Invariants de similitude

Leçons : 150, 151, 153, 154, (159)
Réf : Gourdon, Mansuy.

Thm : $f \in \mathcal{L}(E)$, il existe une unique suite $F_1, \dots, F_r$ de sev de E, stables par f et vérifiant :
i) $E = F_1 \oplus \dots \oplus F_r$
ii) $\forall i$, $f_i := f_{|F_i}$ est un endo. cyclique de F_i
iii) $P_r | \cdots | P_1$ où P_i est le pol. minimal de f_i
La suite $P_1, \dots, P_r$ ne dépend pas de la décomposition : ce sont les invariants de similitude de f. On a $P_1 = \mu_f$ et $P_1 \cdots P_r = \chi_f$.

Dém : Existence : on procède par récurrence sur la dimension n de E.
Pour $n=1$: tous les endo. d'un espace de dim. 1 sont cycliques.
Si le résultat est vrai pour les dim. $\leq n$ et si $f \in \mathcal{L}(E)$ avec $\dim E = n+1$ on choisit $x \in E$ tq $\mu_{f,x} = \mu_f$ et on pose $F_1 = E_{f,x} = \{P(f)(x), P \in \mathbb{K}[X]\}$

F_1 est alors stable par f et de dimension $k := \deg \mu_f$ donc $(e_1, \dots, e_k) = (x, \dots, f^{k-1}(x))$ est une base de F_1. On la complète en $(e_1, \dots, e_n)$ base de E et on note $(e_1^*, \dots, e_n^*)$ la base duale associée. Soit alors $G = \Gamma^\circ$ où $\Gamma = \{{}^t f^i(e_k^*) : i \in \mathbb{N}\}$
$= \{e_k^* \circ f^i : i \in \mathbb{N}\}$

G est l'ens. des x tq la k-ième coord. de $f^i(x)$ est nulle $\forall i$

G est un sev de E, stable par f.
Lemme : on a $E = F_1 \oplus G$
Dém : si $y \in F_1 \cap G$ et $y \neq 0$, on l'écrit $y = a_1 e_1 + \dots + a_p e_p$ où $a_p \neq 0$ et $p \leq k$. En composant par ${}^t f^{k-p}(e_k^*) = e_k^* \circ f^{k-p}$, on obtient
$0 = e_k^*(a_1 e_{k-p+1} + \dots + a_p e_k) = a_p$ d'où une contradiction.
Donc $F_1 \cap G = \{0\}$.
Par ailleurs, comme $G = (\mathrm{Vect}\,\Gamma)^\circ$, pour mq $\dim G = n - \dim F_1 = n-k$ il suffit de mq $\dim \mathrm{Vect}\,\Gamma = k$.
Soit donc $\varphi : g \in \mathcal{Z}_f = \{P(f) : P \in \mathbb{K}[X]\} \longmapsto e_k^* \circ g \in \mathrm{Vect}\,\Gamma$

Par définition de Vect Γ, φ est surjective.

Si $e_k^* \circ g = 0$ avec $g \neq 0$, on écrit $g = a_1 Id_E + \dots + a_p f^{p-1} \in \mathcal{L}_f$ avec $a_p \neq 0$ et $p \leq k$ et $e_k^* \circ g(f^{k-p}(x)) = 0 = e_k^*(a_1 e_{k-p+1} + \dots + a_p e_k) = a_p$ d'où une contradiction. Donc φ est injective. Donc φ est un iso et on a $\dim \text{Vect}\,\Gamma = \dim \mathcal{L}_f = k$. Bref $E = F_1 \oplus G$. $\square$

On applique l'hyp. de récurrence à G : $\exists F_2, \dots, F_r$ tq $G = \bigoplus_{i=2}^{r} F_i$ etc.

On a donc $E = F_1 \oplus F_2 \oplus \dots \oplus F_r$ et on a le ii).

De plus μ_f annule $f_{|G}$ donc $P_2 = \mu_{f_{|G}} \mid \mu_f = P_1$ d'où l'existence.

Unicité : soient $\begin{cases} E_1, \dots, E_r \\ P_1, \dots, P_r \end{cases}$ et $\begin{cases} F_1, \dots, F_s \\ Q_1, \dots, Q_s \end{cases}$ deux suites qui conviennent. Par construction $P_1 = Q_1 = \mu_f$.

Si $(P_1, \dots, P_r) \neq (Q_1, \dots, Q_s)$, comme $\sum \deg P_i = n = \sum \deg Q_j$ il existe $j \in [\![2, \min(r,s)]\!]$ minimal tq $P_j \neq Q_j$.

