DM 16 - Décomposition de Frobenius

1 Sous-espaces cycliques

1. (a) La famille $\left(x, u(x), \dots, u^n(x)\right)$ est une famille de $n+1$ vecteurs dans un espace vectoriel de dimension n. Elle est donc liée.

   On en déduit que si $k > n$, la famille $(x, (u)x, \dots, u^{k-1}(x))$ n'est pas libre. Donc l'ensemble des $k \in \mathbb{N}^*$ tel que $(x, u(x), \dots, u^{k-1}(x))$ est majoré. Il est de plus non vide puisque 1 est un tel entier (la famille (x) est libre car $x \neq 0$). Donc n_x est bien défini.

   (b) Par définition de n_x, la famille $(x, u(x), \dots, u^{n_x-1}(x))$ est libre, mais celle obtenue en lui rajoutant $u^{n_x}(x)$ ne l'est pas. On en déduit que $u^{n_x}(x) \in \mathrm{Vect}(x, u(x), \dots, u^{n_x-1}(x))$, d'où l'existence des a_i.

   (c) On le montre par récurrence sur $k \geq n_x$. L'initialisation a été établie à la question précédente. Soit $k \geq n_x$ tel que $u^k(x) \in \mathrm{Vect}(x, u(x), \dots, u^{n_x-1}(x))$. Alors $u^{k+1}(x) = u(u^k(x)) \in \mathrm{Vect}(u(x), \dots, u^{n_x}(x))$.

   Or, tous les vecteurs $u^i(x)$, pour $i \in [\![1, n_x-1]\!]$ sont dans $\mathrm{Vect}(x, u(x), \dots, u^{n_x-1}(x))$. Et $u_{n_x}(x)$ aussi (c'est la question précédente). Donc, $u^{k+1}(x)$ est aussi élément de $\mathrm{Vect}(x, u(x), \dots, u^{n_x-1}(x))$.

   Ceci conclut la récurrence et la question.

2. (a) La famille $(x, u(x), \dots, u^{n_x-1}(x))$ est libre par hypothèse et est composée de n_x vecteurs. Donc $\dim E_x = n_x$.

   (b) Notons déjà que les éléments de $\mathrm{Vect}(\{u^k(x), k \in \mathbb{N}\})$ sont de la forme $\sum_{k=0}^{d} a_k u^k(x)$, avec $d \in \mathbb{N}$ et les $a_k \in \mathbb{K}$. En notant $P = \sum_{k=0}^{d} a_k X^k$, on a $\sum_{k=0}^{d} a_k u^k(x) = P(u)(x)$, de sorte que les deux ensembles $\mathrm{Vect}(\{u^k(x), k \in \mathbb{N}\})$ et $\{P(u)(x), P \in \mathbb{K}[X]\}$ sont égaux.

   Par définition, $E_x = \mathrm{Vect}(\{u^k(x), k \in [\![0, n_x-1]\!]\})$. Ainsi l'inclusion $E_x \subset \mathrm{Vect}(\{u^k(x), k \in \mathbb{N}\})$ est claire. L'inclusion réciproque a été établie à la question 1.(c).

   (c) Soit $y \in E_x$. D'après la question précédente, on peut trouver $P \in \mathbb{K}[X]$ tel que $y = P(u)(x)$. Alors, $u(y) = u \circ P(u)(x) = (XP)(u)(x)$. Comme $XP \in \mathbb{K}[X]$, on a $u(y) \in E_x$.

3. **L'exemple des projecteurs.**

   (a) Si u est un projecteur de E, on a $u^2 = u$, et donc $u^k = u$, pour tout $k \geq 2$. On en déduit que $E_x = \mathrm{Vect}(x, u(x))$ dans ce cas.

   (b) D'après la question précédente, E_x est engendré par x et $u(x)$. Il est donc au plus de dimension 2, avec égalité ssi $(x, u(x))$ est libre.

