Geometria e Algebra (II), 13.11.12

1. Sappiamo che il prodotto di due numeri reali non cambia invertendo l'ordine dei fattori, cioe' la moltiplicazione di numeri reali possiede la proprieta' commutativa. Ci chiediamo se questa proprieta' vale in qualche modo per la moltiplicazione di matrici.

   Siano A e B due matrici tali che $AB = BA$, sia $m \cdot n$ il tipo di A e sia $p \cdot q$ il tipo di B. Affiche' sia definito il prodotto AB deve essere $n = p$, e affiche' sia definito il prodotto BA deve essere $q = m$; dunque B deve avere tipo $n \cdot m$. Affinche' AB, che ha tipo $m \cdot m$, sia uguale a BA, che ha tipo $n \cdot n$, deve essere $m = n$. In definitiva: affiche' AB possa essere uguale a BA, A e B devono essere entrambe quadrate, e dello stesso ordine.

   Due matrici quadrate dello stesso ordine in generale non commutano; ad esempio per le matrici del secondo ordine si ha

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} p & q \\ r & s \end{bmatrix} = \begin{bmatrix} ap+br & aq+bs \\ cp+dr & cq+ds \end{bmatrix},$$
$$\begin{bmatrix} p & q \\ r & s \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} pa+qc & pb+qd \\ ra+sc & rb+sd \end{bmatrix}.$$

   In definitiva, la moltiplicazione di matrici non possiede in alcun modo la proprieta' commutativa.

2. Ogni $a \in \mathbb{R}$, con $a \neq 0$, possiede un inverso $a^{-1} \in \mathbb{R}$, caratterizzato dalla proprieta'

   $a\, a^{-1} = 1 = a^{-1}\, a.$

   Un'equazione lineare

   $ax = b$

   nell'incognita reale x con coefficiente $a \neq 0$ ha una ed una sola soluzione, data da

   $x = a^{-1}b.$

   In questa lezione vedremo come queste nozioni e questi fatti si estendono al caso delle matrici quadrate di un qualsiasi ordine $n \geq 1$.

3. **Matrice inversa**

   Definizione 1 *Sia A una matrice quadrata di ordine n. Diciamo che A e' invertibile se esiste una matrice B quadrata di ordine n tale che*

$$AB = I_n = BA,$$

   e in tal caso diciamo che B e' una inversa di A

Vengono poste entrambe le condizioni $AB = I_n$ e $BA = I_n$, in quanto il prodotto di matrici non e' commutativo. Inoltre, in prima battuta, si e' usata l'espressione "una inversa" perche' a priori non e detto che sia unica. In realta' lo e':

Proposizione 1 *Se una matrice A possiede qualche inversa, allora A ne possiede una sola; questa viene detta l'inversa di A, e viene indicata con A^{-1}.*

Dimostrazione. Sia A quadrata di ordine n, e siano B e C quadrate di ordine n due inverse di A; vogliamo mostrare che $B = C$.

Per definizione abbiamo

$$AB = I_n = BA,$$
$$AC = I_n = CA.$$

Osserviamo che

$$(BA)C = I_nC = C,$$
$$B(AC) = BI_n = B;$$

d'altro canto per la proprieta' associativa si ha

$$(BA)C = B(AC);$$

dunque $C = B$. $\square$

Osserviamo che nella dimostrazione abbiamo usato solo il fatto che B si comporta da inversa alla sinistra di A e C si comporta da inversa alla destra di A.

L'inversione di matrici ha le seguenti proprieta':

se A e' invertibile, anche A^{-1} e' invertibile, e

$$\left(A^{-1}\right)^{-1} = A;$$

se A e B sono invertibili e dello stesso ordine, allora anche AB e' invertibile, e

$$(AB)^{-1} = B^{-1}A^{-1}.$$

Verifichiamo questa seconda proprieta':

$$(AB)\left(B^{-1}A^{-1}\right) = A\left(BB^{-1}\right)A^{-1} = AI_nA^{-1} = AA^{-1} = I_n$$
$$\left(B^{-1}A^{-1}\right)(AB) = B^{-1}\left(A^{-1}A\right)B = B^{-1}I_nB = B^{-1}B = I_n.$$

4. Nella discussione dei seguenti esempi usiamo un approccio diretto. Vedremo in seguito un metodo efficiente per decidere se una matrice e' invertibile o meno e, in caso affermativo, determinarne l'inversa.

