Invariants de similitudes

Leçons : 151 ; 153 ; 154

Références : GOURDON, *Algèbre* (p.290)

Prérequis :

- Lemme des noyaux
- Endomorphismes cycliques
- Notions de dualité (orthogonal, base duale, etc...)

Notations :

- $C(P)$ désigne la matrice compagnon associée au polynôme $P \in \mathbb{K}[X]$
- Π_u désigne le polynôme minimal de l'endomorphisme $u \in \mathcal{L}(E)$ où E est un espace vectoriel

Introduction :

Supposons que l'on fait agir $GL_n(\mathbb{K})$ sur les matrices de $\mathcal{M}_n(\mathbb{K})$ par similitude, on voudrait décrire les orbites. On sait que deux matrices semblables ont même rang, même trace même déterminant, mais cela ne suffit pas à décrire les orbites, puisqu'il existe des matrices de même rang, même trace et même déterminant qui ne sont pas semblables. On va voir ici ce que l'on appelle invariant de similitude qui permet décrire les orbites de cette action. Autrement dit, deux matrices sont semblables si et seulement si elles ont les mêmes invariants de similitude. On va faire ce développement en parlant d'endomorphismes plutôt que de matrices.

Lemme 1. Soit $u \in \mathcal{L}(E)$ avec E de dimension finie. On note Π_u le polynome minimal de u et Π_u^x le polynôme unitaire qui engendre

$$\{P \in \mathbb{K}[X], P(u)(x) = 0\}$$

Alors il existe $x \in E$ tel que

$$\Pi_u^x = \Pi_u$$

Démonstration du lemme.

Étape 1 : *Étudions le cas où $\Pi_u = P^\alpha$ avec P irréductible*

Pour tout $x \in E$, il existe $n \in [\![0;\alpha]\!]$ tel que

$$P^n(u)(x) = 0$$

On veut trouver un x tel que $P^n(u)(x) \neq 0$ pour tout $n < \alpha$.

Par l'absurde, si pour tout $x \in E$, il existe $n < \alpha$ tel que $P^(u)(x) = 0$, alors

$$P^{\alpha-1}(u) = 0$$

Donc $\Pi_u \mid P^{\alpha-1}$ puisque Π_u est le polynôme minimal de u. On aboutit à une contradiction car $P^{\alpha-1}$ est de degré strictement inférieur à Π_u.

Étape 2 : *Traitons le cas général*

On note
$$\Pi_u = \prod_{i=1}^{r} P_i^{\alpha_i}$$
la décomposition en irréductibles de Π_u. Par le lemme des noyaux, on a
$$E = \ker(\Pi_u(u)) = \bigoplus_{i=1}^{r} \underbrace{\ker(P_i^{\alpha_i}(u))}_{E_i}$$
Par l'étape 1, on a pour tout $i \in [\![1; r]\!]$, un $x_i \in E_i$ tel que
$$\Pi_{u_{|E_i}}^{x_i} = \Pi_{u_{|E_i}}$$
On va montrer le résultat pour $x = x_1 + \cdots + x_r$. On a alors $\Pi_u^x \mid \Pi_u$ car $\Pi_u(u)(x) = 0$. On veut montrer que $\Pi_u \mid \Pi_u^x$, autrement dit $\Pi_u^x(u) = 0$

On a
$$0 = \Pi_u^x(u)(x) = \sum_{i=1}^{r} \Pi_u^x(u)(x_i)$$
Comme les E_i sont en somme directe et que $u(E_i) \subset E_i$ [1], on a alors, pour tout $i \in [\![1; r]\!]$,
$$\Pi_u^x(u)(x_i) = 0$$
Donc
$$\Pi_{u_{|E_i}}^{x_i} = \Pi_{u_{|E_i}} \mid \Pi_u^x$$
Ainsi $\Pi_u^x(u)$ est nul sur chaque E_i donc nul sur E. Ce qui permet de conclure que
$$\Pi_u \mid \Pi_u^x$$
□

Théorème 1. Soit $u \in \mathcal{L}(E)$ avec E de dimension finie n. Alors il existe une suite $F_1, \ldots, F_r$ de sous-espaces vectoriels de E stables par u telle que

- $E = F_1 \oplus \cdots \oplus F_r$
- $\forall i \in [\![1; r]\!]$, $u_i := u_{|F_i}$ est cyclique sur F_i
- En notant P_i le polynôme minimal de u_i, on a
$$\forall i \in [\![1; r-1]\!], \quad P_{i+1} \mid P_i$$

De plus, les (P_i) ne dépendent que de u.

Remarques :
Les F_i sont les invariants de similitude de u.

Démonstration.
Existence : On va raisonner par récurrence sur la dimension de E.

Soit $d = \deg(\Pi_u)$. Par le lemme, il existe $x \in E$ tel que $\Pi_u^x = \Pi_u$. On pose
$$F := \{P(u)(x), P \in \mathbb{K}[X]\}$$

1. il suffit de l'écrire

La dimension de F est alors d puisque

$$\dim(F) = \dim\left(\mathbb{K}[X]/(\Pi_u^x)\right) = \deg(\Pi_u^x) = \deg(\Pi_u) = d$$

La famille des $e_i := u^i(x)$ pour tout $i \in [\![0; d-1]\!]$ forme une base de F. On la complète en $(e_0, \ldots, e_{n-1})$ une base de E.

