come pure le ultime $n-1$; ma allora hanno lo stesso nome a partire dalla seconda e fino alla $n-1$-esima, quindi anche la prima e l'ultima hanno lo stesso nome.

7. Data la funzione $f\colon \mathbb{R} \to \mathbb{R}$ definita da $f(x) = 1 + 2x$, sia f^n la funzione ottenuta componendo f con sé stessa n volte. Si provi per induzione su n che $f^n(x) = 2^n(1 + x) - 1$.

8. Si provi per induzione su n che, per ogni $n \geq 1$, $1 + 3 + 5 + \cdots + (2n-1) = n^2$ e $2 + 4 + 6 + \cdots + 2n = n(n+1)$.

9. Si provi per induzione su $n \geq 1$ che il numero che ha n cifre uguali a 9 coincide con $10^n - 1$.

10. Nelle ipotesi e nella terminologia dell'Esempio 5, si provi per induzione su n che esistono $n!$ serpenti nel quadrato $\mathbf{Q}$. Si dica poi qual è il numero minimo di tessere nere che deve avere il quadrato affinché ogni serpente contenga una tessera nera.

Appendice C

Interpretazione geometrica di $\mathbb{R}^2$ ed $\mathbb{R}^3$

Fissato su di un piano un sistema di riferimento ortogonale e monometrico Oxy, ogni punto P del piano è completamente individuato dalla coppia ordinata di numeri reali (a, b), dove

$$a = x_P = \text{ascissa di } P \text{ e}$$
$$b = y_P = \text{ordinata di } P.$$

Resta quindi definita una corrispondenza biunivoca φ tra $\mathbb{R}^2$ e l'insieme π dei punti del piano:

$$\varphi\colon \mathbb{R}^2 \to \pi$$
$$\begin{bmatrix} a \\ b \end{bmatrix} \mapsto P$$

dove P è il punto di ascissa $x_P = a$ e ordinata $y_P = b$.

Per visualizzare il punto P si identifica P con il segmento orientato $\overrightarrow{OP}$, rappresentato nel piano da una freccia uscente da O con la punta in P (si veda la Figura C.1). Si dice che $\overrightarrow{OP}$ è un vettore applicato nel punto O.

A che cosa corrispondono i sottospazi di dimensione 1 di $\mathbb{R}^2$ nella corrispondenza φ?

Un sottospazio W di $V = \mathbb{R}^2$ ha dimensione 1 se è del tipo $W = \langle \mathbf{v} \rangle = \{\alpha \mathbf{v} \mid \alpha \in \mathbb{R}\}$ con $\mathbf{v} = [a\ b]^T \neq \mathbf{0}$. Con le notazioni adottate precedentemente siano P il punto che corrisponde al vettore $\mathbf{v}$ (per cui $\varphi(\mathbf{v}) = P$) ed r la retta uscente da O e passante per P. Il punto O divide r in due semirette, delle quali una contiene P e l'altra no. È noto che l'equazione di r è $ay = bx$, pertanto per ogni $\alpha \in \mathbb{R}$ si ha

$$\alpha \mathbf{v} = \alpha \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} \alpha a \\ \alpha b \end{bmatrix} \xleftrightarrow{\text{corrisponde a}} Q \xleftrightarrow{\text{visualizzato da}} \overrightarrow{OQ}$$

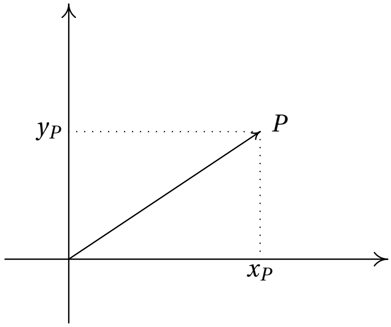


Figura C.1: Vettore applicato nel punto O

dove Q è il punto di ascissa $x_Q = \alpha a$ e ordinata $y_Q = \alpha b$ e dove il punto Q si trova sulla retta r (infatti $a y_Q = a(\alpha b) = b(\alpha a) = b x_Q$).

Più precisamente, se $d = \sqrt{|a|^2 + |b|^2}$ è la distanza di P da O, allora

Q è il punto di r che si trova a distanza $\sqrt{|\alpha a|^2 + |\alpha b|^2} = |\alpha| d$ da O,

- *sulla semiretta a cui appartiene anche il punto P se $\alpha \geq 0$,*
- *sulla semiretta opposta a quella a cui appartiene il punto P se $\alpha \leq 0$.*

Quindi i sottospazi di dimensione 1 di $\mathbb{R}^2$ corrispondono alle rette del piano uscenti dall'origine di un sistema di riferimento su di esso fissato.

A che cosa corrispondono le rette del piano che non passano per O?

Se s è una retta che non passa per O la sua equazione è del tipo $y = mx + q$ con $q \neq 0$ oppure $x = q$ con $q \neq 0$.

Nel primo caso (equazione di s: $y = mx + q$ con $q \neq 0$) un punto P del piano appartiene a s se e solo se le sue coordinate cartesiane (x_P, y_P) soddisfano l'uguaglianza $y_P = m x_P + q$, quindi se e solo se si ha

$$\begin{bmatrix} x_P \\ y_P \end{bmatrix} = \begin{bmatrix} x_P \\ m x_P + q \end{bmatrix} = \begin{bmatrix} 0 \\ q \end{bmatrix} + \begin{bmatrix} x_P \\ m x_P \end{bmatrix} = \begin{bmatrix} 0 \\ q \end{bmatrix} + x_P \begin{bmatrix} 1 \\ m \end{bmatrix}.$$

Pertanto se $\mathbf{u} = [0\ q]^T$ e $W = \langle [1\ m]^T \rangle$ è il sottospazio di $\mathbb{R}^2$ generato da $[1\ m]^T$, l'insieme dei vettori che corrisponde a s è

$$\{\mathbf{u} + \mathbf{w} \mid \mathbf{w} \in W\}.$$

Esso si indica con il simbolo $\mathbf{u} + W$, e si chiama il laterale di W di rappresentante $\mathbf{u}$ (si faccia attenzione al fatto che $\mathbf{u}$ è un vettore di $\mathbb{R}^2$ e W è un sottospazio di dimensione 1 di $\mathbb{R}^2$).

