Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

# Rendiconti

Domenico Lenzi

## Un teorema di decomposizione per alcune matrici quadrate ad elementi in un corpo

*Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8*, Vol. **54** (1973), n.3, p. 328–331.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1973_8_54_3_328_0>

**Algebra.** — *Un teorema di decomposizione per alcune matrici quadrate ad elementi in un corpo.* Nota di DOMENICO LENZI (*), presentata (**) dal Socio B. SEGRE.

SUMMARY. — A necessary and sufficient condition is given in order that a square matrix M over a skew field K be such that its transform in a given non-identical involutive automorphism of K equals the inverse of M.

Riferiamoci ad un qualunque corpo K e ad un automorfismo involutorio $\varphi$ non identico relativo a K. Conveniamo di indicare col simbolo $\bar{k}$ l'immagine tramite $\varphi$ di un qualsiasi elemento $k \in \mathrm{K}$. In analogia, data una qualsiasi matrice A ad elementi in K, conveniamo di indicare con $\bar{\mathrm{A}}$ la matrice ottenuta sostituendo in A ad ogni elemento la sua immagine tramite $\varphi$ e chiamiamo $\bar{\mathrm{A}}$ « la trasformata » di A.

Ci proponiamo ora di dimostrare il seguente

TEOREMA DI DECOMPOSIZIONE (***). *C.N.S. affinchè una matrice quadrata* M *ad elementi in* K *abbia come matrice inversa* (1) *la sua trasformata* $\bar{\mathrm{M}}$ *è che esista una matrice invertibile* S *tale che* $\mathrm{M} = \mathrm{S}^{-1} \cdot \bar{\mathrm{S}}$.

*Dimostrazione*. Se $\mathrm{M} = \mathrm{S}^{-1} \cdot \bar{\mathrm{S}}$ si ha $(\mathrm{S}^{-1} \cdot \bar{\mathrm{S}}) \cdot (\overline{\mathrm{S}^{-1} \cdot \bar{\mathrm{S}}}) = \mathrm{S}^{-1} \cdot \bar{\mathrm{S}} \cdot \bar{\mathrm{S}}^{-1} \cdot \mathrm{S} = \mathrm{E}_n$ (2), il che prova la sufficienza della suddetta condizione.

Giungeremo alla dimostrazione della necessità di quella condizione servendoci di alcune proposizioni che a tal uopo premettiamo.

Iniziamo, riferendoci a matrici del primo ordine, con la seguente prop. 1 ed il successivo cor. 1.

PROPOSIZIONE 1. *Dato* $m \in \mathrm{K}$ *tale che* $m \cdot \bar{m} = 1$ $(= \bar{m} \cdot m)$ *esiste* $s \in \mathrm{K}$ *tale che* $m = s^{-1} \cdot \bar{s}$.

*Dimostrazione*. Consideriamo un elemento $k \in \mathrm{K} - \{0\}$ e poniamo $s = \bar{k} + k \cdot \bar{m}$; si avrà allora $\bar{s} = k + \bar{k} \cdot m$, onde $sm = \bar{k}m + k = \bar{s}$.

(*) Lavoro svolto nell'ambito del Gruppo Nazionale per le Strutture Algebriche e Geometriche e loro applicazioni del C.N.R.

(**) Nella seduta del 10 marzo 1973.

(***) L'enunciato è stato originariamente proposto da R. Ascoli, C. Garola, L. Solombrino e G. Teppati nell'ambito di una loro ricerca sul commutante semilineare di insiemi di operatori lineari.

(1) Ora e nel seguito ci riferiremo sempre al prodotto righe (della matrice scritta a sinistra) per colonne (della matrice scritta a destra).

(2) Con $\mathrm{E}_n$ intendiamo la matrice unitaria d'ordine $n$.

L'asserto risulta allora provato se $k$ è tale che $s$ sia invertibile. All'uopo distinguiamo i due casi:

1) $m \neq -1$ (onde anche $\bar{m} \neq -1$);

2) $m = -1$ (onde anche $\bar{m} = -1$).

