# Réduction de Frobenius

↳ Refs : Mansuy et Mneimné p161-163, H2G2 p 102-105 (Tome 1)

<u>Cadre</u> : Soit $\mathbb{K}$ un corps, $E$ un $\mathbb{K}$-ev de dimension finie $n \in \mathbb{N}^*$. Soit $u \in \mathcal{L}(E)$. Pour $x \in E$, on note $\mu_{u,x}$ le polynôme minimal de $x$ p/r à $u$ ie l'unique polynôme unitaire qui engendre $\mathrm{Ker}(\varphi_{u,x})$, où
$$\varphi_{u,x} : \mathbb{K}[X] \to E,\quad P \mapsto P(u(x))$$
. On note $\mu_u$ le polynôme minimal de $u$.

**Lemme 1 :** Il existe $x \in E$ tel que $\mu_{u,x} = \mu_u$.

**Lemme 2 :** Si $x \in E$ est tel que $\mu_{u,x} = \mu_u$, alors le sous espace $E_{u,x} = \mathrm{Im}\, \varphi_{u,x}$ admet un supplémentaire stable par $u$.

**Théorème : (Réduction de Frobenius)** Il existe une unique suite de polynômes unitaires $P_1, P_2, \dots, P_r$ et une décomposition $E = \bigoplus_{i=1}^{r} E_i$ telles que
1) pour tout $i$ dans $⟦1, r-1⟧$, $P_{i+1}$ divise $P_i$,
2) pour tout $i$ dans $⟦1, r⟧$, l'endo induit $u_{E_i}$ est cyclique de polynôme minimal $P_i$.

(La suite de polynômes $P_1, \dots, P_r$ ne dépend que de $u$ et non du choix de la décomposition, on les appelle des invariants de similitude de $u$)

<u>Preuve du lemme 1</u> : On voit facilement que $\mu_{u,x} \mid \mu$. Il s'agit donc de montrer que l'égalité est atteinte. On va travailler sur les facteurs irréductibles de $\mu_u$ et généraliser grâce au lemme des noyaux.
On écrit $\mu_u = \prod_{i=1}^{p} P_i^{d_i}$ où les $P_i \in \mathbb{K}[X]$ sont irréductibles 2 à 2 distincts et $d_i \in \mathbb{N}^*$. On note $K_i = \mathrm{Ker}\, P_i^{d_i}(u)$, qui est stable par $u$. D'après le lemme des noyaux, $E = \bigoplus_{i=1}^{p} K_i$. On pose $u_i = u_{K_i}$, et alors $u_i \in \mathcal{L}(K_i)$ tq $\mu_{u_i} = P_i^{d_i}$
(en effet, par déf $P_i^{d_i}(u_i) = 0$ donc $\mu_{u_i} \mid P_i^{d_i}$, donc $\mu_{u_i} = P_i^{\beta_i}$, les $\mu_{u_i}$ sont premiers entre eux donc $\mu_u = \mathrm{ppcm}(\mu_1, \dots, \mu_p) = \mu_1 \cdots \mu_p$, donc $\deg(\mu_u) = \sum \deg(P_i^{d_i}) = \deg(\mu_1) + \dots + \deg(\mu_p)$, et $\mu_{u_i} \mid P_i^{d_i}$ donc $\beta_i \leq d_i$, mais nécessairement $\beta_i = d_i$ d'après l'égalité).
Montrons que $\forall i \in ⟦1,p⟧$, $\exists x_i \in K_i$ tq $\mu_{x_i,u_i} = \mu_{u_i}$. Soit $x_i \in K_i \setminus \mathrm{Ker}(P_i^{d_i-1}(u))$ (possible par minimalité de $P_i^{d_i} = \mu_{u_i}$) Alors $\mu_{x,u_i} = \mu_{u_i} = P_i^{d_i}$.
(sinon, on a $\mu_{x,u_i} \mid P_i^{d_i}$ mais $\mu_{x,u_i} \neq P_i^{d_i}$, donc $\mu_{x,u_i} \mid P_i^{\beta_i}$ avec $\beta_i < d_i$, contredit $x \notin \mathrm{Ker}(P_i^{d_i-1}(u))$).
Soit $x = x_1 + \dots + x_p$. Montrons que $\mu_u = \mu_{u,x}$. On a $0 = \mu_{u,x}(u)(x) = \sum_{i=1}^{p} \mu_{u,x}(u)(x_i)$.
Or les $K_i$ sont $u$-stables, donc $\forall i \in ⟦1,p⟧$, $\mu_{u,x}(u)(x_i) \in K_i$, donc puisque les $K_i$ sont en somme directe, $\forall i \in ⟦1,p⟧$, $\mu_{u,x}(u)(x_i) = \mu_{u,x}(u_i)(x_i) = 0$, donc $\mu_{u_i} = \mu_{x_i,u_i} = P_i^{d_i}$ divise $\mu_{u,x}$.
Donc (lemme d'Euclide), $\prod P_i^{d_i} = \mu_u \mid \mu_{u,x}$. D'où $\mu_u = \mu_{u,x}$.

