

Invariants de similitude (Gourdon page 290-291)

Pierre Lissy

May 3, 2010

Lemme 1. *On considère un endomorphisme cyclique u de polynôme minimal $P = X^n - \dots - a_0$. Alors il existe une base dans laquelle la matrice de u est celle de la matrice compagnon de P .*

Proof. Il existe un vecteur x tel que $(x, f(x), \dots, f^{n-1}(x))$ est une base. Cette base convient trivialement (car $f^n = -a_0x - \dots - a_{n-1}f^{n-1}x$) $\square$

Théorème 1. *Il existe une suite de sev $F_1, \dots, F_r$ de sev u -stables en somme directe, sur lequel l'endomorphisme induit u_i est cyclique et si P_i est le polynôme minimal de u_i avec $P_n | P_{n-1} \dots P_1$. De plus, une telle suite de polynôme est unique. Elle est appelée suite des invariants de similitude*

Proof. On considère $k = \deg(\Pi_f)$. On sait qu'il existe un vecteur totalisateur x tel que $P_x = \Pi_f$. Le sous-espace vectoriel engendré par x , noté F , est donc de dimension k et stable par u par définition, de plus on a une base $(x, f(x), \dots, f^{k-1}(x)) = (e_1, \dots, e_k)$ que l'on complète en une base $(e_1, \dots, e_n)$ de E . On considère la base duale $(e_1^*, \dots, e_n^*)$, et on considère G le sev vectoriel de E qui est Γ° avec $\Gamma = \{f(e_k^*) | i \in \mathbb{N}\} = \{e_k^*(f_i) | i \in \mathbb{N}\}$. Autrement dit, G est l'ensemble des $x \in E$ tel que la k -ième coordonnée de f^i est nulle pour tout i . L'ensemble G étant clairement stable par f , il reste à démontrer pour conclure un raisonnement par récurrence qu'il est un supplémentaire de F . Soit $y \in F \cap G$. Si $y \neq 0$, alors $y = \sum^p a_i e^i$ avec $a_p \neq 0$ et $p \leq k$ (puisque $y \in F$). Mais on sait que $e_k^*(f^{k-p}(y)) = 0$, donc $0 = e_k^*(a_1 e_{k-p+1} + \dots + a_p e_k) = a_p$, d'où la contradiction. Il reste à démontrer que $\dim(E) = \dim(F) + \dim(G)$. Mais $G = (\text{Vect}(\Gamma))^\circ$ donc démontrer que G est nul revient à démontrer que $\dim(\Gamma) = k$. Considérons pour cela l'application suivante : $\varphi : K[f] \rightarrow \text{Vect}(\Gamma)$ qui à g associe e_k^*g . Elle est surjective par définition de $\text{Vect}(\Gamma)$. Elle est injective car si $e_k^*g = 0$, comme g s'écrit comme combinaison linéaire des f^i avec $i \leq k$, en utilisant les mêmes notations, à savoir $g = \sum^p a_i f^i$, avec $a_p \neq 0$, on a $0 = e_k^*g(f^{k-p})(x) = a_p$ d'où la contradiction. On voit donc qu'un raisonnement par récurrence se profile. L'initialisation est triviale. Supposons le résultat vrai pour tout ev de $\dim$ inf à $n-1$, avec de plus la propriété que le premier polynôme est le polynôme minimal de l'endomorphisme. Alors il est vrai pour G stable par f et l'induit de f sur G vérifie les propriétés voulues. Mais on remarque que $f_{G_i} = f_{F_i}$ (autrement dit une double induction sur deux sev est la même que l'induction la plus basse), donc on a déjà la décomposition voulue des sous-espaces stables en somme directe, on a déjà que l'induit est cyclique et que $P_n | \dots | P_2$. Reste à voir pourquoi $P_2 | P_1$. Or si l'on regarde la construction que l'on vient de faire, nécessairement P_2 est le polynôme minimal de f_G , qui divise trivialement le polynôme minimal de f (puisque Π_f annule f_G). Mais Π_f est aussi P_1 d'où le résultat.

Pour l'unicité, on considère deux décompositions différentes $F_1, \dots, F_r$ et $G_1, \dots, G_s$ (avec comme polynômes associés $P_1, \dots, P_r$ et $Q_1, \dots, Q_s$.) Alors comme le polynôme minimal de f est par propriété le pgcd des polynômes minimaux de ses induits, et que ce dernier pgcd est justement par la relation de division respectivement P_1 et Q_1 , qui sont donc égaux. Si l'on suppose que les deux suites de polynômes ne sont pas égales, notons j le premier indice à partir duquel elles diffèrent (cet indice est plus grand que 2 d'après ce qui précède, et existe car $\sum \deg(P_i) = \sum \deg(Q_i)$ donc même si $r \neq s$ on va finir par avoir avant le dernier indice quelque chose qui marche pas.) Alors comme E est somme directe des F_i et que $P_j(F_i) = 0$ pour $i \geq j$, on a $P_j(F_1)$ qui est somme directe des $P_j(F_i)$ pour $i \leq j-1$ (les sev sont stables par P_j d'où la directitude de la somme). De même $P_j(F_1)$ est somme directe des $P_j(f)(G_i)$ pour tout i . Donc Q_j divise P_j .

Or on remarque que nécessairement pour $i \leq j-1$, on a $\dim(P_j(f)(F_i)) = \dim(P_j(f)(G_i))$. En effet, d'après notre lemme, comme les polynômes minimaux sont égaux, dans deux bases différentes

les induits de f ont les même matrices, et donc celles de P_j aussi, ce qui signifie que les espaces sont de même dimension). Finalement, en prenant les dimensions dans l'égalité précédente on voit que $P_j(G_i) = 0$ pour $i \geq j$, autrement dit que P_j est nulle sur les G_i , ce qui signifie notamment que $Q_j | P_j$ (puisque Q_j est le polynôme minimal de l'induit sur le sous-espace vectoriel G_j .) Mais par symétrie du raisonnement on démontre de la même manière que P_j divise Q_j et donc $P_j = Q_j$ ce qui est supposé faux. D'où l'unicité. $\square$

Corollaire 1. *On a une représentation matricielle sous la forme de blocs de matrices compagnons.*

Proof. C'est clair avec le lemme que l'on a démontré: on considère les endomorphismes induits sur les sous-espaces d'après le lemme ils s'écrivent dans une base comme une matrice compagnon et on a plus que concaténer les bases entre elles) $\square$

References

[1]