ENDOMORFISMI SEMISEMPLICI

MAURIZIO CORNALBA

Sia V uno spazio vettoriale sul campo K, e sia f un endomorfismo di V. Un sottospazio W di V si dice *invariante* se $f(W) \subset W$. Se consideriamo V un modulo su $K[X]$ ponendo $Pv = P(f)(v)$, questo equivale a dire che W è un sottomodulo di V. Diremo che un sottospazio invariante $W \neq \{0\}$ è *irriducibile* se non ha sottospazi invarianti tranne quelli banali, cioè $\{0\}$ e W; equivalentemente, diremo che W è un sottomodulo irriducibile (o *semplice*) di V. Notiamo che, se W è irriducibile e U è un altro sottospazio invariante di V, allora $W \subset U$ oppure $W \cap U = \{0\}$, dato che $W \cap U$ è un sottospazio invariante di W. Se v è un elemento non nullo di V il più piccolo sottospazio invariante di V contenente v è $K[X]v$, cioè l'insieme dei vettori della forma $P(f)(v)$ dove P varia tra tutti i polinomi a coefficienti in K. Ne segue in particolare che, se V è irriducibile, $V = K[X]v$ per ogni $v \in V$ non nullo; è ovviamente vero anche il viceversa. Il sottospazio $K[X]v$ è chiamato il sottospazio invariante (o il sottomodulo) generato da v.

Siano V e f come sopra. Diremo che f è *semisemplice* (o che il $K[X]$-modulo V è semisemplice) se ogni sottospazio invariante di V ha un complementare invariante; in altre parole, se per ogni $W \subset V$ invariante esiste W' invariante tale che $V = W \oplus W'$. Quando V ha dimensione finita, f è semisemplice se e solo se V è somma diretta di sottospazi invarianti irriducibili. Il "solo se" segue immediatamente dalla definizione di semisemplicità per induzione sulla dimensione; infatti V contiene sicuramente sottospazi invarianti irriducibili, ad esempio i sottospazi invarianti di dimensione minima. Quanto al viceversa, osserviamo innanzitutto che se V è irriducibile f è banalmente semisemplice. Il "se" segue allora dal seguente risultato.

Lemma 1. *Siano V e V' due $K[X]$-moduli. Sia W un sottomodulo di V.*

(i) *Se V è semisemplice anche W lo è.*
(ii) *Se V è semisemplice anche V/W lo è.*
(iii) *$V \oplus V'$ è semisemplice se e solo se lo sono V e V'.*

Dimostrazione. Sia U un sottomodulo di W. Dato che V è semisemplice ha un sottomodulo U' tale che $V = U \oplus U'$. Ma allora $W \cap U'$ è un sottomodulo di W e $W = U \oplus (W \cap U')$. Questo dimostra (1). Sia ora U un sottomodulo di V/W. Indichiamo con U' la sua controimmagine in V. Per semisemplicità U' ha un complementare U''. L'immagine di U'' in V/W è un complementare di U. Questo dimostra (2). Se $V \oplus V'$ è semisemplice lo sono anche V e V', in quanto suoi sottomoduli. Viceversa, supponiamo V e V' semisemplici e sia W un sottomodulo di $V \oplus V'$. Il modulo $(V + W)/V$ ha un complementare in $(V \oplus V')/V \simeq V'$. Dunque c'è un sottomodulo U' di V' tale che $V \oplus V' = (V + W) \oplus U'$. Il sottomodulo $V \cap W$ di V ha un complementare U. Si verifica immediatamente che $U \oplus U'$ è un complementare di W. □

Lemma 2 (Lemma di Schur)**.** *Siano V e V' due $K[X]$-moduli e sia $\alpha : V \to V'$ un omomorfismo di $K[X]$-moduli. Allora*

(i) *Se V è irriducibile α è iniettivo oppure $\alpha = 0$.*
(ii) *Se V' è irriducibile α è suriettivo oppure $\alpha = 0$.*

Date: 9 marzo 2017.

