Esercitazioni di geometria 2 - 2008/2009 (Damiani)

Il polinomio minimo

I) Definizione del polinomio minimo.

Siano k un campo, $\mathcal{A}$ un anello (associativo) unitario, $k \to Z(\mathcal{A}) \subseteq \mathcal{A}$ un omomorfismo di anelli unitari (dove $Z(\mathcal{A})$ è il centro di $\mathcal{A}$); si osservi che sotto queste ipotesi $\mathcal{A}$ è anche un k-spazio vettoriale e si supponga $dim_k \mathcal{A} < \infty$; infine sia $\alpha \in \mathcal{A}$.

Osservazione: la struttura su $\mathcal{A}$ può essere equivalentemente descritta nel modo seguente:

i) $\mathcal{A}$ è un k-spazio vettoriale;

ii) $\mathcal{A}$ è un anello (associativo) unitario;

iii) il prodotto $A \times A \to A$ è k-bilineare (cioè oltre ad essere distributivo commuta con il prodotto per scalari: $(\lambda a)b = \lambda(ab) = a(\lambda b)$ $\forall \lambda \in k$, $\forall a, b \in \mathcal{A}$).

Se valgono i), ii) e iii) si dice che $\mathcal{A}$ è una k-algebra (associativa) unitaria.

Sia $v_\alpha : k[T] \to \mathcal{A}$ la valutazione in α, cioè l'omomorfismo k-lineare di anelli unitari (l'omomorfismo di k-algebre unitarie) definito da $v_\alpha(T) = \alpha$; osservare che $\forall \sum_i a_i T^i \in k[T]$ si ha $v_\alpha(\sum_i a_i T^i) = \sum_i a_i \alpha^i$ dove $\alpha^0 = 1_{\mathcal{A}}$ e $\alpha^{i+1} = \alpha\alpha^i$ $\forall i \in \mathbf{N}$.

Notazione: dato $P \in k[T]$, $v_\alpha(P)$ si scrive anche $P(\alpha)$.

Osservare che $\{P \in k[T] | P(\alpha) = 0\} = ker(v_\alpha)$ è un ideale di $k[T]$. In particolare esiste $p_\alpha \in k[T]$ tale che $\{P \in k[T] | P(\alpha) = 0\} = ker(v_\alpha) = (p_\alpha)$; p_α è unico a meno di scalari.

Osservazione: $p_\alpha \neq 0$.

Dimostrazione: $dim_k \mathcal{A} < dim_k k[T]$, quindi non esiste un omomorfismo iniettivo di $k[T]$ in $\mathcal{A}$; ne segue che $ker(v_\alpha) \neq (0)$.

Notazione: si osservi che p_α è univocamente determinato se si impone la scelta che sia monico. In queste note si indicherà con p_α il generatore monico di $ker(v_\alpha)$; tale polinomio si chiama polinomio minimo di α.

Osservare che $p_\alpha = 1 \Leftrightarrow \mathcal{A} = \{0\}$.

In particolare:

i) Siano V uno spazio vettoriale di dimensione finita su k ed $f \in End_k(V)$. Osservare che $dim_k End_k(V) < \infty$; si chiama polinomio minimo di f il polinomio monico $p_f \in k[T]$ tale che $(p_f) = ker(v_f)$ dove $v_f : k[T] \to End_k(V)$ è la valutazione in f. Osservare che $p_f = 1 \Leftrightarrow V = \{0\}$.

ii) Siano $n \in \mathbf{N}$ e $A \in \mathcal{M}_{n\times n}(k)$. Osservare che $dim_k \mathcal{M}_{n\times n}(k) < \infty$; si chiama polinomio minimo di A il polinomio monico $p_A \in k[T]$ tale che $(p_A) = ker(v_A)$ dove $v_A : k[T] \to \mathcal{M}_{n\times n}(k)$ è la valutazione in A.

