Décomposition de Dunford effective - Applications :

Voici les notes que j'ai réalisées lors de mon année de préparation à l'agrégation. Au delà de la démonstration du théorème, y figurent des applications/compléments.

Table des matières

Dans tout ce document, E désigne un espace vectoriel sur un corps $\mathbb{K}$ quelconque.

1 Décomposition de Dunford

Lemme 1

Soit E un espace vectoriel sur un corps $\mathbb{K}$, et $(u,n) \in \mathcal{L}(E)^2$ avec u inversible et n nilpotent tel que $[u,n]=0$. Alors, $u+n \in GL(E)$.

Démonstration : Soit $m \in \mathbb{N}$ tel que $n^m = 0$. Alors, $u+n = u \circ (I_d + u^{-1} \circ n)$. Or, comme u et n commutent, $(I_d + u^{-1} \circ n) \circ \sum_{k=0}^{m-1} (-u^{-1} \circ n)^k = I_d$. Ceci conclut. ■

Theorème 1 (*Dunford effective*)

Soient $\mathbb{K}$ un corps de caractéristique nulle et E un $\mathbb{K}$-espace vectoriel de dimension finie m. Soit $u \in \mathcal{L}(E)$ dont le polynôme caractéristique est scindé, et $P = \dfrac{\chi_u}{\chi_u \wedge \chi_u'}$. On définit la suite $u_0 = u$ et pour tout $n \in \mathbb{N}$,

$$u_{n+1} = u_n - (P'(u_n))^{-1} \circ P(u_n).$$

Elle est bien définie et stationne vers $d \in \mathcal{L}(E)$, endomorphisme diagonalisable vérifiant $u = d+n$, avec n nilpotent. On a de plus $d, n \in \mathbb{K}[u]$. Cette décomposition est unique.

Démonstration : Puisque χ_u est scindé, on écrit $\chi_u = \prod_{i=1}^{r} (X-\lambda_i)^{m_i}$. Alors, $P = \prod_{i=1}^{r}(X-\lambda_i)$ est un polynôme simplement scindé. Montrons par récurrence sur n que :

1. $u_n \in \mathbb{K}[u]$
2. $P(u_n) \in GL_m(\mathbb{K})$
3. $P(u_n) \in (P(u))^{2^n}\mathbb{K}[u]$.

Pour l'initialisation, puisque $u_0 = u$, on a clairement les points (1) et (3) qui sont vérifiés. Pour le point (2), notons $k = \max_{i \in [\![1,r]\!]}(m_i)$. On sait que $\chi_u | P^k$, donc $P^k(u) = 0$. Puisque $P \wedge P' = 1$, et $P^m \wedge P' = 1$. Par le théorème de Bézout, on obtient l'existence d'un couple $(Q,R) \in \mathbb{K}[X]^2$ tels que $P^m Q + P'R = 1$. Ainsi,

$$\underbrace{P^m(u) \circ Q(u)}_{=0} + R(u) \circ P'(u) = I_d.$$

Ainsi, $P'(u) \in GL_m(\mathbb{K})$.

On suppose le résultat acquis au rang n. On définit alors : $u_{n+1} = u_n - (P'(u_n))^{-1} \circ P(u_n)$. Par l'hypothèse de récurrence, $P'(u_n) \in GL_m(\mathbb{K})$, donc u_{n+1} est bien définie. Le théorème de Cayley-Hamilton assure que l'inverse d'un polynôme en u est un polynôme en u. On déduit de ce fait et de l'hypothèse de récurrence que u_{n+1} vérifie le premier point.

Remarquons que $(X+Y)^l = \sum_{j=0}^{l} \binom{l}{j} X^j Y^{l-j} = X^l + lYX^{l-1} + Y^2 Q_0(X,Y)$. Ainsi,

$$P(X+Y) = P(X) + P'(X)Y + Y^2 Q(X,Y).$$

Donc,

$$P(u_{n+1}) = P(u_n + (u_{n+1} - u_n)) = P(u_n) + P'(u_n) \circ (u_{n+1} - u_n) + (u_{n+1} - u_n)^2 \circ Q(u_n, u_{n+1} - u_n).$$

$$P(u_{n+1}) = \underbrace{P(u_n) + P'(u_n) \circ (-\left(P'(u_n)\right)^{-1} \circ P(u_n))}_{=0} + ((P'(u_n))^{-1} \circ P(u_n)))^2 \circ Q(u_n, u_{n+1} - u_n).$$

