Développement : Invariants de similitude

Leçons : 122, 153, 154, 159.

Soit E un $\mathbb{K}$-espace vectoriel, soit $f \in \mathcal{L}(E)$.
Pour $x \in E$, on note $E_x = \{P(f)(x), P \in \mathbb{K}[X]\}$, $\mathcal{I}_x = \{P \in \mathbb{K}[X], P(f)(x) = 0\}$ et P_x le polynôme engendrant l'idéal $\mathcal{I}_x$. f est dit *cyclique* s'il existe $x \in E$ tel que $E_x = E$.

Théorème. *Soit $f \in \mathcal{L}(E)$. Il existe une suite $F_1, \cdots, F_r$ de sev de E, tous stables par f, tels que :*
- *$E = F_1 \oplus \cdots \oplus F_r$*
- *Pour tout $i \in [\![1, r]\!]$, $f_{|F_i}$ endomorphisme cyclique de F_i.*
- *En notant P_i le polynôme minimal de $f_{|F_i}$, on a $\forall i \in [\![1, r-1]\!], P_{i+1}|P_i$.*

De plus, la suite des $P_1, \cdots, P_r$ ne dépend que de f et pas de la décomposition choisie.

Démonstration.
Étape 1 : Existence.
On admet l'existence de $x \in E$ tel que $\mu_f = P_x$. On note $k = \deg(\mu_f)$. Le sev $F := E_x$ est de dimension k et stable par f, et $e_1 := x, e_2 := f(x), \cdots, e_k := f^{k-1}(x)$ forme une base de F. On la complète en une base $(e_1, \cdots, e_n)$ de E, on note $(e_1^*, \cdots, e_n^*)$ la base duale associée. On pose $\Gamma = \{e_k^* \circ f^i, i \in \mathbb{N}\}$ et $G = \Gamma^\circ$ son orthogonal. C'est un sev de E stable par f. Montrons que $E = F \oplus G$.
- F, G sont en somme directe : soit $y \in F \cap G$. Par l'absurde, si $y \neq 0$, comme $y \in F$, on peut écrire $y = y_0 + y_1 f(x) + \cdots + y_p f^p(x), p \leq k-1, y_p \neq 0$. Mais alors $e_k^* \circ f^{k-1-p}(y) = y_p = 0$, contradiction : $y = 0$.
- $\dim(F) + \dim(G) = n$: on calcule $\dim(Vect(\Gamma))$. On note $\mathcal{L}(f) = \{P(f), P \in \mathbb{K}[X]\}$ et on considère $\varphi \begin{cases} \mathcal{L}(f) & \to Vect(\Gamma) \\ g & \mapsto e_k^* \circ g \end{cases}$. φ est clairement surjective, et elle est aussi injective : soit $g \in \mathcal{L}_f$ tel que $\varphi(g) = 0$. On écrit $g = g_0 Id_E + g_1 f + \cdots + g_p f^p$ et on suppose $g_p \neq 0$. En évaluant cette relation en $f^{k-1-p}(x)$, il vient $g(f^{k-1-p}(x)) = g_0 f^{k-1-p}(x) + \cdots + g_p f^{k-1}(x)$, et donc $e_k^* \circ g(f^{k-1-p}(x)) = g_p = 0$, contradiction. Donc $g = 0$ et φ injective. Comme φ est linéaire, c'est un isomorphisme et $\dim(Vect(\Gamma)) = \dim(\mathcal{L}(f)) = k$. Il s'ensuit que $\dim(G) = n - \dim(Vect(\Gamma)) = n - k$ et $\dim(F) + \dim(G) = n$.

On a donc $E = F \oplus G$. On note P_1 (respectivement P_2) les polynômes minimaux de $f_{|F}$ (respectivement $f_{|G}$). On note que $P_1 = \mu_f$, et comme G stable par $f, P_2|P_1$. Par récurrence, en réappliquant le même processus à G, on obtient la décomposition voulue en un nombre fini d'étapes.

