Note del corso di Geometria 1

Gabriel Antonio Videtta

17 e 19 aprile 2023

Prodotti hermitiani, spazi euclidei e teorema spettrale

Nota. Nel corso del documento, per V si intenderà uno spazio vettoriale di dimensione finita n e per φ un suo prodotto, hermitiano o scalare dipendentemente dal contesto.

Definizione. (prodotto hermitiano) Sia $\mathbb{K} = \mathbb{C}$. Una mappa $\varphi : V \times V \to \mathbb{C}$ si dice **prodotto hermitiano** se:

(i) φ è $\mathbb{C}$-lineare nel secondo argomento, ossia se $\varphi(\underline{v}, \underline{u} + \underline{w}) = \varphi(\underline{v}, \underline{u}) + \varphi(\underline{v}, \underline{w})$ e $\varphi(\underline{v}, a\underline{w}) = a\,\varphi(\underline{v}, \underline{w})$,

(ii) $\varphi(\underline{u}, \underline{w}) = \overline{\varphi(\underline{w}, \underline{u})}$.

Definizione. (prodotto hermitiano canonico in $\mathbb{C}^n$) Si definisce **prodotto hermitiano canonico** di $\mathbb{C}^n$ il prodotto $\varphi : \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}$ tale per cui, detti $\underline{v} = (z_1 \cdots z_n)^\top$ e $\underline{w} = (w_1 \cdots w_n)^\top$, $\varphi(\underline{v}, \underline{w}) = \sum_{i=1}^n \overline{z_i} w_i$.

Osservazione.
▶ $\varphi(\underline{u} + \underline{w}, \underline{v}) = \overline{\varphi(\underline{v}, \underline{u} + \underline{w})} = \overline{\varphi(\underline{v}, \underline{u}) + \varphi(\underline{v}, \underline{w})} = \overline{\varphi(\underline{v}, \underline{u})} + \overline{\varphi(\underline{v}, \underline{u})} = \varphi(\underline{w}, \underline{v}) + \varphi(\underline{u}, \underline{v})$, ossia φ è additiva anche nel primo argomento.
▶ $\varphi(a\underline{v}, \underline{w}) = \overline{\varphi(\underline{w}, a\underline{v})} = \overline{a}\overline{\varphi(\underline{w}, \underline{v})} = \overline{a}\,\varphi(\underline{v}, \underline{w})$.
▶ $\varphi(\underline{v}, \underline{v}) = \overline{\varphi(\underline{v}, \underline{v})}$, e quindi $\varphi(\underline{v}, \underline{v}) \in \mathbb{R}$.
▶ Sia $\underline{v} = \sum_{i=1}^n x_i \underline{v_i}$ e sia $\underline{w} = \sum_{i=1}^n y_i \underline{v_i}$, allora $\varphi(\underline{v}, \underline{w}) = \sum_{i=1}^n \sum_{j=1}^n \overline{x_i} y_i \varphi(\underline{v_i}, \underline{v_j})$.
▶ $\varphi(\underline{v}, \underline{w}) = 0 \iff \varphi(\underline{w}, \underline{v}) = 0$.

Proposizione. Data la forma quadratica $q : V \to \mathbb{R}$ del prodotto hermitiano φ tale che $q(\underline{v}) = \varphi(\underline{v}, \underline{v}) \in \mathbb{R}$, tale forma quadratica individua univocamente il prodotto hermitiano φ.

Dimostrazione. Innanzitutto si osserva che:

$$\varphi(\underline{v}, \underline{w}) = \frac{\varphi(\underline{v}, \underline{w}) + \overline{\varphi(\underline{v}, \underline{w})}}{2} + \frac{\varphi(\underline{v}, \underline{w}) . \overline{\varphi(\underline{v}, \underline{w})}}{2}.$$

Si considerano allora le due identità:

$$q(\underline{v} + \underline{w}) - q(\underline{v}) - q(\underline{w}) = \varphi(\underline{v}, \underline{w}) + \overline{\varphi(\underline{w}, \underline{v})} = 2\,\Re(\varphi(\underline{v}, \underline{w})),$$

$$q(i\underline{v} + \underline{w}) - q(\underline{v}) - q(\underline{w}) = -i(\varphi(\underline{v}, \underline{w}) - \overline{\varphi(\underline{v}, \underline{w})}) = 2\,\Im(\varphi(\underline{v}, \underline{w})),$$

da cui si conclude che il prodotto φ è univocamente determinato dalla sua forma quadratica. □

Definizione. Si definisce **matrice aggiunta** di $A \in M(n, \mathbb{K})$ la matrice coniugata della trasposta di A, ossia:

$$A^* = \overline{A^\top} = \overline{A}^\top.$$

Osservazione. Per quanto riguarda la matrice aggiunta valgono le principali proprietà della matrice trasposta:

- $(A + B)^* = A^* + B^*$,
- $(AB)^* = B^* A^*$,
- $(A^{-1})^* = (A^*)^{-1}$, se A è invertibile.

Definizione. (matrice associata del prodotto hermitiano) Analogamente al caso del prodotto scalare, data una base $\mathcal{B} = \{\underline{v_1}, \ldots, \underline{v_n}\}$ si definisce come **matrice associata del prodotto hermitiano** φ la matrice $M_\mathcal{B}(\varphi) = (\varphi(\underline{v_i}, \underline{v_j}))_{i,j=1—n}$.

Osservazione. Si osserva che, analogamente al caso del prodotto scalare, vale la seguente identità:

$$\varphi(\underline{v}, \underline{w}) = [\underline{v}]_\mathcal{B}^* M_\mathcal{B}(\varphi) [\underline{w}]_\mathcal{B}.$$

Proposizione. (formula del cambiamento di base per i prodotto hermitiani) Siano $\mathcal{B}$, $\mathcal{B}'$ due basi di V. Allora vale la seguente identità:

$$M_{\mathcal{B}'} = M_\mathcal{B}^{\mathcal{B}'}(\mathrm{Id}_V)^* M_\mathcal{B}(\varphi) M_\mathcal{B}^{\mathcal{B}'}(\mathrm{Id}_V).$$

Dimostrazione. Siano $\mathcal{B} = \{\underline{v_1}, \ldots, \underline{v_n}\}$ e $\mathcal{B}' = \{\underline{w_1}, \ldots, \underline{w_n}\}$. Allora $\varphi(\underline{w_i}, \underline{w_j}) = [\underline{w_i}]_{\mathcal{B}}^* M_{\mathcal{B}}(\varphi)[\underline{w_j}]_{\mathcal{B}} = \left(M_{\mathcal{B}}^{\mathcal{B}'}(\mathrm{Id}_V)^i\right)^* M_{\mathcal{B}}(\varphi) M_{\mathcal{B}}^{\mathcal{B}'}(\mathrm{Id}_V)^j = \left(M_{\mathcal{B}}^{\mathcal{B}'}(\mathrm{Id}_V)\right)_i^* M_{\mathcal{B}}(\varphi) M_{\mathcal{B}}^{\mathcal{B}'}(\mathrm{Id}_V)^j$, da cui si ricava l'identità desiderata. $\square$

Definizione. (radicale di un prodotto hermitiano) Analogamente al caso del prodotto scalare, si definisce il **radicale** del prodotto φ come il seguente sottospazio:

$$V^\perp = \{\underline{v} \in V \mid \varphi(\underline{v}, \underline{w}) = 0 \;\forall\, \underline{w} \in V\}.$$

Proposizione. Sia $\mathcal{B}$ una base di V e φ un prodotto hermitiano. Allora $V^\perp = [\cdot]_{\mathcal{B}}^{-1}(\operatorname{Ker} M_{\mathcal{B}}(\varphi))$[1].

Dimostrazione. Sia $\mathcal{B} = \{\underline{v_1}, \ldots, \underline{v_n}\}$ e sia $\underline{v} \in V^\perp$. Siano a_1, ..., $a_n \in \mathbb{K}$ tali che $\underline{v} = a_1\underline{v_1} + \ldots + a_n\underline{v_n}$. Allora, poiché $\underline{v} \in V$, $0 = \varphi(\underline{v_i}, \underline{v}) == a_1\varphi(\underline{v_i}, \underline{v_1}) + \ldots + a_n\varphi(\underline{v_i}, \underline{v_n}) = M_i[\underline{v}]_{\mathcal{B}}$, da cui si ricava che $[\underline{v}]_{\mathcal{B}} \in \operatorname{Ker} M_{\mathcal{B}}(\varphi)$, e quindi che $V^\perp \subseteq [\cdot]_{\mathcal{B}}^{-1}(\operatorname{Ker} M_{\mathcal{B}}(\varphi))$.

Sia ora $\underline{v} \in V$ tale che $[\underline{v}]_{\mathcal{B}} \in \operatorname{Ker} M_{\mathcal{B}}(\varphi)$. Allora, per ogni $\underline{w} \in V$, $\varphi(\underline{w}, \underline{v}) = [\underline{w}]_{\mathcal{B}}^* M_{\mathcal{B}}(\varphi)[\underline{v}]_{\mathcal{B}} = [\underline{w}]_{\mathcal{B}}^* 0 = 0$, da cui si conclude che $\underline{v} \in V^\perp$, e quindi che $V^\perp \supseteq [\cdot]_{\mathcal{B}}^{-1}(\operatorname{Ker} M_{\mathcal{B}}(\varphi))$, da cui $V^\perp = [\cdot]_{\mathcal{B}}^{-1}(\operatorname{Ker} M_{\mathcal{B}}(\varphi))$, ossia la tesi. $\square$

Osservazione. Come conseguenza della proposizione appena dimostrata, valgono le principali proprietà già viste per il prodotto scalare.

- $\det(M_{\mathcal{B}}(\varphi)) = 0 \iff V^\perp \neq \{\underline{0}\} \iff \varphi$ è degenere,
- Vale il teorema di Lagrange, e quindi quello di Sylvester, benché con alcune accortezze: si introduce, come nel caso di $\mathbb{R}$, il concetto di segnatura, che diventa l'invariante completo della nuova congruenza hermitiana, che ancora una volta si dimostra essere una relazione di equivalenza.

Definizione. (restrizione ai reali di uno spazio) Sia V uno spazio vettoriale su $\mathbb{C}$ con base $\mathcal{B}$. Si definisce allora lo spazio $V_{\mathbb{R}}$, detto **spazio di restrizione su** $\mathbb{R}$ di V, come uno spazio su $\mathbb{R}$ generato da $\mathcal{B}_{\mathbb{R}} = \mathcal{B} \cup i\mathcal{B}$.

Esempio. Si consideri $V = \mathbb{C}^3$. Una base di $\mathbb{C}^3$ è chiaramente $\{\underline{e_1}, \underline{e_2}, \underline{e_3}\}$. Allora $V_{\mathbb{R}}$ sarà uno spazio vettoriale su $\mathbb{R}$ generato dai vettori $\{\underline{e_1}, \underline{e_2}, \underline{e_3}, i\underline{e_1}, i\underline{e_2}, i\underline{e_3}\}$.

[1] Stavolta non è sufficiente considerare la mappa $f : V \to V^*$ tale che $f(\underline{v}) = [\underline{w} \mapsto \varphi(\underline{v}, \underline{w})]$, dal momento che f non è lineare, bensì antilineare, ossia $f(a\underline{v}) = \overline{a} f(\underline{v})$.

Osservazione. Si osserva che lo spazio di restrizione su $\mathbb{R}$ e lo spazio di partenza condividono lo stesso insieme di vettori. Infatti, $\mathrm{Span}_{\mathbb{C}}(\mathcal{B}) = \mathrm{Span}_{\mathbb{R}}(\mathcal{B} \cup i\mathcal{B})$. Ciononostante, $\dim V_{\mathbb{R}} = 2 \dim V$[2], se $\dim V \in \mathbb{N}$.

Definizione. (complessificazione di uno spazio) Sia V uno spazio vettoriale su $\mathbb{R}$. Si definisce allora lo **spazio complessificato** $V_{\mathbb{C}} = V \times V$ su $\mathbb{C}$ con le seguenti operazioni:

- $(\underline{v}, \underline{w}) + (\underline{v}', \underline{w}') = (\underline{v} + \underline{v}', \underline{w} + \underline{w}')$,
- $(a + bi)(\underline{v}, \underline{w}) = (a\underline{v} - b\underline{w}, a\underline{w} + b\underline{v})$.

Osservazione. La costruzione dello spazio complessificato emula in realtà la costruzione di $\mathbb{C}$ come spazio $\mathbb{R} \times \mathbb{R}$. Infatti se $z = (c, d)$, vale che $(a + bi)(c, d) = (ac - bd, ad + bc)$, mentre si mantiene l'usuale operazione di addizione. In particolare si può identificare l'insieme $V \times \{\underline{0}\}$ come V, mentre $\{\underline{0}\} \times V$ viene identificato come l'insieme degli immaginari iV di $V_{\mathbb{C}}$. Infine, moltiplicare per uno scalare reale un elemento di $V \times \{\underline{0}\}$ equivale a moltiplicare la sola prima componente con l'usuale operazione di moltiplicazione di V. Allora, come accade per $\mathbb{C}$, si può sostituire la notazione $(\underline{v}, \underline{w})$ con la più comoda notazione $\underline{v} + i\underline{w}$.

Osservazione. Sia $\mathcal{B} = \{\underline{v_1}, \ldots, \underline{v_n}\}$ una base di V. Innanzitutto si osserva che $(a + bi)(\underline{v}, \underline{0}) = (a\underline{v}, b\underline{v})$. Pertanto si può concludere che $\mathcal{B} \times \{\underline{0}\}$ è una base dello spazio complessificato $V_{\mathbb{C}}$ su $\mathbb{C}$.

Infatti, se $(a_1 + b_1 i)(\underline{v_1}, \underline{0}) + \ldots + (a_n + b_n i)(\underline{v_n}, \underline{0}) = (\underline{0}, \underline{0})$, allora $(a_1\underline{v_1} + \ldots + a_n\underline{v_n}, b_1\underline{v_1} + \ldots + b_n\underline{v_n}) = (\underline{0}, \underline{0})$. Poiché però $\mathcal{B}$ è linearmente indipendente per ipotesi, l'ultima identità implica che $a_1 = \cdots = a_n = b_1 = \cdots = b_n = 0$, e quindi che $\mathcal{B} \times \{\underline{0}\}$ è linearmente indipendente.

Inoltre $\mathcal{B} \times \{\underline{0}\}$ genera $V_{\mathbb{C}}$. Se infatti $\underline{v} = (\underline{u}, \underline{w})$, e vale che:

$$\underline{u} = a_1\underline{v_1} + \ldots + a_n\underline{v_n}, \quad \underline{w} = b_1\underline{v_1} + \ldots + b_n\underline{v_n},$$

allora $\underline{v} = (a_1 + b_1 i)(\underline{v_1}, \underline{0}) + \ldots + (a_n + b_n i)(\underline{v_n}, \underline{0})$. Quindi $\dim V_{\mathbb{C}} = \dim V$.

Definizione. Sia f un'applicazione $\mathbb{C}$-lineare di V spazio vettoriale su $\mathbb{C}$. Allora si definisce la **restrizione su** $\mathbb{R}$ di f, detta $f_{\mathbb{R}} : V_{\mathbb{R}} \to V_{\mathbb{R}}$, in modo tale che $f_{\mathbb{R}}(\underline{v}) = f(\underline{v})$.

[2] Si sarebbe potuto ottenere lo stesso risultato utilizzando il teorema delle torri algebriche: $[V_{\mathbb{R}} : \mathbb{R}] = [V : \mathbb{C}][\mathbb{C} : \mathbb{R}] = 2[V : \mathbb{C}]$.

