

Lezione 2

2.1 Prodotto di matrici

In questo paragrafo introdurremo una nuova operazione detta *prodotto tra matrici*, o anche *prodotto righe per colonne*. Procederemo per gradi: definiremo prima il prodotto di una matrice riga per una matrice colonna, e solo in seguito daremo la definizione generale.

Definizione 2.1 (Prodotto di una matrice riga per una matrice colonna).

Siano $R = (r_{1,j})_{1 \leq j \leq p} \in \mathbb{R}^{1,p}$ una matrice riga e $C = (c_{i,1})_{1 \leq i \leq p} \in \mathbb{R}^{p,1}$ una matrice colonna.

Il *prodotto delle matrici* R e C (nell'ordine indicato) è la matrice di $\mathbb{R}^{1,1}$, indicata con RC , definita da

$$RC = (r_{1,1} \quad r_{1,2} \quad \dots \quad r_{1,p}) \begin{pmatrix} c_{1,1} \\ c_{2,1} \\ \vdots \\ c_{p,1} \end{pmatrix} = (r_{1,1}c_{1,1} + r_{1,2}c_{2,1} + \dots + r_{1,p}c_{p,1}) \in \mathbb{R}^{1,1}.$$

In particolare, il prodotto di una matrice riga per una matrice colonna è una matrice 1×1 e si può identificare con uno scalare.

Esempio 2.2. Siano

$$A = (1 \quad 2 \quad -1) \in \mathbb{R}^{1,3}, \quad B = \begin{pmatrix} 3 \\ 2 \\ -5 \end{pmatrix} \in \mathbb{R}^{3,1},$$

allora

$$AB = (1 \quad 2 \quad -1) \begin{pmatrix} 3 \\ 2 \\ -5 \end{pmatrix} = (1 \cdot 3 + 2 \cdot 2 + (-1) \cdot (-5)) = (12) \in \mathbb{R}^{1,1}.$$

Se, invece,

$$C = (1 \quad 3 \quad -5 \quad 1) \in \mathbb{R}^{1,4}, \quad D = \begin{pmatrix} 4 \\ 1 \\ 2 \\ 3 \end{pmatrix} \in \mathbb{R}^{4,1},$$

14

si ha

$$CD = (1 \ 3 \ -5 \ 1) \begin{pmatrix} 4 \\ 1 \\ 2 \\ 3 \end{pmatrix} = (1 \cdot 4 + 3 \cdot 1 + (-5) \cdot 2 + 1 \cdot 3) = 0_{1,1},$$

cioè il prodotto CD è nullo nonostante nessuna delle due matrici che stiamo moltiplicando lo sia. ♠

Passiamo ora alla definizione generale del prodotto tra matrici; dal momento che abbiamo imparato a fare il prodotto di una riga per una colonna, l'idea è quella di pensare la prima matrice come unione delle sue righe e la seconda come unione delle sue colonne, moltiplicandole nel modo descritto nella seguente definizione.

Definizione 2.3 (Prodotto tra matrici). Siano $A \in \mathbb{R}^{m,p}$ e $B \in \mathbb{R}^{p,n}$ due matrici, e poniamo $A = (a_{i,h})_{\substack{1 \leq i \leq m \\ 1 \leq h \leq p}}$, $B = (b_{h,j})_{\substack{1 \leq h \leq p \\ 1 \leq j \leq n}}$. Per ogni $i = 1, \dots, m$ sia

$$R_i = (a_{i,1} \ a_{i,2} \ \dots \ a_{i,p})$$

la i -esima riga di A , quindi $R_i \in \mathbb{R}^{1,p}$, e similmente per ogni $j = 1, \dots, n$ sia

$$C_j = \begin{pmatrix} b_{1,j} \\ b_{2,j} \\ \vdots \\ b_{p,j} \end{pmatrix}$$

la j -esima colonna di B , quindi $C_j \in \mathbb{R}^{p,1}$.

Il *prodotto delle matrici* A e B è la matrice di $\mathbb{R}^{m,n}$, indicata con AB , la cui entrata in posizione (i, j) è $R_i C_j$.