Nel primo caso, con $k = 1$, si ha $s = 1 + \bar{m} \neq 0$; nel secondo caso, invece, scegliendo $k$ in maniera tale che $\bar{k} \neq k$, si ha $s = \bar{k} - k \neq 0$, onde la tesi. C.V.D.

COROLLARIO 1. *In virtù dell'isomorfismo naturale tra* K *e le matrici del primo ordine ad elementi in* K, *si ha che per matrici d'ordine* 1 *il teorema di decomposizione è vero.*

COROLLARIO 2. *Considerato* $-1 \in K$, *esiste* $\varepsilon \in K$ *tale che* $-1 = \varepsilon^{-1} \cdot \bar{\varepsilon}$, cioè tale che $\bar{\varepsilon} = -\varepsilon$.

COROLLARIO 3. *In relazione alla matrice* $-E_n$, *si ha che* $-E_n = (\varepsilon^{-1} E_n) \cdot (\bar{\varepsilon} E_n)$.

PROPOSIZIONE 2. *Data* M, *matrice quadrata d'ordine* $n$ *tale che* $M \cdot \overline{M} = E_n \; (= \overline{M} \cdot M)$, *C.N.S. affinchè il teorema di decomposizione valga per* M *è che tale teorema valga per* $-M$. (*Si noti che* $(-M) \cdot (-\overline{M}) = E_n$).

*Dimostrazione.* Ovviamente basta far vedere che, se il teorema di decomposizione vale per M, esso vale anche per $-M$.

Sia quindi $M = S^{-1} \cdot \bar{S}$; allora $-M = (-E_n) \cdot S^{-1} \cdot \bar{S} = S^{-1} \cdot (-E_n) \cdot \bar{S} = S^{-1} \cdot (\varepsilon^{-1} E_n) \cdot (\bar{\varepsilon} E_n) \cdot \bar{S} = (\varepsilon E_n \cdot S)^{-1} \cdot (\overline{\varepsilon E_n \cdot S})$. C.V.D.

PROPOSIZIONE 3. *Fatte le stesse premesse della prop. 2, C.N.S. affinchè il teorema di decomposizione valga per* M *è che esso valga per* $\overline{M}$.

*Dimostrazione.* Basta osservare che da $M \cdot \overline{M} = E_n$ segue $\overline{M} \cdot \overline{\overline{M}} = \overline{M} \cdot M = E_n$ e viceversa.

PROPOSIZIONE 4. *Fatte ancora le stesse premesse della prop. 2, C.N.S. affinchè il teorema di decomposizione valga per* M *è che, qualunque sia* A, *matrice invertibile d'ordine* $n$ *ad elementi in* K, *il teorema valga per* $A^{-1} M \bar{A}$.

*Dimostrazione.* Si noti che, se $\overline{M} = M^{-1}$, risulta $A^{-1} M \bar{A} \cdot \overline{A^{-1} M \bar{A}} = A^{-1} M \bar{A} \cdot \bar{A}^{-1} M^{-1} A = E_n$. Basta quindi soltanto dimostrare che, se la condizione di decomponibilità è soddisfatta per M, essa lo è anche per $A^{-1} M \bar{A}$. Sia dunque $M = S^{-1} \cdot \bar{S}$; allora $A^{-1} M \bar{A} = (A^{-1} S^{-1}) (\overline{SA}) = (SA)^{-1} \cdot (\overline{SA})$. C.V.D.

Passiamo ora a dimostrare la seconda parte del Teorema di decomposizione; all'uopo ci varremo di argomentazioni che potrebbero venire agevolmente espresse col linguaggio geometrico.

Supponiamo per assurdo che l'asserto non sia vero; e sia M una matrice d'ordine minimo, $n$, nell'insieme delle matrici per cui il teorema non vale. Ovviamente, in virtù del cor. 1, $n \geq 2$; inoltre, combinando le proposizioni 2 e 3, l'asserto non è vero nemmeno per $-\overline{M}$.