   Supposons que cette famille n'est pas libre. Alors, il existe $\lambda \in \mathbb{K}$ tel que $u(x) = \lambda x$ (car $x \neq 0$). En appliquant u et en utilisant $u^2 = u$, on en déduit $u(x) = \lambda u(x) = \lambda^2 x$. Donc (comme $x \neq 0$), $\lambda = \lambda^2$. Ainsi, $\lambda = 0$ ou $\lambda = 1$.

Le cas $\lambda = 0$ correspondant à $x \in \operatorname{Ker} u$; le cas $\lambda = 1$ à $x \in \operatorname{Im} u$. Ainsi : $\dim E_x = 1 \iff x \in \operatorname{Ker} u \cup \operatorname{Im} u$ et $\dim E_x = 2$ sinon.

4. On note $P = \sum_{k=0}^{n_x-1} a_k X^k$, de sorte que la relation de 1.(b) se réécrit $u^{n_x}(x) = P(u)(x)$.

   Soit $y \in E_x$. On peut trouver $Q \in \mathbb{K}[X]$ tel que $y = Q(u)(x)$. Alors,

$$\begin{aligned} u^{n_x}(y) &= u^{n_x}(Q(u)(x)) \\ &= (X^{n_x}Q)(u)(x) \\ &= (QX^{n_x})(u)(x) \\ &= Q(u)(u^{n_x}(x)) \\ &= Q(u)(P(u)(x)) \\ &= P(u)(Q(u)(x)) \\ &= P(u)(y). \end{aligned}$$

   A la fin, on utilise de nouveau que $Q(u) \circ P(u) = P(u) \circ Q(u)$, les deux étant égaux à $(PQ)(u)$.

2 Vecteur u-maximum

5. Soit $x \in \operatorname{Ker}(P(u))$. Alors,

$$P(u)(u(x)) = (PX)(u)(x) = (XP)(u)(x) = u(P(u)(x)) = u(0) = 0.$$

   Donc, $u(x) \in \operatorname{Ker}(P(u))$. Donc, $\operatorname{Ker}(P(u))$ est stable par u.

6. **Polynôme minimal**

   (a) La famille $(u^m)_{m\in\mathbb{N}}$ est liée car c'est une famille infinie dans l'espace vectoriel $\mathscr{L}(E)$, de dimension n^2. On peut donc trouver un entier $m \in \mathbb{N}^*$ tel que $u^m \in \operatorname{Vect}(u^k, k \in [\![0, m-1]\!])$.

   Il existe donc $b_0, \dots, b_{m-1}$ tels que $u^m = \sum_{i=0}^{m-1} b_i u^i$. En notant $P = X^m - \sum_{i=0}^{m-1} b_i X^i$, on a donc $P(u) = 0$.

   (b) On utilise la structure des idéaux de $\mathbb{K}[X]$ (*si on veut s'en passer, on adapte la preuve dans ce cas, en utilisant une division euclidienne*). Notons $\mathscr{I} = \{P \in \mathbb{K}[X] \mid P(u) = 0\}$. Montrons que $\mathscr{I}$ est un idéal de $\mathbb{K}[X]$.

   - $0 \in \mathscr{I}$. Si $P, Q \in \mathscr{I}$, alors $(P - Q)(u) = P(u) - Q(u) = 0$, donc $P - Q \in \mathscr{I}$. Ainsi, $\mathscr{I}$ est un sous-groupe additif de $\mathbb{K}[X]$.
   - Soient $P \in \mathscr{I}$ et $Q \in \mathbb{K}[X]$. Alors, $(PQ)(u) = (QP)(u) = Q(u) \circ P(u) = 0$ car $P(u) = 0$.

   Comme $\mathscr{I}$ est un idéal de $\mathbb{K}[X]$ et que $\mathbb{K}[X]$ est principal, on en déduit qu'il existe $A \in \mathbb{K}[X]$ tel que $\mathscr{I} = A\mathbb{K}[X]$. Ce polynôme A n'est pas nul car $\mathscr{I} \neq \{0\}$, d'après la question précédente. En divisant A par son coefficient dominant, on obtient un polynôme unitaire Π_u tel que $\mathscr{I} = \Pi_u\mathbb{K}[X]$.