Osservazione 2.4. Mettendo insieme le Definizioni 2.1 e 2.3, se $A = (a_{i,h})_{\substack{1 \leq i \leq m \\ 1 \leq h \leq p}}$ e $B = (b_{h,j})_{\substack{1 \leq h \leq p \\ 1 \leq j \leq n}}$, allora l'entrata in posizione (i, j) della matrice prodotto AB è

$$\sum_{k=1}^p a_{i,k} b_{k,j}.$$

Si ricordi che $1 \leq i \leq m$ e $1 \leq j \leq n$.

Esempio 2.5. Riprendiamo le matrici A e B dell'Esempio 2.2. Poiché $A \in \mathbb{R}^{1,3}$ e $B \in \mathbb{R}^{3,1}$ è definito il prodotto BA e risulta

$$\begin{aligned} BA &= \begin{pmatrix} 3 \\ 2 \\ -5 \end{pmatrix} (1 \ 2 \ -1) \\ &= \begin{pmatrix} 3 \cdot 1 & 3 \cdot 2 & 3 \cdot (-1) \\ 2 \cdot 1 & 2 \cdot 2 & 2 \cdot (-1) \\ (-5) \cdot 1 & (-5) \cdot 2 & (-5) \cdot (-1) \end{pmatrix} = \begin{pmatrix} 3 & 6 & -3 \\ 2 & 4 & -2 \\ -5 & -10 & 5 \end{pmatrix}. \end{aligned} \quad \spadesuit$$

⚠ Si noti che, affinché il prodotto di due matrici sia definito, è necessario e sufficiente che il numero di colonne della prima coincida con il numero di righe della seconda! Inoltre

$$A \in \mathbb{R}^{m,P}, \quad B \in \mathbb{R}^{P,n} \quad \Rightarrow \quad AB \in \mathbb{R}^{m,n}.$$

Quindi il prodotto tra matrici non sempre si può fare. Per esempio se

$$A = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \in \mathbb{R}^{2,1}, \quad B = \begin{pmatrix} 1 & 3 & -1 \\ 0 & 2 & 1 \end{pmatrix} \in \mathbb{R}^{2,3},$$

non è definito né AB né BA .

Anche se due matrici si possono moltiplicare in un certo ordine, non è detto che si possano moltiplicare nell'ordine opposto. Per esempio, se

$$C = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \in \mathbb{R}^{2,2}, \quad D = \begin{pmatrix} 1 & 3 & -1 \\ 0 & 2 & 1 \end{pmatrix} \in \mathbb{R}^{2,3},$$

solo il prodotto $CD \in \mathbb{R}^{2,3}$ è definito, mentre DC non si può fare. Se facciamo i conti abbiamo

$$\begin{aligned} CD &= \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 3 & -1 \\ 0 & 2 & 1 \end{pmatrix} = \\ &= \begin{pmatrix} 1 \cdot 1 + 1 \cdot 0 & 1 \cdot 3 + 1 \cdot 2 & 1 \cdot (-1) + 1 \cdot 1 \\ 1 \cdot 1 + (-1) \cdot 0 & 1 \cdot 3 + (-1) \cdot 2 & 1 \cdot (-1) + (-1) \cdot 1 \end{pmatrix} = \begin{pmatrix} 1 & 5 & 0 \\ 1 & 1 & -2 \end{pmatrix}. \end{aligned}$$

Un altro caso che si può verificare è che due matrici si possono moltiplicare in entrambi gli ordini, ma i due prodotti hanno dimensioni diverse. Ad esempio, se

$$E = \begin{pmatrix} 1 & 1 & 1 \\ -1 & 2 & 1 \end{pmatrix} \in \mathbb{R}^{2,3}, \quad F = \begin{pmatrix} 0 & 1 \\ 1 & 0 \\ 2 & -2 \end{pmatrix} \in \mathbb{R}^{3,2},$$

si verifichi che

$$EF = \begin{pmatrix} 3 & -1 \\ 4 & -3 \end{pmatrix} \in \mathbb{R}^{2,2}, \quad FE = \begin{pmatrix} -1 & 2 & 1 \\ 1 & 1 & 1 \\ 4 & -2 & 0 \end{pmatrix} \in \mathbb{R}^{3,3}.$$