<u>Preuve du lemme 2 :</u> Soit $x \in E$ tel que $\mu_{u,x} = \mu_u$. On note $d = \deg(\mu_u)$.
Alors la famille $(e_1 = x, e_2 = u(x), \dots, e_d = u^{d-1}(x))$ est une base de $E_{u,x}$, que l'on complète en une base $(e_1, \dots, e_n)$ de $E$. On considère $e_d^* = u^{d-1}(x)^*$ la p-ième forme linéaire coordonnée de la base duale associée, et on pose $G = \mathrm{Vect}(e_d^*, {}^tu(e_d^*), \dots {}^tu^{d-1}(e_d^*))$ qui est un sev de $E^*$, et on note $H = G^\circ$ (orthogonal dans le sens de la dualité, idée cachée derrière : $G$ stable par ${}^tu \iff G^\circ$ stable par $u$, et c'est ça qu'on veut !)
Montrons que $E = E_{u,x} \oplus H$ et que $H$ est stable par $u$.

- De la même façon que $E_{u,x}$ est stable par $u$, $G$ est stable par ${}^tu$, (car $\mu_{{}^tu} = \mu_u$, en particulier m degré), donc $H = G^\circ$ stable par $u$
- la famille $(e_d^*, {}^tu(e_d^*), \dots {}^tu^{d-1}(e_d^*))$ est libre : en effet, si $\sum_{k=0}^{d-1} \lambda_k \, {}^tu^k(e_d^*) = \sum_{k=0}^{d-1} \lambda_k \, e_d^*(u^k) = 0$ pour $\lambda_k \in \mathbb{K}$, alors en appliquant l'égalité en $u^i(x)$ pour $i$ allant de $0$ à $d-1$, on obtient successivement $\lambda_{d-1} = 0, \lambda_{d-2} = 0, \dots \lambda_0 = 0$. Donc $G$ est de dimension $d$, et ainsi $H$ est de dimension $n-d$.
- Enfin, si $y \in E_{u,x} \cap H$, alors $y = \sum_{k=0}^{d-1} a_k u^k(x)$ avec $a_k \in \mathbb{K}$ car $y \in F$. Mais en appliquant ${}^tu^k(e_d^*)$ pour $k$ allant de $0$ à $d-1$, on obtient que tous les $a_k$ sont nuls donc $y = 0$.

Ainsi $E = E_{u,x} \oplus H$ et $H$ est $u$-stable.

<u>Preuve du théorème :</u> On va montrer le résultat par récurrence sur la dimension de l'espace.

* Si $n=1$, tous les endos sont cycliques, le résultat est évident.
* Soit $n \geq 1$ tel que le résultat ait été établi pour les endomorphismes d'espace de dimension $\leq n$, et considérons un endomorphisme $u$ d'un espace de dimension $n+1$.