Dimostrazione. Dato che $\ker \alpha$ è un sottomodulo di V, può essere uguale solo a $\{0\}$ o a V se quest'ultimo è semplice. Lo stesso ragionamento dimostra (ii), dato che l'immagine di α è un sottomodulo di V'. □

Siano V e f come sopra. Supponiamo che V abbia dimensione finita. Ricordiamo che il polinomio minimo di f è il generatore monico dell'ideale in $K[X]$ costituito da tutti i polinomi P tali che $P(f) = 0$. Sia C il polinomio caratteristico di f; possiamo scrivere $C = \prod Q_i^{k_i}$, dove $Q_1, \dots, Q_n$ sono polinomi monici irriducibili distinti e i k_i sono interi positivi. Allora il polinomio minimo di f è della forma $Q = \prod Q_i^{h_i}$, dove $1 \leq h_i \leq k_i$.

Lemma 3. *Sia V uno spazio vettoriale di dimensione finita sul campo K e sia f un suo endomorfismo. Sia $Q = \prod Q_i^{h_i}$ il polinomio minimo di f, dove $Q_1, \dots, Q_n$ sono monici irriducibili distinti e gli h_i sono interi positivi. Sono condizioni equivalenti:*

(i) *f è semisemplice.*
(ii) *$h_i = 1$ per ogni i.*

Dimostrazione. Dato che i polinomi $Q_i^{h_i}$ sono a due a due primi fra loro, V è somma diretta dei sottospazi invarianti $V_i = \ker Q_i^{h_i}(f)$. L'endomorfismo f induce per restrizione un endomorfismo f_i di V_i, il cui polinomio minimo è $Q_i^{h_i}$. Per il lemma 1, f è semisemplice se e solo se lo è ognuno degli f_i. Possiamo dunque supporre che $Q = P^m$, dove P è un polinomio irriducibile. Supponiamo dapprima che $m = 1$. In questo caso V è uno spazio vettoriale sul campo $K[X]/(P)$, ed è dunque somma diretta di sottospazi unidimensionali, isomorfi cioè a $K[X]/(P)$. Questi sottospazi sono chiaramente $K[X]$-moduli irriducibili, e dunque f è semisemplice. Supponiamo invece che $m > 1$, e mostriamo che in questo caso non vi sono sottomoduli di V complementari a PV. Ragioniamo per assurdo, supponendo che un complementare W ci sia. Esiste un elemento $w \in W$ tale che $P^{m-1}w \neq 0$; in caso contrario infatti $P^{m-1}(f) = 0$ e P^m non sarebbe il polinomio minimo di f. Ma allora $Pw \neq 0$ poiché $m > 1$. D'altra parte $Pw \in PV \cap W$, e dunque W non è un complementare di PV, contro quanto si era supposto. □

Se il campo K contiene tutte le radici del polinomio minimo di f, in particolare se è algebricamente chiuso, segue dal lemma precedente che f è semisemplice se e solo se è diagonalizzabile.

Siano V e f come sopra e sia Q il polinomio minimo di f. Indichiamo con $End_K(V)$ l'algebra degli endomorfismi di V, con α è la moltiplicazione per Q in $K[X]$ e con *val* l'omomorfismo da $K[X]$ a $End_K(V)$ che ad ogni polinomio P associa $P(f)$. La successione

$$K[X] \stackrel{\alpha}{\to} K[X] \stackrel{val}{\to} End_K(V) \tag{1}$$

è esatta. Ora sia $L \supset K$ una estensione del campo K. Diremo che l'endomorfismo di L-spazi vettoriali

$$f \otimes 1 : V \otimes_K L \to V \otimes_K L$$

è ottenuto da f per *estensione degli scalari*. Tensorizzando la (1) con L si ottiene una successione esatta

$$K[X] \otimes_K L \to K[X] \otimes_K L \to End_K(V) \otimes_K L$$

che si identifica con

$$L[X] \to L[X] \to End_L(V \otimes_K L)$$

Questo mostra che il polinomio minimo di $f \otimes 1$ è identico a quello di f, cioè a Q.

