

Endomorfismi semisemplici e decomposizione di Jordan

In queste pagine esponiamo una generalizzazione della teoria di Jordan per gli endomorfismi di uno spazio vettoriale di dimensione finita. Mettiamo in guardia il lettore che, in alcuni punti si farà cenno ad argomenti non sviluppati nel corso e sarà quindi richiesto uno sforzo da parte del lettore.

Lo studio della forma di Jordan ci ha permesso di dimostrare che, dato un endomorfismo $\phi : V \rightarrow V$, di uno spazio vettoriale di dimensione finita su un campo algebricamente chiuso (o, più in generale, su un campo che contenga tutte le radici del polinomio caratteristico), l'endomorfismo ϕ si scrive, in modo unico, come somma di un endomorfismo diagonalizzabile, δ , e di un endomorfismo nilpotente, ν , che commutano tra loro. Inoltre, ϕ e δ hanno lo stesso polinomio caratteristico, e sia δ che ν si possono scrivere come funzioni polinomiali dell'endomorfismo ϕ .

Illustriamo brevemente come si possa verificare l'ultima affermazione che forse non appare evidente da quanto visto sulla forma di Jordan di un endomorfismo. Sia quindi

$$\lambda_\phi(X) = (X - a_1)^{c_1} \cdots (X - a_r)^{c_r}$$

il polinomio minimo di ϕ ove a_1, \dots, a_r sono gli autovalori dell'endomorfismo, a due a due distinti. Per ogni indice $i = 1, \dots, r$, essendo i fattori di $\lambda_\phi(X)$ relativamente primi, esistono dei polinomi, $b_i(X)$ e $c_i(X)$, tali che

$$1 = b_i(X)(X - a_i)^{c_i} + c_i(X) \prod_{j \neq i} (X - a_j)^{c_j}, \quad \text{con} \quad \deg c_i(X) < c_i, \quad \deg b_i(X) < \sum_{j \neq i} c_j.$$

Per ogni vettore $v \in V$, si ha quindi

$$v = b_i(\phi)(\phi - a_i)^{c_i} v + c_i(\phi) \prod_{j \neq i} (\phi - a_j)^{c_j} v$$

e se ne deduce che $\pi_i = c_i(\phi) \prod_{j \neq i} (\phi - a_j)^{c_j}$ è proprio la proiezione sul sottospazio $\ker(\phi - a_i)^{c_i}$ parallelamente alla somma degli spazi di autovettori generalizzati relativi agli altri autovalori. Quindi l'endomorfismo $\delta = \sum_{i=1}^r a_i \pi_i$ è una funzione polinomiale di ϕ e così pure $\nu = \phi - \delta$ ^(†). Si riconosce facilmente che δ è proprio la componente diagonalizzabile di ϕ e che ha lo stesso polinomio caratteristico.

Vogliamo generalizzare questa decomposizione anche al caso in cui gli autovalori non appartengano al corpo di base ed in tal caso, occorre generalizzare a questa nuova situazione la nozione di diagonalizzabilità di un endomorfismo, che richiederà qualche cautela sul campo di base per poter fornire un risultato analogo a quanto esposto sopra^(*).

Definizione. Sia C un campo e V uno spazio vettoriale di dimensione finita su C .

- Diremo che $\phi : V \rightarrow V$ è *semisemplice* se ogni sottospazio $W \subseteq V$, ϕ -stabile, ha un complementare ϕ -stabile.
- Diremo che $\phi : V \rightarrow V$ è *assolutamente semisemplice* se la sua estensione ad una chiusura algebrica di C è diagonalizzabile.

Le due nozioni della definizione precedente sono strettamente collegate, ma, come vedremo, non sono equivalenti. Mostriamo una prima caratterizzazione degli endomorfismi semisemplici.

(†) Con un po' di lavoro in più si può dimostrare che è possibile scrivere gli endomorfismi detti come funzioni polinomiali *senza termine noto* di ϕ . Lasciamo al lettore questa ulteriore verifica.