Considerata ora la matrice $S = E_n - M$, si ha che $\bar{S} = E_n - \bar{M}$, onde $S \cdot (-\bar{M}) = -\bar{M} + E_n = \bar{S}$; quindi la matrice S deve essere non invertibile, altrimenti si avrebbe $-\bar{M} = S^{-1} \cdot \bar{S}$. Di conseguenza esiste $y = (y_1, y_2, \cdots, y_n) \in K^n - \{0\}$ tale che $y(E_n - M) = 0$, ossia $y = yM$; esiste quindi $x \in K_0^n - \{0\}$ (3) tale che $x = xM$. Poichè esiste almeno una matrice invertibile A d'ordine $n$ ad elementi in $K_0$ (onde $\bar{A} = A$) tale che $xA = (1, 0, 0, \cdots, 0)$, si ha che $xAA^{-1} = xAA^{-1}M$, cioè $(1, 0, 0, \cdots, 0) = (1, 0, 0, \cdots, 0) A^{-1}M\bar{A}$.

Si vede subito che la matrice $P = A^{-1}M\bar{A}$ è del tipo

$$\begin{pmatrix} 1, & 0, & \cdots, & 0 \\ p_1^2, & p_2^2, & \cdots, & p_n^2 \\ \cdots & \cdots & \cdots & \cdots \\ p_1^n, & p_2^n, & \cdots, & p_n^n \end{pmatrix}.$$

Naturalmente, com'è stato già osservato nella prop. 4, si ha $P \cdot \bar{P} = E_n$; di conseguenza $\delta_k^h = \sum_{i=1}^{n} p_i^h \cdot \bar{p}_k^i$ (con $h, k = 1, 2, \cdots, n$, e con $\delta_k^h = 1$ se $h = k$, $\delta_k^h = 0$ se $h \neq k$), onde per $h, k = 2, 3, \cdots, n$ si ha che

$$\delta_k^h = p_1^h \cdot \bar{p}_k^1 + \sum_{i=2}^{n} p_i^h \cdot \bar{p}_k^i = \sum_{i=2}^{n} p_i^h \cdot \bar{p}_k^i ;$$

il che sta a significare che, detta Q la matrice ottenuta da P eliminando la prima riga e la prima colonna, si ha $Q \cdot \bar{Q} = E_{n-1}$.

Per il modo com'è stato scelto $n$, si ha che il teorema di decomposizione è applicabile a Q, ossia esiste una matrice U ad elementi in K, invertibile e di ordine $n - 1$, tale che $Q = U^{-1} \cdot \bar{U}$ (onde $UQ\bar{U}^{-1} = E_{n-1}$).

Consideriamo ora, con ovvio significato per i simboli, la matrice d'ordine $n$

$$V = \begin{pmatrix} 1 & 0 \\ 0 & U^{-1} \end{pmatrix} = \begin{pmatrix} 1, & 0, & 0, & \cdots, & 0 \\ 0, & v_2^2, & \cdots & \cdots, & v_n^2 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0, & v_2^n, & \cdots & \cdots, & v_n^n \end{pmatrix};$$

poniamo inoltre, potendosi facilmente verificare che

$$V^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & U \end{pmatrix} \quad , \quad V^{-1} = \begin{pmatrix} 1, & 0, & 0, & \cdots, & 0 \\ 0, & w_2^2, & \cdots & \cdots, & w_n^2 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0, & w_2^n, & \cdots & \cdots, & w_n^n \end{pmatrix};$$

(3) Con $K_0$ indichiamo il sottocorpo (proprio) di K costituito dagli elementi $k \in K$ tali che $k = \bar{k}$. Si osservi che l'$x$ in questione esiste in quanto $\overline{y + \bar{y}} = \bar{y} + y = y + \bar{y}$; inoltre, poichè $y = yM$, si ha $\bar{y} = \overline{yM}$, onde $\bar{y}M = \bar{y}\bar{M}M = \bar{y}$. Ne consegue immediatamente che $y + \bar{y} = (y + \bar{y})M$; per cui, se $\bar{y} \neq -y$, basta porre $x = y + \bar{y}$. Se invece $\bar{y} = -y$ basta porre, alla luce del cor. 2, $x = \varepsilon y$, infatti $\overline{\varepsilon y} = (-\varepsilon) \cdot (-y) = \varepsilon y$ ed $(\varepsilon y) M = \varepsilon (yM) = \varepsilon y$.

sarà allora $U^{-1} = \begin{pmatrix} v_2^2, \cdots, v_n^2 \\ \cdots\cdots\cdots \\ v_2^n, \cdots, v_n^n \end{pmatrix}$ ed $U = \begin{pmatrix} w_2^2, \cdots, w_n^2 \\ \cdots\cdots\cdots \\ w_2^n, \cdots, w_n^n \end{pmatrix}$.