iii) Siano $n \in \mathbf{N}$ e $\tilde{k}$ un campo che contiene k. Se $A \in \mathcal{M}_{n\times n}(k)$ siano $v_A : k[T] \to \mathcal{M}_{n\times n}(k)$ e $\tilde{v}_A : \tilde{k}[T] \to \mathcal{M}_{n\times n}(\tilde{k})$ le valutazioni in A e p_A, $\tilde{p}_A$ i polinomi minimi di A rispettivamente su k e su $\tilde{k}$ (cioè $ker(v_A) = p_A k[T]$ e $ker(\tilde{v}_A) = \tilde{p}_A \tilde{k}[T]$); osservare che:

a) $\tilde{p}_A \in k[T]$;

b) $k[T] \subseteq \tilde{k}[T]$, $\mathcal{M}_{n\times n}(k) \subseteq \mathcal{M}_{n\times n}(\tilde{k})$ e $\tilde{v}_A|_{k[T]} = v_A$;

c) $\tilde{p}_A = p_A$.

iv) Siano $n \in \mathbf{N}$, $\tilde{k}$ un campo che contiene k, $A \in \mathcal{M}_{n\times n}(\tilde{k})$, p_A il polinomio minimo di A. Osservare che non necessariamente $p_A \in k[T]$.

v) Siano $\tilde{k}$ un campo che contiene k con $dim_k \tilde{k} < \infty$, $\lambda \in \tilde{k}$, $v_\lambda : k[T] \to \tilde{k}$ la valutazione in λ; il generatore monico p_λ di $ker(v_\lambda)$ si chiama il polinomio minimo di λ su k. Si osservi che $\lambda \in k$ se e solo se $p_\lambda = T - \lambda$; altro esempio: il polinomio minimo di i su $\mathbf{R}$ è $T^2 + 1$. Si osservi ancora che (a differenza degli esempi i-iv)) in questa situazione p_λ è sempre irriducibile in $k[T]$ (perché?). È vero anche il viceversa: se $q \in k[T]$ è irriducibile, esistono $\tilde{k} \supseteq k$ campo di dimensione finita su k e $\lambda \in \tilde{k}$ tali che $q = p_\lambda$.

Osservazione: Siano $\mathcal{A}$, $\mathcal{B}$ due k-algebre associative unitarie di dimensione finita (su k) e sia $\varphi : \mathcal{A} \to \mathcal{B}$ un isomorfismo. Dato $\alpha \in \mathcal{A}$ si ha che $p_\alpha = p_{\varphi(\alpha)}$ (segue dal fatto che $v_{\varphi(\alpha)} = \varphi \circ v_\alpha$, da cui $ker(v_\alpha) = ker(v_{\varphi(\alpha)})$).

In particolare: se A è la matrice di f rispetto ad una base di V allora il polinomio minimo di A è uguale al polinomio minimo di f ed è indipendente dalla scelta della base di V; analogamente se A e B sono due matrici simili (cioè legate dalla relazione $B = M^{-1}AM$ per qualche M invertibile) il polinomio minimo di A è uguale al polinomio minimo di B.

II) Polinomio minimo e sottospazi stabili.

Sia $U \subseteq V$ un $k-$sottospazio vettoriale.

Osservare che $\mathcal{E}(V,U) = \{f \in End_k(V) | f(U) \subseteq U\}$ è una sottoalgebra unitaria di $End_k(V)$ e che la restrizione $res_U : \mathcal{E}(V,U) \ni f \mapsto f|_U \in End_k(U)$ e l'induzione sul quoziente $ind_U : \mathcal{E}(V,U) \ni f \mapsto f \in End_k(V/U)$ sono omomorfismi. Ne segue che se $f \in \mathcal{E}(V,U)$ si ha che $p_{f|_U} | p_f$ e $p_{\tilde{f}} | p_f$.

Osservare inoltre che $p_{\tilde{f}}$ può essere descritto anche nel modo seguente: sia $I = \{p \in k[T] | p(f)(V) \subseteq U\}$; allora I è un ideale di $k[T]$ e si ha $I = (p_{\tilde{f}})$; notare che naturalmente $ker(v_f) \subseteq I$.

Analogamente $p_{f|_U}$ può essere descritto anche nel modo seguente: sia $I = \{p \in k[T] | p(f)(U) = \{0\}\} = \{p \in k[T] | p(f)|_U = 0\}$; allora I è un ideale di $k[T]$ e si ha $I = (p_{f|_U})$; notare che naturalmente $ker(v_f) \subseteq I$.

Dalle descrizioni date sopra di $p_{\tilde{f}}$ e $p_{f|_U}$ segue subito anche la relazione $p_f | p_{f|_U} p_{\tilde{f}}$: infatti $p_{f|_U}(f)(p_{\tilde{f}}(f)(V)) \subseteq p_{f|_U}(f)(U) = \{0\}$.