Osservazione. Sia $\mathcal{B} = \{\underline{v_1}, \ldots, \underline{v_n}\}$ una base di V su $\mathbb{C}$. Sia $A = M_{\mathcal{B}}(f)$. Si osserva allora che, se $\mathcal{B}' = \mathcal{B} \cup i\mathcal{B}$ e $A = A' + iA''$ con A', $A'' \in M(n, \mathbb{R})$, vale la seguente identità:

$$M_{\mathcal{B}'}(f_{\mathbb{R}}) = \left(\begin{array}{c|c} A' & -A'' \\ \hline A'' & A' \end{array}\right).$$

Infatti, se $f(\underline{v_i}) = (a_1 + b_1 i)\underline{v_1} + \ldots + (a_n + b_n i)\underline{v_n}$, vale che $f_{\mathbb{R}}(\underline{v_i}) = a_1\underline{v_1} + \ldots + a_n\underline{v_n} + b_1(i\underline{v_1}) + \ldots + b_n(i\underline{v_n})$, mentre $f_{\mathbb{R}}(i\underline{v_i}) = if(\underline{v_i}) = -b_1\underline{v_1} + \ldots - b_n\underline{v_n} + a_1(i\underline{v_1}) + \ldots + a_n(i\underline{v_n})$.

Definizione. Sia f un'applicazione $\mathbb{R}$-lineare di V spazio vettoriale su $\mathbb{R}$. Allora si definisce la **complessificazione** di f, detta $f_{\mathbb{C}} : V_{\mathbb{C}} \to V_{\mathbb{C}}$, in modo tale che $f_{\mathbb{C}}(\underline{v} + i\underline{w}) = f(\underline{v}) + if(\underline{w})$.

Osservazione. Si verifica infatti che $f_{\mathbb{C}}$ è $\mathbb{C}$-lineare.

- $f_{\mathbb{C}}((\underline{v_1} + i\underline{w_1}) + (\underline{v_2} + i\underline{w_2})) = f_{\mathbb{C}}((\underline{v_1} + \underline{v_2}) + i(\underline{w_1} + \underline{w_2})) = f(\underline{v_1} + \underline{v_2}) + if(\underline{w_1} + \underline{w_2}) = (f(\underline{v_1}) + if(\underline{w_1})) + (f(\underline{v_2}) + if(\underline{w_2})) = f_{\mathbb{C}}(\underline{v_1} + i\underline{w_1}) + f_{\mathbb{C}}(\underline{v_2} + i\underline{w_2})$.
- $f_{\mathbb{C}}((a+bi)(\underline{v}+i\underline{w})) = f_{\mathbb{C}}(a\underline{v} - b\underline{w} + i(a\underline{w} + b\underline{v})) = f(a\underline{v} - b\underline{w}) + if(a\underline{w} + b\underline{v}) = af(\underline{v}) - bf(\underline{w}) + i(af(\underline{w}) + bf(\underline{v})) = (a + bi)(f(\underline{v}) + if(\underline{w})) = (a + bi)f_{\mathbb{C}}(\underline{v} + i\underline{w})$.

Proposizione. Sia $f_{\mathbb{C}}$ la complessificazione di $f \in \mathrm{End}(V)$, dove V è uno spazio vettoriale su $\mathbb{R}$. Sia inoltre $\mathcal{B} = \{\underline{v_1}, \ldots, \underline{v_n}\}$ una base di V. Valgono allora i seguenti risultati:

(i) $(f_{\mathbb{C}})_{\mathbb{R}}|_V$ assume gli stessi valori di f,

(ii) $M_{\mathcal{B}}(f_{\mathbb{C}}) = M_{\mathcal{B}}(f) \in M(n, \mathbb{R})$,

(iii) $M_{\mathcal{B} \cup i\mathcal{B}}((f_{\mathbb{C}})_{\mathbb{R}}) = \left(\begin{array}{c|c} M_{\mathcal{B}}(f) & 0 \\ \hline 0 & M_{\mathcal{B}}(f) \end{array}\right)$.

Dimostrazione. Si dimostrano i risultati separatamente.

(i) Si osserva che $(f_{\mathbb{C}})_{\mathbb{R}}(\underline{v_i}) = f_{\mathbb{C}}(\underline{v_i}) = f(\underline{v_i})$. Dal momento che $(f_{\mathbb{C}})_{\mathbb{R}}$ è $\mathbb{R}$-lineare, si conclude che $(f_{\mathbb{C}})_{\mathbb{R}}$ assume gli stessi valori di f.

(ii) Dal momento che $\mathcal{B}$, nell'identificazione di $(\underline{v}, \underline{0})$ come $\underline{v}$, è sempre una base di $V_{\mathbb{C}}$, e $f_{\mathbb{C}}(\underline{v_i}) = f(\underline{v_i})$, chiaramente $[f_{\mathbb{C}}(\underline{v_i})]_{\mathcal{B}} = [f(\underline{v_i})]_{\mathcal{B}}$, e quindi $M_{\mathcal{B}}(f_{\mathbb{C}}) = M_{\mathcal{B}}(f)$, dove si osserva anche che $M_{\mathcal{B}}(f) \in M(n, \mathbb{R})$, essendo V uno spazio vettoriale su $\mathbb{R}$.

(iii) Sia $f(\underline{v_i}) = a_1\underline{v_1} + \ldots + a_n\underline{v_n}$ con a_1, ..., $a_n \in \mathbb{R}$. Come osservato in (i), $(f_\mathbb{C})_\mathbb{R}|_\mathcal{B} = (f_\mathbb{C})_\mathbb{R}|_\mathcal{B}$, e quindi la prima metà di $M_{\mathcal{B}\cup i\mathcal{B}}((f_\mathbb{C})_\mathbb{R})$ è formata da due blocchi: uno verticale coincidente con $M_\mathcal{B}(f)$ e un altro completamente nullo, dal momento che non compare alcun termine di $i\mathcal{B}$ nella scrittura di $(f_\mathbb{C})_\mathbb{R}(\underline{v_i})$. Al contrario, per $i\mathcal{B}$, $(f_\mathbb{C})_\mathbb{R}(i\underline{v_i}) = f_\mathbb{C}(i\underline{v_i}) = if(\underline{v_i}) = a_1(i\underline{v_1}) + \ldots + a_n(i\underline{v_n})$; pertanto la seconda metà della matrice avrà i due blocchi della prima metà, benché scambiati.

□

Osservazione. Dal momento che $M_\mathcal{B}(f_\mathbb{C}) = M_\mathcal{B}(f)$, $f_\mathbb{C}$ e f condividono lo stesso polinomio caratteristico e vale che $\mathrm{sp}(f) \subseteq \mathrm{sp}(f_\mathbb{C})$, dove vale l'uguaglianza se e solo se tale polinomio caratteristico è completamente riducibile in $\mathbb{R}$. Inoltre, se V_λ è l'autospazio su V dell'autovalore λ, l'autospazio su $V_\mathbb{C}$, rispetto a $f_\mathbb{C}$, è invece $V_{\mathbb{C}\lambda} = V_\lambda + iV_\lambda$, la cui dimensione rimane invariata rispetto a V_λ, ossia $\dim V_\lambda = \dim V_{\mathbb{C}\lambda}$ (infatti, analogamente a prima, una base di V_λ può essere identificata come base anche per $V_{\mathbb{C}\lambda}$).

Proposizione. Sia $f_\mathbb{C}$ la complessificazione di $f \in \mathrm{End}(V)$, dove V è uno spazio vettoriale su $\mathbb{R}$. Sia inoltre $\mathcal{B} = \{\underline{v_1}, \ldots, \underline{v_n}\}$ una base di V. Allora un endomorfismo $\tilde{g} : V_\mathbb{C} \to V_\mathbb{C}$ complessifica un endomorfismo $g \in \mathrm{End}(V)$ $\iff M_\mathcal{B}(\tilde{g}) \in M(n, \mathbb{R})$.

Dimostrazione. Se $\tilde{g}$ complessifica $g \in \mathrm{End}(V)$, allora, per la proposizione precedente, $M_\mathcal{B}(\tilde{g}) = M_\mathcal{B}(g) \in M(n, \mathbb{R})$. Se invece $A = M_\mathcal{B}(\tilde{g}) \in M(n, \mathbb{R})$, si considera $g = M_\mathcal{B}^{-1}(A) \in \mathrm{End}(V)$. Si verifica facilmente che $\tilde{g}$ non è altro che il complessificato di tale g:

- $\tilde{g}(\underline{v_i}) = g(\underline{v_i})$, dove l'uguaglianza è data dal confronto delle matrici associate, e quindi $\tilde{g}|_V = g$;
- $\tilde{g}(\underline{v} + i\underline{w}) = \tilde{g}(\underline{v}) + i\tilde{g}(\underline{w}) = g(\underline{v}) + ig(\underline{w})$, da cui la tesi.

□

Proposizione. Sia φ un prodotto scalare di V spazio vettoriale su $\mathbb{R}$. Allora esiste un unico prodotto hermitiano $\varphi_\mathbb{C} : V_\mathbb{C} \times V_\mathbb{C} \to \mathbb{C}$ che estende φ (ossia tale che $\varphi_\mathbb{C}|_{V \times V} = \varphi$), il quale assume la stessa segnatura di φ.

Dimostrazione. Sia $\mathcal{B}$ una base di Sylvester per φ. Si consideri allora il prodotto $\varphi_\mathbb{C}$ tale che:

$$\varphi_\mathbb{C}(\underline{v_1} + i\underline{w_1}, \underline{v_2} + i\underline{w_2}) = \varphi(\underline{v_1}, \underline{v_2}) + \varphi(\underline{w_1}, \underline{w_2}) + i(\varphi(\underline{v_1}, \underline{w_1}) - \varphi(\underline{w_1}, \underline{v_2})).$$

Chiaramente $\varphi_{\mathbb{C}}|_{V \times V} = \varphi$. Si verifica allora che $\varphi_{\mathbb{C}}$ è hermitiano:

- $\varphi_{\mathbb{C}}(\underline{v} + i\underline{w}, (\underline{v_1} + i\underline{w_1}) + (\underline{v_2} + i\underline{w_2})) = \varphi(\underline{v}, \underline{v_1} + \underline{v_2}) + \varphi(\underline{w}, \underline{w_1} + \underline{w_2}) + i(\varphi(\underline{v}, \underline{w_1} + \underline{w_2}) - \varphi(\underline{w}, \underline{v_1} + \underline{v_2})) = [\varphi(\underline{v}, \underline{v_1}) + \varphi(\underline{w}, \underline{w_1}) + i(\varphi(\underline{v}, \underline{w_1}) - \varphi(\underline{w}, \underline{v_1}))] + [\varphi(\underline{v}, \underline{v_2}) + \varphi(\underline{w}, \underline{w_2}) + i(\varphi(\underline{v}, \underline{w_2}) - \varphi(\underline{w}, \underline{v_2}))] = \varphi_{\mathbb{C}}(\underline{v} + i\underline{w}, \underline{v_1} + i\underline{w_1}) + \varphi_{\mathbb{C}}(\underline{v} + i\underline{w}, \underline{v_2} + i\underline{w_2})$ (additività nel secondo argomento),

- $\varphi_{\mathbb{C}}(\underline{v} + i\underline{w}, (a+bi)(\underline{v_1} + i\underline{w_1})) = \varphi_{\mathbb{C}}(\underline{v} + i\underline{w}, a\underline{v_1} - b\underline{w_1} + i(b\underline{v_1} + a\underline{w_1})) = \varphi(\underline{v}, a\underline{v_1} - b\underline{w_1}) + \varphi(\underline{w}, b\underline{v_1} + a\underline{w_1}) + i(\varphi(\underline{v}, b\underline{v_1} + a\underline{w_1}) - \varphi(\underline{w}, a\underline{v_1} - b\underline{w_1})) = a\varphi(\underline{v}, \underline{v_1}) - b\varphi(\underline{v}, \underline{w_1}) + b\varphi(\underline{w}, \underline{v_1}) + a\varphi(\underline{w}, \underline{w_1}) + i(b\varphi(\underline{v}, \underline{v_1}) + a\varphi(\underline{v}, \underline{w_1}) - a\varphi(\underline{w}, \underline{v_1}) + b\varphi(\underline{w}, \underline{w_1})) = a(\varphi(\underline{v}, \underline{v_1}) + \varphi(\underline{w}, \underline{w_1})) - b(\varphi(\underline{v}, \underline{w_1}) - \varphi(\underline{w}, \underline{v_1})) + i(a(\varphi(\underline{v}, \underline{w_1}) - \varphi(\underline{w}, \underline{v_1})) + b(\varphi(\underline{v}, \underline{v_1}) + \varphi(\underline{w}, \underline{w_1}))) = (a + bi)(\varphi(\underline{v}, \underline{v_1}) + \varphi(\underline{w}, \underline{w_1}) + i(\varphi(\underline{v}, \underline{w_1}) - \varphi(\underline{w}, \underline{v_1}))) = (a+bi)\varphi_{\mathbb{C}}(\underline{v} + \underline{w}, \underline{v_1} + i\underline{w_1})$ (omogeneità nel secondo argomento),

- $\varphi_{\mathbb{C}}(\underline{v_1} + i\underline{w_1}, \underline{v_2} + i\underline{w_2}) = \varphi(\underline{v_1}, \underline{v_2}) + \varphi(\underline{w_1}, \underline{w_2}) + i(\varphi(\underline{v_1}, \underline{w_2}) - \varphi(\underline{w_1}, \underline{v_2})) = \overline{\varphi(\underline{v_1}, \underline{v_2}) + \varphi(\underline{w_1}, \underline{w_2}) + i(\varphi(\underline{w_1}, \underline{v_2}) - \varphi(\underline{v_1}, \underline{w_2}))} = \overline{\varphi(\underline{v_2}, \underline{v_1}) + \varphi(\underline{w_2}, \underline{w_1}) + i(\varphi(\underline{v_2}, \underline{w_1}) - \varphi(\underline{w_2}, \underline{v_1}))} = \overline{\varphi_{\mathbb{C}}(\underline{v_2} + \underline{w_2}, \underline{v_1} + \underline{w_1})}$ (coniugio nello scambio degli argomenti).

Ogni prodotto hermitiano τ che estende il prodotto scalare φ ha la stessa matrice associata nella base $\mathcal{B}$, essendo $\tau(\underline{v_i}, \underline{v_i}) = \varphi(\underline{v_i}, \underline{v_i})$ vero per ipotesi. Pertanto τ è unico, e vale che $\tau = \varphi_{\mathbb{C}}$. Dal momento che $M_{\mathcal{B}}(\varphi_{\mathbb{C}}) = M_{\mathcal{B}}(\varphi)$ è una matrice di Sylvester, $\varphi_{\mathbb{C}}$ mantiene anche la stessa segnatura di φ. $\square$

Teorema. (di rappresentazione di Riesz per il prodotto scalare) Sia V uno spazio vettoriale e sia φ un suo prodotto scalare non degenere. Allora per ogni $f \in V^*$ esiste un unico $\underline{v} \in V$ tale che $f(\underline{w}) = \varphi(\underline{v}, \underline{w})\ \forall\, \underline{w} \in V$.