Verifichiamo poi che la matrice $V^{-1} P \bar{V}$ è del tipo

$$\begin{pmatrix} 1, 0, 0, \cdots, 0 \\ r_1^2, 1, 0, \cdots, 0 \\ r_1^3, 0, 1, \cdots, 0 \\ \cdots\cdots\cdots\cdots\cdots \\ r_1^n, 0, 0, \cdots, 1 \end{pmatrix},$$

cioè ha le colonne successive alla prima eguali alle corrispondenti colonne della matrice $E_n$, inoltre $r_1^1 = 1$. Infatti $r_1^1 = \sum_{i=1}^{n} \sum_{j=1}^{n} w_i^1 p_j^i \bar{v}_1^j = w_1^1 p_1^1 v_1^1 = 1$; d'altro canto per $k \geq 2$ si ha $r_k^1 = \sum_{i=1}^{n} \sum_{j=1}^{n} w_i^1 p_j^i \bar{v}_k^j = \sum_{j=1}^{n} p_j^1 \bar{v}_k^j = p_1^1 \bar{v}_k^1 + \sum_{j=2}^{n} p_j^1 \bar{v}_k^j = 0$; infine, per $h \geq 2$ e $k \geq 2$, $r_k^h = \sum_{i=1}^{n} \sum_{j=1}^{n} w_i^h p_j^i \bar{v}_k^j = \sum_{i=2}^{n} \sum_{j=2}^{n} w_i^h p_j^i \bar{v}_k^j = \delta_k^h$, dal momento che $UQ\bar{U}^{-1} = E_{n-1}$.

Distinguiamo ora i due casi: 1) Char $K \neq 2$; 2) Char $K = 2$.

*Caso* 1): poniamo $T = E_n + (\overline{V^{-1} P \bar{V}}) = E_n + \bar{V}^{-1} \bar{P} V$; allora $\bar{T} = E_n + V^{-1} P \bar{V}$, onde $T \cdot (V^{-1} P \bar{V}) = V^{-1} P \bar{V} + E_n = \bar{T}$. Essendo

$$T = E_n + \bar{V}^{-1} \bar{P} V = \begin{pmatrix} 2, 0, 0, \cdots, 0 \\ \bar{r}_1^2, 2, 0, \cdots, 0 \\ \cdots\cdots\cdots\cdots\cdots \\ \bar{r}_1^n, 0, 0, \cdots, 2 \end{pmatrix},$$

si ha che T è invertibile, dal momento che le sue righe sono linearmente indipendenti a sinistra. Se ne deduce che l'asserto vale per $V^{-1} P \bar{V}$; e quindi, grazie alla prop. 4, vale anche per $P = A^{-1} M \bar{A}$ e per M, il che è assurdo.

*Caso* 2): considerato $k \in K$ tale che $k + \bar{k} = k - \bar{k} \neq 0$, poniamo $T = \bar{k} E_n + k (\overline{V^{-1} P \bar{V}}) = \bar{k} E_n + k (\bar{V}^{-1} \bar{P} V)$; allora si ha subito $T V^{-1} P \bar{V} = \bar{T}$. Essendo

$$T = \bar{k} E_n + k (\bar{V}^{-1} \bar{P} V) = \begin{pmatrix} \bar{k}+k, 0, 0, \cdots, 0 \\ k\bar{r}_1^2, \bar{k}+k, 0, \cdots, 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ k\bar{r}_1^n, 0, 0, \cdots, \bar{k}+k \end{pmatrix},$$

si ha che anche quest'ultima matrice è invertibile, dal momento che le sue righe sono chiaramente linearmente indipendenti a sinistra. Si conclude che anche in questo secondo caso il teorema vale per $V^{-1} P \bar{V}$; quindi esso vale anche per $P = A^{-1} M \bar{A}$ e per M, il che è assurdo.

Con ciò il teorema resta completamente provato.