Siano ora $U, W \subseteq V$ tali che $V = U \oplus W$ ed $f \in \mathcal{E}(V,U) \cap \mathcal{E}(V,W)$; allora $p_f = m.c.m.(p_{f|_U}, p_{f|_W})$. Infatti sicuramente $p_{f|_U} | p_f$ e $p_{f|_W} | p_f$; d'altra parte se si pone $q = m.c.m.(p_{f|_U}, p_{f|_W})$ si ha $q(f)(U) = \{0\}$ e $q(f)(W) = \{0\}$, quindi $q(f) = 0$.

Il risultato appena visto si generalizza facilmente: siano $V = U_1 \oplus \ldots \oplus U_r$ ed $f \in End_k(V)$ tale che $f(U_i) \subseteq U_i$ $\forall i = 1, ..., r$; allora $p_f = m.c.m.(p_{f|_{U_1}}, ..., p_{f|_{U_r}})$.

Viceversa sia $f \in End_k(V)$ e sia $p_f = q_1 q_2$ con $m.c.d.(q_1, q_2) = 1$; allora $V = ker(q_1(f)) \oplus ker(q_2(f)) = Im(q_1(f)) \oplus Im(q_2(f))$ e questi sottospazi sono tutti $f-$stabili.

Dimostrazione: che $ker(q_i)$, $Im(q_i)$ $(i = 1, 2)$ sono $f-$stabili è ovvio; dimostriamo che $Im(q_i(f)) \subseteq ker(q_j(f))$ $(i \neq j = 1, 2)$, che $ker(q_1(f)) \cap ker(q_2(f)) = \{0\}$ e che $Im(q_1(f)) + Im(q_2(f)) = V$.

i) $Im(q_i(f)) \subseteq ker(q_j(f))$ $(i \neq j = 1, 2)$: $(q_j(f)(Im(q_i(f))) = q_j(f)(q_i(f)(V)) = p_f(f)(V) = \{0\}$;

ii) $ker(q_1(f)) \cap ker(q_2(f)) = \{0\}$: se $U = ker(q_1(f)) \cap ker(q_2(f))$ si ha $p_{f|_U} | p_{f|_{ker(q_i(f))}}$ $\forall i = 1, 2$; ne segue che $p_{f|_U} | m.c.d.(q_1, q_2) = 1$, cioè $U = \{0\}$;

iii) $Im(q_1(f)) + Im(q_2(f)) = V$: siano $r_1, r_2 \in k[T]$ tali che $1 = q_1 r_1 + q_2 r_2$; allora $\forall v \in v$ si ha $v = q_1(f) r_1(f)(v) + q_2(f) r_2(f)(v)$; la tesi segue dal fatto che $q_i(f) r_i(f)(v) \in Im(q_i(f))$ $\forall i = 1, 2$.

Osservazione: per induzione su r si generalizza facilmente il risultato precedente: sia $f \in End_k(V)$ e sia $p_f = q_1 \cdot ... \cdot q_r$ con $m.c.d.(q_i, q_j) = 1$ $\forall i \neq j = 1, ..., r$; allora $V = \bigoplus_{i=1}^{r} ker(q_i(f))$ (e $\forall i = 1, ..., r$ $ker(q_i(f)) = Im(\frac{p_f}{q_i}(f))$).

III) Esempi.

i) $p_f(T) = T - \lambda \Leftrightarrow f = \lambda id_V$; in tal caso $det(f - T id_V) = (T - \lambda)^{dim_k(V)}$;

ii) se $f = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$ con $\lambda \neq \mu$, $p_f = (T - \lambda)(T - \mu) = det(f - T id_V)$;

iii) se $f = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$ $p_f = (T - \lambda)^2 = det(f - T id_V)$;

iv) se $f = \begin{pmatrix} \lambda & 1 & 0 & \dots & 0 & 0 \\ 0 & \lambda & 1 & \dots & 0 & 0 \\ 0 & 0 & \lambda & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \dots & \lambda & 1 \\ 0 & 0 & 0 & \dots & 0 & \lambda \end{pmatrix}$ $(n \times n)$

$p_f(T) = (T - \lambda)^n = det(f - T id_V)$;

v) se $f = \begin{pmatrix} 0 & 0 & \dots & 0 & 0 & a_0 \\ 1 & 0 & \dots & 0 & 0 & a_1 \\ 0 & 1 & \dots & 0 & 0 & a_2 \\ \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 & a_{n-2} \\ 0 & 0 & \dots & 0 & 1 & a_{n-1} \end{pmatrix}$

$p_f(T) = T^n - a_{n-1} T^{n-1} - a_{n-2} T^{n-2} - \dots - a_2 T^2 - a_1 T - a_0 = det(f - T id_V)$;

vi) determinare $p_f(T)$ e $det(f - T id_V)$ nei casi seguenti:

a) $f = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$;

b) $f = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$;

c) $f = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$;

d) $f = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$;

e) $f = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$.