Anche quando entrambi i prodotti sono definiti e hanno le stesse dimensioni, non è detto che coincidano (cioè il prodotto tra matrici non è commutativo). Se

$$G = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad H = \begin{pmatrix} 0 & 3 \\ 2 & 0 \end{pmatrix},$$

entrambi i prodotti GH e HG sono definiti e hanno dimensione 2×2 , tuttavia

$$GH = \begin{pmatrix} 0 & 3 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 2 & 0 \end{pmatrix} = HG.$$

Un'osservazione interessante è che la non commutatività del prodotto di matrici non permette di utilizzare gli usuali "prodotti notevoli" nel fare i calcoli di prodotti di matrici. Per illustrare questa osservazione diamo la seguente definizione.

Definizione 2.6 (Potenze di una matrice quadrata). Sia $A \in \mathbb{R}^{n,n}$ una matrice quadrata; poniamo $A^1 = A$.

Per ogni intero $p \geq 2$ la *potenza p -esima* della matrice A è la matrice $A^p = A^{p-1}A$.

In particolare $A^2 = AA$, $A^3 = A^2A = AAA$ e così via.

Esempio 2.7. Non è vero che, data una coppia di matrici A, B per cui abbiano senso entrambe le espressioni matriciali $(A + B)^2$ e $A^2 + 2AB + B^2$, queste coincidano. Come controesempio, prendiamo

$$E_{1,1} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{e} \quad E_{1,2} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},$$

e calcoliamo

$$(E_{1,1} + E_{1,2})^2 = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}.$$

Invece

$$\begin{aligned} E_{1,1}^2 + 2E_{1,1}E_{1,2} + E_{1,2}^2 &= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}^2 + 2 \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix}. \end{aligned}$$

In maniera simile si può verificare che, in generale, $A^2 - B^2 \neq (A + B)(A - B)$, $A^3 \pm B^3 \neq (A \pm B)(A^2 \mp AB + B^2)$ e così via. ♠

Nonostante quanto visto sopra, il prodotto di matrici soddisfa molte proprietà importanti.

Proposizione 2.8 (Proprietà del prodotto tra matrici). Valgono le seguenti proprietà:

- (PM1) per ogni $A \in \mathbb{R}^{m,p}$, $B \in \mathbb{R}^{p,q}$, $C \in \mathbb{R}^{q,n}$ si ha $A(BC) = (AB)C$ (proprietà associativa);
- (PM2) la matrice identità $I_p \in \mathbb{R}^{p,p}$ è l'unico elemento neutro per il prodotto, cioè l'unica matrice tale che $AI_p = A$ e $I_pB = B$ per ogni $A \in \mathbb{R}^{m,p}$ e $B \in \mathbb{R}^{p,n}$ (esistenza e unicità dell'elemento neutro);
- (PMP) per ogni $A \in \mathbb{R}^{m,p}$ e $B \in \mathbb{R}^{p,n}$ e $\alpha \in \mathbb{R}$, si ha $\alpha(AB) = (\alpha A)B = A(\alpha B)$ (compatibilità col prodotto per scalare);
- (PMS1) per ogni $A, B \in \mathbb{R}^{m,p}$ e $C \in \mathbb{R}^{p,n}$, si ha $(A + B)C = AC + BC$ (proprietà distributiva a destra);

(PMS2) per ogni $A \in \mathbb{R}^{m,p}$ e $B, C \in \mathbb{R}^{p,n}$, si ha $A(B + C) = AB + AC$ (proprietà distributiva a sinistra);

(PMT) per ogni $A \in \mathbb{R}^{m,p}$ e $B \in \mathbb{R}^{p,n}$, si ha ${}^t(AB) = {}^tB{}^tA$ (compatibilità con la trasposta).

Dimostrazione. Per dimostrare le uguaglianze tra matrici usiamo la Definizione 1.6; come in precedenza, in tutte le uguaglianze da dimostrare le dimensioni delle matrici a destra e a sinistra dell'uguale coincidono, quindi dobbiamo solo controllare che coincidano anche le entrate al posto (i, j) .

