Gabllot p. 112

Invariants de similitude

Théorème : Il existe une unique suite de n polynômes unitaires $D_1, \dots, D_n$, où D_i divise D_{i-1} pour tout $i \geq 1$, telle que E se décompose en une somme directe $E = E_1 \oplus \dots \oplus E_m$ de n sous-espaces cycliques E_i, où, pour tout i, $D_i = \mu_{\varphi_i}$, φ_i étant l'endomorphisme de E_i induit par φ.

Démonstration :

① **Existence :** On raisonne par récurrence sur $n = \dim E$.

On commence par fixer $x \in E$ tel que $\mu_x = \mu_\varphi$. On pose $\tilde{E} = E/\langle x \rangle$, qui est muni de l'endomorphisme $\tilde{\varphi}$ induit par φ. Par hypothèse de récurrence, il existe une suite de polynômes $(\tilde{D}_k)$ vérifiant $\tilde{D}_k \mid \tilde{D}_{k-1}$ pour tout $k \geq 1$, et une décomposition $\tilde{E} = \bigoplus \tilde{E}_k$, où $\tilde{E}_k = \langle \tilde{g}_k \rangle$ et $\mu_{\tilde{g}_k} = \tilde{D}_k$.

Pour tout $k \geq 1$, $\tilde{D}_k$ divise $\tilde{D}_1 = \mu_{\tilde{\varphi}}$, et ce dernier divise μ_φ, ce qui permet de fixer $N_k \in K[T]$ tel que $\mu_\varphi = N_k \tilde{D}_k$.

Soit $t_k \in E$ un antécédent quelconque de $\tilde{g}_k$. On a $(\tilde{D}_k(\tilde{\varphi}))(\tilde{g}_k) = 0$, donc $(\tilde{D}_k(\varphi))(t_k) \in \langle x \rangle$. On fixe donc $S_k \in K[T]$ de degré inférieur à celui de μ_φ tel que $(\tilde{D}_k(\varphi))(t_k) = (S_k(\varphi))(x)$.

On a $0 = \mu_\varphi(\varphi) = N_k(\varphi) \circ \tilde{D}_k(\varphi)$, donc $0 = (N_k(\varphi) \circ \tilde{D}_k(\varphi))(t_k)$
$= (N_k(\varphi) \circ S_k(\varphi))(x)$

Comme $\mu_x = \mu_\varphi$, on a $\mu_\varphi = N_k \tilde{D}_k \mid N_k S_k$, donc $\tilde{D}_k \mid S_k$.

On fixe donc $U_k \in K[T]$ tel que $S_k = U_k \tilde{D}_k$.

On a alors $(\widetilde{D_k}(\varphi))(t_k) = (S_k(\varphi))(x) = (\widetilde{D_k}(\varphi) \circ U_k(\varphi))(x)$.

On pose $g_k = t_k - (U_k(\varphi))(x)$, qui est un antécédent de $\tilde{g_k}$ vérifiant $(\widetilde{D_k}(\varphi))(g_k) = 0$, ce qui donne $\mu_{g_k} \mid \widetilde{D_k}$. En passant au quotient dans $\tilde{E}$, on a $\mu_{\tilde{g_k}} = \widetilde{D_k} \mid \mu_{g_k}$. Finalement, on a $\widetilde{D_k} = \mu_{g_k}$ (les polynômes sont unitaires). Pour tout $k \geq 1$, on pose alors $E_{k+1} = \langle g_k \rangle$ et $D_{k+1} = \widetilde{D_k}$.