Dimostrazione. Si consideri l'applicazione a_φ. Poiché φ non è degenere, $\operatorname{Ker} a_\varphi = V^\perp = \{\underline{0}\}$, da cui si deduce che a_φ è un isomorfismo. Quindi $\forall\, f \in V^*$ esiste un unico $\underline{v} \in V$ tale per cui $a_\varphi(\underline{v}) = f$, e dunque tale per cui $\varphi(\underline{v}, \underline{w}) = a_\varphi(\underline{v})(\underline{w}) = f(\underline{w})\ \forall\, \underline{w} \in V$. $\square$

Dimostrazione costruttiva. Sia $\mathcal{B} = \{\underline{v_1}, \ldots, \underline{v_n}\}$ una base ortogonale di V per φ. Allora $\mathcal{B}^*$ è una base di V^*. In particolare $f = f(\underline{v_1})\underline{v_1}^* + \ldots + f(\underline{v_n})\underline{v_n}^*$. Sia $\underline{v} = \frac{f(\underline{v_1})}{\varphi(\underline{v_1}, \underline{v_1})}\underline{v_1} + \ldots + \frac{f(\underline{v_n})}{\varphi(\underline{v_n}, \underline{v_n})}$. Detto $\underline{w} = a_1\underline{v_1} + \ldots + a_n\underline{v_n}$, si deduce che $\varphi(\underline{v}, \underline{w}) = a_1 f(\underline{v_1}) + \ldots + a_n f(\underline{v_n}) = f(\underline{w})$. Se esistesse $\underline{v}' \in V$ con la stessa proprietà di $\underline{v}$, $\varphi(\underline{v}, \underline{w}) = \varphi(\underline{v}', \underline{w}) \implies \varphi(\underline{v} - \underline{v}', \underline{w})\ \forall\, \underline{w} \in V$. Si deduce dunque che $\underline{v} - \underline{v}' \in V^\perp$, contenente solo $\underline{0}$ dacché φ è non degenere; e quindi si conclude che $\underline{v} = \underline{v}'$, ossia che esiste solo un vettore con la stessa proprietà di $\underline{v}$. $\square$

Teorema. (di rappresentazione di Riesz per il prodotto hermitiano) Sia V uno spazio vettoriale su $\mathbb{C}$ e sia φ un suo prodotto hermitiano non degenere. Allora per ogni $f \in V^*$ esiste un unico $\underline{v} \in V$ tale che $f(\underline{w}) = \varphi(\underline{v}, \underline{w})$ $\forall\, \underline{w} \in V$.

Dimostrazione. Sia $\mathcal{B} = \{\underline{v_1}, \ldots, \underline{v_n}\}$ una base ortogonale di V per φ. Allora $\mathcal{B}^*$ è una base di V^*. In particolare $f = f(\underline{v_1})\underline{v_1}^* + \ldots + f(\underline{v_n})\underline{v_n}^*$. Sia $\underline{v} = \frac{\overline{f(v_1)}}{\varphi(\underline{v_1},\underline{v_1})}\underline{v_1} + \ldots + \frac{\overline{f(v_n)}}{\varphi(\underline{v_n},\underline{v_n})}$. Detto $\underline{w} = a_1\underline{v_1} + \ldots + a_n\underline{v_n}$, si deduce che $\varphi(\underline{v}, \underline{w}) = a_1 f(\underline{v_1}) + \ldots + a_n f(\underline{v_n}) = f(\underline{w})$. Se esistesse $\underline{v}' \in V$ con la stessa proprietà di $\underline{v}$, $\varphi(\underline{v}, \underline{w}) = \varphi(\underline{v}', \underline{w}) \implies \varphi(\underline{v} - \underline{v}', \underline{w})$ $\forall\, \underline{w} \in V$. Si deduce dunque che $\underline{v} - \underline{v}' \in V^\perp$, contenente solo $\underline{0}$ dacché φ è non degenere; e quindi si conclude che $\underline{v} = \underline{v}'$, ossia che esiste solo un vettore con la stessa proprietà di $\underline{v}$. $\square$

Proposizione. Sia V uno spazio vettoriale con prodotto scalare φ non degenere. Sia $f \in \mathrm{End}(V)$. Allora esiste un unico endomorfismo $f_\varphi^\top : V \to V$, detto il **trasposto di** f e indicato con $f^\top$ in assenza di ambiguità[3], tale che:

$$a_\varphi \circ g = f^\top \circ a_\varphi,$$

ossia che:

$$\varphi(\underline{v}, f(\underline{w})) = \varphi(g(\underline{v}), \underline{w})\ \forall\, \underline{v}, \underline{w} \in V.$$

Dimostrazione. Si consideri $(f^\top \circ a_\varphi)(\underline{v}) \in V^*$. Per il teorema di rappresentazione di Riesz per il prodotto scalare, esiste un unico $\underline{v}'$ tale che $(f^\top \circ a_\varphi)(\underline{v})(\underline{w}) = \varphi(\underline{v}', \underline{w}) \implies \varphi(\underline{v}, f(\underline{w})) = \varphi(\underline{v}', \underline{w})$ $\forall\, \underline{w} \in V$. Si costruisce allora una mappa $f_\varphi^\top : V \to V$ che associa a $\underline{v}$ tale $\underline{v}'$. Si dimostra che $f_\varphi^\top$ è un'applicazione lineare, e che dunque è un endomorfismo:

(i) Siano $\underline{v_1}$, $\underline{v_2} \in V$. Si deve dimostrare innanzitutto che $f_\varphi^\top(\underline{v_1} + \underline{v_2}) = f_\varphi^\top(\underline{v_1}) + f_\varphi^\top(\underline{v_2})$, ossia che $\varphi(f_\varphi^\top(\underline{v_1}) + f_\varphi^\top(\underline{v_2}), \underline{w}) = \varphi(\underline{v_1} + \underline{v_2}, f(\underline{w}))$ $\forall\, \underline{w} \in V$.

[3] Si tenga infatti in conto della differenza tra $f_\varphi^\top : V \to V$, di cui si discute nell'enunciato, e $f^\top : V^* \to V^*$ che invece è tale che $f^top(g) = g \circ f$.

Si osservano le seguenti identità:

$$\varphi(\underline{v_1} + \underline{v_2}, f(\underline{w})) = \varphi(\underline{v_1}, f(\underline{w})) + \varphi(\underline{v_2}, f(\underline{w})) = (*),$$
$$\varphi(f_\varphi^\top(\underline{v_1}) + f_\varphi^\top(\underline{v_2}), \underline{w}) = \varphi(f_\varphi^\top(\underline{v_1}), \underline{w}) + \varphi(f_\varphi^\top(\underline{v_2}), \underline{w}) = (*),$$

da cui si deduce l'uguaglianza desiderata, essendo $f_\varphi^\top(\underline{v_1} + \underline{v_2})$ l'unico vettore di V con la proprietà enunciata dal teorema di rappresentazione di Riesz.

(ii) Sia $\underline{v} \in V$. Si deve dimostrare che $f_\varphi^\top(a\underline{v}) = af_\varphi^\top(\underline{v})$, ossia che $\varphi(af_\varphi^\top(\underline{v}), \underline{w}) = \varphi(a\underline{v}, f(\underline{w}))\ \forall\, a \in \mathbb{K}$, $\underline{w} \in V$. È sufficiente moltiplicare per a l'identità $\varphi(f_\varphi^\top(\underline{v}), \underline{w}) = \varphi(\underline{v}, f(\underline{w}))$. Analogamente a prima, si deduce che $f_\varphi^\top(a\underline{v}) = af_\varphi^\top(\underline{v})$, essendo $f_\varphi^\top(a\underline{v})$ l'unico vettore di V con la proprietà enunciata dal teorema di rappresentazione di Riesz.

Infine si dimostra che $f_\varphi^\top$ è unico. Sia infatti g un endomorfismo di V che condivide la stessa proprietà di $f_\varphi^\top$. Allora $\varphi(f_\varphi^\top(\underline{v}), \underline{w}) = \varphi(\underline{v}, f(\underline{w})) = \varphi(g(\underline{v}), \underline{w})\ \forall\, \underline{v}$, $\underline{w} \in V$, da cui si deduce che $\varphi(f_\varphi^\top(\underline{v}) -' (\underline{v}), \underline{w}) = 0\ \forall\, \underline{v}$, $\underline{w} \in V$, ossia che $f_\varphi^\top(\underline{v}) - g(\underline{v}) \in V^\perp\ \forall\, \underline{v} \in V$. Tuttavia φ è non degenere, e quindi $V^\perp = \{\underline{0}\}$, da cui si deduce che deve valere l'identità $f_\varphi^\top(\underline{v}) = g(\underline{v})$ $\forall\, \underline{v} \in V$, ossia $g = f_\varphi^\top$. □

Proposizione. Sia V uno spazio vettoriale su $\mathbb{C}$ e sia φ un suo prodotto hermitiano. Allora esiste un'unica mappa[4] $f^* : V \to V$, detta **aggiunto di** f, tale che $\varphi(\underline{v}, f(\underline{w})) = \varphi(f^*(\underline{v}), \underline{w})\ \forall\, \underline{v}$, $\underline{w} \in V$.

Dimostrazione. Sia $\underline{v} \in V$. Si consideri il funzionale σ tale che $\sigma(\underline{w}) = \varphi(\underline{v}, f(\underline{w}))$. Per il teorema di rappresentazione di Riesz per il prodotto scalare esiste un unico $\underline{v}' \in V$ tale per cui $\varphi(\underline{v}, f(\underline{w})) = \sigma(\underline{w}) = \varphi(\underline{v}', \underline{w})$. Si costruisce allora una mappa f^* che associa $\underline{v}$ a tale $\underline{v}'$.

Si dimostra infine che la mappa f^* è unica. Sia infatti $\mu : V \to V$ che condivide la stessa proprietà di f^*. Allora $\varphi(f^*(\underline{v}), \underline{w}) = \varphi(\underline{v}, f(\underline{w})) = \varphi(\mu(\underline{v}), \underline{w})\ \forall\, \underline{v}$, $\underline{w} \in V$, da cui si deduce che $\varphi(f^*(\underline{v}) - \mu(\underline{v}), \underline{w}) = 0\ \forall\, \underline{v}$, $\underline{w} \in V$, ossia che $f^*(\underline{v}) - \mu(\underline{v}) \in V^\perp\ \forall\, \underline{v} \in V$. Tuttavia φ è non degenere, e quindi $V^\perp = \{\underline{0}\}$, da cui si deduce che deve valere l'identità $f^*(\underline{v}) = \mu(\underline{v})$ $\forall\, \underline{v} \in V$, ossia $\mu = f^*$. □

[4]Si osservi che f^* non è un'applicazione lineare, benché sia invece *antilineare*.

Osservazione. L'operazione di trasposizione di un endomorfismo sul prodotto scalare non degenere φ è un'involuzione. Infatti valgono le seguenti identità $\forall \underline{v}, \underline{w} \in V$:

$$\begin{cases} \varphi(\underline{w}, f^\top(\underline{v})) = \varphi(f^\top(\underline{v}), \underline{w}) = \varphi(\underline{v}, f(\underline{w})), \\ \varphi(\underline{w}, f^\top(\underline{v})) = \varphi((f^\top)^\top(\underline{w}), \underline{v}) = \varphi(\underline{v}, (f^\top)^\top(\underline{w})). \end{cases}$$

Si conclude allora, poiché φ è non degenere, che $f(\underline{w}) = (f^\top)^\top(\underline{w})\ \forall\, \underline{w} \in V$, ossia che $f = (f^\top)^\top$.

Osservazione. Analogamente si può dire per l'operazione di aggiunta per un prodotto hermitiano φ non degenere. Valgono infatti le seguenti identità $\forall \underline{v}, \underline{w} \in V$:

$$\begin{cases} \overline{\varphi(\underline{w}, f^*(\underline{v}))} = \varphi(f^*(\underline{v}), \underline{w}) = \varphi(\underline{v}, f(\underline{w})), \\ \overline{\varphi(\underline{w}, f^*(\underline{v}))} = \overline{\varphi((f^*)^*(\underline{w}), \underline{v})} = \varphi(\underline{v}, (f^*)^*(\underline{w})), \end{cases}$$

da cui si deduce, come prima, che $f = (f^*)^*$.

Definizione. (base ortonormale) Si definisce **base ortonormale** di uno spazio vettoriale V su un suo prodotto φ una base ortogonale $\mathcal{B} = \{\underline{v_1}, \ldots, \underline{v_n}\}$ tale che $\varphi(\underline{v_i}, \underline{v_j}) = \delta_{ij}$.

Proposizione. Sia φ un prodotto scalare non degenere di V. Sia $f \in \operatorname{End}(V)$. Allora vale la seguente identità:

$$M_{\mathcal{B}}(f_\varphi^\top) = M_{\mathcal{B}}(\varphi)^{-1} M_{\mathcal{B}}(f)^\top M_{\mathcal{B}}(\varphi),$$

dove $\mathcal{B}$ è una base di V.

Dimostrazione. Sia $\mathcal{B}^*$ la base relativa a $\mathcal{B}$ in V^*. Per la proposizione precedente vale la seguente identità:

$$a_\varphi \circ f_\varphi^\top = f^\top \circ a_\varphi.$$

Pertanto, passando alle matrici associate, si ricava che:

$$M_{\mathcal{B}^*}^{\mathcal{B}}(a_\varphi) M_{\mathcal{B}}(f_\varphi^\top) = M_{\mathcal{B}^*}(f^\top) M_{\mathcal{B}^*}^{\mathcal{B}}(a_\varphi).$$

Dal momento che valgono le seguenti due identità:

$$M_{\mathcal{B}^*}^{\mathcal{B}}(a_\varphi) = M_{\mathcal{B}}(\varphi), \qquad M_{\mathcal{B}^*}(f^\top) = M_{\mathcal{B}}(f)^\top,$$

e a_φ è invertibile (per cui anche $M_{\mathcal{B}}(\varphi)$ lo è), si conclude che:

$$M_{\mathcal{B}}(\varphi)M_{\mathcal{B}}(f_\varphi^\top) = M_{\mathcal{B}}(f)^\top M_{\mathcal{B}}(\varphi) \implies M_{\mathcal{B}}(f_\varphi^\top) = M_{\mathcal{B}}(\varphi)^{-1}M_{\mathcal{B}}(f)^\top M_{\mathcal{B}}(\varphi),$$

da cui la tesi. $\square$

Corollario. Sia φ un prodotto scalare di V. Se $\mathcal{B}$ è una base ortonormale, φ è non degenere e $M_{\mathcal{B}}(f_\varphi^\top) = M_{\mathcal{B}}(f)^\top$.

Dimostrazione. Se $\mathcal{B}$ è una base ortonormale, $M_{\mathcal{B}}(\varphi) = I_n$. Pertanto φ è non degenere. Allora, per la proposizione precedente:

$$M_{\mathcal{B}}(f_\varphi^\top) = M_{\mathcal{B}}(\varphi)^{-1}M_{\mathcal{B}}(f)^\top M_{\mathcal{B}}(\varphi) = M_{\mathcal{B}}(f)^\top.$$

$\square$

Proposizione. Sia φ un prodotto hermitiano non degenere di V. Sia $f \in \operatorname{End}(V)$. Allora vale la seguente identità:

$$M_{\mathcal{B}}(f_\varphi^*) = M_{\mathcal{B}}(\varphi)^{-1}M_{\mathcal{B}}(f)^* M_{\mathcal{B}}(\varphi),$$

dove $\mathcal{B}$ è una base di V.

Dimostrazione. Sia $\mathcal{B} = \{\underline{v_1}, \ldots, \underline{v_n}\}$. Dal momento che φ è non degenere, $\operatorname{Ker} M_{\mathcal{B}}(\varphi) = V^\perp = \{\underline{0}\}$, e quindi $M_{\mathcal{B}}(\varphi)$ è invertibile.