Soit $x \in E$ tel que $\mu_{u,x} = \mu_u$ et $H$ un supplémentaire stable du sous espace $E_1 = E_{u,x}$. Si $H = \{0\}$, c'est terminé (cas $u$ endo cyclique). Sinon, $1 \leq \dim H \leq n$ et alors on applique l'hypothèse de récurrence à l'endo $u_H$ induit par $u$ sur $H$ : il existe une suite de polynômes unitaires $P_2, \dots P_r$ et une décomposition $H = \bigoplus_{i=1}^{r} E_i$ telles que pour tout $i \in [\![2, r-1]\!]$, $P_{i+1} | P_i$ et $u_{E_i}$ est cyclique de polynôme minimal $P_i$.
On vérifie alors que $\mu_{u_H} = P_2$ divise $\mu_u$, car $\mu_u$ annule $u_H$, et $u_{E_1}$ est cyclique de polynôme minimal $\mu_{u,x} = \mu_u$. Donc en posant $P_1 = \mu_u$, $P_2, \dots P_r$ et la décomposition $E = \bigoplus_{i=1}^{r} E_i$, on a bien terminé.

Montrons maintenant l'unicité* de la suite de polynômes : soit $P_1, \dots P_r$, $Q_1, \dots Q_s$ deux suites distinctes de polynômes unitaires et $E = \bigoplus_{i=1}^{r} E_i = \bigoplus_{i=1}^{s} F_i$ les décompositions associées.

Par construction, on a $P_1 = Q_1 = \mu_u$. On a également $\sum_{i=1}^{r} \deg P_i = \sum_{i=1}^{s} \deg Q_i$, donc même si $r \neq s$, il existe $j \in [\![2, \min(r,s)]\!]$, tel que $P_j \neq Q_j$. Intéressons nous à $P_j(u)$.

Pour tout $i \geq j$, $P_i \mid P_j$, donc $P_j(u_{E_i}) = 0$. Ainsi (les $E_i$ étant $u$ stables)

$$P_j(u)(E) = \bigoplus_{i=1}^{r} P_j(u)(E_i) = \bigoplus_{i=1}^{r} P_j(u_{E_i})(E_i) = \bigoplus_{i=1}^{j-1} P_j(u)(E_i)$$

Or $P_j(u)(E) = \bigoplus_{i=1}^{s} P_j(u)(F_i)$, d'où $\bigoplus_{i=1}^{j-1} P_j(u)(E_i) = \bigoplus_{i=1}^{s} P_j(u)(F_i)$, donc en particulier avec les dimensions $\sum_{i=1}^{j-1} \dim P_j(u)(E_i) = \sum_{i=1}^{s} P_j(u)(F_i)$.

Par définition, $P_i = Q_i$ pour $i < j$ donc $u_{E_i}$ et $u_{F_i}$ sont semblables, ainsi

$\dim P_j(u)(E_i) = rg\, P_j \circ u_{E_i} = rg\, P_j \circ u_{F_i} = \dim P_j(u)(F_i)$

Donc en réinjectant, on obtient $\dim P_j(u)(F_j) = 0$ (et de même $\forall i \geq j$), donc $P_j(u_{F_j}) = 0$ ie $Q_j = \mu_{F_j} \mid P_j$. Par symétrie $P_j \mid Q_j$ ie $P_j = Q_j$ car unitaires : contradiction !

*A raconter avec les mains s'il reste éventuellement du temps.

Remarques : * On peut formuler cela matriciellement : il existe une unique suite de polynômes unitaires $P_1, \dots P_r$ tels que

1) Pour tout $i \in [\![1, r-1]\!]$, $P_{i+1}$ divise $P_i$

2) Il existe une base de $E$ dans laquelle la matrice de $u$ est diagonale par blocs : $\begin{pmatrix} \boxed{C_{P_1}} & & & \\ & \boxed{C_{P_2}} & & \\ & & \ddots & \\ & & & \boxed{C_{P_r}} \end{pmatrix}$ où $C_{P_i}$ est la matrice compagnon du polynôme $P_i$.

* Ce théorème comporte de très nombreuses applications, en voici quelques unes :

• Dans le cas nilpotent, on obtient la réduct° de Jordan, et grâce au lemme des noyaux, on peut obtenir Jordan pour tous les endo. (et + généralement on obtient des infos sur dim $\mathcal{C}(u)$)

• (Applicat° plutôt du lemme 2) Un endo est cyclique ssi $\mathcal{C}(u) = \mathbb{K}[u]$.