Esempio. Consideriamo la matrice

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

Ci chiediamo se possiede una inversa destra, cioe' se esiste una matrice

$$B = \begin{bmatrix} p & q \\ r & s \end{bmatrix}$$

tale che $AB = I_2$, cioe'

$$\begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} p & q \\ r & s \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

cioe'

$$\begin{bmatrix} p-r & q-s \\ p+r & q+s \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

cioe'

$$\begin{cases} p-r=1 \\ q-s=0 \\ p+r=0 \\ q+s=1 \end{cases}.$$

Questo sistema lineare di quattro equazioni in quatto incognite in realta' consiste di due sistemi di due equazioni in due incognite ciascuno

$$\begin{cases} p-r=1 \\ p+r=0 \end{cases}, \qquad \begin{cases} q-s=0 \\ q+s=1 \end{cases}.$$

Il primo sistema ha una ed una sola soluzione, data da

$p = 1/2$,

$r = -1/2$;

il secondo sistema ha una ed una sola soluzione, data da

$q = 1/2$,

$s = 1/2$.

Dunque c'e' una ed una sola matrice inversa destra di A, ed e'

$$B = \begin{bmatrix} 1/2 & 1/2 \\ -1/2 & 1/2 \end{bmatrix}.$$

Ci chiediamo ora se B e' anche inversa sinistra di A, cioe' se $BA = I_2$, cioe'

$$\begin{bmatrix} 1/2 & 1/2 \\ -1/2 & 1/2 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \stackrel{?}{=} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

La verifica e' positiva, B e' anche inversa sinistra di $A,$ dunque B e' l'inversa di A :

$$A^{-1} = \begin{bmatrix} 1/2 & 1/2 \\ -1/2 & 1/2 \end{bmatrix}.$$

Esempio. Consideriamo la matrice

$$A = \begin{bmatrix} 2 & 3 \\ 4 & 6 \end{bmatrix}$$

Ci chiediamo se possiede una inversa destra, cioe' se esiste una matrice

$$B = \begin{bmatrix} p & q \\ r & s \end{bmatrix}$$

tale che $AB = I_2,$ cioe'

$$\begin{bmatrix} 2 & 3 \\ 4 & 6 \end{bmatrix} \begin{bmatrix} p & q \\ r & s \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

cioe'

$$\begin{cases} 2p + 3r = 1 \\ 2q + 3s = 0 \\ 4p + 6r = 0 \\ 4q + 6s = 1 \end{cases}.$$

Ora, la prima e la terza equazione di questo sistema sono incompatibili. Dunque A non possiede alcuna inversa destra, e a maggior ragione non possiede alcuna inversa.

Osserviamo che la prima matrice $\left[\begin{smallmatrix} 1 & -1 \\ 1 & 1 \end{smallmatrix}\right]$ ha le righe (e le colonne) linearmente indipendenti ed e' invertibile, mentre la seconda matrice $\left[\begin{smallmatrix} 2 & 3 \\ 4 & 6 \end{smallmatrix}\right]$ ha le righe (e le colonne) linearmente dipendenti e non e' invertibile. Non e' un caso, vale infatti il seguente Teorema, che dimostreremo in seguito.

