

Théorème du bicommutant démontré de manière élémentaire (sans passer par les modules ou je sais pas quoi (cf cobicommutant.pdf))

Pierre Lissy

May 7, 2010

On considère la réduction de Frobenius de noter endomorphisme u . E est somme directe des E_i avec f_i l'endomorphisme induit qui est cyclique engendré par un vecteur noté x_i et π_i le polynôme minimal de f_i avec $\pi_1 | \dots | \pi_s$. On a donc une base de E qui est formée de des x_i et d'un certain nombre de leur itérés. Disons que E_i est de dimension n_i (qui est le degré du polynôme minimal) et que du coup une base de E_i est $(x_i, u_1 x_i, \dots, u_{n_i-1}(x_i))$. Tout x s'écrit donc de façon unique comme $\sum_1^s R_i(u)x_i$ avec R_i de degré inférieur à $n_i - 1$.

Commençons par un lemme qui nous donne une classe d'isomorphie du commutant d'un endomorphisme.

Lemme 1. *$C(u)$ est isomorphe en tant qu'espace vectoriel à $\text{Ker}(\pi_1) \times \dots \times \text{Ker}(\pi_s)$, l'isomorphisme étant donné par $v \mapsto (v(x_1), \dots, v(x_s))$.*

Proof. D'abord, l'application est bien définie à valeurs dans ce qu'on souhaite puisqu'un endomorphisme commutant avec u stabilise tous les sev de E u -stables, notamment il stabilise les E_i . Ensuite, elle est clairement linéaire.

Elle est injective car si pour tout i , $v(x_i) = 0$, alors pour tout i et pour tout $j \leq n_i - 1$, $u^j(v(x_i)) = v(u^j(x_i)) = 0$. famille génératrice de E (car pour tout i par définition $(u^j(x_i))$ engendre E_i), donc v est nul sur une base de E est identiquement nul.

Elle est surjective. En effet, prenons $(y_1, \dots, y_s) \in \text{Ker}(\pi_1) \times \dots \times \text{Ker}(\pi_s)$. On pose v l'endomorphisme qui à $u^j(x_i)$ associe $u^j(y_i)$, pour tout i et tout $j \leq n_i - 1$. Cela détermine v de manière unique. On a du coup clairement que $v(x_i) = y_i$ et le tour est joué pourvu que v commute bien avec u . Mais en fait on remarque que pour tout $P \in K[X]$, on a $v(P(u)x_i) = vP(u)(y_i)$. En effet, par division euclidienne, on écrit $P = Q\pi_i + S$ avec S de degré inférieur ou égal à $n_i - 1$. Du coup comme $x_i \in \text{Ker}(\pi_i)$ on a $v(P(u))(x_i) = v(S(u)(x_i)) = S(u)(y_i) = (Q\pi_i + S)(y_i)$ (car $y_i \in \text{Ker} \pi_i$) et le tour est joué. Du coup, on a que $u(v(x)) = \sum_1^s uv(R_i(u)x_i) = \sum_1^s (RX)(u)(y_i) = \sum_1^s v(RX)(u)(x_i) = v(u(x))$. □

Théorème 1. $K[u] = C(C(u))$.

Proof. l'inclusion directe est évidente. En effet, on prouve très facilement que $C(C(u))$ est une sous-algèbre de $L(E)$. On a que si $x \in C(C(u)), y \in C(C(u)), \lambda \in k$, et si $v \in C(u)$, alors $xv = vx$ donc $(\lambda x)v = v(\lambda x)$, de plus $yv = vy$, d'où $xyv = xvy = vxy$ et $(x+y)v = xv + yv = vx + vy = v(x+y)$. L'identité appartient trivialement à $C(C(u))$ vu que l'identité commute avec tout le monde. Du coup, pour montrer que $C(C(u))$ contient $K[u]$, comme ce dernier ensemble est la plus petite algèbre contenant u , il suffit de montrer que $u \in C(C(u))$ mais c'est une tautologie.

Il reste donc à démontrer le sens difficile, à savoir $C(C(u)) \subset K[u]$. Soit $w \in C(C(u))$ et p_i le projecteur sur E_i parallèlement aux autres E_j . p_i commute trivialement avec u . En effet, si l'on décompose x en $x_1 + x_2$ avec $x_1 \in E_i$ et $x_2 \in \{E_j\}$, alors $p_i(u(x_1 + x_2)) = p_i(u(x_1)) + p_i(u(x_2)) = u(x_1)$ car les deux sous-espaces en somme directe sont u -stables. Enfin, $u(x_1) = u(p_i(x))$ par définition. Ainsi, w doit commuter avec tous les p_i . Du coup, l'image de p_i est stable par w , ie $w(E_i) \subset E_i$, notamment $w(x_s) \in E_s$. Il existe donc un polynôme R tel que $w(x_s) = R(u)x_s$. Notre but ultime est de démontrer que $w = R(u)$, ce qui achèvera notre preuve.

Décomposons x sous la forme $\sum P_i(u)x_i$ avec P_i polynôme de degré inférieur à $n_i - 1$. Si l'on arrive à démontrer pour tout i que $w(x_i) = R(u)(x_i)$, alors on aura gagné car comme w commute avec les polynômes de u on aura $w(x) = w(\sum P_i(u)x_i) = \sum P_i(u)w(x_i) = \sum P_i(u)R(u)(x_i) = R(u)\sum P_i(u)(x_i) = R(u)(x)$, et ceci pour tout x , donc $w = R(u)$.

Pour démontrer $w(x_i) = R(u)(x_i)$, on va utiliser l'isomorphisme précédent. Soit $i \in [1, s]$. Comme $(x_1, \dots, x_{s-1}, x_i) \in \text{Im}(F)$ (vu que π_s est le polynôme minimal de u le dernier noyau est E tout entier), on a existence et unicité de $v \in C(u)$ tel que $v(x_k) = x_k$ pour $k < s$ et $v(x_s) = x_i$. Du coup, on a

$$w(x_i) = w(v(x_s)) = v(w(x_s)) = v(R(u))(x_s) = R(u)v(x_s) = R(u)x_i,$$

Ceci achève la preuve. □