Ricordiamo che un campo K si dice *perfetto* se ha caratteristica zero oppure $K = K^p$, dove $p > 0$ è la caratteristica.

Lemma 4. *Siano V uno spazio vettoriale di dimensione finita su K e f un endomorfismo di V. Sia $L \supset K$ una estensione di K. Se $f \otimes 1 : V \otimes_K L \to V \otimes_K L$ è semisemplice lo è anche f. Viceversa, se f è semisemplice e K è perfetto anche $f \otimes 1$ è semisemplice.*

Dimostrazione. Scriviamo $Q = \prod Q_i^{h_i}$, dove i Q_i sono i fattori irriducibili distinti di Q su K. I fattori irriducibili di Q su L sono i fattori irriducibili dei Q_i. Se f non è semisemplice h_i è maggiore di 1 per qualche i. Quindi i fattori irriducibili di Q_i su L compaiono con molteplicità maggiore di 1 in Q, il che implica, in base al lemma 3, che $f \otimes 1$ non è semisemplice. Supponiamo ora che K sia perfetto. In questo caso ogni polinomio a coefficienti in K è separabile; in particolare ogni polinomio irriducibile su K non ha radici multiple. Se f è semisemplice segue dal lemma 3 che il suo polinomio minimo Q non ha radici multiple. Quindi, sempre per il lemma 3, anche $f \otimes 1$ è semisemplice. □

Sia V uno spazio vettoriale di dimensione finita e sia f un endomorfismo di V. Osserviamo che, se f è simultaneamente semisemplice e nilpotente, è necessariamente nullo. Infatti per semisemplicità V è somma diretta di sottospazi invarianti irriducibili; se la restrizione di f a uno di questi sottospazi non è nulla, è un automorfismo per il lemma 2, e quindi nessuna sua potenza è nulla.

Teorema 1 (decomposizione di Jordan-Chevalley)**.** *Sia V uno spazio vettoriale di dimensione finita su un campo K e sia f un endomorfismo di V. Supponiamo che K sia perfetto o che contenga tutte le radici del polinomio minimo di f. Allora*

(i) *Esistono endomorfismi s e n di V tali che*
  (a) *$f=s+n$,*
  (b) *$sn = ns$,*
  (c) *s è semisemplice e n è nilpotente;*

(ii) *s e n sono univocamente determinati;*

(iii) *esistono $S, N \in K[X]$ tali che $s = S(f)$ e $n = N(f)$. Inoltre si possono scegliere S e N in modo che siano divisibili per X.*

Dimostrazione. Sia Q il polinomio minimo di f. Supponiamo inizialmente che Q si decomponga in fattori di primo grado su K. Quindi

$$Q = \prod_{i=1}^{m} (X - \lambda_i)^{k_i}$$

dove i λ_i sono gli autovalori di f e appartengono a K. In questo caso V è somma diretta degli autospazi generalizzati

$$V_i = \ker(f - \lambda_i \mathbf{id})^{k_i}$$

Sia s l'endomorfismo di V la cui restrizione a V_i è la moltiplicazione per λ_i per ogni i; è diagonalizzabile, quindi semisemplice. Se poniamo $n = f - s$ e k è il massimo dei k_i, allora $n^k = 0$. In effetti se $v \in V$ possiamo scrivere $v = \sum v_i$, dove $v_i \in V_i$. Allora

$$n^{k_i}(v_i) = (f - \lambda_i \mathbf{id})^{k_i}(v_i) = 0$$

e quindi $n^k(v) = 0$. Inoltre $ns(v_i) = n(\lambda_i v_i) = \lambda_i n(v_i) = sn(v_i)$. Quindi $ns = sn$. Per dimostrare (iii) poniamo