Teorema 1 (Invertibilita' e rango) *Una matrice quadrata e' invertibile se e solo se le sue righe (e le sue colonne) sono linearmente indipendenti. In altri termini, una matrice A quadrata di ordine n e' invertibile se e solo se ha rango $r(A) = n$.*

5. Matrici invertibili e sistemi lineari.

Teorema 2 *Se una matrice A quadrata di ordine n e' invertibile, allora ciascun sistema lineare di n equazioni in n incognite*

$$Ax = b$$

con matrice dei coefficienti A ha una ed una sola soluzione, data da

$$x = A^{-1}b.$$

Dimostrazione. Dal fatto che A^{-1} e' inversa sinistra di A, ricaviamo

$$\begin{aligned} Ax &= b \\ A^{-1}(Ax) &= A^{-1}b \\ \left(A^{-1}A\right)x &= A^{-1}b \\ I_n x &= A^{-1}b \\ x &= A^{-1}b. \end{aligned}$$

Usando il fatto che A^{-1} e' inversa destra di A, mostriamo che questa e' davvero una soluzione:

$$A\left(A^{-1}b\right) = \left(AA^{-1}\right)b = I_n b = b. \qquad \square$$

Esempio. Sappiamo che la matrice

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

e' invertible. Per il Th. precedente, possimo dire che ogni sistema

$Ax = b$

ha una ed una sola soluzione, data da

$x = A^{-1}b$

dove

$$A^{-1} = \begin{bmatrix} 1/2 & 1/2 \\ -1/2 & 1/2 \end{bmatrix}.$$

Esplicitamente: ogni sistema

$$\begin{cases} x_1 - x_2 = b_1 \\ x_1 + x_2 = b_2 \end{cases}$$

ha una ed una sola soluzione, data da

$$\begin{cases} x_1 = b_1/2 + b_2/2 \\ x_2 = -b_1/2 + b_2/2 \end{cases}.$$

6. Potenze

Sia A una matrice quadrata di ordine n. Per ogni intero relativo $p = 0, \pm 1, \pm 2, \ldots,$ la potenza $p-$ma della matrice A e' definita da

$$A^p = \begin{cases} A\,A\,\cdots\,A \quad (p\ volte) & \text{per } p > 0 \\ I_n & \text{per } p = 0 \\ A^{-1}\,A^{-1}\,\cdots\,A^{-1} \quad (-p\ volte) & \text{per } p < 0 \end{cases};$$

le potenze con esponente negativo sono definite solo per matrici invertibili.

Esempio:

$$\begin{aligned}
\begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}^{-2} &= \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}^{-1} \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}^{-1} \\
&= \begin{bmatrix} 1/2 & 1/2 \\ -1/2 & 1/2 \end{bmatrix} \begin{bmatrix} 1/2 & 1/2 \\ -1/2 & 1/2 \end{bmatrix} \\
&= \begin{bmatrix} 0 & 1/2 \\ -1/2 & 0 \end{bmatrix}.
\end{aligned}$$

Valgono le proprieta' delle potenze:

$A^p A^q = A^{p+q}$;

$(A^p)^q = A^{pq}$;

sotto la condizione $AB = BA$, vale anche la proprieta'

$(AB)^p = A^p B^p$.

Verifichiamo questa proprieta' nel caso $p = 2$:

$(AB)^2 = (AB)(AB) = A(BA)B = A(AB)B = A^2B^2$.

7. **Calcolo della matrice inversa**

Un modo efficiente per invertire una matrice e' dato dal seguente

Teorema 3 *Sia A una matrice quadrata di ordine n. Consideriamo la matrice*

$[A|I_n]$

ottenuta affiancando ad A la matrice I_n unita' di ordine n; applicando a questa matrice l'algoritmo di Gauss, si ottiene una matrice

$[T|S]$.

Se tutti i pivot di $[T|S]$ stanno nel primo blocco T, allora A e' invertibile; tramite operazioni elementari si puo' trasformare $[T|S]$ in un matrice del tipo

$[I_n|B]$

e si ha

$A^{-1} = B$.

Se qualche pivot di $[T|S]$ sta nel secondo blocco S, allora A non e' invertibile,

La procedura sottesa a questo teorema nel caso in cui la matrice sia invertibile viene detta "algoritmo di Gauss-Jordan per il calcolo della matrice inversa".

