MATRICI E POLINOMI MINIMI

Cosa vogliamo mostrare? Mostreremo che, dato un campo $\mathbb{K}$ infinto ed un polinomio $q(t) \in \mathbb{K}[t]$, esiste una matrice $A \in \mathfrak{M}(r, \mathbb{K})$ tale che il suo polinomio minimo $m_A(t) = q(t)$.

CASO 1 Supponiamo che $q(t)$ sia irriducibile in $\mathbb{K}[t]$, e sia $\mathbb{K}^*$ il campo di spezzamento di q su $\mathbb{K}$. Allora si ha che

$$\mathbb{K}^* \cong \frac{\mathbb{K}[t]}{q(t)} \cong \mathbb{K}^{n+1}$$

dove $n = \deg q$. Vogliamo mostrare che esiste un morfismo φ di campi iniettivo tra $\mathbb{K}^*$ e $\mathfrak{M}(n+1, \mathbb{K})$. Siano f l'isomorfismo di campi tra $\mathbb{K}^*$ e $\frac{\mathbb{K}[t]}{q(t)}$ e g l'isomorfismo di spazi vettoriali tra $\frac{\mathbb{K}[t]}{q(t)}$ e $\mathbb{K}^{n+1}$. Definiamo

$$\varphi(y) = (g(f(y))|g(xf(y))|\cdots|g(x^n f(y)))$$

Si verifica piuttosto agevolmente che φ è un morfismo di campi. L'iniettività segue dal fatto che $\varphi(1) = I$, ovvero che non tutto viene mandato in 0.
Ora, siccome φ è iniettivo, conserva i polinomi minimi. Sia $\alpha \in \mathbb{K}^*$ e $m_\alpha \in \mathbb{K}^*[t]$ il polinomio minimo di α, $m_{\varphi(\alpha)}$ quello di $\varphi(\alpha)$. Allora $0 = \varphi(m_\alpha(\alpha)) = m_\alpha(\varphi(\alpha)) \implies m_{\varphi(\alpha)} \mid m_\alpha$, analogamente per l'altra divisione. Quindi $m_\alpha = m_{\varphi(\alpha)}$.
Quindi, se α è radice di q, siccome q è irriducibile, si ha che anche il polinomio minimo di $\varphi(\alpha)$ è q.

CASO 2 $q(t) = r(t)^s$, con r irriducibile. Dimostriamo per induzione che esiste la matrice che vogliamo. Per $s = 1$ siamo nel caso precedente.
Per passare da s a $s+1$, sia M_s la matrice corrispondente al passo s e consideriamo la matrice $M_{s+1} = \left(\begin{array}{c|c} M_s & I \\ \hline 0 & M_s \end{array}\right)$. Si verifica facilmente che $p(M_{s+1}) = \left(\begin{array}{c|c} p(M_s) & p'(M_s) \\ \hline 0 & p(M_s) \end{array}\right)$.
Calcolando ora $r(M_{s+1})^s + 1 = 0$, quindi $m_{M_{s+1}} \mid r(t)^{s+1}$. D'altro canto $p(M_{s+1}) = 0 \implies p(M_s) = 0, p'(M_s) = 0$, quindi per ipotesi induttiva $r(t)^s \mid p, r(t)^s \mid p' \implies r(t)^{s+1} \mid p$. Perciò $r(t)^{s+1}$ è proprio il polinomio minimo di M_{s+1}.

CASO 3 $q(t) = \prod_{i=1}^k p_i(t)^{\beta_i}$. Riduciamoci al caso $p_i(t)$ irriducibile $\forall i$. Allora la matrice che funziona è $M = \left(\begin{array}{c|c|c} M_1 & & \\ \hline & \ddots & \\ \hline & & M_k \end{array}\right)$, poiché $m_M = \text{mcm}\,(m_{M_1}, \ldots, m_{M_k})$.