Dacché allora $\varphi(f^*(\underline{v}), \underline{w}) = \varphi(\underline{v}, f(\underline{w}))\ \forall\, \underline{v}, \underline{w} \in V$, vale la seguente identità:

$$[f^*(\underline{v})]_{\mathcal{B}}^* M_{\mathcal{B}}(\varphi)[\underline{w}]_{\mathcal{B}} = [\underline{v}]_{\mathcal{B}}^* M_{\mathcal{B}}(\varphi)[f(\underline{w})]_{\mathcal{B}},$$

ossia si deduce che:

$$[\underline{v}]_{\mathcal{B}}^* M_{\mathcal{B}}(f^*)^* M_{\mathcal{B}}(\varphi)[\underline{w}]_{\mathcal{B}} = [\underline{v}]_{\mathcal{B}}^* M_{\mathcal{B}}(\varphi)M_{\mathcal{B}}(f)[\underline{w}]_{\mathcal{B}}.$$

Sostituendo allora a $\underline{v}$ e $\underline{w}$ i vettori della base $\mathcal{B}$, si ottiene che:

$$\begin{aligned}(M_{\mathcal{B}}(f^*)^* M_{\mathcal{B}}(\varphi))_{ij} &= [\underline{v_i}]_{\mathcal{B}}^* M_{\mathcal{B}}(f^*)^* M_{\mathcal{B}}(\varphi)[\underline{v_j}]_{\mathcal{B}} = \\ &= [\underline{v_i}]_{\mathcal{B}}^* M_{\mathcal{B}}(\varphi)M_{\mathcal{B}}(f)[\underline{v_j}]_{\mathcal{B}} = (M_{\mathcal{B}}(\varphi)M_{\mathcal{B}}(f))_{ij},\end{aligned}$$

e quindi che $M_{\mathcal{B}}(f^*)^* M_{\mathcal{B}}(\varphi) = M_{\mathcal{B}}(\varphi)M_{\mathcal{B}}(f)$. Moltiplicando a destra per l'inversa di $M_{\mathcal{B}}(\varphi)$ e prendendo l'aggiunta di ambo i membri (ricordando che $M_{\mathcal{B}}(\varphi)^* = M_{\mathcal{B}}(\varphi)$, essendo φ un prodotto hermitiano), si ricava l'identità desiderata.

$\square$

Corollario. Sia φ un prodotto hermitiano di V spazio vettoriale su $\mathbb{C}$. Se $\mathcal{B}$ è una base ortonormale, φ è non degenere e $M_\mathcal{B}(f_\varphi^*) = M_\mathcal{B}(f)^*$.

Dimostrazione. Se $\mathcal{B}$ è una base ortonormale, $M_\mathcal{B}(\varphi) = I_n$. Pertanto φ è non degenere. Allora, per la proposizione precedente:

$$M_\mathcal{B}(f_\varphi^*) = M_\mathcal{B}(\varphi)^{-1} M_\mathcal{B}(f)^* M_\mathcal{B}(\varphi) = M_\mathcal{B}(f)^*.$$

$\square$

Nota. D'ora in poi, nel corso del documento, s'intenderà per φ un prodotto scalare (o eventualmente hermitiano) non degenere di V.

Definizione. (operatori simmetrici) Sia $f \in \mathrm{End}(V)$. Si dice allora che f è **simmetrico** (o *autoaggiunto*) se $f = f^\top$.

Definizione. (applicazioni e matrici ortogonali) Sia $f \in \mathrm{End}(V)$. Si dice allora che f è **ortogonale** se $\varphi(\underline{v}, \underline{w}) = \varphi(f(\underline{v}), f(\underline{w}))$, ossia se è un'isometria in V. Sia $A \in M(n, \mathbb{K})$. Si dice dunque che A è **ortogonale** se $A^\top A = AA^\top = I_n$.

Definizione. Le matrici ortogonali di $M(n, \mathbb{K})$ formano un sottogruppo moltiplicativo di $\mathrm{GL}(n, \mathbb{K})$, detto **gruppo ortogonale**, e indicato con O_n. Il sottogruppo di O_n contenente solo le matrici con determinante pari a 1 è detto **gruppo ortogonale speciale**, e si denota con SO_n.

Osservazione. Si possono classificare in modo semplice alcuni di questi gruppi ortogonali per $\mathbb{K} = \mathbb{R}$.

▶ $A \in O_n \implies 1 = \det(I_n) = \det(AA^\top) = \det(A)^2 \implies \det(A) = \pm 1$.
▶ $A = (a) \in O_1 \iff A^\top A = I_1 \iff a^2 = 1 \iff a = \pm 1$, da cui si ricava che l'unica matrice di SO_1 è (1). Si osserva inoltre che O_1 è abeliano di ordine 2, e quindi che $O_1 \cong \mathbb{Z}/2\mathbb{Z}$.
▶ $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in O_2 \iff \begin{pmatrix} a^2+b^2 & ab+cd \\ ab+cd & c^2+d^2 \end{pmatrix} = A^\top A = I_2$.

Pertanto deve essere soddisfatto il seguente sistema di equazioni:

$$\begin{cases} a^2 + b^2 = c^2 + d^2 = 1, \\ ac + bd = 0. \end{cases}$$

Si ricava dunque che si può identificare A con le funzioni trigonometriche $\cos(\theta)$ e $\sin(\theta)$ con $\theta \in [0, 2\pi)$ nelle due forme:

$$A = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \qquad (\det(A) = 1, A \in SO_2),$$
$$A = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{pmatrix} \qquad (\det(A) = -1).$$

Definizione. (applicazioni e matrici hermitiane) Sia $f \in \operatorname{End}(V)$ e si consideri il prodotto hermitiano φ. Si dice allora che f è **hermitiano** se $f = f^*$. Sia $A \in M(n, \mathbb{C})$. Si dice dunque che A è **hermitiana** se $A = A^*$.

Definizione. (applicazioni e matrici unitarie) Sia $f \in \operatorname{End}(V)$ e si consideri il prodotto hermitiano φ. Si dice allora che f è **unitario** se $\varphi(\underline{v}, \underline{w}) = \varphi(f(\underline{v}), f(\underline{w}))$. Sia $A \in M(n, \mathbb{C})$. Si dice dunque che A è **unitaria** se $A^*A = AA^* = I_n$.

Definizione. Le matrici unitarie di $M(n, \mathbb{C})$ formano un sottogruppo moltiplicativo di $\mathrm{GL}(n, \mathbb{C})$, detto **gruppo unitario**, e indicato con U_n. Il sottogruppo di U_n contenente solo le matrici con determinante pari a 1 è detto **gruppo unitario speciale**, e si denota con SU_n.

Osservazione.
Si possono classificare in modo semplice alcuni di questi gruppi unitari.
▶ $A \in U_n \implies 1 = \det(I_n) = \det(AA^*) = \det(A)\overline{\det(A)} = |\det(A)|^2 = 1$.
▶ $A = (a) \in U_1 \iff A^*A = I_1 \iff |a|^2 = 1 \iff a = e^{i\theta}$, $\theta \in [0, 2\pi)$, ossia il numero complesso a appartiene alla circonferenza di raggio unitario.
▶ $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SU_2 \iff AA^* = \begin{pmatrix} |a|^2 + |b|^2 & a\overline{c} + b\overline{d} \\ \overline{a}c + \overline{b}d & |c|^2 + |d|^2 \end{pmatrix} = I_2$, $\det(A) = 1$, ossia se il seguente sistema di equazioni è soddisfatto:

$$\begin{cases} |a|^2 + |b|^2 = |c|^2 + |d|^2 = 1, \\ a\overline{c} + b\overline{d} = 0, \\ ad - bc = 1, \end{cases}$$

le cui soluzioni riassumono il gruppo SU_2 nel seguente modo:

$$SU_2 = \left\{ \begin{pmatrix} x & -y \\ \overline{y} & \overline{x} \end{pmatrix} \in M(2, \mathbb{C}) \;\middle|\; |x|^2 + |y|^2 = 1 \right\}.$$

Definizione. (spazio euclideo reale) Si definisce **spazio euclideo reale** uno spazio vettoriale V su $\mathbb{R}$ dotato del prodotto scalare standard $\varphi = \langle \cdot, \cdot \rangle$.

Definizione. (spazio euclideo complesso) Si definisce **spazio euclideo complesso** uno spazio vettoriale V su $\mathbb{C}$ dotato del prodotto hermitiano standard $\varphi = \langle \cdot, \cdot \rangle$.

Proposizione. Sia (V, φ) uno spazio euclideo reale e sia $\mathcal{B}$ una base ortonormale di V. Allora $f \in \operatorname{End}(V)$ è simmetrico $\iff M_\mathcal{B}(f) = M_\mathcal{B}(f)^\top \iff M_\mathcal{B}(f)$ è simmetrica.

Dimostrazione. Per il corollario precedente, f è simmetrico $\iff f = f^\top \iff M_\mathcal{B}(f) = M_\mathcal{B}(f^\top) = M_\mathcal{B}(f)^\top$. $\square$

Proposizione. Sia (V, φ) uno spazio euclideo reale e sia $\mathcal{B}$ una base ortonormale di V. Allora $f \in \operatorname{End}(V)$ è ortogonale $\iff M_\mathcal{B}(f) M_\mathcal{B}(f)^\top = M_\mathcal{B}(f)^\top M_\mathcal{B}(f) = I_n \overset{\text{def}}{\iff} M_\mathcal{B}(f)$ è ortogonale.

Dimostrazione. Si osserva che $M_\mathcal{B}(\varphi) = I_n$. Sia $\mathcal{B} = \{\underline{v_1}, \ldots, \underline{v_n}\}$. Se f è ortogonale, allora $[\underline{v}]_\mathcal{B}^\top [\underline{w}]_\mathcal{B} = [\underline{v}]_\mathcal{B}^\top M_\mathcal{B}(\varphi)[\underline{w}]_\mathcal{B} = \varphi(\underline{v}, \underline{w}) = \varphi(f(\underline{v}), f(\underline{w})) = (M_\mathcal{B}(f)[\underline{v}]_\mathcal{B})^\top M_\mathcal{B}(\varphi)(M_\mathcal{B}(f)[\underline{w}]_\mathcal{B}) = [\underline{v}]_\mathcal{B}^\top M_\mathcal{B}(f)^\top M_\mathcal{B}(\varphi) M_\mathcal{B}(f)[\underline{w}]_\mathcal{B} = [\underline{v}]_\mathcal{B}^\top M_\mathcal{B}(f)^\top M_\mathcal{B}(f)[\underline{w}]_\mathcal{B}$. Allora, come visto nel corollario precedente, si ricava che $M_\mathcal{B}(f)^\top M_\mathcal{B}(f) = I_n$. Dal momento che gli inversi sinistri sono anche inversi destri, $M_\mathcal{B}(f)^\top M_\mathcal{B}(f) = M_\mathcal{B}(f) M_\mathcal{B}(f)^\top = I_n$.

Se invece $M_\mathcal{B}(f)^\top M_\mathcal{B}(f) = M_\mathcal{B}(f) M_\mathcal{B}(f)^\top = I_n$, $\varphi(\underline{v}, \underline{w}) = [\underline{v}]_\mathcal{B}^\top [\underline{w}]_\mathcal{B} = [\underline{v}]_\mathcal{B}^\top M_\mathcal{B}(f)^\top M_\mathcal{B}(f)[\underline{w}]_\mathcal{B} = (M_\mathcal{B}(f)[\underline{v}]_\mathcal{B})^\top (M_\mathcal{B}(f)[\underline{w}]_\mathcal{B}) = (M_\mathcal{B}(f)[\underline{v}]_\mathcal{B})^\top M_\mathcal{B}(\varphi)(M_\mathcal{B}(f)[\underline{w}]_\mathcal{B}) = \varphi(f(\underline{v}), f(\underline{w}))$, e quindi f è ortogonale. $\square$

Proposizione. Sia (V, φ) uno spazio euclideo complesso e sia $\mathcal{B}$ una base ortonormale di V. Allora $f \in \operatorname{End}(V)$ è hermitiano $\iff M_\mathcal{B}(f) = M_\mathcal{B}(f)^* \overset{\text{def}}{\iff} M_\mathcal{B}(f)$ è hermitiana.

Dimostrazione. Per il corollario precedente, f è hermitiana $\iff f = f^* \iff M_\mathcal{B}(f) = M_\mathcal{B}(f^*) = M_\mathcal{B}(f)^*$. $\square$

Proposizione. Sia (V, φ) uno spazio euclideo complesso e sia $\mathcal{B}$ una base ortonormale di V. Allora $f \in \operatorname{End}(V)$ è unitario $\iff M_\mathcal{B}(f) M_\mathcal{B}(f)^* = M_\mathcal{B}(f)^* M_\mathcal{B}(f) = I_n \overset{\text{def}}{\iff} M_\mathcal{B}(f)$ è unitaria.

Dimostrazione. Si osserva che $M_\mathcal{B}(\varphi) = I_n$. Sia $\mathcal{B} = \{\underline{v_1}, \ldots, \underline{v_n}\}$. Se f è unitario, allora $[\underline{v}]_\mathcal{B}^* [\underline{w}]_\mathcal{B} = [\underline{v}]_\mathcal{B}^* M_\mathcal{B}(\varphi)[\underline{w}]_\mathcal{B} = \varphi(\underline{v}, \underline{w}) = \varphi(f(\underline{v}), f(\underline{w})) = (M_\mathcal{B}(f)[\underline{v}]_\mathcal{B})^* M_\mathcal{B}(\varphi)(M_\mathcal{B}(f)[\underline{w}]_\mathcal{B}) = [\underline{v}]_\mathcal{B}^* M_\mathcal{B}(f)^* M_\mathcal{B}(\varphi) M_\mathcal{B}(f)[\underline{w}]_\mathcal{B} =$

$[\underline{v}]_{\mathcal{B}}^* M_{\mathcal{B}}(f)^* M_{\mathcal{B}}(f) [\underline{w}]_{\mathcal{B}}$. Allora, come visto nel corollario precedente, si ricava che $M_{\mathcal{B}}(f)^* M_{\mathcal{B}}(f) = I_n$. Dal momento che gli inversi sinistri sono anche inversi destri, $M_{\mathcal{B}}(f)^* M_{\mathcal{B}}(f) = M_{\mathcal{B}}(f) M_{\mathcal{B}}(f)^* = I_n$.

Se invece $M_{\mathcal{B}}(f)^* M_{\mathcal{B}}(f) = M_{\mathcal{B}}(f) M_{\mathcal{B}}(f)^* = I_n$, $\varphi(\underline{v}, \underline{w}) = [\underline{v}]_{\mathcal{B}}^* [\underline{w}]_{\mathcal{B}} = [\underline{v}]_{\mathcal{B}}^* M_{\mathcal{B}}(f)^* M_{\mathcal{B}}(f) [\underline{w}]_{\mathcal{B}} = (M_{\mathcal{B}}(f)[\underline{v}]_{\mathcal{B}})^* (M_{\mathcal{B}}(f)[\underline{w}]_{\mathcal{B}}) = (M_{\mathcal{B}}(f)[\underline{v}]_{\mathcal{B}})^* M_{\mathcal{B}}(\varphi) (M_{\mathcal{B}}(f)[\underline{w}]_{\mathcal{B}}) = \varphi(f(\underline{v}), f(\underline{w}))$, e quindi f è unitario. $\square$

Osservazione. Se $\mathcal{B}$ è una base ortonormale di (V, φ), ricordando che $M_{\mathcal{B}}(f^\top) = M_{\mathcal{B}}(f)^\top$ e che $M_{\mathcal{B}}(f^*) = M_{\mathcal{B}}(f)^*$, sono equivalenti allora i seguenti fatti:

▶ $f \circ f^\top = f^\top \circ f = \mathrm{Id}_V \iff M_{\mathcal{B}}(f)$ è ortogonale $\iff f$ è ortogonale,
▶ $f \circ f^* = f^* \circ f = \mathrm{Id}_V \iff M_{\mathcal{B}}(f)$ è unitaria $\iff f$ è unitario (se V è uno spazio vettoriale su $\mathbb{C}$).