Puisque $P(u_n), P'(u_n)^{-1} \in \mathbb{K}[u]$, $[P(u_n), P'(u_n)^{-1}] = 0$, donc,

$$P(u_{n+1}) = P(u_n)^2 \circ (P'(u_n))^{-2} \circ Q(u_n, u_{n+1} - u_n).$$

Par hypothèse de récurrence, il existe $A \in \mathbb{K}[X]$ tel que $P(u_n) = P(u)^{2^n} \circ A(u)$. Ainsi, en utilisant à nouveau la propriété de commutativité des polynômes en u,

$$P(u_{n+1}) = (P(u))^{2^{n+1}} \circ (A(u))^2 \circ (P'(u_n))^{-2} \circ Q(u_n, u_{n+1} - u_n) \in (P(u))^{2^{n+1}} \mathbb{K}[u].$$

Pour le deuxième point, on a par le théorème de Bézout l'existence d'un couple $(U,V) \in \mathbb{K}[X]^2$ tels que $PU + P'V = 1$. Alors,

$$P'(u_{n+1}) \circ V(u_{n+1}) = I_d - P(u_{n+1}) \circ U(u_{n+1}).$$

Puisque $P(u)$ est nilpotent, $P(u_{n+1})$ l'est aussi car $u_{n+1} \in P(u)^{2^{n+1}}\mathbb{K}[u]$. Par commutation, $P(u_{n+1}) \circ U(u_{n+1})$ est nilpotent. Par le lemme, $P'(u_{n+1}) \circ V(u_{n+1})$ est inversible. Ainsi, $P'(u_{n+1}) \in Gl_m(\mathbb{K})$. Ceci conclut l'hérédité.

Remarquons que si $2^n \geq k$ (*i.e.* $n \geq n_0 := \lfloor \log_2(k) \rfloor + 1$), alors, $(P(u))^{2^n} = 0$. Ainsi, $P(u_n) = 0$ et $u_{n+1} = u_n$. La suite stationne vers $d \in \mathbb{K}[u]$, et $P(d) = 0$, donc d est annulé par un polynôme simplement scindé, il est diagonalisable. De plus :

$$n = u - d = u - u_{n_0} = \sum_{k=0}^{n_0 - 1} (u_k - u_{k-1}) = -\sum_{k=0}^{n_0-1} P'(u_k)^{-1} \circ P(u_k),$$

qui est nilpotent comme somme de tels endomorphismes qui commutent. Ainsi, $u = d + n$, et $n \in \mathbb{K}[u]$. Ceci assure que $d \circ n = n \circ d$.

Unicité : si $u = d + n = d' + n'$, alors $d - d' = n' - n$. Comme d' commute avec n' et lui-même, d' commute avec u, donc avec d qui est un polynôme en u. Ainsi, $d \circ d' = d' \circ d$. De même, $n \circ n' = n' \circ n$. Les endomorphismes d et d' sont diagonalisables, et commutent, donc ils sont codiagonalisables. Ainsi, $d - d'$ est diagonalisable. De même $n' - n$ est nilpotent comme somme de tels endomorphismes qui commutent. Le seul endomorphisme diagonalisable et nilpotent étant 0, on obtient $d = d'$ et $n = n'$. ■

2 Discussion des hypothèses

2.1 $\mathbb{K}$ est de caractéristique nulle

Il n'est a priori pas évident d'identifier précisement où l'hypothèse de caractéristique sur $\mathbb{K}$ est utilisée : voici quelques éléments de réponse.

Proposition 1

Soit $\mathbb{K}$ un corps et $P \in \mathbb{K}[X]$. Si $P \wedge P' = 1$, P est sans facteur carré.