- Pour $i \in [\![1, j-1]\!]$, $f_{|F_i}$ et $f_{|E_i}$ sont semblables car les deux sont cycliques de même polynôme minimal $P_i = Q_i$ donc $P_j(f_{|F_i})$ et $P_j(f_{|G_i})$ sont semblables
- Pour $i \geq j$, $P_i \mid P_j$ donc $P_j(f_{|E_i}) = 0$.

Autrement dit, on a $P_j(f)(E) = P_j(f)(F_1) \oplus \dots \oplus P_j(f)(F_{j-1})$
$= P_j(f)(G_1) \oplus \dots \oplus P_j(f)(G_s)$

et $\forall 1 \leq i \leq j-1$, $\dim P_j(f)(F_i) = \dim P_j(f)(G_i)$

donc en prenant les dimensions, on trouve $0 = \dim P_j(f)(G_j)$
$= \dots$
$= \dim P_j(f)(G_s)$

donc en particulier $Q_j \mid P_j$.

Par symétrie $P_j \mid Q_j$ et comme ils sont uni., $P_j = Q_j$: contradiction $\square$

Thm : (Frobenius) $f \in \mathcal{L}(E)$, il existe une unique suite $P_1, \dots, P_r$ de pol. unitaires tq $P_r \mid \dots \mid P_1$ et une base de E dans laquelle la matrice de f est

$$\begin{pmatrix} C_{P_1} & & \\ & \ddots & \\ & & C_{P_r} \end{pmatrix}$$

Dém : d'après le thm des invariants de similitude, si $F_1, \dots, F_r$ est la décomposition précédente, $\forall i$, $f_{|F_i}$ est cyclique de pol. minimal P_i donc il existe une base $\mathcal{B}_i$ de F_i dans laquelle $[f_{|F_i}]_{\mathcal{B}_i} = C_{P_i}$ et on prend la base $\mathcal{B} = \mathcal{B}_1 \cup \dots \cup \mathcal{B}_r$ de E pour avoir le résultat. $\square$

Conséquence : deux endo. $f, g \in \mathcal{L}(E)$ sont semblables ssi ils ont les mêmes invariants de similitude.
(plan)

Si $x \in E$, on note $\mu_{f,x}$ le polynôme unitaire engendrant l'idéal $\{P \in \mathbb{K}[X] : P(f)(x) = 0\}$.

Prop : Si $k = \deg \mu_f$, $\mathcal{L}_f = \{P(f) : P \in \mathbb{K}[X]\}$ est un sev de $\mathcal{L}(E)$ de dimension k dont une base est $(\mathrm{Id}_E, f, \dots, f^{k-1})$.
Si $k = \deg \mu_{f,x}$, $E_{f,x} = \{P(f)(x) : P \in \mathbb{K}[X]\}$ est un sev de E de dim k dont une base est $(x, f(x), \dots, f^{k-1}(x))$.

Dém : L'application $\varphi : \begin{array}{l} \mathbb{K}[X] \longrightarrow \mathcal{L}_f \\ P \longmapsto P(f) \end{array}$ est linéaire. Son image est $\mathcal{L}_f$, c'est donc un sev et son noyau est $\{P \in \mathbb{K}[X] : P(f) = 0\} = (\mu_f)$.
Ainsi $\mathcal{L}_f$ est isomorphe à $\mathbb{K}[X]/(\mu_f)$. Ce dernier est de dimension k (dont une base est $(1, \bar{X}, \dots, \bar{X}^{k-1})$) d'où le résultat.
Pareil pour le second point avec $\tilde{\varphi} : P \in \mathbb{K}[X] \longmapsto P(f)(x) \in E$. $\square$

Prop : $\exists x \in E$ tq $\mu_{f,x} = \mu_f$.
Dém : on écrit $\mu_f = \prod_{k=1}^{p} P_k^{\alpha_k}$ où les P_k sont irré. 2 à 2 distincts.
Par le lemme des noyaux, $E = \bigoplus_{k=1}^{p} \mathrm{Ker}\, P_k^{\alpha_k}(f) = \mathrm{Ker}\, \mu_f(f)$.
Par strict. $\uparrow$ de la suite des noyaux itérés, $\forall k$, $\exists x_k \in \mathrm{Ker}\, P_k^{\alpha_k} \setminus \mathrm{Ker}\, P_k^{\alpha_k - 1}$.
On pose $x = x_1 + \dots + x_p \in E$ de sorte que $0 = \mu_{f,x}(f)(x) = \sum_k \mu_{f,x}(f)(x_k)$.
Or, $\forall k$, $\mu_{f,x}(f)(x_k) \in \mathrm{Ker}\, P_k^{\alpha_k}(f)$, qui sont en somme directe donc cela impose $\mu_{f,x}(f)(x_k) = 0$ et donc $P_k^{\alpha_k} \mid \mu_{f,x}$ (car $P_k^{\alpha_k}$ est le pol. min. de x_k). Par lemme d'Euclide, $\mu_f \mid \mu_{f,x}$ d'où $\mu_{f,x} = \mu_f$. $\square$