Nel secondo caso (equazione di s: $x = q$ con $q \neq 0$) un punto P del piano appartiene a s se e solo se le sue coordinate cartesiane (x_P, y_P) soddisfano l'uguaglianza $x_P = q$, quindi se e solo se si ha

$$\begin{bmatrix} x_P \\ y_P \end{bmatrix} = \begin{bmatrix} q \\ y_P \end{bmatrix} = \begin{bmatrix} q \\ 0 \end{bmatrix} + y_P \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Pertanto se $\mathbf{u}' = [q\ 0]^T$ e $W' = \langle [0\ 1]^T \rangle$ è il sottospazio di $\mathbb{R}^2$ generato da $[0\ 1]^T$, l'insieme dei vettori che corrisponde a s è

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

ossia il laterale di W' di rappresentante $\mathbf{u}'$.

Analogamente al caso del piano, fissando nello spazio tridimensionale un sistema di riferimento ortogonale e monometrico $Oxyz$, ogni punto P dello spazio è completamente individuato da una terna ordinata di numeri reali (a, b, c) (si veda la Figura C.2). Resta quindi definita una corrispondenza biunivoca tra $\mathbb{R}^3$ e lo spazio tridimensionale e si ha:

$$\mathbf{v} = \begin{bmatrix} a \\ b \\ c \end{bmatrix} \xleftrightarrow{\text{corrisponde a}} P \xleftrightarrow{\text{visualizzato da}} \overrightarrow{OP}$$

dove P è il punto di coordinate $x_P = a$, $y_P = b$, $z_P = c$ e dove O è l'origine degli assi del sistema di riferimento.

La distanza di P da O è $d = \sqrt{|a|^2 + |b|^2 + |c|^2}$, lunghezza di $\overrightarrow{OP}$.

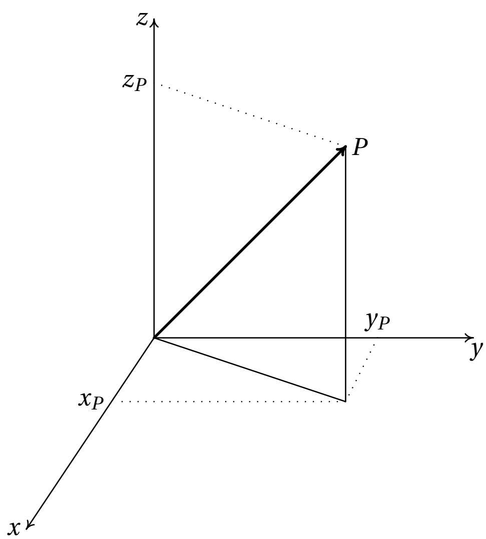


Figura C.2: Vettori nello spazio

Come nel caso di $\mathbb{R}^2$, una retta r passante per O è completamente individuata da un vettore $\mathbf{v} \neq \mathbf{0}$ che ne dà la "direzione".

Se P è un punto di r diverso da O e $\mathbf{v} \neq \mathbf{0}$ è il vettore corrispondente a P, ogni altro punto Q di r corrisponde a un vettore del tipo $\alpha\mathbf{v}$ con $\alpha \in \mathbb{R}$, per cui r corrisponde al sottospazio $\langle \mathbf{v} \rangle$ di $\mathbb{R}^3$ di dimensione 1.

Una retta s che non contiene l'origine O del sistema di riferimento corrisponde invece a un insieme del tipo

$$\mathbf{u} + W = \{\mathbf{u} + \mathbf{w} \mid \mathbf{w} \in W\}$$

dove W è un sottospazio di dimensione 1 di $\mathbb{R}^3$.

A cosa corrispondono i sottospazi di dimensione 2?

Nel caso di $\mathbb{R}^2$ l'unico sottospazio di dimensione 2 è $\mathbb{R}^2$ stesso, e corrisponde all'intero piano.

Sia ora $U = \langle \mathbf{u}; \mathbf{v} \rangle$ un sottospazio di dimensione 2 di $\mathbb{R}^3$ e $Oxyz$ un fissato sistema di riferimento ortogonale e monometrico nello spazio. Se P e Q sono i punti che corrispondono ai due vettori $\mathbf{u}$ e $\mathbf{v}$ rispettivamente, allora

$$\mathbf{u} = \begin{bmatrix} x_P \\ y_P \\ z_P \end{bmatrix} \quad \text{e} \quad \mathbf{v} = \begin{bmatrix} x_Q \\ y_Q \\ z_Q \end{bmatrix}$$

dove (x_P, y_P, z_P) e (x_Q, y_Q, z_Q) sono le coordinate di P e Q rispetto a $Oxyz$.