Proposizione. Sia $V = \mathbb{R}^n$ uno spazio vettoriale col prodotto scalare standard φ. Allora sono equivalenti i seguenti fatti:

(i) $A \in O_n$,

(ii) f_A è un operatore ortogonale,

(iii) le colonne e le righe di A formano una base ortonormale di V.

Dimostrazione. Sia $\mathcal{B}$ la base canonica di V. Allora $M_{\mathcal{B}}(f_A) = A$, e quindi, per una proposizione precedente, f_A è un operatore ortogonale. Viceversa si deduce che se f_A è un operatore ortogonale, $A \in O_n$. Dunque è sufficiente dimostrare che $A \in O_n \iff$ le colonne e le righe di A formano una base ortonormale di V.

($\implies$) Se $A \in O_n$, in particolare $A \in \mathrm{GL}(n, \mathbb{R})$, e quindi A è invertibile. Allora le sue colonne e le sue righe formano già una base di V, essendo n vettori di V linearmente indipendenti. Inoltre, poiché $A \in O_n$, $\varphi(\underline{e_i}, \underline{e_j}) = \varphi(A\underline{e_i}, A\underline{e_j})$, e quindi le colonne di A si mantengono a due a due ortogonali tra di loro, mentre $\varphi(A\underline{e_i}, A\underline{e_i}) = \varphi(\underline{e_i}, \underline{e_i}) = 1$. Pertanto le colonne di A formano una base ortonormale di V.

Si osserva che anche $A^\top \in O_n$. Allora le righe di A, che non sono altro che le colonne di $A^\top$, formano anch'esse una base ortonormale di V.

($\Longleftarrow$) Nel moltiplicare $A^\top$ con A altro non si sta facendo che calcolare il prodotto scalare φ tra ogni riga di $A^\top$ e ogni colonna di A , ossia $(A^*A)_{ij} = \varphi((A^\top)_i, A^j) = \varphi(A^i, A^j) = \delta_{ij}$. Quindi $A^\top A = AA^\top = I_n$, da cui si deduce che $A \in O_n$. $\square$

Proposizione. Sia $V = \mathbb{C}^n$ uno spazio vettoriale col prodotto hermitiano standard φ. Allora sono equivalenti i seguenti fatti:

(i) $A \in U_n$,

(ii) f_A è un operatore unitario,

(iii) le colonne e le righe di A formano una base ortonormale di V.

Dimostrazione. Sia $\mathcal{B}$ la base canonica di V. Allora $M_\mathcal{B}(f_A) = A$, e quindi, per una proposizione precedente, f_A è un operatore unitario. Viceversa si deduce che se f_A è un operatore unitario, $A \in U_n$. Dunque è sufficiente dimostrare che $A \in U_n \iff$ le colonne e le righe di A formano una base ortonormale di V.

($\Longrightarrow$) Se $A \in U_n$, in particolare $A \in \mathrm{GL}(n, \mathbb{R})$, e quindi A è invertibile. Allora le sue colonne e le sue righe formano già una base di V, essendo n vettori di V linearmente indipendenti. Inoltre, poiché $A \in U_n$, $\varphi(\underline{e_i}, \underline{e_j}) = \varphi(A\underline{e_i}, A\underline{e_j})$, e quindi le colonne di A si mantengono a due a due ortogonali tra di loro, mentre $\varphi(A\underline{e_i}, A\underline{e_i}) = \varphi(\underline{e_i}, \underline{e_i}) = 1$. Pertanto le colonne di A formano una base ortonormale di V.

Si osserva che anche $A^\top \in U_n$. Allora le righe di A, che non sono altro che le colonne di $A^\top$, formano anch'esse una base ortonormale di V.

($\Longleftarrow$) Nel moltiplicare A^* con A altro non si sta facendo che calcolare il prodotto hermitiano φ tra ogni riga coniugata di A^* e ogni colonna di A, ossia $(A^*A)_{ij} = \varphi((A^\top)_i, A^j) = \varphi(A^i, A^j) = \delta_{ij}$. Quindi $A^*A = AA^* = I_n$, da cui si deduce che $A \in U_n$. $\square$

Proposizione. Sia (V, φ) uno spazio euclideo reale. Allora valgono i seguenti tre risultati:

(i) $(V_\mathbb{C}, \varphi_\mathbb{C})$ è uno spazio euclideo complesso.

(ii) Se $f \in \mathrm{End}(V)$ è simmetrico, allora $f_\mathbb{C} \in \mathrm{End}(V)$ è hermitiano.

(iii) Se $f \in \mathrm{End}(V)$ è ortogonale, allora $f_{\mathbb{C}} \in \mathrm{End}(V)$ è unitario.

Dimostrazione. Dacché φ è il prodotto scalare standard dello spazio euclideo reale V, esiste una base ortnormale di V. Sia allora $\mathcal{B}$ una base ortonormale di V. Si dimostrano i tre risultati separatamente.

- È sufficiente dimostrare che $\varphi_{\mathbb{C}}$ altro non è che il prodotto hermitiano standard. Come si è già osservato precedentemente, $M_{\mathcal{B}}(\varphi_{\mathbb{C}}) = M_{\mathcal{B}}(\varphi)$, e quindi, dacché $M_{\mathcal{B}}(\varphi) = I_n$, essendo $\mathcal{B}$ ortonormale, vale anche che $M_{\mathcal{B}}(\varphi_{\mathbb{C}}) = I_n$, ossia $\varphi_{\mathbb{C}}$ è proprio il prodotto hermitiano standard.

- Poiché f è simmetrico, $M_{\mathcal{B}}(f) = M_{\mathcal{B}}(f)^\top$, e quindi anche $M_{\mathcal{B}}(f_{\mathbb{C}}) = M_{\mathcal{B}}(f_{\mathbb{C}})^\top$. Dal momento che $M_{\mathcal{B}}(f) \in M(n, \mathbb{R})$, $M_{\mathcal{B}}(f) = \overline{M_{\mathcal{B}}(f)} \implies M_{\mathcal{B}}(f_{\mathbb{C}})^\top = M_{\mathcal{B}}(f_{\mathbb{C}})^*$. Quindi $M_{\mathcal{B}}(f_{\mathbb{C}}) = M_{\mathcal{B}}(f_{\mathbb{C}})^*$, ossia $M_{\mathcal{B}}(f_{\mathbb{C}})$ è hermitiana, e pertanto anche $f_{\mathbb{C}}$ è hermitiano.

- Poiché f è ortogonale, $M_{\mathcal{B}}(f)M_{\mathcal{B}}(f)^\top = I_n$, e quindi anche $M_{\mathcal{B}}(f_{\mathbb{C}})M_{\mathcal{B}}(f_{\mathbb{C}})^\top = I_n$. Allora, come prima, si deduce che $M_{\mathcal{B}}(f_{\mathbb{C}})^\top = M_{\mathcal{B}}(f_{\mathbb{C}})^*$, essendo $M_{\mathcal{B}}(f_{\mathbb{C}}) = M_{\mathcal{B}}(f) \in M(n, \mathbb{R})$, da cui si ricava che $M_{\mathcal{B}}(f_{\mathbb{C}})M_{\mathcal{B}}(f_{\mathbb{C}})^* = M_{\mathcal{B}}(f_{\mathbb{C}})M_{\mathcal{B}}(f_{\mathbb{C}})^\top = I_n$, ossia che $f_{\mathbb{C}}$ è unitario.

$\square$

Esercizio 1. Sia (V, φ) uno spazio euclideo reale. Allora valgono i seguenti risultati:

- Se f, $g \in \mathrm{End}(V)$ commutano, allora anche $f_{\mathbb{C}}$, $g_{\mathbb{C}} \in \mathrm{End}(V_{\mathbb{C}})$ commutano.

- Se $f \in \mathrm{End}(V)$, $(f^\top)_{\mathbb{C}} = (f_{\mathbb{C}})^*$.

- Se $f \in \mathrm{End}(V)$, f diagonalizzabile $\iff$ $f^\top$ diagonalizzabile.

Soluzione. Dacché φ è il prodotto scalare standard dello spazio euclideo reale V, esiste una base ortonormale $\mathcal{B} = \{\underline{v_1}, \ldots, \underline{v_n}\}$ di V. Si dimostrano allora separatamente i tre risultati.

- Si osserva che $M_{\mathcal{B}}(f_{\mathbb{C}})M_{\mathcal{B}}(g_{\mathbb{C}}) = M_{\mathcal{B}}(f)M_{\mathcal{B}}(g) = M_{\mathcal{B}}(g)M_{\mathcal{B}}(f) = M_{\mathcal{B}}(g_{\mathbb{C}})M_{\mathcal{B}}(f_{\mathbb{C}})$, e quindi che $f_{\mathbb{C}} \circ g_{\mathbb{C}} = g_{\mathbb{C}} \circ f_{\mathbb{C}}$.

- Si osserva che $M_{\mathcal{B}}(f) \in M(n, \mathbb{R}) \implies M_{\mathcal{B}}(f)^\top = M_{\mathcal{B}}(f)^*$, e quindi che $M_{\mathcal{B}}((f^\top)_{\mathbb{C}}) = M_{\mathcal{B}}(f^\top) = M_{\mathcal{B}}(f)^\top = M_{\mathcal{B}}(f)^* = M_{\mathcal{B}}(f_{\mathbb{C}})^* = M_{\mathcal{B}}((f_{\mathbb{C}})^*)$. Allora $(f^\top)_{\mathbb{C}} = (f_{\mathbb{C}})^*$.

- Poiché $\mathcal{B}$ è ortonormale, $M_\mathcal{B}(f^\top) = M_\mathcal{B}(f)^\top$. Allora, se f è diagonalizzabile, anche $M_\mathcal{B}(f)$ lo è, e quindi $\exists\, P \in \mathrm{GL}(n, \mathbb{K})$, $D \in M(n, \mathbb{K})$ diagonale tale che $M_\mathcal{B}(f) = PDP^{-1}$. Allora $M_\mathcal{B}(f^\top) = M_\mathcal{B}(f)^\top = (P^\top)^{-1}D^\top P^\top$ è simile ad una matrice diagonale, e pertanto $M_\mathcal{B}(f^\top)$ è diagonalizzabile. Allora anche $f^\top$ è diagonalizzabile. Vale anche il viceversa considerando l'identità $f = (f^\top)^\top$ e l'implicazione appena dimostrata.

Nota. D'ora in poi, qualora non specificato diversamente, si assumerà che V sia uno spazio euclideo, reale o complesso.

Definizione. (norma euclidea) Sia (V, φ) un qualunque spazio euclideo. Si definisce **norma** la mappa $\|\cdot\| : V \to \mathbb{R}^+$ tale che $\|\underline{v}\| = \sqrt{\varphi(\underline{v}, \underline{v})}$.

Definizione. (distanza euclidea tra due vettori) Sia (V, φ) un qualunque spazio euclideo. Si definisce **distanza** la mappa $d : V \times V \to \mathbb{R}^+$ tale che $d(\underline{v}, \underline{w}) = \|\underline{v} - \underline{w}\|$.

Osservazione.
▶ Si osserva che in effetti $\varphi(\underline{v}, \underline{v}) \in \mathbb{R}^+ \;\forall\, \underline{v} \in V$. Infatti, sia per il caso reale che per il caso complesso, φ è definito positivo.
▶ Vale che $\|\underline{v}\| = 0 \iff \underline{v} = \underline{0}$. Infatti, se $\underline{v} = \underline{0}$, chiaramente $\varphi(\underline{v}, \underline{v}) = 0 \implies \|\underline{v}\| = 0$; se invece $\|\underline{v}\| = 0$, $\varphi(\underline{v}, \underline{v}) = 0$, e quindi $\underline{v} = \underline{0}$, dacché $V^\perp = \{\underline{0}\}$, essendo φ definito positivo.
▶ Inoltre, vale chiaramente che $\|\alpha\underline{v}\| = |\alpha|\,\|\underline{v}\|$.
▶ Se f è un operatore ortogonale (o unitario), allora f mantiene sia le norme che le distanze tra vettori. Infatti $\|\underline{v} - \underline{w}\|^2 = \varphi(\underline{v} - \underline{w}, \underline{v} - \underline{w}) = \varphi(f(\underline{v} - \underline{w}), f(\underline{v} - \underline{w})) = \varphi(f(\underline{v}) - f(\underline{w}), f(\underline{v}) - f(\underline{w})) = \|f(\underline{v}) - f(\underline{w})\|^2$, da cui segue che $\|\underline{v} - \underline{w}\| = \|f(\underline{v}) - f(\underline{w})\|$.

Proposizione. (disuguaglianza di Cauchy-Schwarz) Vale che $\|\underline{v}\|\,\|\underline{w}\| \geq |\varphi(\underline{v}, \underline{w})|$, $\forall\, \underline{v}$, $\underline{w} \in V$, dove l'uguaglianza è raggiunta soltanto se $\underline{v}$ e $\underline{w}$ sono linearmente dipendenti.

Dimostrazione. Si consideri innanzitutto il caso $\mathbb{K} = \mathbb{R}$, e quindi il caso in cui φ è il prodotto scalare standard. Siano $\underline{v}$, $\underline{w} \in V$. Si consideri la disuguaglianza $\|\underline{v} + t\underline{w}\|^2 \geq 0$, valida per ogni elemento di V. Allora $\|\underline{v} + t\underline{w}\|^2 = \|\underline{v}\|^2 + 2\varphi(\underline{v}, \underline{w})t + \|\underline{w}\|^2 t^2 \geq 0$. L'ultima disuguaglianza è possibile se e solo se $\frac{\Delta}{4} \leq 0$, e quindi se e solo se $\varphi(\underline{v}, \underline{w})^2 - \|\underline{v}\|^2\,\|\underline{w}\|^2 \leq 0 \iff \|\underline{v}\|\,\|\underline{w}\| \geq \varphi(\underline{v}, \underline{w})$. Vale in particolare l'equivalenza se e solo se

$\|\underline{v}+t\underline{w}\|=0$, ossia se $\underline{v}+t\underline{w}=\underline{0}$, da cui la tesi.