(*) Chi non conosca il prodotto tensoriale di spazi vettoriali, può sentirsi a disagio con il passaggio di uno spazio vettoriale o di un endomorfismo da un campo di base ad un altro. In estrema sintesi, possiamo descrivere la cosa in questo modo. Sia V uno spazio vettoriale su C , e $\phi : V \rightarrow V$ un endomorfismo. Sia data un'estensione L di C (o equivalentemente, sia dato un omomorfismo di anelli, $\rho : C \rightarrow L$, tra i due campi). L'estensione dello spazio vettoriale V su L , che si indica con $L \otimes_C V$, si può fare così: si fissa una base di V su C e si considerano le combinazioni lineari a coefficienti in L dei vettori della base. Analogamente, si considera la matrice dell'endomorfismo ϕ nella base fissata e la si fa agire sulle colonne di coordinate in L . Si può verificare che la costruzione fatta non dipende dalla scelta della base, ovvero che i cambiamenti di base dello spazio V su C si estendono a cambiamenti di base di $L \otimes_C V$ (ovvero che $\text{GL}_n(C)$ si immerge in $\text{GL}_n(L)$). Può essere di esempio pensare ad \mathbb{R}^n immerso in $\mathbb{C}^n = \mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}^n$.

Proposizione. Sia C un campo e V uno spazio vettoriale di dimensione finita su C . Un endomorfismo $\phi : V \rightarrow V$ è semisemplice se, e solo se, il suo polinomio minimo, $\lambda_\phi(X)$, è prodotto di fattori irriducibili distinti in $C[X]$.

dim. Mostriamo dapprima che se $\lambda_\phi(X) = f(X)^c g(X)$, con $f(X)$ irriducibile e $c > 1$, allora ϕ non può essere semisemplice. Il sottospazio $W = \ker f(\phi)$ è ϕ -stabile e il polinomio minimo della restrizione di ϕ a W è proprio uguale a $f(X)$. Se esistesse un complementare ϕ -stabile, T , il polinomio minimo di $\phi|_T$, $h(X)$, dovrebbe soddisfare alla condizione $\lambda_\phi(X) = \text{mcm}(f(X), h(X))$ e quindi, $f(X)^c \mid h(X)$ ($c > 1$). Perciò esiste un elemento non nullo, $t_0 \in T$, tale che $f(\phi)(t_0) = 0$, contro l'ipotesi che $T \cap W = \langle 0 \rangle$.

Supponiamo ora che $\lambda_\phi(X) = f_1(X) \cdots f_r(X)$, con $f_1(X), \dots, f_r(X)$ irriducibili e, a due a due, coprimi. Per il lemma di Decomposizione (cf. Lemma C.2.3 del testo) $V = W_1 \oplus \cdots \oplus W_r$, ove $W_i = \ker f_i(\phi)$ per $i = 1, \dots, r$. Se W è un sottospazio ϕ -stabile, esiste un'analoga decomposizione di W basata sul polinomio minimo di $\phi|_W$ e si ha $W = (W \cap W_1) \oplus \cdots \oplus (W \cap W_r)$. Quindi è sufficiente dimostrare che, per ogni $i = 1, \dots, r$, esiste un sottospazio ϕ -stabile T_i , tale che $W_i = T_i \oplus (W \cap W_i)$. Se $W_i = W_i \cap W$, allora $T_i = \langle 0 \rangle$ e abbiamo concluso. Se invece esiste un vettore non nullo $w \in W_i \setminus (W_i \cap W)$ consideriamo il più piccolo sottospazio ϕ -stabile contenente w , ovvero $V_\phi(w) = \langle w, \phi(w), \dots, \phi^{d_i-1}(w) \rangle$, ove $d_i = \deg f_i(X)$. È evidente che si tratta di un sottospazio ϕ -stabile, perché $f_i(\phi)(w) = 0$ e quindi $\phi^{d_i}(w)$ si scrive come combinazione lineare dei generatori di $V_\phi(w)$ e lo stesso accade per i vettori $\phi^k(w)$ con $k \geq d_i$. Inoltre, i generatori $w, \phi(w), \dots, \phi^{d_i-1}(w)$ sono linearmente indipendenti, perché in caso contrario, esisterebbe un polinomio non nullo, $h(X)$, di grado minore di d_i , appartenente all'ideale $J_w = \{ f(X) \in C[X] \mid f(\phi)(w) = 0 \}$. Poiché $f_i(X) \in J_w$ ed è irriducibile, si avrebbe $1 = \text{MCD}(h(X), f_i(X)) \in J_w$, contro l'ipotesi che w sia un vettore non nullo. Infine, osserviamo che, se w' è un vettore non nullo in $V_\phi(w)$, allora $V_\phi(w') = V_\phi(w)$, perché essendo entrambi ϕ -stabili, deve aversi $V_\phi(w') \subseteq V_\phi(w)$ e, ripetendo per w' il ragionamento fatto sopra per w , i due sottospazi hanno la stessa dimensione. Dunque, deve aversi $V_\phi(w) \cap (W_i \cap W) = \langle 0 \rangle$, perché se esistesse un vettore non nullo, w' , nell'intersezione dei due sottospazi, essendo $W_i \cap W$ un sottospazio ϕ -stabile, si avrebbe $V_\phi(w) = V_\phi(w') \subseteq (W_i \cap W)$, contro l'ipotesi che $w \notin W_i \cap W$. Se $W_i = V_\phi(w) \oplus (W_i \cap W)$ abbiamo concluso, altrimenti esiste un vettore non nullo in $W_i \setminus (V_\phi(w) \oplus (W_i \cap W))$ e si prosegue analogamente fino a determinare un complementare ϕ -stabile. **CVD** \square