Étape 2 : Unicité.
Supposons qu'il existe deux suites différentes de sous-espaces $F_1, \cdots, F_r$ et $G_1, \cdots, G_s$ stables par f et qui vérifient toutes les conditions. On note, pour tout $i \in [\![1, r]\!], P_i = \mu_{f_{|F_i}}$ et, pour tout $i \in [\![1, s]\!], Q_i = \mu_{f_{|G_i}}$.
Soit j le plus petit indice tel que $P_j \neq Q_j$: il existe même si $r \neq s$ puisque $\sum_{i=1}^{r} \deg(P_i) = n = \sum_{i=1}^{s} \deg(Q_i)$: en effet, les restrictions étant cycliques, on a $\deg(P_i) = \dim(F_i)$ et $\deg(Q_i) = \dim(G_i)$.
De plus, on a $\mu_f(f_{|F_1}) = 0$, donc $P_1|\mu_f$. Mais comme tous les P_i divisent P_1, on a aussi $P_1(f_{|F_i}) = 0$ pour tout i, donc comme les F_i sont supplémentaires, $P_1(f) = 0$ et $\mu_f|P_1$. Donc $\mu_f = P_1$, de même $Q_1 = \mu_f = P_1$ et donc $j \geq 2$.
Comme les F_i sont stables par f, on a $P_j(f)(E) = P_j(f)(F_1) \oplus \cdots \oplus P_j(f)(F_r)$. Mais par définition du polynôme minimal,$P_j(f)(F_j) = \{0\}$ et comme pour $m \geq j, P_m|P_j$, on a aussi $P_j(f)(F_m) = \{0\}$. Donc

$$P_j(f)(E) = P_j(f)(F_1) \oplus \cdots \oplus P_j(f)(F_{j-1}) \tag{1}$$

Par ailleurs, comme les G_i sont stables par f, on a

$$P_j(f)(E) = P_j(f)(G_1) \oplus \cdots \oplus P_j(f)(G_s) \tag{2}$$

Pour tout $i \in [\![1, j-1]\!]$, $\dim(P_j(f)(F_i)) = \dim(P_j(f)(G_i))$: en effet, les endomorphismes cycliques $f_{|F_i}, f_{|G_i}$ peuvent être représentés dans une certaine base par la matrice compagnon de leur polynôme minimal, et $P_i = Q_i$ pour $i \leq j-1$. En prenant les dimensions dans (1) et (2) et en égalant, on tire $\dim(P_j(f)(G_j) = \cdots = \dim(P_j(f)(G_s)) = 0$, ce qui prouve que $Q_j|P_j$. Par symétrie, on a $P_j|Q_j$, donc $P_j = Q_j$, contradiction. Donc $r = s$ et pour tout $i, P_i = Q_i$.
□

Compléments

Existence de l'élément tel que $P_x = \mu_f$

Pour $x \in E$, si on note $k = \deg(P_x)$, E_x est un espace vectoriel, dont $(x, f(x), \cdots, f^{k-1}(x))$ forme une base.
Soient x, y tels que $E_x \cap E_y = \{0\}$. On a $P_{x+y}(f)(x+y) = 0 \Leftrightarrow P_{x+y}(f)(x) = -P_{x+y}(f)(y) \in E_x \cap E_y$, donc $P_{x+y}(f)(x) = P_{x+y}(f)(y) = 0$, ainsi $P_x | P_{x+y}, P_y | P_{x+y}$, ainsi $(P_x \vee P_y) | P_{x+y}$.
Réciproquement, $(P_x \vee P_y)(x+y) = 0$ donc $P_{x+y} | (P_x \vee P_y)$, et donc $P_{x+y} = P_x \vee P_y$.