$$A_i = (X - \lambda_i)^{k_i}, \qquad B_i = \prod_{j \neq i} A_j$$

Dato che A_i e B_i sono primi fra loro esistono polinomi R_i e T_i tali che $R_i A_i + T_i B_i = 1$. Dato $v \in V$, come sopra scriviamo $v = \sum v_i$, dove $v_i \in V_i$. Allora

$$v_i = R_i(f)A_i(f)(v_i) + T_i(f)B_i(f)(v_i) = T_i(f)B_i(f)(v_i) = T_i(f)B_i(f)(v)$$

dato che $A_i(f)(v_i) = 0$ e $B_i(f)(v_j) = 0$ per $j \neq i$. In altre parole, la proiezione di V su V_i è $T_iB_i(f)$. Quindi $s = S(f)$ e $n = N(f)$, dove

$$S = \sum_i \lambda_i T_i B_i \,, \qquad N = X - S$$

Supponiamo infine che $f = s' + n'$, dove s' e n' commutano, s' è semisemplice e n' è nilpotente. Una prima conseguenza è che s' e n' commutano con f. Quindi s' e n' commutano con s e n, dato che questi sono polinomi in f. Ne segue che $n - n'$ è nilpotente e, dato che s e s' sono semisemplici e commutano, che $s - s'$ è semisemplice. In effetti ogni V_i è s'-invariante e quindi somma diretta di sottospazi s'-irriducibili; dato che f è la moltiplicazione per λ_i su V_i, essi sono anche $(s - s')$-irriducibili. Ma allora $s - s' = n' - n$ è simultaneamente semisemplice e nilpotente, quindi nullo. Questo conclude la dimostrazione del teorema nel caso in cui K contiene tutte le radici del polinomio minimo di f, salvo che per l'ultima parte di (iii).

Affrontiamo ora il caso generale. Sia L un campo di spezzamento (splitting field) di Q. Scegliamo una base $\{v_1, \dots, v_n\}$ di V e sia F la matrice di f rispetto a questa base. Osserviamo che F è anche la matrice di $\widehat{f} = f \otimes 1$ rispetto alla base $\{v_1 \otimes 1, \dots, v_n \otimes 1\}$ di $V \otimes_K L$. Il polinomio minimo di f è anche il polinomio minimo di F su K. È conveniente dimostrare, invece di (i), (ii), (iii), gli analoghi di queste affermazioni per F, che sono a loro equivalenti. Sappiamo già che il teorema è vero per $f \otimes 1$. Per il lemma 4 la proprietà (ii) per f segue immediatamente dalla corrispondente proprietà per $f \otimes 1$. Possiamo scrivere

$$F = S(F) + N(F) \tag{2}$$

dove S e N sono polinomi a coefficienti in L, $S(F)$ è una matrice semisemplice e $N(F)$ è una matrice nilpotente. Tutto sta a dimostrare che si possono scegliere S e N in modo che abbiano coefficienti in K; in questo caso infatti $S(F)$ è semisemplice anche su K per il lemma 4. Come osservato possiamo supporre che S e N abbiano grado minore di quello di Q. Sia σ un elemento del gruppo di Galois di L su K. Dunque $\sigma(F) = F$. Applicando σ alla (2) si ottiene

$$F = \sigma(S)(F) + \sigma(N)(F)$$

Anche $\sigma(S)(F)$ e $\sigma(N)(F)$ sono rispettivamente semisemplice e nilpotente. Per l'unicità della decomposizione (punto (ii))

$$\sigma(S)(F) = S(F) \,, \qquad \sigma(N)(F) = N(F)$$

In altre parole $\sigma(S) - S$ e $\sigma(N) - N$ si annullano su F; dato che hanno grado minore di quello di Q sono nulli. Poiché K è perfetto L è una estensione galoisiana di K. Dato che $\sigma(S) = S$ e $\sigma(N) = N$ per ogni elemento σ del gruppo di Galois di L su K, S e N appartengono a $K[X]$.