On note $(e_0^*, e_1^*, \ldots, e_{n-1}^*)$ sa base duale associée. On pose l'ensemble

$$\begin{aligned} G &= \left\{x \in E, \forall i \in \mathbb{N}, (e_{d-1}^* \circ u^i)(x) = 0\right\} \\ &= \mathrm{Vect}\underbrace{\left\{e_{d-1}^* \circ u^i, i \in \mathbb{N}\right\}}_{\Gamma}^{\perp} \end{aligned}$$

On veut montrer que $F \oplus G = E$.

Soit $y \in F \cap G$. On suppose que $y \neq 0$. On écrit

$$y = a_0 e_0 + \cdots + a_p e_p \text{ avec } a_p \neq 0 \text{ et } p \leqslant d-1$$

Comme $y \in G$, on a

$$e_{d-1}^* \circ u^{d-1-p}(y) = 0$$

Ce qui donne

$$e_{d-1}^*(a_0 e_{d-1-p} + \cdots + a_p e_{d-1}) = a_p = 0$$

On a une contradiction. Donc $F \oplus G$.

On veut montrer que $\dim(\mathrm{Vect}(\Gamma) = d$.

On pose l'application linéaire

$$\varphi : \left\{ \begin{array}{ccc} \mathbb{K}[u] & \to & \mathrm{Vect}(\Gamma) \\ P(u) & \mapsto & e_{d-1}^* \circ P(u) \end{array} \right.$$

qui est bien définie et surjective par définition de Γ. L'application φ est injective par les mêmes techniques que pour montrer que $F \cap G = \{0\}$.

En effet, soit $P(u) \in \ker\varphi$. Si $P(u) \neq 0$, on peut écrire

$$P(u) = a_0 Id + a_1 u + \cdots + a_p u^p \text{ avec } a_p \neq 0 \text{ et } p \leqslant d-1$$

Comme on a

$$e_{d-1}^* \circ P(u) = 0$$

(car $P(u) \in \ker\varphi$), on trouve que $a_p = 0$, donc $P(u) = 0$ et φ est injective.

L'application φ est donc un isomorphisme, ce qui nous permet d'écrire

$$\dim(\mathrm{Vect}(\Gamma)) = \dim \mathbb{K}[u] = \dim(\mathbb{K}[X]/(\Pi_u)) = \deg(\Pi_u) = d$$

Donc $E = F \oplus G$ avec F et G stables par u. De plus, on a

$$\Pi_{u_{|F}} = \Pi_u^x = \Pi_u$$

et comme G est stable par u, on a

$$\Pi_{u_{|G}} \mid \Pi_u = \Pi_{u_{|F}}$$

Car pour tout $x \in G$, on a $\Pi_u(u)(x) = 0$, autrement dit, $\Pi_u(u_{|G}) = 0$.

Si $F = E$, on a le résultat voulue, sinon on effectue le même raisonnement à $u_{|G}$. On obtient le résultat souhaité car E est de dimension finie.

Unicité : Supposons qu'il existe $F_1, \dots, F_r$ et $G_1, \dots, G_s$ qui vérifient le théorème et qui ne sont pas égaux [2]. On pose

$$P_i := \Pi_{u_{|F_i}} \quad \text{et} \quad Q_i := \Pi_{u_{|G_i}}$$

Soit j le premier indice tel que $P_j \neq Q_j$. Cet indice existe car

$$n = \sum_{i=1}^{r} \deg P_i = \sum_{i=1}^{s} \deg Q_i$$

On a

$$E = F_1 \oplus \cdots \oplus F_r = G_1 \oplus \cdots \oplus G_s$$

On a donc

$$P_j(u)(E) = P_j(u)(F_1) \oplus \cdots \oplus P_j(u)(F_{j-1}) \text{ car } \forall i \geqslant j, P_i \mid P_j \tag{1}$$
$$P_j(u)(E) = P_j(u)(G_1) \oplus \cdots \oplus P_j(u)(G_s) \tag{2}$$

Or $P_i = Q_i$ pour tout $i \in [\![1; j-1]\!]$, en regardant les matrices compagnons, on a donc, pour tout $i \in [\![1; j-1]\!]$,

$$\dim(P_j(u)(F_i) = \operatorname{rg}(P_j(C(P_i))) = \operatorname{rg}(P_j(C(Q_i))) = \dim(P_j(u)(G_i)$$

On passe aux dimensions dans les équations (**??**) et (**??**). On trouve donc

$$\dim(P_j(u)(G_i)) = 0 \text{ pour tout } i \geqslant j$$

Donc $Q_i \mid P_j$ par définition de Q_i. En particulier, on a

$$Q_j \mid P_j$$

On peut faire le même raisonnement pour Q_j. On a donc $Q_j = P_j$, ce qui est absurde. Donc

$$r = s \quad \text{et} \quad (P_1, \dots, P_r = (Q_1, \dots, Q_r)$$

Ce qui conclut la preuve du théorème. □

Remarques :

Ce théorème est parfois appelé théorème de Frobenius.

C'est plus fort que la décomposition de Jordan, car ici on n'a pas besoin que le polynôme caractéristique soit scindé.

On peut montrer ce résultat avec l'algorithme donnant la forme normale de Smith.

Astuces de l'agrégatif :

Il faut bien comprendre où vivent les égalités. Est-ce une inégalité sur E ? sur $\mathcal{L}(E)$?

Le développement est long. Il ne faut pas trainer sur le lemme, pour avoir le temps de montrer le théorème.

2. On n'a pas ($r = s$ et $P_i = Q_i$ pour tout $i \in [\![1; r]\!]$).