Déf : f est cyclique s'il existe $x \in E$ tq $E = E_{f,x}$, ce qui équivaut à dire $\deg \mu_f = n$

Prop : Si $f \in \mathcal{L}(E)$ est cyclique, il existe une base B de E tq $[f]_B = C_{\mu_f}$.

Dém : Comme f est cyclique, $\exists x \in E$ tq $E_{f,x} = E$.
Ainsi $(x, f(x), \dots, f^{n-1}(x))$ est une base de E et dans cette base, la matrice de f est C_{μ_f}. □

Il existe $x \in \operatorname{Ker} P_i^{\alpha_i}(f)$ tq $\mu_{f,x} = P_i^{\alpha_i}$?

Par lemme des noyaux, $E = \bigoplus \operatorname{Ker} P_i^{\alpha_i}(f)$

Soit $x \in \operatorname{Ker} P_i^{\alpha_i}(f)$. On a $\mu_{f,x} \mid P_i^{\alpha_i}$.

Comme P_i est irréductible, $\mu_{f,x} = P_i^{\beta_x}$

Supp. que $\forall x \in \operatorname{Ker} P_i^{\alpha_i}(f)$, $\beta_x \leq \alpha_i - 1$

Alors $P_i^{\alpha_i - 1}(f)\Big|_{\operatorname{Ker} P_i^{\alpha_i}(f)} = 0$ donc $\operatorname{Ker} P_i^{\alpha_i - 1}(f) = \operatorname{Ker} P_i^{\alpha_i}(f)$

Donc $E = \bigoplus_{j \neq i} \operatorname{Ker} P_j^{\alpha_j}(f) \oplus \operatorname{Ker} P_i^{\alpha_i - 1}(f)$

donc $P_i^{\alpha_i - 1} \circ \prod P_j^{\alpha_j}$ est annulateur de f, ce qui contredit la minimalité de μ_f.

Donc $\forall i$, $\exists x_i \in \operatorname{Ker} P_i^{\alpha_i}(f)$ tq $\mu_{f,x_i} = P_i^{\alpha_i}$

$P_i^{\alpha_i} = \mu_{f,x_i}$ sont premiers entre eux deux à deux,

$$\mathbb{K}[f](x_1 + \dots + x_p) = \bigoplus \underbrace{\mathbb{K}[f](x_k)}_{\operatorname{Ker} P_k^{\alpha_k}(f)}$$

Ainsi $\mu_{f, x_1 + \dots + x_p} = \prod P_i^{\alpha_i} = \mu_f$.

Quelques applications...

Si L est un surcorps de k et si $A, B \in \mathcal{M}_n(k)$ sont semblables dans $\mathcal{M}_n(L)$ alors elles le sont sur $\mathcal{M}_n(k)$.
En effet, via l'unicité, les invariants de similitude dans $\mathcal{M}_n(k)$ sont les mêmes que ceux dans $\mathcal{M}_n(L)$ (par invariance du polynôme minimal par extension de corps)

Si les seuls endo. qui commutent avec $f \in \mathcal{L}(E)$ sont des polynômes en f, alors f est cyclique.
Si ce n'est pas le cas, $\deg \mu_f < n$ donc le nombre r d'invariants de similitude de f vérifie $r \geq 2$. On écrit $E = F_1 \oplus G$ avec $G = F_2 \oplus \dots \oplus F_r \neq \{0\}$.
Soit p la projection sur G parallèlement à F_1, p et f commutent car F_1 et G sont stables par f. On a donc $p = Q(f)$ et comme $p_{|F_1} = 0$ on a $Q(f_{|F_1}) = 0$ donc $\mu_f = \mu_{f_{|F_1}}$ divise Q et donc $p = Q(f) = 0$: contradiction.

$n \leq \dim C(u) \leq n^2$.
voir Rombaldi.

Topologie des classes de similitude : voir FGN Algèbre 1.