È noto che il piano contenente i tre punti distinti O, P e Q ha un'equazione del tipo

$$ax + yb + cz = 0$$

con a, b, $c \in \mathbb{R}$ non tutti nulli. In particolare si ha che

$$ax_P + by_P + cz_P = 0 \quad \text{e} \quad ax_Q + by_Q + cz_Q = 0,$$

ossia, posto $\mathbf{n} = [a\ b\ c]^T \neq \mathbf{0}$, che

$$\mathbf{n}^T\mathbf{u} = \begin{bmatrix} a & b & c \end{bmatrix} \begin{bmatrix} x_P \\ y_P \\ z_P \end{bmatrix} = 0 \quad \text{e} \quad \mathbf{n}^T\mathbf{v} = \begin{bmatrix} a & b & c \end{bmatrix} \begin{bmatrix} x_Q \\ y_Q \\ z_Q \end{bmatrix} = 0.$$

Per ogni vettore $\mathbf{w} \in U = \langle \mathbf{u}; \mathbf{v} \rangle$ esistono $\alpha, \beta \in \mathbb{R}$ tali che $\mathbf{w} = \alpha\mathbf{u} + \beta\mathbf{v}$, per cui

$$\mathbf{n}^T\mathbf{w} = \mathbf{n}^T(\alpha\mathbf{u} + \beta\mathbf{v}) = \alpha\mathbf{n}^T\mathbf{u} + \beta\mathbf{n}^T\mathbf{v} = \alpha 0 + \beta 0 = 0.$$

Se R è il punto corrispondente a $\mathbf{w}$ e (x_R, y_R, z_R) sono le sue coordinate rispetto a $Oxyz$, da $\mathbf{w} = [x_R\ y_R\ z_R]^T$ e $\mathbf{n}^T\mathbf{w} = 0$ segue che

$$0 = \mathbf{n}^T\mathbf{w} = \begin{bmatrix} a & b & c \end{bmatrix} \begin{bmatrix} x_R \\ y_R \\ z_R \end{bmatrix} = ax_R + by_R + cz_R$$

e dunque R si trova sul piano individuato dai punti O, P e Q.

Viceversa, se R' è un punto del piano individuato dai punti O, P e Q, allora il vettore $\mathbf{w}' = [x_{R'}\ y_{R'}\ z_{R'}]^T$ che corrisponde a R' è soluzione dell'equazione del piano $ax + by + cz = 0$, ossia è un elemento dello spazio nullo $\mathrm{N}(\mathbf{A})$ della matrice $\mathbf{A} = [a\ b\ c]$.

Essendo $\mathbf{n}^T = \mathbf{A} = [a\ b\ c] \neq \mathbf{0}^T$, il rango di $\mathbf{A}$ è uguale a 1, per cui dal teorema nullità+ rango segue che la dimensione dello spazio nullo $\mathrm{N}(\mathbf{A})$ è

$$\dim(\mathrm{N}(\mathbf{A})) = \text{numero delle colonne di } \mathbf{A} - \text{rango di } \mathbf{A} = 3 - 1 = 2.$$

Poiché abbiamo già visto che $U \subseteq \mathrm{N}(\mathbf{A})$, e U ha dimensione 2, allora $U = \mathrm{N}(\mathbf{A})$ e $\mathbf{w}' \in \mathrm{N}(\mathbf{A}) = U$. Dunque i vettori che corrispondono ai punti del piano individuato da O, P e Q sono elementi dello spazio U.

Concludendo, a un sottospazio $U = \langle \mathbf{u}; \mathbf{v} \rangle$ di dimensione 2 corrisponde il piano contenente i punti O, P e Q, dove O è l'origine di un fissato sistema di riferimento, P è il punto corrispondente a $\mathbf{u}$ e Q è il punto corrispondente a $\mathbf{v}$.

Regola del parallelogramma

Siano $[a\ b]^T, [c\ d]^T \in \mathbb{R}^2$. In un piano in cui si sia fissato un sistema di riferimento ortogonale e monometrico siano P e Q i punti che corrispondono a $[a\ b]^T$ e $[c\ d]^T$ rispettivamente. Allora il punto R del piano che corrisponde a

$$\begin{bmatrix} a \\ b \end{bmatrix} + \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} a+c \\ b+d \end{bmatrix}$$

è il punto visualizzato dal segmento orientato che sia la diagonale del parallelogramma con lati $\overrightarrow{OP}$ e $\overrightarrow{OQ}$.

Sia L il punto di intersezione tra la retta passante per P parallela all'asse delle x e la retta passante per R parallela all'asse delle y. Sia H la proiezione di Q sull'asse delle x (si veda la Figura C.3).

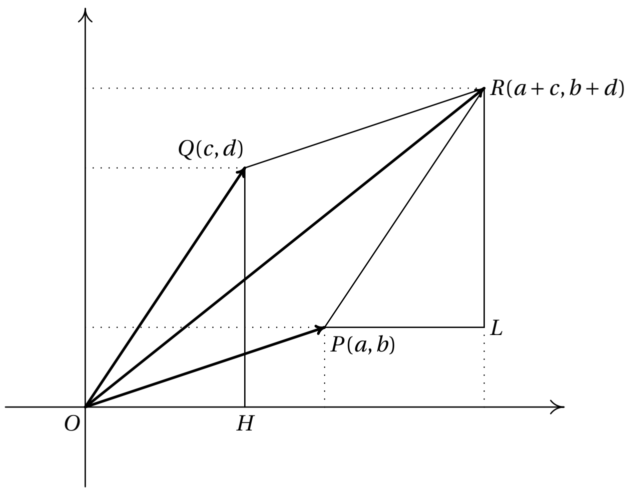


Figura C.3: Regola del parallelogramma

I due triangoli PRL e OQH, avendo lati corrispondenti paralleli per costruzione, e una coppia di lati corrispondenti ($\overrightarrow{PR}$ e $\overrightarrow{OQ}$) uguali, sono uguali. In particolare

$$d = |QH| = |RL| \quad \text{e} \quad c = |OH| = |PL|.$$

Dunque si ha:

$$\begin{aligned}&\text{l'ordinata di } R = (\text{l'ordinata di } P) + |RL| = b + d,\\ &\text{l'ascissa di } R = (\text{l'ascissa di } P) + |PL| = a + c.\end{aligned}$$

Appendice D

Teorema Fondamentale dell'Algebra ed esistenza di autovalori

Il Teorema Fondamentale dell'Algebra dice che ogni polinomio a coefficienti complessi che non sia una costante ha una radice complessa. Ciò si esprime dicendo che il campo dei numeri complessi $\mathbb{C}$ è *algebricamente chiuso*.