Montrons maintenant que si $P_x \wedge P_y = 1$, alors $E_{x+y} = E_x \oplus E_y$. Soit $z \in E_x \cap E_y$, ainsi $z = P(f)(x) = Q(f)(y)$.
On a $(P_xQ)(f)(y) = P_x(f)(P(x)) = P(f)(P_x(x)) = 0$, donc $P_y | P_xQ$, et par le lemme de Gauss, $P_y | Q$. Donc $Q(f)(y) = 0$ et $z = 0$. Donc $E_x \cap E_y = \{0\}$. Et on a donc $P_{x+y} = P_x \vee P_y = P_xP_y$.
Alors $\dim(E_{x+y}) = \deg(P_{x+y}) = \deg(P_x) + \deg(P_y) + \dim(E_x) + \dim(E_y)$, et $E_{x+y} = E_x \oplus E_y$.

Si $\mu_f = P^mQ$ avec P irréductible, $P^m \wedge Q = 1$, le lemme des noyaux donne $E = \ker(P^m(f)) \oplus \ker(Q(f))$. Et si $x \in \ker(P^m(f)), P^m(f)(x) = 0$ implique $P_x | P^m$ donc il existe $m_x \leq m$ tel que $P_x = P^{m_x}$ car P irréductible. Par l'absurde, si pour tout $x, m_x < m$, alors pour tout $x \in \ker(P^m(f))$, on a $P_x | P^{m-1}$ donc $P^{m-1}(f)(x) = 0$, ce qui prouve $\ker(P^m(f)) = \ker(P^{m-1}(f))$. D'après le lemme des noyaux, on a donc $\ker((P^{m-1}Q)(f)) = E$, donc $(P^{m-1}Q)(f) = 0$, contradiction avec la minimalité de μ_f puisque $\deg(P^{m-1}Q) < \deg(\mu_f)$. Donc il existe $x \in E$ tel que $m_x = m$.

Maintenant, si on décompose $\mu_f = \prod_{i=1}^{k} P_i^{m_i}$, pour tout i, il existe $x_i \in E$ tel que $P_{x_i} = P_i^{m_i}$.

Les (P_{x_i}) étant premiers entre eux, on a $E_{x_1+\cdots+x_k}) E_{x_1} \oplus \cdots \oplus E_{x_k}$, et donc $P_{x_1+\cdots+x_k} = \prod_{i=1}^{k} P_{x_i} = \prod_{i=1}^{k} P_i^{m_i} = \mu_f$.

Donc l'élément $x_1 + \cdots + x_k$ convient.

Application : Réduction de Fröbenius

Si $P = X^p + a_{p-1}X^{p-1} + \cdots + a_1X + a_0$, on appelle *matrice compagnon* de P la matrice $C(P) = \begin{pmatrix} 0 & \cdots & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{p-2} \\ 0 & \cdots & 0 & 1 & -a_{p-1} \end{pmatrix}$.

$C(P)$ admet P pour polynôme minimal et $(-1)^pP$ pour polynôme caractéristique.
Si f cyclique, alors il existe $x \in E$ tel que $E_x = E$. Alors $(x, f(x), \cdots, f^{n-1}(x))$ base de E, et dans cette base, $C(\mu_f)$ est la matrice de f (comme $\mu_f(f) = 0$, on a $f^n(x) = -a_{n-1}f^{n-1}(x) - \cdots - a_1x - a_0$).

Théorème (Réduction de Fröbenius)**.** *Si $f \in \mathcal{L}(E)$ et si $P_1, \cdots, P_r$ sont ses invariants de similitude, alors il existe une base dans laquelle la matrice de f est (par blocs) $diag(C(P_1), \cdots, C(P_r))$.*

Démonstration. Il suffit de prendre pour tout i, une base B_i telle que la matrice de $f_{|F_i}$ soit $C(P_i)$, puis prendre $B = (B_1, \cdots, B_r)$. □

Références

X. Gourdon, Les maths en tête - Algèbre, Ellipses, p. 289.

Notes personnelles

Long et pas évident (d'autant que d'après des camarades qui l'ont fait à l'oral, le jury demande de prouver l'existence du x qui va bien). Mais la réduction de Frobenius est de toute façon à connaître. Il faut aussi savoir la déterminer dans des cas d'école si on veut présenter ce développement. Une autre version se trouve dans Mansuy-Mneimné.