Si consideri ora il caso $\mathbb{K}=\mathbb{C}$, e dunque il caso in cui φ è il prodotto hermitiano standard. Siano $\underline{v}$, $\underline{w}\in V$, e siano α, $\beta\in\mathbb{C}$. Si consideri allora la disuguaglianza $\|\alpha\underline{v}+\beta\underline{w}\|^2\geq 0$, valida per ogni elemento di V. Allora $\|\alpha\underline{v}+\beta\underline{w}\|^2=\|\alpha\underline{v}\|^2+\varphi(\alpha\underline{v},\beta\underline{w})+\varphi(\beta\underline{w},\alpha\underline{v})+\|\beta\underline{w}\|^2=|\alpha|^2\,\|\underline{v}\|^2+\overline{\alpha}\beta\,\varphi(\underline{v},\underline{w})+\alpha\overline{\beta}\,\varphi(\underline{w},\underline{v})+|\beta|^2\,\|\underline{w}\|^2\geq 0$. Ponendo allora $\alpha=\|\underline{w}\|^2$ e $\beta=-\varphi(\underline{w},\underline{v})=\overline{-\varphi(\underline{v},\underline{w})}$, si deduce che:

$$\|\underline{v}\|^2\,\|\underline{w}\|^4-\|\underline{w}\|^2\,|\varphi(\underline{v},\underline{w})|\geq 0.$$

Se $\underline{w}=\underline{0}$, la disuguaglianza di Cauchy-Schwarz è già dimostrata. Altrimenti, è sufficiente dividere per $\|\underline{w}\|^2$ (dal momento che $\underline{w}\neq\underline{0}\iff\|\underline{w}\|\neq 0$) per ottenere la tesi. Come prima, is osserva che l'uguaglianza si ottiene se e solo se $\underline{v}$ e $\underline{w}$ sono linearmente dipendenti. $\square$

Proposizione. (disuguaglianza triangolare) $\|\underline{v}+\underline{w}\|\leq\|\underline{v}\|+\|\underline{w}\|$.

Dimostrazione. Si osserva che $\|\underline{v}+\underline{w}\|^2=\|\underline{v}\|^2+\varphi(\underline{v},\underline{w})+\varphi(\underline{w},\underline{v})+\|\underline{w}\|^2$. Se φ è il prodotto scalare standard, si ricava che:

$$\|\underline{v}+\underline{w}\|^2=\|\underline{v}\|^2+2\varphi(\underline{v},\underline{w})+\|\underline{w}\|^2\leq\|\underline{v}\|^2+2\,\|\underline{v}\|\,\|\underline{w}\|+\|\underline{w}\|^2=(\|\underline{v}\|+\|\underline{w}\|)^2,$$

dove si è utilizzata la disuguaglianza di Cauchy-Schwarz. Da quest'ultima disuguaglianza si ricava, prendendo la radice quadrata, la disuguaglianza desiderata.

Se invece φ è il prodotto hermitiano standard, $\|\underline{v}+\underline{w}\|^2=\|\underline{v}\|^2+2\,\Re(\varphi(\underline{v},\underline{w}))+\|\underline{w}\|^2\leq\|\underline{v}\|^2+2\,|\varphi(\underline{v},\underline{w})|+\|\underline{w}\|^2$. Allora, riapplicando la disuguaglianza di Cauchy-Schwarz, si ottiene che:

$$\|\underline{v}+\underline{w}\|^2\leq(\|\underline{v}\|+\|\underline{w}\|)^2,$$

da cui, come prima, si ottiene la disuguaglianza desiderata. $\square$

Osservazione. Utilizzando il concetto di norma euclidea, si possono ricavare due teoremi fondamentali della geometria, e già noti dalla geometria euclidea.

- ► Se $\underline{v}\perp\underline{w}$, allora $\|\underline{v}+\underline{w}\|^2=\|\underline{v}\|^2+\overbrace{(\varphi(\underline{v},\underline{w})+\varphi(\underline{w},\underline{v}))}^{=0}+\|\underline{w}\|^2=\|\underline{v}\|^2+\|\underline{w}\|^2$ (teorema di Pitagora),

▶ Se $\|\underline{v}\| = \|\underline{w}\|$ e φ è un prodotto scalare, allora $\varphi(\underline{v}+\underline{w}, \underline{v}-\underline{w}) = \|\underline{v}\|^2 - \varphi(\underline{v}, \underline{w}) + \varphi(\underline{w}, \underline{v}) - \|\underline{w}\|^2 = \|\underline{v}\|^2 - \|\underline{w}\|^2 = 0$, e quindi $\underline{v}+\underline{w} \perp \underline{v}-\underline{w}$ (le diagonali di un rombo sono ortogonali tra loro).

Osservazione. Sia $\mathcal{B} = \{\underline{v_1}, \ldots, \underline{v_n}\}$ è una base ortogonale di V per φ.

▶ Se $\underline{v} = a_1\underline{v_1} + \ldots + a_n\underline{v_n}$, con a_1, ..., $a_n \in \mathbb{K}$, si osserva che $\varphi(\underline{v}, \underline{v_i}) = a_i\varphi(\underline{v_i}, \underline{v_i})$. Quindi $\underline{v} = \sum_{i=1}^n \frac{\varphi(\underline{v}, \underline{v_i})}{\varphi(\underline{v_i}, \underline{v_i})} \underline{v_i}$. In particolare, $\frac{\varphi(\underline{v}, \underline{v_i})}{\varphi(\underline{v_i}, \underline{v_i})}$ è detto **coefficiente di Fourier** di $\underline{v}$ rispetto a $\underline{v_i}$, e si indica con $C(\underline{v}, \underline{v_i})$. Se $\mathcal{B}$ è ortonormale, $\underline{v} = \sum_{i=1}^n \varphi(\underline{v}, \underline{v_i})\, \underline{v_i}$.

▶ Quindi $\|\underline{v}\|^2 = \varphi(\underline{v}, \underline{v}) = \sum_{i=1}^n \frac{\varphi(\underline{v}, \underline{v_i})^2}{\varphi(\underline{v_i}, \underline{v_i})}$. In particolare, se $\mathcal{B}$ è ortonormale, $\|\underline{v}\|^2 = \sum_{i=1}^n \varphi(\underline{v}, \underline{v_i})^2$. In tal caso, si può esprimere la disuguaglianza di Bessel: $\|\underline{v}\|^2 \geq \sum_{i=1}^k \varphi(\underline{v}, \underline{v_i})^2$ per $k \leq n$.

Osservazione. (algoritmo di ortogonalizzazione di Gram-Schmidt) Se φ è non degenere (o in generale, se $\mathrm{CI}(\varphi) = \{\underline{0}\}$) ed è data una base $\mathcal{B} = \{\underline{v_1}, \ldots, \underline{v_n}\}$ per V (dove si ricorda che deve valere $\operatorname{char} \mathbb{K} \neq 2$), è possibile applicare l'**algoritmo di ortogonalizzazione di Gram-Schmidt** per ottenere da $\mathcal{B}$ una nuova base $\mathcal{B}' = \{\underline{v_1}', \ldots, \underline{v_n}'\}$ con le seguenti proprietà:

(i) $\mathcal{B}'$ è una base ortogonale,

(ii) $\mathcal{B}'$ mantiene la stessa bandiera di $\mathcal{B}$ (ossia $\mathrm{Span}(\underline{v_1}, \ldots, \underline{v_i}) = \mathrm{Span}(\underline{v_1}', \ldots, \underline{v_i}')$ per ogni $1 \leq i \leq n$).

L'algoritmo si applica nel seguente modo: si prenda in considerazione $\underline{v_1}$ e sottragga ad ogni altro vettore della base il vettore $C(\underline{v_1}, \underline{v_i})\underline{v_1} = \frac{\varphi(\underline{v_1}, \underline{v_i})}{\varphi(\underline{v_1}, \underline{v_1})}\underline{v_1}$, rendendo ortogonale ogni altro vettore della base con $\underline{v_1}$. Pertanto si applica la mappa $\underline{v_i} \mapsto \underline{v_i} - \frac{\varphi(\underline{v_1}, \underline{v_i})}{\varphi(\underline{v_1}, \underline{v_1})}\underline{v_i} = \underline{v_i}^{(1)}$. Si verifica infatti che $\underline{v_1}$ e $\underline{v_i}^{(1)}$ sono ortogonali per $2 \leq i \leq n$:

$$\varphi(\underline{v_1}, \underline{v_i}^{(1)}) = \varphi(\underline{v_1}, \underline{v_i}) - \varphi\left(\underline{v_1}, \frac{\varphi(\underline{v_1}, \underline{v_i})}{\varphi(\underline{v_1}, \underline{v_1})}\underline{v_i}\right) = \varphi(\underline{v_1}, \underline{v_i}) - \varphi(\underline{v_1}, \underline{v_i}) = 0.$$

Poiché $\underline{v_1}$ non è isotropo, si deduce la decomposizione $V = \mathrm{Span}(\underline{v_1}) \oplus \mathrm{Span}(\underline{v_1})^\perp$. In particolare $\dim \mathrm{Span}(\underline{v_1})^\perp = n-1$: essendo allora i vettori $\underline{v_2}^{(1)}, \ldots, \underline{v_n}^{(1)}$ linearmente indipendenti e appartenenti a $\mathrm{Span}(\underline{v_1})^\perp$, ne sono una base. Si conclude quindi che vale la seguente decomposizione:

$$V = \mathrm{Span}(\underline{v_1}) \oplus^\perp \mathrm{Span}(\underline{v_2}^{(1)}, \ldots, \underline{v_n}^{(1)}).$$

Si riapplica dunque l'algoritmo di Gram-Schmidt prendendo come spazio vettoriale lo spazio generato dai vettori a cui si è applicato precedentemente l'algoritmo, ossia $V' = \mathrm{Span}(\underline{v_2}^{(1)}, \ldots, \underline{v_n}^{(1)})$, fino a che non si ottiene $V' = \{\underline{0}\}$.

Si può addirittura ottenere una base ortonormale a partire da $\mathcal{B}'$ normalizzando ogni vettore (ossia dividendo per la propria norma), se si sta considerando uno spazio euclideo.

Osservazione. Poiché la base ottenuta tramite Gram-Schmidt mantiene la stessa bandiera della base di partenza, ogni matrice triangolabile è anche triangolabile mediante una base ortogonale.

Esempio. Si consideri $V = (\mathbb{R}^3, \langle \cdot, \cdot \rangle)$, ossia $\mathbb{R}^3$ dotato del prodotto scalare standard. Si applica l'algoritmo di ortogonalizzazione di Gram-Schmidt sulla seguente base:

$$\mathcal{B} = \left\{ \underbrace{\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}}_{\underline{v_1} = \underline{e_1}}, \underbrace{\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}}_{\underline{v_2}}, \underbrace{\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}}_{\underline{v_3}} \right\}.$$

Alla prima iterazione dell'algoritmo si ottengono i seguenti vettori:

- $\underline{v_2}^{(1)} = \underline{v_2} - \frac{\varphi(\underline{v_1}, \underline{v_2})}{\varphi(\underline{v_1}, \underline{v_1})} \underline{v_1} = \underline{v_2} - \underline{v_1} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \underline{e_2}$,
- $\underline{v_3}^{(1)} = \underline{v_3} - \frac{\varphi(\underline{v_1}, \underline{v_3})}{\varphi(\underline{v_1}, \underline{v_1})} \underline{v_1} = \underline{v_3} - \underline{v_1} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$.

Si considera ora $V' = \mathrm{Span}(\underline{v_2}^{(1)}, \underline{v_3}^{(1)})$. Alla seconda iterazione dell'algoritmo si ottiene allora il seguente vettore:

- $\underline{v_3}^{(2)} = \underline{v_3}^{(1)} - \frac{\varphi(\underline{v_2}^{(1)}, \underline{v_3}^{(1)})}{\varphi(\underline{v_2}^{(1)}, \underline{v_2}^{(1)})} \underline{v_2}^{(1)} = \underline{v_3}^{(1)} - \underline{v_2}^{(1)} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \underline{e_3}$.

Quindi la base ottenuta è $\mathcal{B}' = \{\underline{e_1}, \underline{e_2}, \underline{e_3}\}$, ossia la base canonica di $\mathbb{R}^3$, già ortonormale.

Osservazione. Si osserva adesso che se (V, φ) è uno spazio euclideo (e quindi $\varphi > 0$), e W è un sottospazio di V, vale la seguente decomposizione:

$$V = W \oplus^{\perp} W^{\perp}.$$

Pertanto ogni vettore $\underline{v} \in V$ può scriversi come $\underline{w} + \underline{w}'$ dove $\underline{w} \in W$ e $\underline{w}' \in W^{\perp}$, dove $\varphi(\underline{w}, \underline{w}') = 0$.

Definizione. (proiezione ortogonale) Si definisce l'applicazione $\mathrm{pr}_W : V \to V$, detta **proiezione ortogonale** su W, in modo tale che $\mathrm{pr}_W(\underline{v}) = \underline{w}$, dove $\underline{v} = \underline{w} + \underline{w}'$, con $\underline{w} \in W$ e $\underline{w}' \in W^{\perp}$.

Osservazione.
▶ Dacché la proiezione ortogonale è un caso particolare della classica applicazione lineare di proiezione su un sottospazio di una somma diretta, pr_W è un'applicazione lineare.
▶ Vale chiaramente che $\mathrm{pr}_W^2 = \mathrm{pr}_W$, da cui si ricava, se $W^{\perp} \neq \{\underline{0}\}$, che $\varphi_{\mathrm{pr}_W}(\lambda) = \lambda(\lambda - 1)$, ossia che $\mathrm{sp}(\mathrm{pr}_W) = \{0, 1\}$. Infatti $\mathrm{pr}_W(\underline{v})$ appartiene già a W, ed essendo la scrittura in somma di due elementi, uno di W e uno di W', unica, $\mathrm{pr}_W(\mathrm{pr}_W(\underline{v})) = \mathrm{pr}_W(\underline{v})$, da cui l'identità $\mathrm{pr}_W^2 = \mathrm{pr}_W$.
▶ Seguendo il ragionamento di prima, vale anche che $\mathrm{pr}_W|_W = \mathrm{Id}_W$ e che $\mathrm{pr}_W|_{W^{\perp}} = 0$.
▶ Inoltre, vale la seguente riscrittura di $\underline{v} \in V$: $\underline{v} = \mathrm{pr}_W(\underline{v}) + \mathrm{pr}_{W^{\perp}}(\underline{v})$.
▶ Se $\mathcal{B} = \{\underline{v_1}, \ldots, \underline{v_n}\}$ è una base ortogonale di W, allora $\mathrm{pr}_W(\underline{v}) = \sum_{i=1}^n \frac{\varphi(\underline{v}, \underline{v_i})}{\varphi(\underline{v_i}, \underline{v_i})} \underline{v_i} = \sum_{i=1}^n C(\underline{v}, \underline{v_i}) \underline{v_i}$. Infatti $\underline{v} - \sum_{i=1}^n C(\underline{v}, \underline{v_i}) \underline{v_i} \in W^{\perp}$.
▶ pr_W è un operatore simmetrico (o hermitiano se lo spazio è complesso). Infatti $\varphi(\mathrm{pr}_W(\underline{v}), \underline{w}) = \varphi(\mathrm{pr}_W(\underline{v}), \mathrm{pr}_W(\underline{w}) + \mathrm{pr}_{W^{\perp}}(\underline{w})) = \varphi(\mathrm{pr}_W(\underline{v}), \mathrm{pr}_W(\underline{w})) = \varphi(\mathrm{pr}_W(\underline{v}) + \mathrm{pr}_{W^{\perp}}(\underline{v}), \mathrm{pr}_W(\underline{w})) = \varphi(\underline{v}, \mathrm{pr}_W(\underline{w}))$.

Proposizione. Sia (V, φ) uno spazio euclideo. Allora valgono i seguenti risultati:

(i) Siano U, $W \subseteq V$ sono sottospazi di V, allora $U \perp W$, ossia[5] $U \subseteq W^{\perp}$, $\iff$ $\mathrm{pr}_U \circ \mathrm{pr}_W = \mathrm{pr}_W \circ \mathrm{pr}_U = 0$.

[5] È sufficiente che valga $U \subseteq W^{\perp}$ affinché valga anche $W \subseteq U^{\perp}$. Infatti $U \subseteq W^{\perp} \implies W = W^{\perp\perp} \subseteq U^{\perp}$. Si osserva che in generale vale che $W \subseteq W^{\perp\perp}$, dove vale l'uguaglianza nel caso di un prodotto φ non degenere, com'è nel caso di uno spazio euclideo, essendo $\varphi > 0$ per ipotesi.