La prima dimostrazione del Teorema Fondamentale dell'Algebra venne data nel 1799 da Gauss nella sua tesi di laurea. Nel 1814 Argand ne dette una seconda dimostrazione basata su una prova difettosa di d'Alembert. La storia successiva delle molteplici dimostrazioni del teorema, di carattere topologico, analitico ed algebrico, si può trovare in una serie di articoli apparsi sulla rivista American Math. Monthly, di cui elenchiamo autore, numero del volume, anno e pagine: B. H. Arnold, 56 (1949), 465–466; S. Stein, 61 (1954), 109; H. Zassenhaus, 74 (1967), 485–497; F. Terkelsen, 83 (1976), 647. Per un'altra dimostrazione di tipo algebrico che fa uso della teoria di Galois si veda l'articolo di L. Horowitz su Nieuw Arch. Wisk. (3) 14 (1966), 95–96. Nel 1997 è uscito un libro di B. Fine e G. Rosenberg (Springer-Verlag) che raccoglie varie dimostrazioni del teorema.

Il Teorema Fondamentale dell'Algebra è indispensabile in Algebra Lineare quando si trattano gli autovalori di matrici complesse. Esso assicura infatti che tali matrici possiedono sempre un autovalore complesso, con relativo autovettore a coordinate complesse. Da ciò discende facilmente che una matrice complessa di ordine n ha esattamente n autovalori complessi, contati con le rispettive molteplicità algebriche.

In questa Appendice daremo una dimostrazione del Teorema Fondamentale dell'Algebra provando, con i soli strumenti dell'Algebra Lineare ed usando fatti elementari sui polinomi reali e sui numeri complessi, che ogni matrice complessa quadrata ha un autovalore. Che ciò implichi il Teorema Fondamentale dell'Algebra, e quindi sia ad esso equivalente, è provato di seguito.

Proposizione 1. *Se ogni matrice complessa quadrata ha un autovalore, allora vale il Teorema Fondamentale dell'Algebra.*

Dimostrazione. Sia $f(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0 \in \mathscr{P}(\mathbb{C})$. Si consideri la cosiddetta *matrice compagna* di $f(X)$:

$$\mathbf{A} = \begin{bmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & \ldots & 0 & -a_2 \\ \vdots & \vdots & \ldots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -a_{n-1} \end{bmatrix}.$$

Un calcolo immediato mostra che il polinomio caratteristico $p_{\mathbf{A}}(X)$ di $\mathbf{A}$ coincide con $(-1)^n f(X)$ (si veda l'Esercizio 4.18). Per ipotesi, $\mathbf{A}$ ha un autovalore, che è una radice di $p_{\mathbf{A}}(X) = -f(X)$. □

Vogliamo allora dimostrare il seguente risultato.

Teorema 2. *Ogni matrice complessa quadrata ha un autovalore.*

La trattazione che segue è dedotta dall'articolo di H. Derksen: "The Fundamental Theorem of Algebra and Linear Algebra", apparso sull'American Math. Monthly, 110 (2003), 620–623. I due fatti elementari ricordati sopra che useremo sono

(I) l'esistenza di radici reali di polinomi reali di grado dispari;

(II) l'esistenza di radici quadrate di numeri complessi:

$$z = a + ib = \left[\left(\frac{|z|+a}{2}\right)^{1/2} \pm i\left(\frac{|z|-a}{2}\right)^{1/2}\right]^2$$

dove vale il segno + se $b \geq 0$ e vale il segno − se $b < 0$.

L'idea alla base della dimostrazione è di fare induzione sul massimo intero k tale che 2^k divide l'ordine n della matrice. Pertanto inizialmente si mostra che ogni matrice complessa di ordine dispari (caso $k = 0$) ha un autovalore (Proposizione 5). Per far questo si prova preliminarmente che due matrici reali di ordine dispari che commutano hanno un autovettore a coordinate reali in comune (Corollario 4).

Si procede poi per induzione su k, utilizzando anche in questo caso un risultato (si veda il seguente Lemma 3) sull'esistenza di un autovettore comune a due matrici complesse che commutano, sotto una opportuna ipotesi di esistenza di autovalori.

Come in precedenza, il simbolo K denoterà un campo che potrà essere sia quello $\mathbb{R}$ dei reali o quello $\mathbb{C}$ dei complessi. Ricordiamo che un'applicazione lineare di uno spazio vettoriale in sé stesso si chiama anche endomorfismo.

Lemma 3. *Siano* $\mathbf{A}$ *e* $\mathbf{B}$ *due matrici di ordine n a coefficienti in un campo K che commutano, e sia d un intero che non divide n. Se tutte le matrici a coefficienti in K di ordine non divisibile per d hanno un autovalore in K, allora* $\mathbf{A}$ *e* $\mathbf{B}$ *hanno un autovettore in comune in K^n.*

Dimostrazione. Ragioniamo per induzione su n. Per $n = 1$ l'asserto è banale. Sia $n > 1$ e l'asserto vero per ogni $m < n$ non divisibile per d. Per ipotesi $\mathbf{A}$ e $\mathbf{B}$ hanno un autovalore in K. Sia $\lambda \in K$ un autovalore di $\mathbf{A}$ con relativo autovettore $\mathbf{v} \in K^n$. Denotiamo con V l'autospazio $\mathrm{E}_{\mathbf{A}}(\lambda)$ e con W il sottospazio $\mathrm{Im}(\mathbf{A} - \lambda I)$ di K^n. Siano m ed r le dimensioni rispettivamente di V e W. Per il Teorema nullità + rango, risulta $m + r = n$.