(PM1) In posizione (i, j) della matrice $A(BC)$ troviamo

$$\sum_{k=1}^p a_{i,k} \left(\sum_{\ell=1}^q b_{k,\ell} c_{\ell,j} \right) = \sum_{k=1}^p \sum_{\ell=1}^q a_{i,k} b_{k,\ell} c_{\ell,j} = \sum_{\ell=1}^q \left(\sum_{k=1}^p a_{i,k} b_{k,\ell} \right) c_{\ell,j}$$

che coincide con l'entrata in posizione (i, j) della matrice $(AB)C$.

(PM2) L'identità $AI_p = A$ è immediata dalla definizione. Per dimostrare l'unicità, supponiamo che esista un'altra matrice quadrata $X = (x_{i,j})_{1 \leq i, j \leq p} \in \mathbb{R}^{p,p}$ tale che $AX = A$ per ogni matrice $A \in \mathbb{R}^{m,p}$. In particolare per la matrice

$$A_1 = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \in \mathbb{R}^{m,p}$$

deve valere che

$$A_1 X = \begin{pmatrix} x_{1,1} & x_{1,2} & \cdots & x_{1,p} \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} = A_1,$$

per cui necessariamente $x_{1,1} = 1$ e $x_{1,j} = 0$ per $2 \leq j \leq p$. Ripetendo il ragionamento con la matrice

$$A_2 = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \in \mathbb{R}^{m,p}$$

ricaviamo che $x_{2,2} = 1$ e $x_{2,j} = 0$ per $j \neq 2$, e così via, fino a dimostrare che $x_{i,j} = \delta_{i,j}$, ovvero che $X = I_p$.

Una dimostrazione analoga, che omettiamo, vale per il prodotto BI_p .

(PMP) In posizione (i, j) troviamo l'elemento:

$$\alpha \left(\sum_{k=1}^p a_{i,k} b_{k,j} \right) = \sum_{k=1}^p (\alpha a_{i,k}) b_{k,j} = \sum_{k=1}^p a_{i,k} (\alpha b_{k,j}).$$

(PMS1) In posizione (i, j) della matrice $(A + B)C$ troviamo l'elemento:

$$\sum_{k=1}^p (a_{i,k} + b_{i,k}) c_{k,j} = \sum_{k=1}^p (a_{i,k} c_{k,j}) + (b_{i,k} c_{k,j}) = \sum_{k=1}^p a_{i,k} c_{k,j} + \sum_{k=1}^p b_{i,k} c_{k,j}$$

che coincide con l'entrata in posizione (i, j) della matrice $AC + BC$.

(PMS2) In posizione (i, j) della matrice $A(B + C)$ troviamo l'elemento:

$$\sum_{k=1}^p a_{i,k}(b_{k,j} + c_{k,j}) = \sum_{k=1}^p (a_{i,k}b_{k,j}) + (a_{i,k}c_{k,j}) = \sum_{k=1}^p a_{i,k}b_{k,j} + \sum_{k=1}^p a_{i,k}c_{k,j}$$

che coincide con l'entrata in posizione (i, j) della matrice $AB + AC$.

(PMT) L'entrata (i, j) di ${}^tB{}^tA$ è

$$\sum_{k=1}^p b_{k,i}a_{j,k} = \sum_{k=1}^p a_{j,k}b_{k,i},$$

che è proprio l'entrata (i, j) di ${}^t(AB)$. \square

! Osserviamo che quando trasponiamo un prodotto l'ordine di moltiplicazione si inverte! Non potrebbe essere altrimenti, visto che se $A \in \mathbb{R}^{m,p}$ e $B \in \mathbb{R}^{p,n}$ e quindi è definito il prodotto AB , si ha che ${}^tA \in \mathbb{R}^{p,m}$ e ${}^tB \in \mathbb{R}^{n,p}$, quindi è definito il prodotto ${}^tB{}^tA$.