   Ce polynôme est unitaire car si deux polynômes conviennent, chacun divise l'autre. Ils sont alors associés, donc égaux car tous deux unitaires.

(c) Dire que $u^p = 0$ revient à dire que $X^p \in \mathscr{I}$, avec la notation introduite dans la question précédente. Donc, Π_u divise X^p. Comme Π_u est unitaire, il est donc de la forme X^k, pour un $k \in [\![0, p-1]\!]$. Mais comme $u^{p-1} \neq 0$, Π_u ne divise pas X^{p-1}. On a donc en fait $\Pi_u = X^p$.

7. **Lemme des noyaux**.

(a) Comme P et Q sont premiers entre eux, on peut trouver par le théorème de Bézout $U, V \in \mathbb{K}[X]$ tels que $UP + VQ = 1$. On en déduit que

$$U(u) \circ P(u) + V(u) \circ Q(u) = \mathrm{id}_E.$$

On applique à x et on trouve :

$$U(u)(P(u)(x)) + V(u)(Q(u)(x)) = x.$$

Notons $z = U(u)(P(u)(x)) = (UP)(u)(x)$ et $y = (VQ)(u)(x)$. On a $P(y) = (PVQ)(u)(x) = V(u)((PQ)(x)) = 0$ car $x \in \operatorname{Ker} P(u)$. Donc, $y \in \operatorname{Ker} P$. De même, $z \in \operatorname{Ker} Q$. Ainsi,

$$\operatorname{Ker}(PQ)(u) = \operatorname{Ker} P(u) + \operatorname{Ker} Q(u).$$

Montrons maintenant que la somme est directe. Soit $x \in \operatorname{Ker} P(u) \cap \operatorname{Ker} Q(u)$. On a $P(u)(x) = Q(u)(x) = 0$ et donc, d'après la relation donnée plus haut,

$$x = U(u)(P(u)(x)) + V(u)(Q(u)(x)) = 0.$$

D'où, $\operatorname{Ker}(PQ)(u) = \operatorname{Ker} P(u) \bigoplus \operatorname{Ker} Q(u)$.

(b) On procède par récurrence sur $k \in [\![1, r]\!]$. Le cas $k = 1$ est trivial et le cas $k = 2$ vient d'être traité. Soit $k \in [\![1, r-1]\!]$ tel que $\operatorname{Ker}((P_1 \dots P_k)(u)) = \bigoplus_{i=1}^{k} \operatorname{Ker} P_i(u)$.

Alors, P_{k+1} est premier avec chaque P_i (pour $i \leq k$) donc il est premier avec leur produit $P_1 \dots P_k$. Par la question précédente, on a donc

$$\operatorname{Ker}((P_1 \dots P_k P_{k+1})(u)) = \operatorname{Ker}((P_1 \dots P_k)(u)) \bigoplus \operatorname{Ker}(P_{k+1}(u)).$$

En utilisant l'hypothèse de récurrence, on a donc :

$$\operatorname{Ker}((P_1 \dots P_{k+1})(u)) = \left(\bigoplus_{i=1}^{k} \operatorname{Ker} P_i(u)\right) \bigoplus \operatorname{Ker} P_{k+1}(u) = \bigoplus_{i=1}^{k+1} \operatorname{Ker} P_i(u).$$

On utilise implicitement une propriété d'associativité des sommes directes : si $E_1, \dots, E_n$ sont en somme directe et si E_{n+1} est en somme directe avec $\bigoplus_{i=1}^{n} E_i$, alors $E_1, \dots, E_{n+1}$ sont en somme directe. Le démontrer si ce n'est pas clair.

8. Notons $E_i = \operatorname{Ker} P_i^{m_i}(u)$. Le lemme des noyaux donne (les P_i sont irréductibles et deux à deux non associés donc deux à deux premiers entre eux) :

$$\operatorname{Ker} \Pi_u(u) = \bigoplus_{i=1}^{r} E_i.$$

Or, par définition $\Pi_u(u) = 0$, de sorte que $\operatorname{Ker}\Pi_u(u) = E$. Chaque E_i est stable par u, par la question 5.

