Lemme des noyaux
CNS de diagonalisabilité

Léo Gayral

2017-2018

ref : Gourdon – Algèbre, 2e édition – p.175

Lemme 1. Soient $M \in M_n(\mathbb{K})$ et $P = QR \in \mathbb{K}[X]$ tel que $Q \wedge R = 1$. Alors $\ker P(M) = \ker Q(M) \oplus \ker R(M)$.

Démonstration.
Si $x \in \ker Q(M)$, alors $P(M) \times x = [QR](M) \times x = R(M) \times Q(M) \times x = R(M) \times 0 = 0$, donc $x \in \ker P(M)$. On en déduit l'inclusion $\ker Q(M) + \ker R(M) \subset \ker P(M)$.

Pour obtenir la somme directe et l'autre égalité, on va utiliser le théorème de Bezout. Soient donc $S, T \in K[X]$ tels que $QS + RT = 1$.

Si $x \in \ker Q(M) \cap \ker R(M)$, alors $x = S(M) \times Q(M) \times x + T(M) \times R(M) \times x = 0$, d'où la somme directe.

Plus largement, pour $x \in \ker P(M)$ quelconque, on a les projections $y = [RT](M) \times x \in \ker Q(M)$ et $z = [QS](M) \times x \in \ker R(M)$, tels que $x = y + z$, d'où l'autre inclusion.

Notons en particulier que, connaissant les polynômes Q et R, on peut explicitement déterminer S et T par l'algorithme d'Euclide, et calculer les projecteurs pour toute matrice M en conséquence. $\square$

Corollaire 1. Soit $P = \prod_{i=1}^{r} P_i^{\alpha_i}$ une décomposition en facteurs premiers. Alors, par récurrence sur le lemme précédent, $\ker P(M) = \bigoplus_{i=1}^{r} \ker P_i^{\alpha_i}(M)$.

Proposition 1. Soit $M \in M_n(K)$. M est diagonalisable ssi elle admet un polynôme annulateur scindé à racines simples.

Démonstration.
Supposons $M = BDB^{-1}$ diagonalisable, avec $B \in GL_n(\mathbb{K})$ et :

$$D = \operatorname{diag}(\overbrace{\lambda_1, \dots, \lambda_1}^{n_1 \text{ fois}}, \dots, \overbrace{\lambda_r, \dots, \lambda_r}^{n_r \text{ fois}}) .$$

Dans ce cas, pour tout $P \in \mathbb{K}[X]$ on a $P(M) = B \times P(D) \times B^{-1}$ donc en particulier, M et D ont les mêmes polynômes annulateurs. On vérifier ainsi, en raisonnant par blocs, que $P = \prod_{i=1}^{r} (X - \lambda_i)$, scindé à racines simples, annule D et donc M.

Réciproquement, supposons que $P(M) = 0$, avec P sous la forme ci-dessus. Par le lemme des noyaux, $\mathbb{R}^n = \ker P(M) = \bigoplus_{i=1}^{r} \ker(M - \lambda_i I_n)$. Sur l'espace propre $E_i = \ker(M - \lambda_i I_n)$, de dimension n_i, M s'identifie à l'homothétie de rapport λ_i. En considérant un changement de base $B \in GL_n(\mathbb{K})$ adapté à cette décomposition, on en déduit bien $M = BDB^{-1}$. $\square$

Corollaire 2. Soit $M \in M_n(\mathbb{R})$ diagonalisable. En connaissant ses valeurs propres, on peut déterminer $\exp(M)$ explicitement.

Démonstration.
En connaissant les valeurs propres λ_i, via des identités de Bezout, on peut en particulier en déduire une famille de projecteurs $P_i(M)$ adaptée à la décomposition $\mathbb{R}^n = \bigoplus_{i=1}^{r} E_i$.

On a alors $M = \sum_{i=1}^{r} \lambda_i \times P_i(M)$. En tant que projecteurs sur des espaces supplémentaires, ces matrices vérifient $P_i(M) \times P_j(M) = 0$ si $i \neq j$, et $P_i(M)^2 = P_i(M)$. On en déduit, par récurrence, que $M^k = \sum_{i=1}^{r} \lambda_i^k P_i(M)$.

Tous les objets manipulés étant sommables, on a alors :

$$e^M = \sum_{k \in \mathbb{N}} \frac{M^k}{k!} = \sum_{k \in \mathbb{N}} \sum_{1 \leq i \leq r} \frac{\lambda_i^k}{k!} P_i(M) = \sum_{1 \leq i \leq r} \left(\sum_{k \in \mathbb{N}} \frac{\lambda_i^k}{k!} \right) P_i(M) = \sum_{i=1}^{r} e^{\lambda_i} P_i(M) .$$

$\square$

Corollaire 3. Soit $M \in M_n(\mathbb{F}_q)$, avec $\mathbb{F}_q$ un corps fini.

M est diagonalisable ssi $M^q = M$.

Démonstration.
En effet, le morphisme de Frobenius nous garantit que $X^q - X = \prod_{\alpha \in \mathbb{F}_q} (X - \alpha)$, donc M est annulée par un polynôme scindé à racines simples de $\mathbb{F}_q[X]$ ssi $M^q = M$. $\square$