(ii) Sia $V = W_1 \oplus \cdots \oplus W_n$. Allora $\underline{v} = \sum_{i=1}^n \mathrm{pr}_{W_i}(\underline{v}) \iff W_i \perp W_j$ $\forall\, i \neq j$, $1 \leq i, j \leq n$.

Dimostrazione. Si dimostrano i due risultati separatamente.

(i) Sia $\underline{v} \in V$. Allora $\mathrm{pr}_W(\underline{v}) \in W = W^{\perp\perp} \subseteq U^\perp$. Pertanto $\mathrm{pr}_U(\mathrm{pr}_W(\underline{v})) = \underline{0}$. Analogamente $\mathrm{pr}_W(\mathrm{pr}_U(\underline{v})) = \underline{0}$, da cui la tesi.

(ii) Sia vero che $\underline{v} = \sum_{i=1}^n \mathrm{pr}_{W_i}(\underline{v})$ $\forall\, \underline{v} \in V$. Sia $\underline{w} \in W_j$. Allora $\underline{w} = \sum_{i=1}^n \mathrm{pr}_{W_i}(\underline{w}) = \underline{w} + \sum_{\substack{i=1 \\ i\neq j}} \mathrm{pr}_{W_i}(\underline{w}) \implies \mathrm{pr}_{W_i}(\underline{w}) = \underline{0}$ $\forall\, i \neq j$. Quindi $\underline{w} \in W_i^\perp$ $\forall\, i \neq j$, e si conclude che $W_i \subseteq W_j^\perp \implies W_i \perp W_j$. Se invece $W_i \perp W_j$ $\forall\, i \neq j$, sia $\mathcal{B}_i = \left\{ \underline{w}_i^{(1)}, \ldots, \underline{w}_i^{(k_i)} \right\}$ una base ortogonale di W_i. Allora $\mathcal{B} = \cup_{i=1}^n \mathcal{B}_i$ è anch'essa una base ortogonale di V, essendo $\varphi\left(\underline{w}_i^{(t_i)}, \underline{w}_j^{(t_j)}\right) = 0$ per ipotesi. Pertanto $\underline{v} = \sum_{i=1}^n \sum_{j=1}^{k_i} C\left(\underline{v}, \underline{w}_i^{(j)}\right) \underline{w}_i^{(j)} = \sum_{i=1}^n \mathrm{pr}_{W_i}(\underline{v})$, da cui la tesi. □

Definizione. (inversione ortogonale) Si definisce l'applicazione $\rho_W : V \to V$, detta **inversione ortogonale**, in modo tale che, detto $\underline{v} = \underline{w} + \underline{w}' \in V$ con $\underline{w} \in W$, $\underline{w} \in W^\perp$, $\rho_W(\underline{v}) = \underline{w} - \underline{w}'$. Se $\dim W = \dim V - 1$, si dice che ρ_W è una **riflessione**.

Osservazione.
► Si osserva che ρ_W è un'applicazione lineare.
► Vale l'identità $\rho_W^2 = \mathrm{Id}_V$, da cui si ricava che $\varphi_{\rho_W}(\lambda) \mid (\lambda - 1)(\lambda + 1)$. In particolare, se $W^\perp \neq \{\underline{0}\}$, vale proprio che $\mathrm{sp}(\rho_W) = \{\pm 1\}$, dove $V_1 = W$ e $V_{-1} = W^\perp$.
► ρ_W è ortogonale (o unitaria, se V è uno spazio euclideo complesso). Infatti se $\underline{v_1} = \underline{w_1} + \underline{w_1}'$ e $\underline{v_2} = \underline{w_2} + \underline{w_2}'$, con $\underline{w_1}$, $\underline{w_2} \in W$ e $\underline{w_1}'$, $\underline{w_2}' \in W$, $\varphi(\rho_W(\underline{v_1}), \rho_W(\underline{v_2})) = \varphi(\underline{w_1} - \underline{w_1}', \underline{w_2} - \underline{w_2}') = \varphi(\underline{w_1}, \underline{w_2}) \underbrace{-\varphi(\underline{w_1}', \underline{w_2}) - \varphi(\underline{w_1}, \underline{w_2}')}_{=0} + \varphi(\underline{w_1}', \underline{w_2}') = \varphi(\underline{w_1} - \underline{w_1}', \underline{w_2} - \underline{w_2}')$.

Quindi $\varphi(\rho_W(\underline{v_1}), \rho_W(\underline{v_2})) = \varphi(\underline{w_1}, \underline{w_2}) + \varphi(\underline{w_1}', \underline{w_2}) + \varphi(\underline{w_1}, \underline{w_2}') + \varphi(\underline{w_1}', \underline{w_2}') = \varphi(\underline{v_1}, \underline{v_2})$.

Lemma 1. Sia (V, φ) uno spazio euclideo reale. Siano $\underline{u}$, $\underline{w} \in V$. Se $\|\underline{u}\| = \|\underline{w}\|$, allora esiste un sottospazio W di dimensione $n - 1$ per cui la riflessione ρ_W relativa a φ è tale che $\rho_W(\underline{u}) = \underline{w}$.

Dimostrazione. Se $\underline{v}$ e $\underline{w}$ sono linearmente dipendenti, dal momento che $\|v\| = \|w\|$, deve valere anche che $\underline{v} = \underline{w}$. Sia $\underline{u} \neq \underline{0}$, $\underline{u} \in \mathrm{Span}(\underline{v})^\perp$. Si consideri $U = \mathrm{Span}(\underline{u})$: si osserva che $\dim U = 1$ e che, essendo φ non degenere,

$\dim U^\perp = n-1$. Posto allora $W = U^\perp$, si ricava, sempre perché φ è non degenere, che $U = U^{\perp\perp} = W^\perp$. Si conclude pertanto che $\rho_W(\underline{v}) = \underline{v} = \underline{w}$.

Siano adesso $\underline{v}$ e $\underline{w}$ linearmente indipendenti e sia $U = \operatorname{Span}(\underline{v} - \underline{w})$. Dal momento che $\dim U = 1$ e φ è non degenere, $\dim U^\perp = n-1$. Sia allora $W = U^\perp$. Allora, come prima, $U = U^{\perp\perp} = W^\perp$. Si consideri dunque la riflessione ρ_W: dacché $\underline{v} = \frac{\underline{v}+\underline{w}}{2} + \frac{\underline{v}-\underline{w}}{2}$, e $\varphi(\frac{\underline{v}+\underline{w}}{2}, \frac{\underline{v}-\underline{w}}{2}) = \frac{\|\underline{v}\|-\|\underline{w}\|}{4} = 0$, $\underline{v}$ è già decomposto in un elemento di W e in uno di $W^\perp$, per cui si conclude che $\rho_W(\underline{v}) = \frac{\underline{v}+\underline{w}}{2} - \frac{\underline{v}-\underline{w}}{2} = \underline{w}$, ottenendo la tesi.

□

Teorema (di Cartan–Dieudonné)**.** Sia (V, φ) uno spazio euclideo reale. Ogni isometria di V è allora prodotto di al più n riflessioni.

Dimostrazione. Si dimostra la tesi applicando il principio di induzione sulla dimensione n di V.

(*passo base*) Sia $n = 1$ e sia inoltre f un'isometria di V. Sia $\underline{v_1}$ l'unico elemento di una base ortonormale $\mathcal{B}$ di V. Allora $\left\|f(\underline{v_1})\right\| = \left\|\underline{v_1}\right\| = 1$, da cui si ricava che[6] $f(\underline{v_1}) = \pm\underline{v_1}$, ossia che $f = \pm \operatorname{Id}_V$. Se $f = \operatorname{Id}_V$, f è un prodotto vuoto, e già verifica la tesi; altrimenti $f = \rho_{\{\underline{0}\}}$, dove si considera $V = V \oplus^\perp \{\underline{0}\}$. Pertanto f è prodotto di al più una riflessione.

(*passo induttivo*) Sia $\mathcal{B} = \{\underline{v_1}, \ldots, \underline{v_n}\}$ una base di V. Sia f un'isometria di V. Si assuma inizialmente l'esistenza di $\underline{v_i}$ tale per cui $f(\underline{v_i}) = \underline{v_i}$. Allora, detto $W = \operatorname{Span}(\underline{v_i})$, si può decomporre V come $W \oplus^\perp W^\perp$. Si osserva che $W^\perp$ è f-invariante: infatti, se $\underline{u} \in W^\perp$, $\varphi(\underline{v_i}, f(\underline{u})) = \varphi(f(\underline{v_i}), f(\underline{u})) = \varphi(\underline{v_i}, \underline{u}) = 0 \implies f(\underline{u}) \in W^\perp$. Pertanto si può considerare l'isometria $f|_{W^\perp}$. Dacché $\dim W^\perp = n-1$, per il passo induttivo esistono W_1, ..., W_k sottospazi di $W^\perp$ con $k \leq n-1$ per cui ρ_{W_1}, ..., $\rho_{W_k} \in \operatorname{End}(W^\perp)$ sono tali che $f|_{W^\perp} = \rho_{W_1} \circ \cdots \circ \rho_{W_k}$.

Si considerino allora le riflessioni $\rho_{W_1 \oplus^\perp W}$, ..., $\rho_{W_k \oplus^\perp W}$. Si mostra che $\rho_{W_1 \oplus^\perp W} \circ \cdots \circ \rho_{W_k \oplus^\perp W}|_W = \operatorname{Id}_W = f|_W$. Affinché si faccia ciò è sufficiente mostrare che $(\rho_{W_1 \oplus^\perp W} \circ \cdots \circ \rho_{W_k \oplus^\perp W})(\underline{v_i}) = \underline{v_i}$. Si osserva che $\underline{v_i} \in W_i \oplus^\perp W$ $\forall\, 1 \leq i \leq k$, e quindi che $\rho_{W_k \oplus^\perp W}(\underline{v_i}) = \underline{v_i}$. Reiterando l'applicazione di questa identità nel prodotto, si ottiene infine il risultato desiderato. Infine, si

[6] Infatti, detto $\lambda \in \mathbb{R}$ tale che $f(\underline{v_1}) = \lambda\underline{v_1}$, $\left\|\underline{v_1}\right\| = \left\|f(\underline{v_1})\right\| = \lambda^2 \left\|\underline{v_1}\right\| \implies \lambda = \pm 1$, ossia $f = \pm\operatorname{Id}$, come volevasi dimostrare.

dimostra che $\rho_{W_1 \oplus^\perp W} \circ \cdots \circ \rho_{W_k \oplus^\perp W}|_{W^\perp} = \rho_{W_1} \circ \cdots \circ \rho_{W_k} = f|_{W^\perp}$. Analogamente a prima, è sufficiente mostrare che $\rho_{W_k \oplus^\perp W}(\underline{u}) = \rho_{W_k}(\underline{u}) \; \forall \, \underline{u} \in W^\perp$. Sia $\underline{u} = \rho_{W_k}(\underline{u}) + \underline{u}'$ con $\underline{u}' \in W_k^\perp \cap W^\perp \subseteq (W_k \oplus^\perp W)^\perp$, ricordando che $W^\perp = W_k \oplus^\perp (W^\perp \cap W_k^\perp)$. Allora, poiché $\rho_{W_k}(\underline{u}) \in W_k \subseteq (W_k \oplus^\perp W)$, si conclude che $\rho_{W_k \oplus^\perp W}(\underline{u}) = \rho_{W_k}(\underline{u})$. Pertanto, dacché vale che $V = W \oplus^\perp W^\perp$ e che $\rho_{W_1 \oplus^\perp W} \circ \cdots \circ \rho_{W_k \oplus^\perp W}$ e f, ristretti su W o su $W^\perp$, sono le stesse identiche mappe, allora in particolare vale l'uguaglianza più generale:

$$f = \rho_{W_1 \oplus^\perp W} \circ \cdots \circ \rho_{W_k \oplus^\perp W},$$

e quindi f è prodotto di $k \leq n-1$ riflessioni.

Se invece non esiste alcun $\underline{v_i}$ tale per cui $f(\underline{v_i}) = \underline{v_i}$, per il *Lemma 1* esiste una riflessione τ tale per cui $\tau(f(\underline{v_i})) = \underline{v_i}$. In particolare $\tau \circ f$ è anch'essa un'isometria, essendo composizione di due isometrie. Allora, da prima, esistono U_1, ..., U_k sottospazi di V con $k \leq n-1$ tali per cui $\tau \circ f = \rho_{U_1} \circ \cdots \circ \rho_{U_k}$, da cui $f = \tau \circ \rho_{U_1} \circ \cdots \circ \rho_{U_k}$, ossia f è prodotto di al più n riflessioni, concludendo il passo induttivo. $\square$

Lemma 1. Sia $f \in \mathrm{End}(V)$ simmetrico (o hermitiano). Allora f ha solo autovalori reali[7].

Dimostrazione. Si assuma che V è uno spazio euclideo complesso, e quindi che φ è un prodotto hermitiano. Allora, se f è hermitiano, sia $\lambda \in \mathbb{C}$ un suo autovalore[8] e sia $\underline{v} \in V_\lambda$. Allora $\varphi(\underline{v}, f(\underline{v})) = \varphi(f(\underline{v}), \underline{v}) = \overline{\varphi(\underline{v}, f(\underline{v}))} \implies \varphi(\underline{v}, f(\underline{v})) \in \mathbb{R}$. Inoltre vale la seguente identità:

$$\varphi(\underline{v}, f(\underline{v})) = \varphi(\underline{v}, \lambda \underline{v}) = \lambda \varphi(\underline{v}, \underline{v}),$$

da cui, ricordando che φ è non degenere e che $\varphi(\underline{v}, \underline{v}) \in \mathbb{R}$, si ricava che:

$$\lambda = \frac{\varphi(\underline{v}, f(\underline{v}))}{\varphi(\underline{v}, \underline{v})} \in \mathbb{R}.$$

Sia ora invece V è uno spazio euclideo reale e φ è un prodotto scalare. Allora, $(V_\mathbb{C}, \varphi_\mathbb{C})$ è uno spazio euclideo complesso, e $f_\mathbb{C}$ è hermitiano. Sia $\mathcal{B}$

[7] Nel caso di f simmetrico, si intende in particolare che tutte le radici del suo polinomio caratteristico sono reali.

[8] Tale autovalore esiste sicuramente dal momento che $\mathbb{K} = \mathbb{C}$ è un campo algebricamente chiuso.

una base di V. Allora, come visto all'inizio di questa dimostrazione, $f_{\mathbb{C}}$ ha solo autovalori reali, da cui si ricava che il polinomio caratteristico di $f_{\mathbb{C}}$ è completamente riducibile in $\mathbb{R}$. Si osserva inoltre che $p_f(\lambda) = \det(M_{\mathcal{B}}(f) - \lambda I_n) = \det(M_{\mathcal{B}}(f_{\mathbb{C}}) - \lambda I_n) = p_{f_{\mathbb{C}}}(\lambda)$. Si conclude dunque che anche p_f è completamente riducibile in $\mathbb{R}$. $\square$

Osservazione. Dal lemma precedente consegue immediatamente che se $A \in M(n, \mathbb{R})$ è simmetrica (o se appartiene a $M(n, \mathbb{C})$ ed è hermitiana), considerando l'operatore simmetrico f_A indotto da A in $\mathbb{R}^n$ (o $\mathbb{C}^n$), f_A ha tutti autovalori reali, e dunque così anche A.