2.2 Complessità computazionale del prodotto di matrici

Ora che sappiamo moltiplicare due matrici, possiamo osservare che eseguendo un prodotto seguiamo una serie di istruzioni successive, ovvero un *algoritmo*, e che quindi possiamo facilmente far fare queste operazioni a un computer. Ovviamente vorremmo che questo computer moltiplicasse le matrici in modo più veloce possibile. Quanto veloce possiamo farlo lavorare?

Prendiamo il primo caso interessante di matrici quadrate, quello della moltiplicazione di matrici 2×2 . Se

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} \quad \text{e} \quad B = \begin{pmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{pmatrix},$$

l'algoritmo per calcolare $C = AB$ ci dice che

$$\begin{aligned} c_{1,1} &= a_{1,1}b_{1,1} + a_{1,2}b_{2,1}, & c_{1,2} &= a_{1,1}b_{1,2} + a_{1,2}b_{2,2}, \\ c_{2,1} &= a_{2,1}b_{1,1} + a_{2,2}b_{2,1}, & c_{2,2} &= a_{2,1}b_{1,2} + a_{2,2}b_{2,2}, \end{aligned}$$

e quindi l'algoritmo ci chiede di eseguire 4 addizioni e 8 moltiplicazioni.

Dal punto di vista della memoria del computer addizioni e moltiplicazioni sono molto diverse, in quanto le prime non usano praticamente memoria, mentre le seconde sì. La *complessità computazionale* di un algoritmo si misura quindi col numero di moltiplicazioni che vanno eseguite, e quanto scritto sopra si può tradurre dicendo che il costo computazionale di moltiplicare due matrici 2×2 con l'algoritmo del prodotto riga per colonna è di 8 moltiplicazioni. È possibile fare meglio?

Nel 1969 il matematico tedesco V. Strassen, mentre cercava di dimostrare che non era possibile usare meno di 8 moltiplicazioni, trovò un algoritmo che invece ne usava solo 7. Tale algoritmo viene oggi proprio chiamato *algoritmo di Strassen*.

Vediamo di cosa si tratta. Definiamo le seguenti quantità

$$\begin{aligned} I &= (a_{1,1} + a_{2,2})(b_{1,1} + b_{2,2}), \\ II &= (a_{2,1} + a_{2,2})b_{1,1}, \\ III &= a_{1,1}(b_{1,2} - b_{2,2}), \\ IV &= a_{2,2}(-b_{1,1} + b_{2,1}), \\ V &= (a_{1,1} + a_{1,2})b_{2,2}, \\ VI &= (-a_{1,1} + a_{2,1})(b_{1,1} + b_{1,2}), \\ VII &= (a_{1,2} - a_{2,2})(b_{2,1} + b_{2,2}). \end{aligned}$$

Si verifichi che

$$\begin{aligned} c_{1,1} &= I + IV - V + VII, & c_{1,2} &= II + IV, \\ c_{2,1} &= III + V, & c_{2,2} &= I + III - II + VI. \end{aligned}$$

Questa scrittura che a noi sembra inutilmente complicata, a un computer permette di eseguire la moltiplicazione di matrici molto più velocemente!

Non solo: se moltiplichiamo riga per colonna due matrici $n \times n$, dobbiamo eseguire $n^3 - n^2$ addizioni e soprattutto n^3 moltiplicazioni. Però, se abbiamo matrici 4×4 possiamo dividerle in blocchi 2×2 e usare l'algoritmo di Strassen per ogni blocco, riducendo il numero di moltiplicazioni da $4^3 = 64$ a $7^2 = 49$. Se abbiamo matrici di dimensione $2^k \times 2^k$ Strassen ci permette di ridurre il numero di moltiplicazioni da 8^k a 7^k ; se le matrici hanno una dimensione che non è una potenza di 2 possiamo sempre aggiungere blocchi di zeri e ricondurci al caso $2^k \times 2^k$.

Si può dimostrare che, mentre l'algoritmo classico permette di eseguire un prodotto di matrici $n \times n$ usando n^3 moltiplicazioni, Strassen permette di usarne $n^{\log_2(7)} \simeq n^{2,81}$. L'algoritmo di Strassen (e le sue varianti) sono effettivamente usati ancora oggi nei casi in cui la dimensione delle matrici da moltiplicare sia molto grande.