Resta da dimostrare che si possono scegliere S e N in modo che siano divisibili per X. Supponiamo dapprima che f sia un isomorfismo. In questo caso il termine noto di Q non è nullo, e i polinomi $\widetilde{S} = S + hQ$ e $\widetilde{N} = N + \ell Q$ hanno termine noto nullo per un h e un ℓ opportuni. D'altra parte $\widetilde{S}(f) = S(f) + hQ(f) = S(f)$, e analogamente $\widetilde{N}(f) = N(f)$. Supponiamo invece che f non sia un isomorfismo. Dato che $\ker f$ è invariante per $N(f)$ e quest'ultimo è nilpotente, esiste un $v \in V$ non nullo tale che $f(v) = N(f)(v) = 0$. Ma allora $0 = N(f)(v) = av$ dove a è il termine noto di N, che deve quindi essere nullo. Infine possiamo scegliere come S la differenza $X - N$, che ha termine noto nullo. □

Diremo che s è la parte semisemplice e che n è la parte nilpotente di f.

Proposizione 1. *Sia V uno spazio vettoriale di dimensione finita su un campo K e sia f un endomorfismo di V. Supponiamo che K sia perfetto o che contenga tutte le radici*

del polinomio minimo di f. Siano s e n la parte semisemplice e la parte nilpotente di f. Allora la parte semisemplice e la parte nilpotente dell'endomorfismo $\mathrm{ad}(f)$ *di* $\mathfrak{g}l(V)$ *sono* $\mathrm{ad}(s)$ *e* $\mathrm{ad}(n)$.

Dimostrazione. Per la parte (ii) del teorema 1 basta mostrare che $\mathrm{ad}(s)$ e $\mathrm{ad}(n)$ commutano e che sono rispettivamente semisemplice e nilpotente. Notiamo innanzitutto che

$$[\mathrm{ad}(s), \mathrm{ad}(n)] = \mathrm{ad}[s, n] = 0.$$

Per mostrare che $\mathrm{ad}(n)$ è nilpotente scriviamo

$$\mathrm{ad}(n)^k(x) = \sum_{i=0}^{k} (-1)^i \binom{k}{i} n^{k-i} x n^i$$

Questo mostra che, se $n^h = 0$, allora $\mathrm{ad}(n)^{2h} = 0$. Resta da mostrare che $\mathrm{ad}(s)$ è semisemplice. Sia L un campo di spezzamento del polinomio minimo di f. Notiamo che

$$\mathfrak{g}l(V \otimes L) = \mathfrak{g}l(V) \otimes L$$

e che $\mathrm{ad}(f \otimes 1) = \mathrm{ad}(f) \otimes 1$. Per il lemma 4 basta quindi dimostrare che $\mathrm{ad}(f \otimes 1)$ è semisemplice. Detto altrimenti, possiamo supporre che f sia diagonalizzabile. Sia $v_1, \ldots, v_n$ una base di V costituita da autovettori di f. Dunque ci sono scalari λ_i, $i = 1, \ldots, n$, tali che $f(v_i) = \lambda_i v_i$ per ogni i. Una base di $\mathfrak{g}l(V)$ è data dagli endomorfismi e_{ij} definiti da

$$e_{ij}(v_j) = v_i\,, \qquad e_{ij}(v_h) = 0 \text{ se } h \neq j.$$

Un calcolo immediato mostra che

$$\mathrm{ad}(f)(e_{ij}) = [f, e_{ij}] = (\lambda_i - \lambda_j) e_{ij}.$$

Questo dice che gli e_{ij} sono autovettori per $\mathrm{ad}(f)$, che è dunque diagonalizzabile, e quindi semisemplice. □