Prop: siano $A, B \in M_{m,p}(\mathbb{R})$ e sia $C, D \in M_{p,n}(\mathbb{R})$; allora valgono le seguenti uguaglianze:

1. $(A+B)\cdot C = A\cdot C + BC$ (proprietà distributiva a destra)
2. $A\cdot(C+D) = A\cdot C + A\cdot D$ (proprietà distributiva a sinistra)

Prop: sia $A \in M_{m,p}(\mathbb{R})$, $B \in M_{p,q}(\mathbb{R})$ e $C \in M_{q,n}(\mathbb{R})$; allora vale che

$$\underbrace{\underbrace{(A\cdot B)}_{m\times q}\cdot \underbrace{C}_{q\times n}}_{m\times n} = \underbrace{\underbrace{A}_{m\times p}\cdot\underbrace{(B\cdot C)}_{p\times n}}_{m\times n}$$

(proprietà associativa del prodotto)

Prop: sia $A \in M_{m,p}(\mathbb{R})$ e $B \in M_{q,n}(\mathbb{R})$; allora

$$\underbrace{{}^t\underbrace{(A\cdot B)}_{m\times n}}_{n\times m} \neq \underbrace{{}^tA}_{p\times m}\cdot\underbrace{{}^tB}_{n\times p}$$

! Le matrici ${}^tA$ e ${}^tB$ non si possono moltiplicare tra loro in generale (se $m \neq n$)

vale invece che

$${}^t(A\cdot B) = {}^tB \cdot {}^tA$$

Dim: per mostrare che ${}^t(A\cdot B)$ è uguale a ${}^tB\cdot{}^tA$, mostriamo che tutte le loro entrate sono uguali: sia dunque $i \in \{1,\dots,n\}$ e sia $j \in \{1,\dots,m\}$; allora

$$({}^t(A\cdot B))_{ij} = (A\cdot B)_{ji} = \underbrace{A_{(j)}}_{j\text{-esima riga}} \cdot \underbrace{B^{(i)}}_{i\text{-esima colonna}}$$

$$({}^tB\cdot{}^tA)_{ij} = ({}^tB)_{(i)}\cdot({}^tA)^{(j)} = A_{(j)}\cdot B^{(i)}$$

e questo mostra che le due matrici sono uguali.

Prop: sia $A \in M_{m,n}(\mathbb{R})$, allora

$$\mathbb{1}_m \cdot A = A \quad \text{e} \quad A\cdot\mathbb{1}_n = A.$$

Oss: nel caso delle matrici quadrate, la matrice unità $\mathbb{1}_n$ funge dunque da elemento neutro per il prodotto righe per colonne: per ogni $A \in M_n(\mathbb{R})$ vale che

$$\mathbb{1}_n\cdot A = A\cdot\mathbb{1}_n = A$$

Oss: nei numeri reali, dato $a\in\mathbb{R}$, diciamo che b è inverso di a se vale che $a\cdot b = b\cdot a = 1$; ogni numero reale non nullo ammette un unico inverso; l'inverso di $a \in \mathbb{R}\setminus\{0\}$ si denota a^{-1}.

Def: sia $A \in M_n(\mathbb{R})$; A si dice invertibile se esiste $B \in M_n(\mathbb{R})$ (inverso di A) tale che valga

$$A\cdot B = B\cdot A = \mathbb{1}_n$$

Prop: sia $A, B \in M_n(\mathbb{R})$, allora

1. se A è invertibile, allora l'inverso di A è unico
2. se A e B sono invertibili, allora anche $A\cdot B$ è invertibile e la sua inversa è $B^{-1}\cdot A^{-1}$

Dim: 1. siano B e C entrambe inverse di A, allora

$$A\cdot B = B\cdot A = \mathbb{1}_n$$
$$A\cdot C = C\cdot A = \mathbb{1}_n$$

allora

$$B = B\cdot\mathbb{1}_n = B\cdot(A\cdot C) = (B\cdot A)\cdot C$$
$$= \mathbb{1}_n\cdot C = C$$

2. mostriamo che $B^{-1}A^{-1}$ è inversa di $A\cdot B$:

$$(A\cdot B)\cdot(B^{-1}\cdot A^{-1}) = A\cdot(B\cdot B^{-1})\cdot A^{-1} =$$
$$= A\cdot\mathbb{1}_n\cdot A^{-1} =$$
$$= A\cdot A^{-1} = \mathbb{1}_n$$

analogamente

$$(B^{-1}\cdot A^{-1})\cdot(A\cdot B) = B^{-1}\cdot(A^{-1}\cdot A)\cdot B =$$
$$= B^{-1}\cdot\mathbb{1}_n\cdot B =$$
$$= B^{-1}\cdot B = \mathbb{1}_n$$

Oss: l'analogia tra invertibilità rispetto al prodotto di numeri reali e l'invertibilità rispetto al prodotto righe per colonne di matrici non si estende fino al punto di dire che ogni matrice non nulla è invertibile

Esempio: consideriamo la matrice $A \in M_2(\mathbb{R})$:

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

mostriamo che A non è invertibile (anche se $A \neq 0$); supponiamo che esista un'inversa B

$$B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$$

dovrebbe essere che

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

quindi in particolare

- $(1 \ \ 1)\cdot\begin{pmatrix} b_{11} \\ b_{21}\end{pmatrix} = 1$, ovvero $b_{11} + b_{21} = 1$
- $(1 \ \ 1)\cdot\begin{pmatrix} b_{11} \\ b_{21}\end{pmatrix} = 0$, ovvero $b_{11} + b_{21} = 0$

e questo è impossibile perché implicherebbe $1 = 0$.