La surjection $\sum_{k\geq 1} E_{k+1} \longrightarrow \sum_{k\geq 1} \tilde{E_k} = \bigoplus_{k\geq 1} \tilde{E_k}$ induite par

$$\sum_{k\geq 1} (P_k(\varphi))(g_k) \longmapsto \sum_{k\geq 1} (P_k(\tilde{\varphi}))(\tilde{g_k})$$

la surjection $E \longrightarrow \tilde{E}$ est alors bijective. En effet, si $\sum_{k\geq 1} (P_k(\tilde{\varphi}))(\tilde{g_k}) = 0$, on a $(P_k(\tilde{\varphi}))(\tilde{g_k}) = 0$ pour tout $k \geq 1$ (car la somme est directe), donc $\mu_{\tilde{g_k}} = \widetilde{D_k} = \mu_{g_k}$ divise P_k, ce qui donne $(P_k(\varphi))(g_k) = 0$. La somme $\sum_{k\geq 1} E_{k+1}$ est donc directe, et est un supplémentaire de $\langle x \rangle$ dans E.

On conclut en posant $E_1 = \langle x \rangle$.

② <u>Unicité :</u> Soit $E = \bigoplus_{k\geq 1} E_k$ une décomposition vérifiant les hypothèses du théorème, et, pour tout $k \geq 1$, D_k le polynôme minimal de l'endomorphisme φ_k de E_k induit par φ. On va montrer que la suite (D_k) ne dépend que de (E, φ), et pas de la décomposition $E = \bigoplus_{k\geq 1} E_k$. On écrit $\mu_\varphi = P_1^{m_1} \dots P_n^{m_n}$ la décomposition de μ_φ en produit d'irréductibles.

On va raisonner par récurrence sur $m_1 + \dots + m_n$.

- <u>Initialisation :</u> On suppose μ_φ irréductible. Les D_k sont alors égaux à 1 ou μ_φ, donc il existe $p \in [\![1, n]\!]$ tel que $D_k = \mu_\varphi$ pour $k \leq p$

et $D_k = 1$ pour $k > p$. On a alors $E = E_1 \oplus \dots \oplus E_p$, et les E_i, $i \in [\![1, p]\!]$, sont tous isomorphes de dimension $\deg \mu_\varphi$. On en déduit l'unicité de $p = \frac{n}{\deg \mu_\varphi}$.

- Hérédité : On commence par remarquer que $D_1 = \mu_\varphi$.

Soit P un facteur irréductible de μ_φ. On pose $\Phi = P(\varphi)$, $E' = \operatorname{Im} \Phi$, φ' l'endomorphisme de E' induit par φ, qui est de polynôme minimal $\mu_{\varphi'} = \frac{\mu_\varphi}{P}$.

Pour tout k, $E'_k = \Phi(E_k)$ est cyclique, de polynôme minimal D'_k.

On a $E' = \bigoplus_k E'_k$. Soit r l'indice tel que P divise $D_1, \dots, D_r$ et soit premier avec D_k pour $k > r$.

* Pour $k > r$, il existe des polynômes U_k, V_k tels que $1 = U_k P + V_k D_k$ (par Bézout) d'où $\mathrm{id}_{E_k} = U_k(\varphi_k) \circ P(\varphi_k)$, donc $E_k = U(\varphi_k) \circ P(\varphi_k)(E_k)$

$= P(\varphi_k) \circ U(\varphi_k)(E_k)$

$\subset P(\varphi_k)(E_k) = P(\varphi)(E_k) = E'_k$

donc $E_k = E'_k$ (l'inclusion $E'_k \subset E_k$ est claire), avec $D'_k = D_k$.

* Pour $k \leq r$, P divise D_k. Alors E_k / E'_k et $E'_k \subset E_k$ sont cycliques de polynômes minimaux P et $D'_k = \frac{D_k}{P}$.

Pour tout $k > 1$, D'_k divise D'_{k-1}. La suite de polynômes (D'_k), qui est associée à E', est alors intrinsèque par hypothèse de récurrence.

Donc on a $D_k = D'_k$ si $k > r$. Il reste à montrer que r est indépendant de la décomposition de E. On a $n = \dim E = \sum_k \deg D_k$

$= \sum_{k=1}^{r} (\deg P + \deg D'_k) + \sum_{k=r+1}^{+\infty} \deg D'_k$

$= r \deg P + \sum_{k=1}^{+\infty} \deg D'_k$

$= r \deg P + \dim E'$

Ceci achève la preuve du théorème.