Se $V = K^n$ la conclusione segue banalmente: ogni autovettore di $\mathbf{B}$ è anche autovettore di $\mathbf{A}$. Sia allora $V \neq K^n$; quindi risulta $m < n$ ed $r < n$, ed uno dei due tra m ed r non è divisibile per d. È immediato verificare che, siccome $\mathbf{A}$ e $\mathbf{B}$ commutano, dal fatto che V e W sono $\mathbf{A}$-invarianti segue che V e W sono $\mathbf{B}$-invarianti.

Supponiamo da prima che d non divida m; in maniera del tutto analoga si ragiona se d non divide r, utilizzando lo spazio W anziché lo spazio V. Esiste un isomorfismo di K-spazi vettoriali $\varphi\colon K^m \to V$. Se, come al solito, $f_{\mathbf{A}}$ denota l'endomorfismo di V indotto dalla moltiplicazione per la matrice $\mathbf{A}$, l'omomorfismo composto $\varphi^{-1} f_{\mathbf{A}} \varphi\colon K^m \to K^m$ è indotto (rispetto alle basi canoniche) da una matrice $m \times m$ $\mathbf{A}_0$, cioè risulta (identificando $\mathbf{A}_0$ con la pre-moltiplicazione in K^m per tale matrice):

$$\varphi^{-1} f_{\mathbf{A}} \varphi = \mathbf{A}_0$$

e analogamente, giacché V è $\mathbf{B}$-invariante:

$$\varphi^{-1} f_{\mathbf{B}} \varphi = \mathbf{B}_0$$

per una opportuna matrice $m \times m$ $\mathbf{B}_0$. Proviamo che $\mathbf{A}_0$ e $\mathbf{B}_0$ commutano:

$$\begin{aligned}\mathbf{A}_0\mathbf{B}_0 &= \varphi^{-1} f_{\mathbf{A}} \varphi \varphi^{-1} f_{\mathbf{B}} \varphi = \varphi^{-1} f_{\mathbf{A}} f_{\mathbf{B}} \varphi \\ &= \varphi^{-1} f_{\mathbf{B}} f_{\mathbf{A}} \varphi = \varphi^{-1} f_{\mathbf{B}} \varphi \varphi^{-1} f_{\mathbf{A}} \varphi = \mathbf{B}_0\mathbf{A}_0.\end{aligned}$$

Poiché d non divide m, $\mathbf{A}_0$ e $\mathbf{B}_0$ hanno entrambi per ipotesi un autovalore in K. Per l'ipotesi induttiva, $\mathbf{A}_0$ e $\mathbf{B}_0$ hanno un autovettore in comune $\mathbf{v}_0 \in K^m$:

$$\mathbf{A}_0\mathbf{v}_0 = \alpha\mathbf{v}_0, \qquad \mathbf{B}_0\mathbf{v}_0 = \beta\mathbf{v}_0,$$

dove $\alpha, \beta \in K$ (in realtà, in questo caso in cui d non divide m e si usa lo spazio V, $\alpha = \lambda$ e $\mathbf{A}_0 = \lambda\mathbf{I}_m$, si veda l'Esercizio 1; però ciò non accade quando si ragiona sostituendo V con W nel caso in cui d non divide r). Ne consegue:

$$\begin{aligned}\mathbf{A}\varphi(\mathbf{v}_0) &= (\varphi\mathbf{A}_0\varphi^{-1})(\varphi(\mathbf{v}_0)) = \varphi(\mathbf{A}_0\mathbf{v}_0) = \alpha(\varphi(\mathbf{v}_0)) \\ \mathbf{B}\varphi(\mathbf{v}_0) &= (\varphi\mathbf{B}_0\varphi^{-1})(\varphi(\mathbf{v}_0)) = \varphi(\mathbf{B}_0\mathbf{v}_0) = \beta(\varphi(\mathbf{v}_0)).\end{aligned}$$

Pertanto $\varphi(\mathbf{v}_0)$ è un autovettore comune di $\mathbf{A}$ e $\mathbf{B}$. □

Faremo uso due volte del Lemma 3: una prima volta ponendo $K = \mathbb{R}$ e $d = 2$, ottenendo in modo immediato il seguente Corollario 4; una seconda volta ponendo $K = \mathbb{C}$ e $d = 2^k$, dove k denoterà un intero ≥ 1, nella dimostrazione del Teorema 2.

Corollario 4. *Due matrici reali di ordine dispari che commutano hanno un autovettore a coordinate reali in comune.*

Dimostrazione. Si ponga $K = \mathbb{R}$, $d = 2$ nel Lemma 3 e si ricordi che vale il fatto (I). $\square$

Il risultato analogo al Corollario 4 per matrici reali di ordine pari non vale (si veda l'Esercizio 4). Il Corollario 4 interviene nella dimostrazione della seguente proposizione.