Fermiamoci un attimo! Se ci guardiamo indietro, vediamo come ogniqualvolta abbiamo usato i numeri reali, abbiamo solamente utilizzato le loro proprietà rispetto a somma e moltiplicazione. Queste sono infatti le proprietà che lo rendono un campo.

Definizione: sia K un insieme su cui siano definite una operazione di somma e una operazione di moltiplicazione, ovvero

$$+ : K\times K \longrightarrow K \qquad \cdot : K\times K \longrightarrow K$$
$$(a,b) \longmapsto a+b \qquad (a,b)\longmapsto a\cdot b$$

tale per cui siano soddisfatte le seguenti proprietà:

K1: commutatività: $\forall a,b\in K$, $a+b = b+a$, $a\cdot b = b\cdot a$

K2: associatività: $\forall a,b,c\in K$ $(a+b)+c = a+(b+c)$
$a\cdot(b\cdot c) = (a\cdot b)\cdot c$

K3: esistenza elemento neutro: esiste $0\in K$ tale che $\forall a\in K$, $a+0 = 0+a = a$
esiste $1 \in K$ tale che $\forall a\in K$, $a\cdot 1 = 1\cdot a = a$
e inoltre, $0 \neq 1$.

K4: esistenza di opposto e inverso: $\forall a\in K$, esiste $b\in K$ tale che $a+b = b+a = 0$ (e denotiamo b con $-a$)
$\forall a \in K\setminus\{0\}$ esiste $c\in K$ tale che $a\cdot c = c\cdot a = 1$ (e denotiamo c con a^{-1} oppure $1/a$)

K5: distributività: $\forall a,b,c\in K$ vale $(a+b)\cdot c = a\cdot c + b\cdot c$.

un tale insieme si dice campo.

Esempio: $\mathbb{Q}$ è un campo, $\mathbb{R}$ è un campo, $\mathbb{C}$ è un campo
$\mathbb{N}$ non è un campo, $\mathbb{Z}$ non è un campo

Oss: l'insieme delle funzioni razionali:

$$\left\{\frac{p}{q} : p \text{ e } q \text{ sono polinomi in una variabile}\right\}$$

può essere dotato di somma e prodotto in modo da renderlo un campo.

Esempio: l'insieme $\mathbb{Z}_2 = \{0,1\}$ su cui definiamo una somma e prodotto nel modo seguente

$$+ : \mathbb{Z}_2\times\mathbb{Z}_2 \longrightarrow \mathbb{Z}_2 \qquad \cdot : \mathbb{Z}_2\times\mathbb{Z}_2\longrightarrow\mathbb{Z}_2$$
$$(a,b)\longmapsto a+b \qquad (a,b)\longmapsto a\cdot b$$

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

è un campo

Pertanto la precedente nozione di $\mathbb{R}$-spazio vettoriale sarà d'ora in poi sostituita da quella di K-spazio vettoriale con K un campo.

Sistemi lineari

Def: sia K un campo; un sistema di m equazioni in n incognite a coefficienti in K è un sistema di equazioni della forma seguente:

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

dove ogni a_{ij} è un elemento di K per ogni $i\in\{1,\dots,m\}$, $j\in\{1,\dots,n\}$ e ogni b_i è un elemento di K per ogni $i\in\{1,\dots,m\}$; $x_1,\dots,x_n$ sono dette incognite, mentre gli elementi $b_1,\dots,b_m$ sono detti i termini noti e gli elementi a_{ij} sono detti i coefficienti del sistema; una soluzione del sistema è una n-upla ordinata (che rappresentiamo come vettore colonna) $s\in K^n$, ovvero $s = \begin{pmatrix} s_1 \\ \vdots \\ s_n\end{pmatrix}$ con $s_i \in K$ tale per cui se per ogni $i\in\{1,\dots,n\}$ sostituiamo x_i con s_i, allora tutte le uguaglianze del sistema sono vere; il sistema si dice omogeneo se $b_1 = \dots = b_m = 0$, ovvero tutti i termini noti sono nulli; un sistema si dice non-omogeneo se non è omogeneo; un sistema si dice compatibile se ammette almeno una soluzione; altrimenti si dice incompatibile.

Oss: la n-upla nulla $\begin{pmatrix} 0 \\ \vdots \\ 0\end{pmatrix}$ è sempre soluzione di un sistema omogeneo; pertanto ogni sistema omogeneo è compatibile.

Def: dato un sistema lineare come nella definizione precedente, definiamo

$$A = (a_{ij})_{\substack{i\in\{1,\dots,m\}\\ j\in\{1,\dots,n\}}} \in M_{m,n}(K)$$

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \qquad b = \begin{pmatrix} b_1 \\ \vdots \\ b_m\end{pmatrix} \in M_{m,1}(K)$$

allora il sistema precedente si può scrivere come

$$\underbrace{A}_{m\times n}\cdot\underbrace{X}_{n\times 1} = \underbrace{b}_{m\times 1}$$