IV) Legame tra polinomio minimo e polinomio caratteristico.

Osservazione: $p_f | det(f - Tid_V)$; in particolare $deg(p_f) \leq dim_k(V)$.

Dimostrazione: la tesi è un corollario immediato del teorema di Cayley-Hamilton (il polinomio caratteristico di f è annullato da f). Si osservi che questa è un'altra dimostrazione del fatto che $p_f \neq 0$.

Proposizione: $p_f(\lambda) = 0 \Leftrightarrow det(f - \lambda id_V) = 0$ (cioè $\Leftrightarrow \lambda$ è un autovalore per f).

Dimostrazione: ($\Rightarrow$) segue dal fatto che $p_f | det(f - Tid_V)$. Altra dimostrazione (senza usare il teorema di Cayley-Hamilton): $p_f(\lambda) = 0 \Rightarrow \exists q \in k[T]$ tale che $p_f = (T - \lambda)q$. Ne segue che $0 = p_f(f) = (f - \lambda id_V) \circ q(f)$. Ma la minimalità di p_f implica che $q(f) \neq 0$, quindi $f - \lambda id_V$ non è invertibile, dunque $det(f - \lambda id_V) = 0$.

($\Leftarrow$) Sia $V_\lambda \subseteq V$ l'autospazio per f relativo a λ, cioè $V_\lambda = \{v \in V | f(v) = \lambda v\}$. Osservare che $f|_{V_\lambda} = \lambda id_{V_\lambda}$, quindi $(f - \mu id_V)|_{V_\lambda}$ è invertibile $\forall \mu \neq \lambda$. Ne segue che se λ è un autovalore per f e $q \in k[T]$ è un polinomio tale che $q(\lambda) \neq 0$ si ha $q(f)|_{V_\lambda}$ invertibile e in particolare $q(f)|_{V_\lambda} \neq 0$, da cui $q(f) \neq 0$ e $q \neq p_f$. Dunque $p_f(\lambda) = 0$.

Osservare che in questa dimostrazione si è supposto che gli autovalori siano contenuti in k; questa ipotesi è lecita grazie al risultato dell'esempio iii,c).

La proposizione può essere riformulata e dimostrata nel modo seguente (senza assumere il teorema di Cayley-Hamilton, di cui si fornisce un'ulteriore dimostrazione):

Proposizione$'$: p_f e $det(f - Tid_V)$ hanno gli stessi fattori irriducibili (e $p_f | det(f - id_V)$).

Dimostrazione:

a) supponiamo inizialmente che V non contenga sottospazi f-stabili non banali; allora dato $v \neq 0$ si ha che $U =< f^i(v) | i \in \mathbf{N} >$ è un sottospazio stabile non nullo, quindi $U = V$; d'altra parte se $d = deg(p_f)$ si ha che $\{f^i(v) | i = 0, ..., d-1\}$ è linearmente indipendente (perché?) e $V =< f^i(v) | i = 0, ..., d-1 >$, quindi $d = deg(p_f) = dim_k V$.

Se $p_f = T^d + a_{d-1}T^{d-1} + ... + a_0$, la matrice di f rispetto alla base $\{v, f(v), ..., f^{d-1}(v)\}$

è $\begin{pmatrix} 0 & 0 & \dots & 0 & 0 & -a_0 \\ 1 & 0 & \dots & 0 & 0 & -a_1 \\ 0 & 1 & \dots & 0 & 0 & -a_2 \\ \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 & -a_{d-2} \\ 0 & 0 & \dots & 0 & 1 & -a_{d-1} \end{pmatrix}$ da cui con un semplice conto (cfr. III,v)) si trova $det(f - Tid_V) = \pm p_f$ e la tesi è ovvia.