Démonstration : Supposons que $P \wedge P' = 1$. Soit $Q \in \mathbb{K}[X]$ tel que $Q^2 | P$. Montrons que $Q \in \mathbb{K}[X]^\times$. Il existe $R \in \mathbb{K}[X]$ tel que $P = Q^2 R$. Alors, $P' = Q(2Q'R + QR')$; Ainsi, $Q | P'$. Par suite, $Q | P \wedge P' = 1$. Ceci montre que $Q \in \mathbb{K}[X]^\times$. ∎

Remarque 1. *La réciproque et fausse en général. On considère le corps $\mathbb{K} = \mathbb{F}_2(X)$, le corps des fractions rationnelles dans $\mathbb{F}_2$ en X. Soit $P = Y^2 - X \in \mathbb{K}[Y]$. Il n'a pas de facteur carré (il est sans racine, de degré 2, donc irréductible). Or, $P' = 2Y = 0$. Ainsi, $P \wedge P' = P \neq 1$. La réciproque est vraie dans un corps parfait.*

Définition 1

Un corps $\mathbb{K}$ est dit parfait s'il est de caractéristique nulle ou de caractéristique strictement positive, pour lesquel le morphisme de Frobénius est un automorphisme.

Remarque 2. *Un endomorphisme de corps étant toujours injectif, un corps fini est toujours parfait.*

Proposition 2

Soit $\mathbb{K}$ un corps parfait et $P \in \mathbb{K}[X]$. Si P est sans facteur carré, alors $P \wedge P' = 1$.

Démonstration : On décompose P en produit de facteurs irréductibles sur $\mathbb{K}$, $P = \prod_{i=1}^{r} P_i$, deux à deux distincts. On considère $Q \in \mathbb{K}[X]$ un facteur commun de P et P', irréductible.

Puisque $Q \mid \prod_{i=1}^{r} P_i \Longrightarrow \exists i_0 \in [\![1, r]\!]$ tel que $Q = P_{i_0}$.

De plus, $Q \mid P' = \sum_{i=1}^{r} P_i' \prod_{\substack{j=1,\\ j\neq i}}^{r} P_j = \underbrace{\sum_{\substack{i=1,\\ i\neq i_0}}^{r} P_i' \prod_{\substack{j=1,\\ j\neq i}}^{r} P_j}_{Q|} + P_{i_0}' \prod_{\substack{j=1,\\ j\neq i_0}}^{r} P_j$. Par suite, $Q | P_{i_0}' \prod_{\substack{j=1,\\ j\neq i_0}}^{r} P_j$. Or, $Q = P_{i_0} \wedge \prod_{\substack{j=1,\\ j\neq i_0}}^{r} P_j$. Le lemme de Gauss fournit $Q | P_{i_0}'$, *i.e.* $P_{i_0} | P_{i_0}'$, d'où $P_{i_0}' = 0$. Si le corps est de caractéristique nulle, on obtient $P_{i_0} = Q \in \mathbb{K}$, c'est impossible pour un facteur irréductible. Si k est de caractéristique $p > 0$, et le morphisme de Frobénius est un automorphisme, alors, $Q = P_{i_0} = R^p$ pour $R \in \mathbb{K}[X]$. Il n'est donc pas irréductible. ∎

Remarque 3. *La théorème de décomposition de Dunford (i.e. l'existence d'une unique décomposition - avec la méthode classique des projecteurs spectraux) est vraie pour un corps $\mathbb{K}$ quelconque, mais ce procédé algorithmique n'est a priori valable que pour un corps parfait.*

Ainsi, l'hypothèse $\mathbb{K}$ de caractéristique nulle peut être remplacée par $\mathbb{K}$, corps parfait.

2.2 χ_u scindé

L'hypothèse est utilisée pour affirmer que P est scindé, afin d'obtenir le caractère diagonalisable de d. Elle peut néanmoins être relaxée de la manière suivante :

Définition 2

Un endomorphisme $u \in \mathcal{L}(E)$ d'un espace vectoriel de dimension finie E est dit semi-simple si son polynôme minimal est sans facteur carré.

Proposition 3

Soit $\mathbb{K}$ un corps, et E un $\mathbb{K}$-espace vectoriel de dimension finie. Alors, $u \in \mathcal{L}(E)$ est semi-simple *ssi u est diagonalisable dans $\overline{\mathbb{K}}$.*

Démonstration : Si u n'est pas diagonalisable dans $\overline{\mathbb{K}}$, alors π_u n'est pas à racines simples (il est forcément scindé, car le corps $\overline{\mathbb{K}}$ est algébriquement clos). On rappelle que $\pi_{u,\mathbb{K}} = \pi_{u,\overline{\mathbb{K}}}$. Ainsi, π_u a un facteur carré, et u n'est pas semi-simple.
Réciproquement, si u est diagonalisable dans $\overline{\mathbb{K}}$, alors π_u est simplement scindé dans $\overline{\mathbb{K}}$, donc sans facteur carré dans $\overline{\mathbb{K}}$, donc dans $\mathbb{K}$ puique le polynôme minimal ne dépend pas du corps. ■

Remarques.