È sicuramente possibile fare meglio: infatti nel 1990 gli informatici sono riusciti a scendere a $n^{2,375}$, utilizzando anche altri strumenti. Nondimeno, il valore minimo di ω tale che la complessità computazionale sia dell'ordine di n^ω è tuttora oggetto di indagine.

2.3 Matrici invertibili e inversa di una matrice quadrata

Quando si ha a che fare con un prodotto è naturale porsi il problema dell'esistenza dell'elemento inverso. Nel caso del prodotto tra scalari sappiamo che ogni numero reale a non nullo ammette un inverso a^{-1} , ovvero un altro numero reale non nullo univocamente determinato tale che $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Vediamo cosa succede nel caso delle matrici; in questa trattazione ci ridurremo a considerare *matrici quadrate*.

Definizione 2.9 (Matrici invertibili). Sia $A \in \mathbb{R}^{n,n}$ una matrice quadrata.

A è detta *invertibile* se esiste $B \in \mathbb{R}^{n,n}$ tale che $AB = BA = I_n$.

Esempio 2.10. La matrice

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

è invertibile. Infatti la matrice

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

è tale che $BA = AB = I_2$. ♠

⚠ Contrariamente a quanto accade per i numeri reali, non tutte le matrici quadrate non nulle sono invertibili!

Esempio 2.11. La matrice

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

non è invertibile, vediamo perchè. Se esistesse una matrice

$$D = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{R}^{2,2}$$

tale che $CD = DC = I_2$, calcolando il prodotto CD , avremmo che

$$CD = \begin{pmatrix} 1 & 2 \\ -2 & -4 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a + 2c & b + 2d \\ -2a - 4c & -2b - 4d \end{pmatrix}.$$

Se però esistessero $a, c \in \mathbb{R}$ tali che $a + 2c = 1$, allora si avrebbe anche $-2a - 4c = -2(a + 2c) = -2 \neq 0$, quindi il prodotto CD non può essere uguale alla matrice identità per alcun valore di $a, b, c, d \in \mathbb{R}$.

Esiste un'interessante classe di matrici quadrate che non sono invertibili, le matrici nilpotenti: una matrice $A \in \mathbb{R}^{n,n}$ è detta *nilpotente* se esiste un intero $p \geq 1$ tale che $A^p = 0_{n,n}$. Per esempio la matrice

$$E_{1,2} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

è tale che $E_{1,2}^2 = 0_{2,2}$, e quindi nilpotente.

Mostriamo che nessuna matrice nilpotente A può avere un'inversa. Se esistesse una matrice B tale che $AB = I_n$ allora

$$A^{p-1} = A^{p-1}I_n = A^{p-1}AB = A^pB = 0_{n,n}B = 0_{n,n}.$$

Poiché $A^{p-1} = 0_{n,n}$, sostituendo A^{p-1} ad A^p in quanto scritto sopra, otterremo $A^{p-2} = 0_{n,n}$. Ripetendo il ragionamento otterremo alla fine $AB = 0_{n,n}$, in contraddizione con l'ipotesi che A sia invertibile. ♠

Finora abbiamo parlato di “una” inversa di una matrice invertibile. Vediamo adesso che invece “la” matrice inversa, come succede nel caso degli scalari, è univocamente determinata.

Proposizione 2.12 (Proprietà delle matrici invertibili). *Valgono le seguenti proprietà:*

- (MI1) per ogni $A \in \mathbb{R}^{n,n}$ si ha che $B \in \mathbb{R}^{n,n}$ è tale che $AB = I_n$ se e solo se $BA = I_n$;
 (MI2) per ogni $A \in \mathbb{R}^{n,n}$ se esistono due matrici $B, C \in \mathbb{R}^{n,n}$ tali che $AB = BA = I_n$ e $AC = CA = I_n$, allora $B = C$.

Dimostrazione. Omettiamo la dimostrazione della prima proprietà (MI1). L’unicità nella proprietà (MI2) è conseguenza della catena di uguaglianze

$$B = BI_n = B(AC) = (BA)C = I_n C = C. \quad \square$$

Grazie alla Proposizione 2.12 siamo finalmente pronti a dare la seguente definizione.