b) consideriamo ora il caso generale e procediamo per induzione su $dim_k V$. Se V non contiene sottospazi f-stabili non banali la tesi è provata in a). Sia $U \subseteq V$ un sottospazio f-stabile non banale; osservare che $dim_k(U), dim_k(V/U) < dim_k V$, quindi per l'ipotesi induttiva la proposizione è vera per $f|_U$ e per $\tilde{f}$, dove $\tilde{f} \in End_k(V/U)$ è l'applicazione lineare indotta da f sul quoziente. Ma ovviamente $det(f - Tid_V) = det(f|_U - Tid_U) det(\tilde{f} - Tid_{V/U})$ e (v. II)) $p_{f|_U}|p_f$, $p_{\tilde{f}}|p_f$ e $p_f|p_{f|_U}p_{\tilde{f}}$: la tesi segue.

Corollario: Sia $q \in k[T]$ irriducibile. Allora $q|det(f - Tid_V) \Leftrightarrow V_q = ker(q(f)) \neq \{0\}$.

Si osservi che se $q = T - \lambda$ allora V_q è l'autospazio relativo a λ; inoltre se $q_1, ..., q_r$ sono i fattori irriducibili di $det(f - Tid_V)$ si ha che $\sum_{i=1}^{r} V_{q_i} = \oplus_{i=1}^{r} V_{q_i} \subseteq V$.

Corollario: Sia $q \in k[T]$ irriducibile; allora $degq | dim_k V_q$.

Dimostrazione:

$k[T]/(q)$ è un campo e V_q è un $k[T]/(q)$-spazio vettoriale: si ha allora che $dim_k V_q = (dim_k k[T]/(q))(dim_{k[T]/(q)} V_q) = (degq)(dim_{k[T]/(q)} V_q)$.

V) Polinomio minimo e diagonalizzabilità.

Proposizione: sia $f \in End_k(V)$. Allora f è diagonalizzabile $\Leftrightarrow \exists \lambda_1, ..., \lambda_r \in k$ distinti tali che $p_f = (T - \lambda_1) \cdot ... \cdot (T - \lambda_r)$.

Dimostrazione:

($\Rightarrow$) siano $\lambda_1, ..., \lambda_r$ gli autovalori di f; allora $\lambda_i \in k \ \forall i \in k$ e $V = \bigoplus_{i=1}^{r} V_{\lambda_i}$ dove V_{λ_i} è l'autospazio relativo a λ_i. Ma $p_{f|_{V_{\lambda_i}}} = T - \lambda_i \ \forall i = 1, ..., r$, quindi $p_f = m.c.m.(T - \lambda_1, ..., T - \lambda_r) = (T - \lambda_1) \cdot ... \cdot (T - \lambda_r)$.

($\Leftarrow$) $V = \bigoplus_{i_1}^{r} ker(f - \lambda_i id_V)$; ma $ker(f - \lambda_i id_V) = V_{\lambda_i}$, quindi f è diagonalizzabile.

Corollario: sia $f \in End_k(V)$ diagonalizzabile e sia $U \subseteq V$ tale che $f(U) \subseteq U$. Allora:

i) $f|_U$ è diagonalizzabile;

ii) $U = \bigoplus_\lambda U \cap V_\lambda$;

iii) $\tilde{f} \in End_k(V/U)$ è diagonalizzabile;

iv) $(V/U)_\lambda = V_\lambda / U_\lambda$.

Viceversa (e banalmente) se $W \subseteq V$ è un sottospazio tale che $W = \bigoplus_\lambda W \cap V_\lambda$ allora $f(W) \subseteq W$.

Osservazione: siano $f \in End_k(V)$, $U \subseteq V$ tale che $f(U) \subseteq U$ $\tilde{f} \in End_k(V/U)$ l'omomorfismo indotto da f sul quoziente. Allora:

i) $f|U$, $\tilde{f}$ diagonalizzabili $\not\Rightarrow$ f diagonalizzabile;

ii) $(V/U)_\lambda \supseteq V_\lambda / U_\lambda$;

iii) se $U = V_\lambda \neq \{0\}$ per qualche $\lambda \in k$ si ha $p_{\tilde{f}} = \frac{p_f}{T - \lambda}$;

iv) se $U = \oplus_{\lambda \in k} V_\lambda$ si ha $p_{\tilde{f}} = \frac{p_f}{\prod_{\lambda \in k \text{ autovalore}} T - \lambda}$.