Le théorème des invariants de similitude.

Rémi Lajugie

On se place sur k un corps (donc commutatif). On considère l'ensemble des matrices $\mathcal{M}_n(k)$. On rappelle que le polynôme minimal μ_u de u est le générateur unitaire de l'idéal des polynômes annulateurs de u. On note également $\mu_{u,x}$ le polynôme minimal local en x, c'est à dire le générateur unitaire de l'idéal des polynômes annulateurs du vecteur $u(x)$.

On commence par rappeler la proposition suivante, qui peut se démontrer par récurrence.

Proposition 1 *Il existe un élément $x \in k^n$ tel que $\mu_{u,x} = \mu_u$.*

Proposition 2 *Soit x tel que $\mu_{u,x} = \mu_u$, alors il existe un supplémentaire u-stable au sous espace cyclique $(x, u(x), \ldots, u^{d-1}(x))$ où d est le degré de μ_u.*

Preuve :

Considérons la base $(x, u(x), \ldots, u^{d-1}(x))$. Soit un élément ϕ du dual tel que $\phi(u^{d-1}) = 1$ et $\phi(u^k) = 0$ si $k < d-1$. La famille des $\phi \circ u^i$ est une famille libre du dual, que l'on peut compléter en une base via des formes linéaires $f_d^*, \ldots, f_n^*$.

On considère la base antéduale des $(\phi(u^k), f_d^*, \ldots, f_n^*)$. Par construction de ϕ, les d premiers vecteurs de la base sont bien les $(x, u(x), \ldots, u^{d-1}(x))$.

Soit $i \in \{d, \ldots, n\}$, alors on a $\phi(u^k)(u(f_j) = 0, \forall k < d-1$ car f_j^* est orthogonal à $\phi(u^k)^*$.

Reste à considérer le cas $k = d-1$. Comme le polynôme minimal est de degré $d-1$ on peut écrire u^{d-1} comme combinaison linéaire des u^k pour $k < d-1$. On conclue alors comme dans les cas précédents.

Théorème 1 *Soit $u \in \mathcal{M}_n()$ alors il existe une unique suite de polynômes $P_1|P_2|\ldots|P_r = \mu_u$ tels que l'espace soit la somme directe de sous espaces cycliques associés au polynôme P.*

De manière équivalente on peut écrire l'espace comme somme directe de sous espace telle que u induise sur chaque sous espace un endomorphisme cyclique. $u = \begin{pmatrix} C(P_r) & & & \\ & C(P_{r-1}) & & \\ & & \ldots & \\ & & & C(P_1) \end{pmatrix}$

Preuve :

Etape 1 : existence On procède par récurrence sur la dimension. Le cas de la dimension 1 étant évident.

Si c'est vrai pour la dimension n, alors il existe x tel que

1. $\mu_{u,x} = \mu$.
2. l'espace cyclique admette un supplémentaire $u-$stable.

On conclue en appliquant l'hypothèse de récurrence au sous espace supplémentaire qui est de dimension strictement inférieure à n (et en notant que tout polynôme annulateur de u restreint à ce sous espace divise μ).

Etape 2 : unicité Par l'absurde. Si on a deux telles suites distinctes qui conviennent $P_1|P_2|\ldots|P_r$, $P_1'|P_2'|\ldots|P_s'$. Tout d'abord notons que $P_s = P_r = \mu_u$. Soit i le plus grand indice tel que $\forall j > i, P_j =$

$P'_j, P_i \neq P'_i$. (notons qu'un tel indice existe pour des raisons de degré, la somme des degrés des deux suites de polynômes étant identiques)

Ecrivons l'espace $k^n = \oplus_{i=1}^r F_i = \oplus_{i=1}^s G_i$ comme somme directe adaptée aux décomposition induite par les sous espaces cycliques des deux suites.

Considérons une application de changement de base envoyant les F_i sur les G_i. Comme pour $j \geq i$, $P_j = P'_j$, les endomorphismes induits par u sur F_i et G_i sont semblables (sous espaces cycliques de même polynome minimal), ces endomorphismes sont semblables à un endomorphisme dont la matrice est la matrice compagnon du polynôme P_j. Il y a donc un changement de base tel que

1. Les blocs F_i soient envoyés sur les blocs G_i pour $i \geq j$.
2. $\oplus_{i=j}^r F_i$ soit envoyé sur $\oplus_{i=j}^s G_i$ (qui sont bien de même dimension).

Regardons maintenant $P_j(u)$, sur $\oplus_{i=j}^r F_i$ il induit l'endomorphisme nul. Donc par le changement de base évoqué plus haut, on déduit $P_j(\oplus_{i=j}^s G_i)$ est l'endomorphisme nul.

Donc P'_j divise P_j car P'_j est le polynôme minimal de u induit sur $\oplus_{i=j}^r G_i$. On déduit la divisibilité inverse de la même manière. Donc on obtient une contradiction.

Références

— Mansuy, Mneimné.
— H2G2.