Dato che su un campo algebricamente chiuso i polinomi irriducibili sono tutti di primo grado, discende immediatamente il seguente (cf. Proposizione 6.2.8 del testo)

Corollario. Sia C un campo algebricamente chiuso e V uno spazio vettoriale di dimensione finita su C . Un endomorfismo $\phi : V \rightarrow V$ è semisemplice se, e solo se, è diagonalizzabile.

Il Corollario mette in evidenza le relazioni esistenti tra endomorfismi semisemplici ed assolutamente semisemplici, ma bisogna fare attenzione al fatto che, in generale, non è vero che un endomorfismo semisemplice resti tale dopo un'estensione del campo di base. L'esempio fondamentale è il seguente.

Sia k un campo di caratteristica $p > 0$ ed a un elemento di k con $a \notin k^p$ (quindi k non è un campo perfetto^(*)). Il polinomio $X^p - a$ è irriducibile in $k[X]$ e quindi l'endomorfismo di $k \oplus \cdots \oplus k$ (p copie) di matrice uguale alla matrice compagna di $X^p - a$ è semisemplice per quanto visto nella Proposizione precedente. Se ora estendiamo il campo k aggiungendo una radice p -esima di a cioè consideriamo $L = k(x)$, con $x^p = a$ [ovvero $L \cong k[X]/(X^p - a)$]. Il polinomio minimo dell'endomorfismo di $L \oplus \cdots \oplus L$ (p copie) avente la stessa matrice non cambia ed è quindi uguale a $X^p - a = X^p - x^p = (X - x)^p$. Dunque l'endomorfismo esteso su L non è più semisemplice, infatti, pur avendo tutti gli autovalori su L , si guarda bene dall'essere diagonalizzabile (la sua forma di Jordan è un unico blocco di ordine p relativo all'autovalore x).

Dunque, poiché il polinomio minimo di un endomorfismo non varia estendendo il campo di base, può cadere la condizione di semisemplicità solo se il polinomio minimo non è separabile, cosa che può accadere solo se ci troviamo su un campo di base non perfetto di caratteristica positiva. Per cui su campi di caratteristica 0 o su campi perfetti di caratteristica positiva (quali, ad esempio, tutti i campi finiti) un endomorfismo è semisemplice se, e solo se, è assolutamente semisemplice. Lasciamo al lettore la verifica che la somma e la composizione di due endomorfismi assolutamente semisemplici che commutino, sono endomorfismi assolutamente semisemplici. Si possono quindi concludere queste osservazioni affermando che

Corollario. Sia C un campo e V uno spazio vettoriale di dimensione finita su C . Un endomorfismo $\phi : V \rightarrow V$ è assolutamente semisemplice se, e solo se, è semisemplice su un'estensione perfetta del campo C .

Si può quindi parlare della decomposizione di Jordan di un endomorfismo, restringendo l'attenzione ai campi perfetti.

Definizione. Sia C un campo e V uno spazio vettoriale di dimensione finita su C . Una decomposizione di Jordan dell'endomorfismo $\phi : V \rightarrow V$ è una coppia (δ, ν) di endomorfismi di V , ove δ è semisemplice, ν è nilpotente, $\delta \circ \nu = \nu \circ \delta$ e $\phi = \delta + \nu$.

(*) Un campo k è perfetto se ha caratteristica 0, oppure ha caratteristica $p > 0$ e l'omomorfismo $x \mapsto x^p$ è suriettivo ($k = k^p$).

Si può riassumere quanto visto nel testo sulla teoria di Jordan (con le integrazioni poste all'inizio di queste pagine) nel seguente

Lemma. Sia C un campo e V uno spazio vettoriale di dimensione finita su C . Un endomorfismo $\phi : V \rightarrow V$ che abbia tutti gli autovalori nel campo C ammette un'unica decomposizione di Jordan, (δ, ν) , ove δ è diagonalizzabile, ν è nilpotente, $\delta \circ \nu = \nu \circ \delta$ e $\phi = \delta + \nu$. Inoltre, il polinomio caratteristico di δ coincide con il polinomio caratteristico di ϕ ; e δ e ν sono funzioni polinomiali di ϕ .