Proposizione 5. *Ogni matrice complessa* $\mathbf{A}$ *di ordine n dispari ha un autovalore.*

Dimostrazione. Sia H lo spazio vettoriale su $\mathbb{R}$ formato dalle matrici complesse hermitiane di ordine n. È facile verificare (si veda l'Esercizio 2) che la dimensione di H è n^2, e quindi è dispari. Definiamo due endomorfismi τ e σ di H nel modo seguente:

$$\tau(\mathbf{B}) = \frac{1}{2}(\mathbf{AB} + \mathbf{BA}^H), \quad \sigma(\mathbf{B}) = \frac{1}{2i}(\mathbf{AB} - \mathbf{BA}^H)$$

per ogni $\mathbf{B} \in H$. È immediato verificare che $\tau(\mathbf{B})$ e $\sigma(\mathbf{B})$ sono matrici hermitiane se $\mathbf{B}$ lo è. Sia $\varepsilon\colon \mathbb{R}^{n^2} \to H$ un isomorfismo di spazi vettoriali reali. Allora $\varepsilon^{-1}\tau\varepsilon$ e $\varepsilon^{-1}\sigma\varepsilon$ sono due endomorfismi di $\mathbb{R}^{n^2}$, quindi risulterà

$$\varepsilon^{-1}\tau\varepsilon = \mathbf{T}, \quad \varepsilon^{-1}\sigma\varepsilon = \mathbf{S}$$

con $\mathbf{T}$ ed $\mathbf{S}$ opportune matrici reali di ordine n^2 (identificando $\mathbf{T}$ ed $\mathbf{S}$ con la pre-moltiplicazione in $\mathbb{R}^{n^2}$ per tali matrici). Se $\mathbf{B} \in H$ risulta:

$$\tau(\mathbf{B}) = (\varepsilon\mathbf{T}\varepsilon^{-1})(\mathbf{B}), \quad \sigma(\mathbf{B}) = (\varepsilon\mathbf{S}\varepsilon^{-1})(\mathbf{B}).$$

Proviamo che le due matrici $\mathbf{T}$ ed $\mathbf{S}$ commutano. A tal fine è sufficiente provare che $\tau\sigma = \sigma\tau$. Se allora $\mathbf{B} \in H$ risulta:

$$\begin{aligned}
\tau(\sigma(\mathbf{B})) &= \tau\left(\frac{1}{2i}(\mathbf{AB} - \mathbf{BA}^H\right) \\
&= \frac{1}{2}\left(\mathbf{A}\frac{1}{2i}(\mathbf{AB} - \mathbf{BA}^H) + \frac{1}{2i}(\mathbf{AB} - \mathbf{BA}^H)\mathbf{A}^H\right) \\
&= \frac{1}{4i}(\mathbf{A}^2\mathbf{B} - \mathbf{B}(\mathbf{A}^H)^2)
\end{aligned}$$

e similmente

$$\begin{aligned}
\sigma(\tau(\mathbf{B})) &= \sigma\left(\frac{1}{2}(\mathbf{AB} + \mathbf{BA}^H)\right) \\
&= \frac{1}{2i}\left(\mathbf{A}\frac{1}{2}(\mathbf{AB} + \mathbf{BA}^H) - \frac{1}{2}(\mathbf{AB} + \mathbf{BA}^H)\mathbf{A}^H\right) \\
&= \frac{1}{4i}(\mathbf{A}^2\mathbf{B} - \mathbf{B}(\mathbf{A}^H)^2).
\end{aligned}$$

Il Corollario 4 assicura che le matrici $\mathbf{T}$ ed $\mathbf{S}$ hanno un autovettore $\mathbf{v} \in \mathbb{R}^{n^2}$ in comune, cioè risulta

$$\mathbf{Tv} = a\mathbf{v}, \quad \mathbf{Sv} = b\mathbf{v}$$

per opportuni numeri reali a e b. Detta $\mathbf{C}$ la matrice hermitiana corrispondente all'autovettore $\mathbf{v}$ tramite l'isomorfismo ε, si ha:

$$\begin{aligned}
\mathbf{AC} &= \frac{1}{2}(\mathbf{AC}+\mathbf{CA}^H) + i\left(\frac{1}{2i}(\mathbf{AC}-\mathbf{CA}^H)\right)\\
&= \tau(\mathbf{C}) + i\sigma(\mathbf{C}) = (\varepsilon\mathbf{T}\varepsilon^{-1})(\mathbf{C}) + i(\varepsilon\mathbf{S}\varepsilon^{-1})(\mathbf{C})\\
&= \varepsilon(\mathbf{Tv}) + i\varepsilon(\mathbf{Sv}) = \varepsilon(a\mathbf{v}) + i\varepsilon(b\mathbf{v})\\
&= a\varepsilon(\mathbf{v}) + ib\varepsilon(\mathbf{v}) = (a+ib)\mathbf{C}.
\end{aligned}$$

Se ne deduce che ogni colonna non nulla di $\mathbf{C}$ (certamente esistente perché $\mathbf{C} = \varepsilon(\mathbf{v})$ e $\mathbf{v} \neq \mathbf{0}$) è un autovettore della matrice $\mathbf{A}$, con relativo autovettore il numero complesso $a+ib$. □

Possiamo ora passare alla

Dimostrazione del Teorema 2. Sia $\mathbf{A}$ una matrice complessa di ordine $n = 2^k m$, con m dispari e $k \geq 0$. Proviamo che $\mathbf{A}$ ha un autovalore in $\mathbb{C}^n$ ragionando per induzione su k. Il caso $k = 0$ è provato nella Proposizione 5, che fornisce la base dell'induzione. Sia allora $k > 0$ e l'asserto vero per $h < k$. Denotiamo con W lo spazio vettoriale su $\mathbb{C}$ formato dalle matrici complesse anti-simmetriche di ordine n. È facile verificare (si veda l'Esercizio 3) che la dimensione di W è

$$\frac{n(n-1)}{2} = \frac{2^k m(2^k m - 1)}{2} = 2^{k-1} r$$

dove r è dispari, perché $k > 0$. Definiamo due endomorfismi τ e σ di W nel modo seguente:

$$\tau(\mathbf{B}) = \mathbf{AB} + \mathbf{BA}^T, \quad \sigma(\mathbf{B}) = \mathbf{ABA}^T$$

per ogni $\mathbf{B} \in W$. È immediato verificare che $\tau(\mathbf{B})$ e $\sigma(\mathbf{B})$ sono matrici anti-simmetriche se $\mathbf{B}$ lo è. Proviamo che $\tau\sigma = \sigma\tau$:

$$\begin{aligned}
\tau(\sigma(\mathbf{B})) &= \tau(\mathbf{ABA}^T) = \mathbf{A}(\mathbf{ABA}^T) + (\mathbf{ABA}^T)\mathbf{A}^T\\
&= \mathbf{A}^2\mathbf{BA}^T + \mathbf{AB}(\mathbf{A}^T)^2\\
\sigma(\tau(\mathbf{B}) &= \sigma(\mathbf{AB} + \mathbf{BA}^T) = \mathbf{A}(\mathbf{AB} + \mathbf{BA}^T)\mathbf{A}^T\\
&= \mathbf{A}^2\mathbf{BA}^T + \mathbf{AB}(\mathbf{A}^T)^2.
\end{aligned}$$

Sia ora $\eta\colon \mathbb{C}^{n(n-1)/2} \to W$ un isomorfismo di spazi vettoriali complessi. Si hanno due endomorfismi di $\mathbb{C}^{n(n-1)/2}$:

$$\eta^{-1}\tau\eta = \mathbf{T}, \quad \eta^{-1}\sigma\eta = \mathbf{S}$$

che saranno indotti rispettivamente da $\mathbf{T}$ ed $\mathbf{S}$, opportune matrici complesse di ordine $n(n-1)/2$. Perciò, se $\mathbf{B} \in W$, risulta:

$$\tau(\mathbf{B}) = (\eta\mathbf{T}\eta^{-1})(\mathbf{B}), \quad \sigma(\mathbf{B}) = (\eta\mathbf{S}\eta^{-1})(\mathbf{B}).$$

Dal fatto che τ e σ commutano discende (come nella dimostrazione della Proposizione 5) che le matrici $\mathbf{T}$ ed $\mathbf{S}$ commutano. Per l'ipotesi induttiva, tutte la matrici di ordine $2^h s$ con $h < k$ ed s dispari hanno un autovalore complesso. Applicando il Lemma 3 con $d = 2^k$ e $K = \mathbb{C}$ segue che $\mathbf{T}$ ed $\mathbf{S}$ hanno un autovettore in comune $\mathbf{u} \in \mathbb{C}^{n(n-1)/2}$:

$$\mathbf{Tu} = \lambda\mathbf{u}, \quad \mathbf{Su} = \mu\mathbf{u}$$

dove $\lambda, \mu \in \mathbb{C}$. Detta $\mathbf{C} = \eta(\mathbf{u})$ la matrice anti-simmetrica corrispondente a $\mathbf{u}$ tramite l'isomorfismo η, si ha:

$$\mathbf{Tu} = \lambda\mathbf{u} \implies (\eta^{-1}\tau\eta)(\mathbf{u}) = \lambda\mathbf{u} \implies \tau(\eta(\mathbf{u})) = \lambda\eta(\mathbf{u}) \implies \tau(\mathbf{C}) = \lambda\mathbf{C}$$

e analogamente $\sigma(\mathbf{C}) = \mu\mathbf{C}$. Abbiamo pertanto:

$$\mu\mathbf{C} = \sigma(\mathbf{C}) = \mathbf{ACA}^T = -\mathbf{A}(\mathbf{AC} - \tau(\mathbf{C})) = -\mathbf{A}(\mathbf{AC} - \lambda\mathbf{C})$$

da cui discende

$$(\mathbf{A}^2 - \lambda\mathbf{A} - \mu\mathbf{I})\mathbf{C} = \mathbb{O}.$$

Per il fatto (II) ricordato sopra, esiste $\delta \in \mathbb{C}$ tale che $\delta^2 = \lambda^2 + 4\mu$. È allora immediato verificare che

$$\mathbf{A}^2 - \lambda\mathbf{A} - \mu\mathbf{I} = \left(\mathbf{A} - \frac{\lambda+\delta}{2}\mathbf{I}\right)\left(\mathbf{A} - \frac{\lambda-\delta}{2}\mathbf{I}\right).$$

Poiché $\mathbf{C} = \eta(\mathbf{u})$ e $\mathbf{u} \neq \mathbf{0}$, risulta $\mathbf{C} \neq \mathbb{O}$. Se $\mathbf{v}$ è una colonna non nulla di $\mathbf{C}$ si ottiene:

$$\left(\mathbf{A} - \frac{\lambda+\delta}{2}\mathbf{I}\right)\left(\mathbf{A} - \frac{\lambda-\delta}{2}\mathbf{I}\right)\mathbf{v} = \mathbf{0}.$$

Se $(\mathbf{A} - \frac{\lambda-\delta}{2}\mathbf{I})\mathbf{v} = \mathbf{0}$, allora $(\lambda-\delta)/2$ è un autovalore di $\mathbf{A}$; se invece $\left(\mathbf{A} - \frac{\lambda-\delta}{2}\mathbf{I}\right)\mathbf{v} \neq \mathbf{0}$, allora $(\lambda+\delta)/2$ è un autovalore di $\mathbf{A}$. □

Dal Teorema 2 e dal Lemma 3 si ricava immediatamente il seguente corollario.