• L'utilisation du fait que les polynômes sont des invariants totaux de similitude : ▶ deux matrices sont semblables ssi elles ont les m invariants

▶ si $u \in \mathcal{L}(\mathbb{K}^n)$ et si $\mathbb{L}$ est une extension de $\mathbb{K}$, alors $u$ et $u_{\mathbb{L}}$ ont les m invariants

$\Rightarrow$ si $\mathbb{L}$ est une extension de $\mathbb{K}$, si $A$ et $B$ dans $\mathcal{M}_n(\mathbb{K})$ sont semblables sur $\mathbb{L}$, elles sont semblables sur $\mathbb{K}$.

▶ $\deg(\mu_u) \leq 1 + rg(u)$. (optimal si on considère $\begin{pmatrix} 0 & 1 & & (0) \\ & \ddots & \ddots & \\ & & & 1 \\ (0) & & & 0 \end{pmatrix}$ ▷ $\deg(\mu) = n$, $rg = n-1$

* Contrairement à Jordan qui exige $\chi_u$ scindé, Frobenius ne demande aucune hypothèse sur $u$.

* En parlant de Jordan, comment faire le lien ?

• Si $u$ a un poly. carac. scindé et qu'on a Frobenius, il suffit de remplacer chaque invariant (scindé) par des blocs de Jordan associés à chaque v.p.

ex : si $\underbrace{P_1 = X^2(X-2)^3}_{J_2 \text{ et } 2I_3+J_3}$ ; $\underbrace{P_2 = X(X-2)}_{J_1 \text{ et } 2I_1+J_1}$ et $\underbrace{P_3 = X}_{J_1}$ → Jordan : $\begin{pmatrix} 2 & 1 & 0 & & & & & \\ 0 & 2 & 1 & & & & & \\ 0 & 0 & 2 & & & & & \\ & & & 2 & & & & \\ & & & & 0 & 1 & & \\ & & & & 0 & 0 & & \\ & & & & & & 0 & \\ & & & & & & & 0 \end{pmatrix}$

• Si $u$ a un poly carac scindé et qu'on a Frobenius, on fait la liste des polynômes minimaux des blocs, et on en prend dans chaque polynôme le polynôme de plus haut degré pour chaque VP → le produit donne un invariant (et ainsi de suite)

ex : Si les blocs sont $2I_3+J_3$, $2I_3+J_3$, $I_3+J_3$, $I_3+J_3$, $I_1+J_1$, $I_1+J_1$, $J_2$, $J_1$ alors on obtient

| | | | |
|---|---|---|---|
| $(X-2)^3$ | $(X-2)^3$ | | |
| $(X-1)^3$ | $(X-1)^3$ | $X-1$ | $X-1$ |
| $X^2$ | $X$ | | |
| $P_1$ | $P_2$ | $P_3$ | $P_4$ |

* le thm découle du thm fondamental de la structure des modules de type fini sur un anneau principal, avec $\mathbb{K}[X]$ = anneau et le $\mathbb{K}[X]$ module défini par la matrice = module. C'est le m thm qui permet d'obtenir que les gp abéliens finis s'écrivent $\mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_k\mathbb{Z}$ avec $d_1 | d_2 | \dots | d_k$.

→ grâce à tous ces liens, on peut obtenir en pratique les invariants de $A$ en utilisant le fait que ce sont les facteurs invariants non constants de la matrice $XI_n - A \in M_n(\mathbb{K}[X])$ que l'on peut calculer via la réduct° de Smith, exemple avec $A = \begin{pmatrix} 2 & -4 & 1 & 3 \\ 2 & -3 & 0 & 2 \\ 0 & -1 & 1 & 2 \\ 1 & -1 & -1 & 0 \end{pmatrix} \in M_4(\mathbb{Q})$. (cf dev correspondant)

$$XI_4 - A = \begin{pmatrix} X-2 & 4 & -1 & -3 \\ -2 & X+3 & 0 & -2 \\ 0 & 1 & X-1 & -2 \\ -1 & 1 & 1 & X \end{pmatrix} \xrightarrow[\text{et colonnes}]{\text{transfo lignes}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & X^2+1 & 0 \\ 0 & 0 & 0 & X^2+1 \end{pmatrix}$$

facteurs invariants de $A$ :
$P_1 = X^2+1$
$P_2 = X^2+1$.