Vogliamo dimostrare il seguente

Teorema. Sia C un campo perfetto e V uno spazio vettoriale di dimensione finita su C . Un endomorfismo $\phi : V \rightarrow V$ ammette un'unica decomposizione di Jordan, (δ, ν) . Inoltre, il polinomio caratteristico di δ coincide con il polinomio caratteristico di ϕ ; e δ e ν sono funzioni polinomiali di ϕ .

dim. Sia L un'estensione finita, di Galois^(*), di C che contenga tutti gli autovalori di ϕ . Allora, l'estensione ϕ_L di ϕ , si scrive in modo unico come $\phi_L = \delta + \nu$ con δ diagonalizzabile, ν nilpotente e $\delta \circ \nu = \nu \circ \delta$. Sia $\mathcal{V} = \{v_1, \dots, v_n\}$ una base di V su C ed A la matrice di ϕ rispetto a questa base. ed indichiamo con S ed N le matrici di δ e ν rispetto all'estensione della stessa base ad $L \otimes_C V$. Per ogni automorfismo σ di L/C , si ha $A = A^\sigma = S^\sigma + N^\sigma$ e $S^\sigma N^\sigma = (SN)^\sigma = (NS)^\sigma = N^\sigma S^\sigma$. Quindi per l'unicità della decomposizione di Jordan su L stabilita nel Lemma, deve aversi $S = S^\sigma$ ed $N = N^\sigma$. Si conclude che i due endomorfismi, δ e ν , hanno matrici ad elementi in C e sono quindi estensione di (omonimi) endomorfismi di V . La loro unicità discende dal fatto che sono uniche le estensioni a $L \otimes_C V$. Infine, poiché δ e ν appartengono a $End_C V$ e si scrivono come combinazioni lineari a coefficienti in L delle potenze di ϕ , allora si scrivono come combinazione lineare delle stesse potenze di ϕ a coefficienti in C . **CVD** \square

I risultati del Teorema sono veri anche per endomorfismi di un campo non perfetto, purché tutti i fattori irriducibili del polinomio minimo siano separabili. In caso contrario viene a cadere l'unicità della decomposizione, come si può vedere dal seguente esempio.

Sia k un campo di caratteristica $p > 0$ ed a un elemento di k con $a \notin k^p$. Si estenda il campo k aggiungendo una radice p -esima di a cioè sia $L = k(x)$, con $x^p = a$, e si considerino i due endomorfismi di $L \otimes_k L$, $\phi_1 : v \mapsto (x \otimes 1)v$ e $\phi_2 : v \mapsto (1 \otimes x)v$. La loro differenza $\phi_1 - \phi_2$ è nilpotente di ordine p , ma entrambi gli endomorfismi sono semisemplici, visto che il loro polinomio minimo è $X^p - a$, che è irriducibile su k ; inoltre i due endomorfismi commutano^(†). In conclusione, si ha $\phi_1 = \phi_2 + (\phi_1 - \phi_2)$ e quindi si può scrivere lo stesso endomorfismo in due modi diversi come somma di un semisemplice e di un nilpotente che commutano.

(*) Anche qui si chiede molto al lettore inesperto. Un'estensione finita di un campo C è un campo L , contenente C , che sia uno spazio vettoriale di dimensione finita su C . Gli automorfismi di L/K sono gli automorfismi, $\sigma : L \rightarrow L$, che lasciano fissi gli elementi di K . Le estensioni di Galois godono della proprietà che gli elementi di K sono gli unici elementi di L che restano fissi per tutti gli automorfismi di L/K . Rinviamo ad una qualsiasi trattazione della teoria di Galois il lettore interessato a conoscere questi argomenti.

(†) Proviamo a dare qualche dettaglio utile per chi non conosca il prodotto tensoriale. Lo spazio vettoriale $L \otimes_k L$ è lo spazio vettoriale su k che ha come base l'insieme $\{x^i \otimes x^j \mid 0 \leq i, j \leq p-1\}$ e gli endomorfismi indicati sopra sono definiti da

$$\phi_1(x^i \otimes x^j) = \begin{cases} x^{i+1} \otimes x^j & \text{se } i < p-1 \\ a(x^0 \otimes x^j) & \text{altrimenti} \end{cases} \quad \phi_2(x^i \otimes x^j) = \begin{cases} x^i \otimes x^{j+1} & \text{se } j < p-1 \\ a(x^i \otimes x^0) & \text{altrimenti} \end{cases} .$$

Il lettore può verificare le affermazioni fatte con calcoli diretti.