Polinomio minimo

Fatti salienti sul polinomio minimo:

- L'anello $K[x]$ dei polinomi a coefficienti in un campo K è *euclideo*. In particolare, ogni ideale è principale e ogni elemento $p \in K[x]$ si scrive in modo unico come prodotto
$$p = p_1^{i_1} \cdots p_k^{i_k}$$
di polinomi irriducibili (ovvero polinomi che non sono prodotto di polinomi di grado minore). Il modo è unico a meno di permutare i fattori e di moltiplicare alcuni fattori per una costante non nulla.

- Data una matrice quadrata A a coefficienti in K, l'insieme dei polinomi $p \in K[x]$ tali che $p(A) = 0$ è un ideale, che chiamiamo $I(A)$. Ha quindi un generatore, unico a meno di moltiplicazione per costante. Per ottenere l'unicità chiediamo che sia monico: il polinomio risultante è il *polinomio minimo* di A, che chiamiamo $m_A(x)$. Quindi
$$I(A) = \big\{ m_A(x) \cdot q(x) \bigm| q(x) \in K[x] \big\}.$$

- Per il teorema di Hamilton-Cayley, il polinomio caratteristico $p_A(x)$ appartiene all'ideale $I(A)$.

- Vale un risultato più forte: se
$$m_A(x) = p_1^{i_1} \cdots p_k^{i_k}$$
è la decomposizione in fattori irriducibili di m_A, allora la decomposizione di p_A è del tipo
$$p_A(x) = p_1^{l_1} \cdots p_k^{l_k}$$
con $l_j \geqslant i_j$ per ogni j. In altre parole, il polinomio caratteristico ha gli stessi fattori irriducibili del polinomio minimo, con esponenti che possono essere uguali o superiori.

- La matrice A è triangolabile se e solo se p_j ha grado uno per ogni j.

- La matrice A è diagonalizzabile se e solo se p_j ha grado uno e $l_j = 1$ per ogni j. Più in generale, se A è triangolabile, i_j è la massima grandezza di un blocco di Jordan relativo all'autovalore che è radice di p_j.

- Il polinomio minimo, come il polinomio caratteristico, non dipende dal campo K fissato. La decomposizione in fattori primi di entrambi dipende però dal campo.

- Il polinomio minimo, come il polinomio caratteristico, non cambia per similitudine ed è quindi un invariante definito per ogni endomorfismo (non dipende dalla scelta di una base). Il polinomio minimo di un endomorfismo f può anche essere definito intrinsecamente allo stesso modo usando f al posto di A: è il generatore monico di $I(f)$, l'ideale di tutti i polinomi che annullano f.
- Il polinomio minimo di un vettore è definito in modo analogo, prendendo l'ideale
$$I = \{p \in K[x] \mid p(f)(v) = 0\}.$$
Il polinomio minimo è il minimo comune multiplo dei polinomi minimi dei vettori di una qualunque base.

Applicazioni ed esempi:

1. Se f è un endomorfismo su uno spazio vettoriale reale con polinomio caratteristico $p(x) = (x-1)^2(x+1)$, allora il polinomio minimo può essere:
   - $m(x) = (x-1)^2(x+1)$, e l'endomorfismo non è diagonalizzabile,
   - $m(x) = (x-1)(x+1)$, e l'endomorfismo è diagonalizzabile.

   Se il polinomio caratteristico è $p(x) = (x-1)^2(x^2+1)$ ci sono due casi analoghi, ma in entrambi l'endomorfismo non viene diagonalizzabile.
2. Sia f un endomorfismo. Se esiste un polinomio q tale che
   - $q(f) = 0$,
   - nella decomposizione in fattori irriducibili di q, ogni fattore ha grado uno e compare con esponente uno (cioè q ha tutte le radici nel campo, ciascuna con molteplicità uno),

   allora f è diagonalizzabile. Infatti $q \in I(f)$ ed il polinomio minimo divide q, quindi anche la decomposizione del polinomio minimo soddisfa le stesse proprietà elencate.
3. Un endomorfismo $f : V \to V$ tale che $f^2 = f$ è diagonalizzabile. Infatti il polinomio $p(x) = x^2 - x = x(x-1)$ annulla f, e si decompone con esponenti uno.
4. Un endomorfismo idempotente $f : V \to V$ su uno spazio vettoriale complesso ($K = \mathbb{C}$) è diagonalizzabile. Infatti per ipotesi $f^n = f$ per qualche n. Quindi $q(x) = x^n - x \in I(f)$. Ma $x^n - x = x(x^{n-1} - 1)$ e $x^{n-1} - 1 = (x-\lambda_1)\cdots(x-\lambda_{n-1})$ dove $\lambda_1, \ldots, \lambda_{n-1}$ sono le $n-1$ radici distinte dell'unità. Come sopra.

Dal fatto che il polinomio minimo è il minimo comune multiplo dei polinomi minimi dei vettori di una qualunque base, seguono facilmente i fatti seguenti:

1. Se $f : V \to V$ ha un sottospazio invariante W, il polinomio minimo di $f|_W$ divide quello di f (analoga proprietà vale per il polinomio caratteristico).

2. Data una matrice a blocchi
$$M = \begin{pmatrix} A & 0 \\ 0 & C \end{pmatrix}$$
vale $m_M = \text{m.c.m.}(m_A, m_C)$.

Altri fatti:

- Se $f : V \to V$ è un endomorfismo con polinomio minimo $m_f = p_1^{i_1} \cdots p_k^{i_k}$, vale la decomposizione in somma diretta
$$V = \ker p_1^{i_1}(f) \oplus \cdots \oplus \ker p_k^{i_k}(f)$$
detta *decomposizione primaria.*

- Per ogni j, la successione $d_n = \dim \ker p_j^n$ è strettamente crescente fino a $n = i_j$ e quindi si stabilizza. Se si costruisce la decomposizione partendo dal polinomio caratteristico p_f invece che dal minimo m_f, si ottiene quindi la stessa cosa.

Applicazioni ed esempi:

1. Sia $f : V \to V$ un endomorfismo con decomposizione primaria
$$V = \ker p_1^{i_1}(f) \oplus \cdots \oplus \ker p_k^{i_k}(f)$$
indotta dal polinomio minimo. Un sottospazio f-invariante W deve essere del tipo
$$W = W_1 \oplus \cdots \oplus W_k$$
dove $W_j = W \cap \ker p_j^{i_j}$. Infatti il polinomio minimo $m_{f|_W}$ della restrizione $f|_W$ deve dividere il polinomio minimo m_f di f, quindi è del tipo
$$m_{f|_W} = p_1^{n_1} \cdots p_k^{n_k}$$
per qualche $n_j \leqslant i_j$ che può essere anche nullo. Si ottiene una decomposizione primaria
$$W = \ker p_1^{n_1}(f|_W) \oplus \cdots \oplus \ker p_k^{n_k}(f|_W).$$
La tesi segue dalla relazione
$$\ker p_j^{n_j}(f|_W) = W \cap \ker p_j^{n_j}(f) \subset W \cap \ker p_j^{i_j}(f).$$