Definizione 2.13 (Matrice inversa). Sia $A \in \mathbb{R}^{n,n}$ una matrice invertibile.

L’unica matrice $B \in \mathbb{R}^{n,n}$ tale che $AB = BA = I_n$ viene detta *inversa di A* e viene denotata con A^{-1} . In tal caso si pone anche $A^0 = I_n$ ed $A^{-p} = (A^{-1})^p$ per ogni intero $p \geq 1$.

Siano A e $B \in \mathbb{R}^{n,n}$ due matrici invertibili. Cosa si può dire circa l’invertibilità della trasposta tA ? e circa l’invertibilità del prodotto AB ?

Proposizione 2.14 (Inversa della trasposta e inversa del prodotto). *Valgono le seguenti proprietà:*

- (MIT) sia $A \in \mathbb{R}^{n,n}$, allora A è invertibile se e solo se la trasposta tA è invertibile e si ha che $({}^tA)^{-1} = {}^t(A^{-1})$;
 (MIP) siano $A, B \in \mathbb{R}^{n,n}$, allora A e B sono invertibili se e solo se il prodotto AB è invertibile e si ha che $(AB)^{-1} = B^{-1}A^{-1}$.

Dimostrazione.

- (MIT) La matrice trasposta tA è invertibile se e solo se esiste una matrice X tale che ${}^tAX = I_n$. Trasponendo entrambi i membri dell’equazione troviamo che questo equivale a $({}^tX)A = {}^tI_n$, e visto che ${}^tI_n = I_n$ questo equivale a sua volta all’invertibilità di A . Inoltre $({}^tX) = A^{-1}$, e cioè $({}^tA)^{-1} = {}^t(A^{-1})$. (Osserviamo che abbiamo usato le proprietà della Proposizione 2.12!)
 (MIP) Supponiamo prima che A e B siano entrambe invertibili con inversa A^{-1} e B^{-1} rispettivamente. Allora

$$(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AI_nA^{-1} = AA^{-1} = I_n,$$

e similmente $(B^{-1}A^{-1})(AB) = I_n$, cioè AB è invertibile con inversa $(AB)^{-1} = B^{-1}A^{-1}$. Viceversa, supponiamo che AB sia invertibile, ovvero che esista una matrice X tale che $(AB)X = X(AB) = I_n$. Allora vale che $A(BX) = I_n$, cioè A è invertibile con inversa $A^{-1} = BX$, e similmente $(XA)B = I_n$, cioè B è invertibile con inversa $B^{-1} = XA$. \square

2.4 Algebra lineare sui numeri complessi

Concludiamo questa lezione con un'osservazione importante: le nozioni e le operazioni definite finora sulle matrici a coefficienti in \mathbb{R} si possono estendere a matrici a coefficienti nel campo dei numeri complessi \mathbb{C} . Poiché $\mathbb{R} \subseteq \mathbb{C}$, segue che $\mathbb{R}^{m,n} \subseteq \mathbb{C}^{m,n}$.

Per questo motivo, da adesso in poi, nelle definizioni e negli enunciati delle proposizioni spesso sostituirò al simbolo \mathbb{R} il simbolo K che indicherà o il campo reale \mathbb{R} o il campo complesso \mathbb{C} .

Esempio 2.15. Si considerino le matrici in $\mathbb{C}^{2,2}$

$$A = \begin{pmatrix} 1 - 2i & 2 - i \\ 1 - i & 1 - i \end{pmatrix} \quad \text{e} \quad B = \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}.$$

A e B possono essere moltiplicate, e risulta

$$AB = \begin{pmatrix} 1 - 2i & 2 - i \\ 1 - i & 1 - i \end{pmatrix} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} = \begin{pmatrix} 2 & 4 \\ 2 & 2 \end{pmatrix}.$$

Si noti che mentre $A, B \in \mathbb{C}^{2,2} \setminus \mathbb{R}^{2,2}$, il prodotto $AB \in \mathbb{R}^{2,2} (\subseteq \mathbb{C}^{2,2})$.