Lemma 2. Sia $f \in \mathrm{End}(V)$ simmetrico (o hermitiano). Allora se λ, μ sono due autovalori distinti di f, $V_\lambda \perp V_\mu$.

Dimostrazione. Siano $\underline{v} \in V_\lambda$ e $\underline{w} \in V_\mu$. Allora[9] $\lambda\varphi(\underline{v}, \underline{w}) = \varphi(\lambda\underline{v}, \underline{w}) = \varphi(f(\underline{v}), \underline{w}) = \varphi(\underline{v}, f(\underline{w})) = \varphi(\underline{v}, \mu\underline{w}) = \mu\varphi(\underline{v}, \underline{w})$. Pertanto vale la seguente identità:

$$(\lambda - \mu)\varphi(\underline{v}, \underline{w}) = 0.$$

In particolare, valendo $\lambda - \mu \neq 0$ per ipotesi, $\varphi(\underline{v}, \underline{w}) = 0 \implies V_\lambda \perp V_\mu$, da cui la tesi. $\square$

Lemma 3. Sia $f \in \mathrm{End}(V)$ simmetrico (o hermitiano). Se $W \subseteq V$ è f-invariante, allora anche $W^\perp$ lo è.

Dimostrazione. Siano $\underline{w} \in W$ e $\underline{v} \in W^\perp$. Allora $\varphi(\underline{w}, f(\underline{v})) = \varphi(\underbrace{f(\underline{w})}_{\in W}, \underline{v}) = 0$, da cui si ricava che $f(\underline{v}) \in W^\perp$, ossia la tesi. $\square$

Teorema (spettrale reale)**.** Sia (V, φ) uno spazio euclideo reale (o complesso) e sia $f \in \mathrm{End}(V)$ simmetrico (o hermitiano). Allora esiste una base ortogonale $\mathcal{B}$ di V composta di autovettori per f.

Dimostrazione. Siano λ_1, ..., λ_k tutti gli autovalori reali di f. Sia inoltre $W = V_{\lambda_1} \oplus \cdots \oplus V_{\lambda_k}$. Per i lemmi precedenti, vale che:

$$W = V_{\lambda_1} \oplus^\perp \cdots \oplus^\perp V_{\lambda_k}.$$

Sicuramente $W \subset V$. Si assuma però che $W \subsetneq V$. Allora $V = W \oplus^\perp W^\perp$. In particolare, per il lemma precedente, $W^\perp$ è f-invariante. Quindi $f|_{W^\perp}$

[9] Si osserva che non è stato coniugato λ nei passaggi algebrici, valendo $\lambda \in \mathbb{R}$ dallo scorso lemma.

è un endomorfismo di uno spazio di dimensione non nulla. Si osserva che $f|_{W^\perp}$ è chiaramente simmetrico (o hermitiano), essendo solo una restrizione di f. Allora $f|_{W^\perp}$ ammette autovalori reali per i lemmi precedenti; tuttavia questo è un assurdo, dal momento che ogni autovalore di $f|_{W^\perp}$ è anche autovalore di f e si era supposto che[10] λ_1, ..., λ_k fossero tutti gli autovalori di f, $\lightning$. Quindi $W = V$. Pertanto, detta $\mathcal{B}_i$ una base ortonormale di V_{λ_i}, $\mathcal{B} = \cup_{i=1}^k \mathcal{B}_i$ è una base ortonormale di V, da cui la tesi. $\square$

Corollario (teorema spettrale per le matrici)**.** Sia $A \in M(n, \mathbb{R})$ simmetrica (o appartenente a $M(n, \mathbb{C})$ ed hermitiana). Allora $\exists\, P \in O_n$ (o $P \in U_n$) tale che $P^{-1}AP = P^\top AP$ (o $P^{-1}AP = P^*AP$ nel caso hermitiano) sia una matrice diagonale reale.

Dimostrazione. Si consideri f_A, l'operatore indotto dalla matrice A in $\mathbb{R}^n$ (o $\mathbb{C}^n$). Allora f_A è un operatore simmetrico (o hermitiano) sul prodotto scalare (o hermitiano) standard. Pertanto, per il teorema spettrale reale, esiste una base ortonormale $\mathcal{B} = \{\underline{v_1}, \ldots, \underline{v_n}\}$ composta di autovettori di f_A. In particolare, detta $\mathcal{B}'$ la base canonica di $\mathbb{R}^n$ (o $\mathbb{C}^n$), vale la seguente identità:

$$M_{\mathcal{B}}(f) = M_{\mathcal{B}'}^{\mathcal{B}}(\mathrm{Id})^{-1} M_{\mathcal{B}'}(f) M_{\mathcal{B}'}^{\mathcal{B}}(\mathrm{Id}),$$

dove $M_{\mathcal{B}'}(f) = A$, $M_{\mathcal{B}}(f)$ è diagonale, essendo $\mathcal{B}$ composta di autovettori, e $P = M_{\mathcal{B}'}^{\mathcal{B}}$ si configura nel seguente modo:

$$M_{\mathcal{B}'}^{\mathcal{B}}(f) = \left(\underline{v_1} \mid \cdots \mid \underline{v_n}\right).$$

Dacché $\mathcal{B}$ è ortogonale, P è anch'essa ortogonale, da cui la tesi. $\square$

Osservazione.

▶ Un importante risultato che consegue direttamente dal teorema spettrale per le matrici riguarda la segnatura di un prodotto scalare (o hermitiano). Infatti, detta $A = M_{\mathcal{B}}(\varphi)$, $D = P^\top AP$, e dunque $D \cong A$. Allora, essendo D diagonale, l'indice di positività è esattamente il numero di valori positivi sulla diagonale, ossia il numero di autovalori positivi di A. Analogamente l'indice di negatività è il numero di autovalori negativi, e quello di nullità è la molteplicità algebrica di 0 come autovalore (ossia esattamente la dimensione di $V_\varphi^\perp = \operatorname{Ker} a_\varphi$).

[10] Infatti tale autovalore λ non può già comparire tra questi autovalori, altrimenti, detto $i \in \mathbb{N}$ tale che $\lambda = \lambda_i$, $V_{\lambda_i} \cap W^\perp \neq \{\underline{0}\}$, violando la somma diretta supposta.

Teorema (di triangolazione con base ortonormale)**.** Sia $f \in \mathrm{End}(V)$, dove (V, φ) è uno spazio euclideo su $\mathbb{K}$. Allora, se p_f è completamente riducibile in $\mathbb{K}$, esiste una base ortonormale $\mathcal{B}$ tale per cui $M_{\mathcal{B}}(f)$ è triangolare superiore (ossia esiste una base ortonormale a bandiera per f).

Dimostrazione. Per il teorema di triangolazione, esiste una base $\mathcal{B}$ a bandiera per f. Allora, applicando l'algoritmo di ortogonalizzazione di Gram-Schmidt, si può ottenere da $\mathcal{B}$ una nuova base $\mathcal{B}'$ ortonormale e che mantenga le stesse bandiere. Allora, se $\mathcal{B}' = \{\underline{v_1}, \ldots, \underline{v_n}\}$ è ordinata, dacché $\mathrm{Span}(\underline{v_1}, \ldots, \underline{v_i})$ è f-invariante, $f(\underline{v_i}) \in \mathrm{Span}(\underline{v_1}, \ldots, \underline{v_i})$, e quindi $M_{\mathcal{B}'}(f)$ è triangolare superiore, da cui la tesi. $\square$

Corollario. Sia $A \in M(n, \mathbb{R})$ (o $M(n, \mathbb{C})$) tale per cui p_A è completamente riducibile. Allora $\exists\, P \in O_n$ (o U_n) tale per cui $P^{-1}AP = P^\top AP$ (o $P^{-1}AP = P^*AP$) è triangolare superiore.

Dimostrazione. Si consideri l'operatore f_A indotto da A in $\mathbb{R}^n$ (o $\mathbb{C}^n$). Sia $\mathcal{B}$ la base canonica di $\mathbb{R}^n$ (o di $\mathbb{C}^n$). Allora, per il teorema di triangolazione con base ortonormale, esiste una base ortonormale $\mathcal{B}' = \{\underline{v_1}, \ldots, \underline{v_n}\}$ di $\mathbb{R}^n$ (o di $\mathbb{C}^n$) tale per cui $T = M_{\mathcal{B}'}(f_A)$ è triangolare superiore. Si osserva inoltre che $M_{\mathcal{B}}(f_A) = A$ e che $P = M_{\mathcal{B}}^{\mathcal{B}'}(f_A) = \left(\underline{v_1} \mid \cdots \mid \underline{v_n}\right)$ è ortogonale (o unitaria), dacché le sue colonne formano una base ortonormale. Allora, dalla formula del cambiamento di base per la applicazioni lineari, si ricava che:

$$A = PTP^{-1} \implies T = P^{-1}TP,$$

da cui, osservando che $P^{-1} = P^\top$ (o $P^{-1} = P^*$), si ricava la tesi. $\square$

Definizione (operatore normale)**.** Sia (V, φ) uno spazio euclideo reale. Allora $f \in \mathrm{End}(V)$ si dice **normale** se commuta con il suo trasposto (i.e. se $ff^\top = f^\top f$). Analogamente, se (V, φ) è uno spazio euclideo complesso, allora f si dice normale se commuta con il suo aggiunto (i.e. se $ff^* = f^*f$).

Definizione (matrice normale)**.** Una matrice $A \in M(n, \mathbb{R})$ (o $M(n, \mathbb{C})$) si dice **normale** se $AA^\top = A^\top A$ (o $AA^* = A^*A$).

Osservazione.
▶ Se $A \in M(n, \mathbb{R})$ e A è simmetrica ($A = A^\top$), antisimmetrica ($A = -A^\top$) o ortogonale ($AA^\top = A^\top A = I_n$), sicuramente A è normale.
▶ Se $A \in M(n, \mathbb{C})$ e A è hermitiana ($A = A^*$), antihermitiana ($A = -A^*$) o unitaria ($AA^* = A^*A = I_n$), sicuramente A è normale.
▶ f è normale $\iff$ $M_{\mathcal{B}}(f)$ è normale, con $\mathcal{B}$ ortonormale di V.
▶ A è normale $\iff$ f_A è normale, considerando che la base canonica di

$\mathbb{C}^n$ è già ortonormale rispetto al prodotto hermitiano standard.
► Se V è euclideo reale, f è normale $\iff$ $f_\mathbb{C}$ è normale. Infatti, se f è normale, f e $f^\top$ commutano. Allora anche $f_\mathbb{C}$ e $(f^\top)_\mathbb{C} = (f_\mathbb{C})^*$ commutano, e quindi $f_\mathbb{C}$ è normale. Ripercorrendo i passaggi al contrario, si osserva infine che vale anche il viceversa.

Lemma 1. Sia $A \in M(n, \mathbb{C})$ triangolare superiore e normale (i.e. $AA^* = A^*A$). Allora A è diagonale.

Dimostrazione. Se A è normale, allora $(A^*)_i A^i = \overline{A}^i A^i$ deve essere uguale a $A_i (A^*)^i = A_i \overline{A}_i$ $\forall\, 1 \leq i \leq n$. Si dimostra per induzione su i da 1 a n che tutti gli elementi, eccetto per quelli diagonali, delle righe A_1, ..., A_i sono nulli.

(*passo base*) Si osserva che valgono le seguenti identità:

$$\overline{A}^1 A^1 = |a_{11}|^2 ,$$
$$A_1 \overline{A}_1 = |a_{11}|^2 + |a_{12}|^2 + \ldots + |a_{1n}|^2 .$$

Dovendo vale l'uguaglianza, si ricava che $|a_{12}|^2 \ldots + |a_{1n}|^2$, e quindi che $|a_{1i}|^2 = 0 \implies a_{1i} = 0 \quad \forall\, 2 \leq i \leq n$, dimostrando il passo base[11].

(*passo induttivo*) Analogamente a prima, si considerano le seguenti identità:

$$\overline{A}^i A^i = |a_{1i}|^2 + \ldots + |a_{ii}|^2 = |a_{ii}|^2 ,$$
$$A_i \overline{A}_i = |a_{ii}|^2 + \left|a_{i(i+1)}\right|^2 + \ldots + |a_{in}|^2 ,$$

dove si è usato che, per il passo induttivo, tutti gli elementi, eccetto per quelli diagonali, delle righe A_1, ..., A_{i-1} sono nulli. Allora, analogamente a prima, si ricava che $a_{ij} = 0 \quad \forall\, i < j \leq n$, dimostrando il passo induttivo, e quindi la tesi. □

Osservazione. Chiaramente vale anche il viceversa del precedente lemma: se infatti $A \in M(n, \mathbb{C})$ è diagonale, A è anche normale, dal momento che commuta con A^*.

Teorema. Sia (V, φ) uno spazio euclideo complesso. Allora f è un operatore normale $\iff$ esiste una base ortonormale $\mathcal{B}$ di autovettori per f.

[11] Gli altri elementi sono infatti già nulli per ipotesi, essendo A triangolare superiore

Dimostrazione. Si dimostrano le due implicazioni separatamente.

($\Longrightarrow$) Poiché $\mathbb{C}$ è algebricamente chiuso, p_f è sicuramente riducibile. Pertanto, per il teorema di triangolazione con base ortonormale, esiste una base ortonormale $\mathcal{B}$ a bandiera per f. In particolare, $M_\mathcal{B}(f)$ è sia normale che triangolare superiore. Allora, per il *Lemma 1*, $M_\mathcal{B}(f)$ è diagonale, e dunque $\mathcal{B}$ è anche una base di autovettori per f.

($\Longleftarrow$) Se esiste una base ortonormale $\mathcal{B}$ di autovettori per f, $M_\mathcal{B}(f)$ è diagonale, e dunque anche normale. Allora, poiché $\mathcal{B}$ è ortonormale, anche f è normale. □

Corollario. Sia $A \in M(n, \mathbb{C})$. Allora A è normale $\iff \exists U \in U_n$ tale che $U^{-1}AU = U^*AU$ è diagonale.

Dimostrazione. Si dimostrano le due implicazioni separatamente.

($\Longrightarrow$) Sia $\mathcal{B}$ la base canonica di $\mathbb{C}^n$. Si consideri l'applicazione lineare f_A indotta da A su $\mathbb{C}^n$. Se A è normale, allora anche f_A lo è. Pertanto, per il precedente teorema, esiste una base ortonormale $\mathcal{B}' = \{\underline{v_1}, \ldots, \underline{v_n}\}$ di autovettori per f_A. In particolare, $U = M_\mathcal{B}^{\mathcal{B}'}(\mathrm{Id}) = \left(\underline{v_1} \mid \cdots \mid \underline{v_n}\right)$ è unitaria ($U \in U_n$), dacché le colonne di U sono ortonormali. Si osserva inoltre che $M_\mathcal{B}(f_A) = A$ e che $D = M_{\mathcal{B}'}(f_A)$ è diagonale. Allora, per la formula del cambiamento di base per le applicazioni lineari, si conclude che:

$$A = UDU^{-1} \implies D = U^{-1}AU = U^*AU,$$

ossia che U^*AU è diagonale.

($\Longleftarrow$) Sia $D = U^*AU$. Dacché D è diagonale, D è anche normale. Pertanto $DD^* = D^*D$. Sostituendo, si ottiene che $U^*AUU^*A^*U = U^*A^*UU^*AU$. Ricordando che $U^*U = I_n$ e che $U \in U_n$ è sempre invertibile, si conclude che $AA^* = A^*A$, ossia che A è normale a sua volta, da cui la tesi. □