1. *On a la caractérisation suivante : soit E un $\mathbb{K}$-espace vectoriel de dimension finie et $u \in \mathcal{L}(E)$. Alors, u est semi-simple ssi tout sous-espace vectoriel de E stable par u admet un supplémentaire stable par u.*
2. *On peut aussi définir la notion d'endomorphisme simple : soit E un $\mathbb{K}$-espace vectoriel de dimension finie et $u \in \mathcal{L}(E)$. Alors, u est dit simple si les seuls sous-espaces vectoriels de E stables par u sont $\{0\}$ et E.*
   En effet, si u est simple, écrivons $\chi_u = PQ$. Alors, $\chi_u(u) = P(u) \circ Q(u) = 0$. Donc, $P(u)$ ou $Q(u)$ n'est pas injectif, par exemple $P(u)$. Alors, $\ker(P(u))$ est un sous-espace vectoriel de E, stable par u, et $\ker(u) \neq \{0\}$. Alors, $\ker(P(u)) = E$, donc, $P(u) = 0$, d'où $\pi_u | P$. Or, pour tout $x \neq 0$, $Vect(u^i(x),\ i \in \mathbb{N})$ est un sous espace vectoriel non trivial, stable par u, donc valant E. L'endomorphisme est cyclique, donc, $\chi_u = \pi_u | P$. Par suite, $Q \in \mathbb{K}[X]^\times$, donc χ_u est irréductible.
   Réciproquement, si χ_u est irréductible, alors, pour F sous-espace vectoriel de E, stable par u, $\chi_{u_{|F}} | \chi_u$, donc $\chi_{u_{|F}} = 1$ ou χ_u, donc $F = \{0\}$ ou $F = E$.
3. *Si u est simple, alors χ_u est irreductible, donc $\chi = \pi_u$, donc u est cyclique.*

Dans le théorème, on peut alors supprimer l'hypothèse : u a son polynôme caractéristique scindé. On peut alors effectuer la même preuve avec $P = P_1 \cdots P_r$, où la décomposition en produit de facteurs irréductibles est la suivante : $\pi_u = P_1^{\alpha_1} \cdots P_r^{\alpha_r}$. On obtiendra à la fin $P(u_{n_0}) = 0$, donc, $\pi_{u_{n_0}} | P$, donc est facteur carré. Alors, u_{n_0} est semi-simple.

2.3 Généralisation

Le théorème de Dunford admet la généralisation suivante :

Theorème 2 (*Dunford généralisé*)

Soient $\mathbb{K}$ un corps parfait et E un $\mathbb{K}$-espace vectoriel de dimension finie. Soit $u \in \mathcal{L}(E)$ inversible. Alors, il existe une unique décomposition $u = s \circ n$, où s est un endomorphisme semi-simple inversible, et n un endomorphisme unipotent. De plus, $(s, n) \in \mathbb{K}[u]^2$, $s \circ n = n \circ s$.

Démonstration : On écrit la décomposition de Dunford "classique" de u, $u = d + \tilde{n}$. Alors, on obtient $u = d \circ (I_d + d^{-1} \circ \tilde{n})$. On pose $s = d$ et $n = I_d + d^{-1} \circ \tilde{n}$. On a : s est diagonalisable, donc semi-simple, $s \in \mathbb{K}[u]$. Pour n, on a $n - I_d = d^{-1} \circ \tilde{n}$, est nilpotent par propriété de commutation, donc n est unipotent. On a aussi $n \in \mathbb{K}[u]$. Enfin, $s = u - n$ est inversible comme la somme d'un inversible et d'un nilpotent. Pour l'unicité : on remarque que si $u = s \circ n$, alors, $d = s$ et $\tilde{n} = d \circ (n - I_d)$ est l'unique décomposition de Dunford "classique" de u. Ainsi, on obtient l'unicité. ■

3 Applications

3.1 Exponentielles

Proposition 4

Soit $u \in \mathcal{L}(E)$ un endomorphisme de E, un $\mathbb{C}$-espace vectoriel de dimension finie. Alors, la décomposition de Dunford de e^u est $e^u = e^d + e^d \circ (e^n - I_d)$.