Corollario 6. *Due matrici complesse che commutano hanno un autovettore a coordinate complesse in comune.* □

Osservazione 7. Atteso che

(a) per provare che $\mathbb{C}$ è algebricamente chiuso è sufficiente provare, come è ben noto e facile da vedere, che ogni polinomio a coefficienti *reali* ha una radice in $\mathbb{C}$;

(b) ciò equivale a provare che ogni matrice *reale* ha un autovalore complesso;

si potrebbe essere tentati di procedere con la dimostrazione del Teorema 2 a partire da una matrice $\mathbf{A}$ a coefficienti reali di ordine $n = 2^k r$ (r dispari) provando per induzione su k che $\mathbf{A}$ ha un autovalore complesso; in tal caso la base dell'induzione (caso $k = 0$) è assicurata dal fatto (I) e non occorrerebbe dimostrare la Proposizione 5. Procedendo con questa dimostrazione, si userebbe lo spazio vettoriale *reale* V delle matrici *reali* anti-simmetriche di ordine n, che ha dimensione su $\mathbb{R}$ $2^{k-1}r$, nonché l'isomorfismo di spazi vettoriali reali $\eta\colon \mathbb{R}^{2^{k-1}r} \to V$ e le due matrici di ordine $2^{k-1}r$ $\mathbf{T}$ ed $\mathbf{S}$ risulterebbero *reali*.

A questo punto:

- se $k = 1$, si applica il Lemma 3 a $\mathbf{T}$ ed $\mathbf{S}$ con $d = 2$ e $K = \mathbb{R}$; in tal caso risultano *reali*: λ, μ, $\mathbf{u}$, $\mathbf{C}$; non risulta però in generale reale il numero δ. Se $\delta \notin \mathbb{R}$, si conclude allora che, non potendo essere $(\lambda - \delta)/2$ autovalore (perché ci sarebbe un autovettore *reale* $\mathbf{v}$), necessariamente è autovalore (complesso) $(\lambda + \delta)/2$, con autovettore (complesso) $\left(\mathbf{A} - \frac{\lambda-\delta}{2}\mathbf{I}\right)\mathbf{v}$;
- se $k > 1$, il Lemma 3 si può applicare solo con $K = \mathbb{C}$, ma allora bisogna sapere che tutte le matrici *complesse* di ordine non divisibile per 2^k hanno autovalori complessi, che non fa parte dell'ipotesi di induzione di questa dimostrazione; quindi qui ci si blocca.

Si vede pertanto che non si può eludere la Proposizione 5 quando si passa da matrici di ordine $2r$ (r dispari) a matrici di ordine $2^k r$ con $k > 1$.

Esercizi

1. Nella dimostrazione del Lemma 3 si provi che $\mathbf{A}_0 = \lambda \mathbf{I}_m$ ricordando che V coincide con l'autospazio di $\mathbf{A}$ relativo a λ, e che di conseguenza $\mathbf{A}_0$ ha λ come autovalore con relativo autospazio K^m. Dal fatto che $\mathbf{B}_0$ ha un autovalore, dedurre immediatamente che $\mathbf{A}_0$ e $\mathbf{B}_0$ hanno un autovettore in comune.

2. Si provi che le matrici complesse hermitiane di ordine n formano uno spazio vettoriale reale di dimensione n^2. (Suggerimento: una base su $\mathbb{R}$ è costituita dalle matrici con 1 sulla diagonale e 0 altrove, dalle matrici con 1 su un posto sopra alla diagonale e sul posto simmetrico e 0 altrove, e dalle matrici con i su un posto sopra alla diagonale, $-i$ sul posto simmetrico e 0 altrove.)

3. Si provi che le matrici complesse anti-simmetriche di ordine n formano uno spazio vettoriale complesso di dimensione $n(n-1)/2$. (Suggerimento: una base su $\mathbb{C}$ è costituita dalle matrici con 1 su un posto sopra alla diagonale, -1 sul posto simmetrico e 0 altrove.)

4. Si considerino le matrici reali

$$\mathbf{A} = \begin{bmatrix} 1 & 2 \\ -1 & -1 \end{bmatrix}, \quad \mathbf{B} = \begin{bmatrix} 1 & -2 \\ 1 & 3 \end{bmatrix}.$$

Si provi che $\mathbf{A}$ e $\mathbf{B}$ commutano e che non hanno autovalori reali e quindi nemmeno autovettori reali.

5. Si provi che due matrici reali 2×2 che commutano e che hanno entrambi un autovalore reale (e quindi due autovalori reali) hanno un autovettore reale in comune (si applichi la dimostrazione del Lemma 3).

6. Si considerino le matrici reali

$$\mathbf{A} = \begin{bmatrix} 2 & -5 & 0 & 0 \\ 1 & -2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \mathbf{B} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & -5 \\ 0 & 0 & 1 & -2 \end{bmatrix}.$$

Si provi che **A** e **B** commutano, che entrambi hanno un autovalore reale, ma che non hanno autovettori reali in comune.

Appendice E

Alfabeto greco

Per comodità del lettore, riportiamo una tabella con le lettere dell'alfabeto greco, da noi spesso usate nel testo.

Maiuscole	Minuscole	Nome italiano
A	α	alfa
B	β	beta
Γ	γ	gamma
Δ	δ	delta
E	ε	epsilon
Z	ζ	zeta
H	η	eta
Θ	ϑ	teta
I	ι	iota
K	κ	cappa
Λ	λ	lambda
M	μ	mi
N	ν	ni
Ξ	ξ	csi
O	o	omicron
Π	π	pi
P	ρ	ro
Σ	σ	sigma
T	τ	tau
Υ	υ	ipsilon
Φ	φ	fi
X	χ	chi
Ψ	ψ	psi
Ω	ω	omega

Indice analitico