Esempio Consideriamo la matrice

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

Affianchiamo ad A la matrice unita' I_3 :

$$\left[\ A \mid I_3\ \right] = \left[\begin{array}{ccc|ccc} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 2 & 2 & 0 & 1 & 0 \\ 1 & 2 & 3 & 0 & 0 & 1 \end{array}\right].$$

Applicando l'algoritmo di Gauss otteneniamo la matrice a scala

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

Tutti i pivot sono nel primo blocco, dunque A e' invertibile; tramite operazioni elementari possiamo trasformare questa matrice in modo che nel primo blocco compaia la matrice unita' I_3.

Annulliamo gli elementi sopra il pivot della terza riga, sottraendo la terza riga alla seconda ed alla prima, ed otteniamo

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

annulliamo gli elementi sopra il pivot della seconda riga, sottraendo la seconda riga alla prima, ed otteniamo

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 2 & -1 & 0 \\ 0 & 1 & 0 & -1 & 2 & -1 \\ 0 & 0 & 1 & 0 & -1 & 1 \end{array}\right] = \left[\ I_3 \mid B\ \right].$$

Dunque

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

Esempio Sia data la matrice

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}.$$

Affianchiamo ad A la matrice unita' I_3 :

$$\left[\ A \mid I_3\ \right] = \left[\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 4 & 5 & 6 & 0 & 1 & 0 \\ 7 & 8 & 9 & 0 & 0 & 1 \end{array}\right].$$

Applicando l'algoritmo di Gauss otteniamo la matrice a scala

$$\left[\begin{array}{rrr|rrr} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & -3 & -6 & -4 & 1 & 0 \\ 0 & 0 & 0 & 1 & -2 & 1 \end{array}\right].$$

Osserviamo che il pivot della terza riga sta nel secondo blocco, dunque la matrice A non e' invertibile.

Avremmo potuto arrivare direttamente a questa conclusione nel modo seguente. Osserviamo che le colonne di A sono linearmente dipendenti in quanto la seconda colonna di A e' la media fra la prima e la terza:

$$A_{*2} = \frac{1}{2}(A_{*1} + A_{*3}),$$

o in altri termini, le colonne di A soddisfano la relazione non banale

$$A_{*1} - 2A_{*2} + A_{*3} = 0.$$

Per il teorema su invertibilita' e rango, deduciamo che A non e' invertibile.

8. **Algebra delle matrici**

Ricordiamo che $\mathcal{M}_{m,n}(\mathbb{R})$ indica l'insieme di tutte le matrici di tipo $m \cdot n$ ad entrate reali; col simbolo $\mathcal{M}(\mathbb{R})$ indicheremo l'insieme di tutte le matrici ad entrate reali, in altri termini poniamo

$$\mathcal{M}(\mathbb{R}) = \bigcup_{m,n\in\mathbb{N}} \mathcal{M}_{m,n}(\mathbb{R}).$$

Su questo insieme sono definite

- un'operazione parziale di somma di matrici
  $\mathcal{M}_{m,n}(\mathbb{R}) \times \mathcal{M}_{m,n}(\mathbb{R}) \to \mathcal{M}_{m,n}(\mathbb{R}),$
  $(A, B) \mapsto A + B; \qquad (A + B)_{ij} = A_{ij} + B_{ij};$
- un'operazione di prodotto di scalari per matrici
  $\mathbb{R} \times \mathcal{M}_{m,n}(\mathbb{R}) \to \mathcal{M}_{m,n}(\mathbb{R}),$
  $(\alpha, A) \mapsto \alpha A; \qquad (\alpha A)_{ij} = \alpha A_{ij};$
- un'operazione parziale di prodotto di matrici
  $\mathcal{M}_{m,n}(\mathbb{R}) \times \mathcal{M}_{n,p}(\mathbb{R}) \to \mathcal{M}_{m,p}(\mathbb{R}),$
  $(A, B) \mapsto AB; \qquad (AB)_{ij} = \sum_k A_{ik}B_{kj};$

Risulta utile inoltre definire anche un'operazione di prodotto di matrici per scalari

$\mathcal{M}_{m,n}(\mathbb{R}) \times \mathbb{R} \to \mathcal{M}_{m,n}(\mathbb{R}),$
$(A, \alpha) \mapsto A\alpha; \qquad (A\alpha)_{ij} = A_{ij}\alpha.$

Le operazioni di somma e prodotto per scalari danno ad ogni insieme $\mathcal{M}_{m,n}(\mathbb{R})$ la struttura di spazio vettoriale reale.