Démonstration : On note $u = d + n$. Alors, e^d est un endomorphisme diagonalisable. Puisque $e^d \in \mathbb{K}[d]$, $e^d \in \mathbb{K}[u]$. De même $e^d \circ (e^n - I_d) \in \mathbb{K}[u]$. De plus,

$$e^d - I_d = \sum_{k=0}^{m} \frac{n^k}{k!} - I_d = n \circ \left(\sum_{k=1}^{m} \frac{n^{k-1}}{k!} \right) \in n\mathbb{K}[n]$$

est nilpotent. Ceci conclut. ∎

Proposition 5

Soit $u \in \mathcal{L}(E)$ un endomorphisme de E, un $\mathbb{C}$-espace vectoriel de dimension finie. Alors, u est diagonalisable ssi e^d est diagonalisable.

Démonstration : Le sens direct est connu. Réciproquement : on a, $e^u = e^d + e^d \circ (e^n - I_d)$ Par hypothèse, $e^d \circ (e^n - I_d) = 0$, donc, $e^n = I_d$. Si q désigne l'indice de nilpotence de n, alors : $\sum_{k=1}^{q-1} \frac{n^k}{k!} = 0$. Donc, $P(n) = 0$, où $P = \sum_{k=1}^{q-1} \frac{X^k}{k!}$. Or, $\pi_n = X^q$. Donc, $X^q | P$. Nécessairement, $q = 1$, donc $n = 0$. Ainsi, u est diagonalisable. ∎

Proposition 6

$\forall A \in \mathcal{M}_n(\mathbb{C})$, $e^A = I_n$ ssi $\sigma(A) \subset 2i\pi\mathbb{Z}$ et A et diagonalisable

Démonstration : Si $e^A = I_n$, alors e^A est diagonalisable, donc A est diagonalisable, par la proposition précédente. On note $A = PDP^{-1}$, où $D =$Diag$(\lambda_1, \cdots, \lambda_n)$. Ainsi, $e^A = P\text{Diag}(e^{\lambda_1}, \cdots, e^{\lambda_n})P^{-1}$. Alors,

$$e^A = I_n \Leftrightarrow \text{Diag}(e^{\lambda_1}, \cdots, e^{\lambda_n}) = I_n \Leftrightarrow \forall i \in [\![, n]\!], \ \lambda_i \in 2i\pi\mathbb{Z} \Leftrightarrow \sigma(A) \subset 2i\pi\mathbb{Z}.$$

La réciproque est évidente. ∎

3.2 Équations différentielles

Theorème 3

Soient $\delta > 0$ et $A \in \mathcal{M}_n(\mathbb{C})$ telle que $\sigma(A) \subset \{z \in \mathbb{C}, \ Re(z) \leq -2\delta\}$. Alors, il existe $C > 0$ telle que :

$$\forall t \in \mathbb{R}^+, \ \ |||e^{tA}||| \leq Ce^{-\sigma t}.$$

Démonstration : On note $A = D + N$, la décomposition de Dunford de A. Soit $m \in \mathbb{N}^*$ l'indice de nilpotence de N. Alors, pour tout réel t,

$$e^{tA} = e^{tD} \sum_{k=0}^{m-1} \frac{N^k t^k}{k!}.$$

On note $D =$Diag$(\lambda_1, \cdots, \lambda_n)$, où $\sigma(A) = \{\lambda_1, \cdots, \lambda_n\}$. Ainsi, pour tout réel positif, t,

$$|||e^{tA}||| \leq |||e^{tD}||| \sum_{k=0}^{m-1} \frac{|||N^k|||}{k!} |t|^k \lesssim e^{-\delta t} \left(\underbrace{\sum_{k=0}^{m-1} \frac{|||N^k|||}{k!} |t|^k}_{:=P(t)} e^{-\delta t} \right).$$

Par croissance comparée, puique $\delta > 0$, $\lim_{t \to +\infty} P(t)e^{-\delta t} = 0$, donc la fonction continue est bornée. On obtient ainsi la conclusion souhaitée. ∎

Remarque 4. *Ce lemme est utile afin d'étudier la stabilité asymptotique des points d'équilibre des équations différentielles linéaires à coefficients constants. Il intervient également dans la démonstration du théorème de linéarisation en première approche de Lyapounov.*