Il prodotto di matrici e' legato alla somma dalle proprieta' distributive

$$(A+B)C = AC + BC,$$
$$A(C+D) = AC + AD;$$

queste identita' vanno intese come segue: per ogni tre matrici $A, B, C,$ il primo membro dell'uguaglianza e' definito se e solo se e' definito il secondo membro; per ogni tre matrici $A, B, C,$ per le quali entrambe i membri sono definti, vale l'uguale.

Il prodotto di matrici e' legato alla moltiplicazione per scalari dalla proprieta' pseudoassociativa

$$\alpha(AB) = (\alpha A)B = (A\alpha)B = A(\alpha B) = A(B\alpha) = (AB)\alpha.$$

Per ogni intero positivo $n,$ l'insieme $\mathcal{M}_{n,n}(\mathbb{R})$ delle matrici quadrate di ordine n e' chiuso rispetto a tutte le operazioni (somma, prodotto per scalari, prodotto). La struttura

$$(\mathcal{M}_{m,n}(\mathbb{R});\ +, \cdot; \cdot)$$

viene detta "algebra delle matrici quadrate di ordine n". Per $n = 1$ quest'algebra si puo' identificare col campo dei numeri reali.

Viene naturale chiedersi che forma assumono in $\mathcal{M}_{n,n}(\mathbb{R})$ le identita' notevoli come la "somma per differenza = differenza di quadrati" il "quadrato del binomio", ...

Ad esempio, si ha

$$(A+B)(A-B) = A(A-B) + B(A-B) = A^2 - AB + BA - B^2$$

dunque l'identita'

$$(A+B)(A-B) = A^2 - B^2$$

in generale non vale; vale sotto la condizione $AB = BA.$

Un argomento analogo vale per le altre identita' notevoli.

9. **Dimostrazione di una parte del teorema su invertibilita' e rango.**

Premettiamo un'osservazione sulle relazioni fra le righe della matrice inversa e le colonne di una matrice. Sia A una matrice invertibile e sia $B = A^{-1}$ la sua inversa. Dall'uguaglianza

$$BA = I_n$$

otteniamo

$$B_{i*}A_{*j} = (BA)_{ij} = (I_n)_{ij} = \begin{cases} 1, & \text{se } i = j \\ 0, & \text{se } i \neq j \end{cases}.$$

Siamo ora nella posizione di mostrare che se una matrice A quadrata di ordine n e' invertibile, allora le sue n colonne $A_{*1}, A_{*2}, \ldots, A_{*n}$ sono linearmente indipendenti.

Sia

$$\alpha_1 A_{*1} + \alpha_2 A_{*2} + \cdots + \alpha_n A_{*n} = 0$$

una combinazione lineare delle colonne di A il cui risultato e' la colonna nulla. Moltiplicando entrambe i membri a sinistra per la prima riga B_{1*} della matrice $B = A^{-1}$ inversa di A, otteniamo

$$B_{1*}\left(\alpha_1 A_{*1} + \alpha_2 A_{*2} + \cdots + \alpha_n A_{*n}\right) = B_{1*}0,$$

che per la proprieta' distributiva e pseudoassociativa possiamo riscrivere

$$\alpha_1\left(B_{1*}A_{*1}\right) + \alpha_2\left(B_{1*}A_{*2}\right) + \cdots + \alpha_n\left(B_{1*}A_{*n}\right) = 0,$$

e per quanto osservato sopra,

$$\alpha_1 \cdot 1 + \alpha_2 \cdot 0 + \cdots + \alpha_n \cdot 0 = 0,$$

cioe' $\alpha_1 = 0$.

Moltiplicando entrambe i membri a sinistra per le altre righe $B_{2*}, \ldots, B_{n*}$ delle matrice inversa B, si ottine rispettivamente $\alpha_2 = 0, \ldots, \alpha_n = 0$.