Il reste à montrer que chaque E_i est distinct de $\{0\}$. Si ce n'était pas le cas, on aurait un des E_i égal à $\{0\}$, disons E_1. Alors,

$$E = \bigoplus_{i=2}^{r} E_i.$$

En appliquant de nouveau le lemme des noyaux, on aurait donc $E = \operatorname{Ker} Q(u)$, où $Q = \prod_{i=2}^{r} P_i^{m_i}$. Ceci revient à dire que $Q(u) = 0$. Comme $\deg Q < \deg \Pi_u$, on obtient une contradiction avec la définition de Π_u.

Donc chaque E_i est non réduit à $\{0\}$.

9. **Polynôme minimal ponctuel.**

   (a) On procède comme à la question 6.(b) en montrant que $\mathscr{I}_x$ est un idéal de $\mathbb{K}[X]$.

   (b) Avec les notations introduites, on a $Q = X^{n_x} - \sum_{i=0}^{n_x-1} a_i X^i \in \mathscr{I}_x$. De plus, la famille $(x, u(x), \dots, u_{n_x-1})$ est libre, ce qui revient à dire qu'aucun polynôme non nul de $\mathbb{K}[X]$ de degré strictement inférieur à n_x n'est dans $\mathscr{I}_x$. Ainsi, $\Pi_{u,x}$ divise Q et ces deux polynômes sont unitaires et ont même degré n_x. Ils sont donc égaux : $\Pi_{u,x} = X^{n_x} - \sum_{i=0}^{n_x-1} a_i X^i \in \mathscr{I}_x$.

   (c) Si $P \in \mathbb{K}[X]$ est tel que $P(u) = 0$, alors en particulier $P(u)(x) = 0$ et donc $P \in \mathscr{I}_x$. On a donc $\Pi_u\mathbb{K}[X] \subset \Pi_{u,x}\mathbb{K}[X]$.
   En particulier $\Pi_u \in \Pi_{u,x}\mathbb{K}[X]$, ce qui revient à dire que $\Pi_{u,x}$ divise Π_u.

10. (a) Soit $i \in [\![1, n]\!]$. D'après la question précédente, Π_{u,e_i} divise Π_u. Comme $\Pi_u = P^m$ et que P est irréductible, les seuls diviseurs unitaires de Π_u sont de la forme P^k, avec $k \in [\![0, m]\!]$. Il existe donc $m_i \in [\![1, m]\!]$ tel que $\Pi_{u,e_i} = P^{m_i}$. (m_i n'est pas égal à 0 car sinon on aurait $\mathrm{Id}_E(e_i) = 0$, c'est-à-dire $e_i = 0$, mais e_i est non nul car c'est un élément d'une base de E)

    (b) Notons $m_\infty = \max(m_1, \dots, m_n)$. On a donc $m_\infty \leq m$ et pour tout $i \in [\![1, n]\!]$, $\Pi_{u,e_i} \mid P^{m_\infty}$. Soit $x \in E$. On peut écrire $x = \sum_{k=1}^{n} x_k e_k$. Donc $P^{m_\infty}(u)(x) = \sum_{k=1}^{n} x_k P^{m_\infty}(u)(e_k) = 0$. Comme x est quelconque, on en déduit que $P^{m_\infty}(u) = 0$, donc que $\Pi_u \mid P^{m_\infty}$. Ceci impose que $m_\infty = m$. Il existe donc un $i \in [\![1, n]\!]$ tel que $\Pi_{u,e_i} = \Pi_u$.

11. On pose $E_i = \operatorname{Ker}(P_i^{m_i}(u))$ pour tout $i \in [\![1, r]\!]$. Par la question 8 (et sa preuve), on a

$$E = \bigoplus_{i=1}^{r} E_i.$$

De plus, chaque E_i est stable par u. Notons $u_i : E_i \to E_i, x \mapsto u(x)$, l'application u restreinte et co-restreinte à E_i.

Par définition, tout $x \in E_i$ vérifie $P_i^{m_i}(u)(x) = 0$. Ceci montre que Π_{u_i} divise $P_i^{m_i}$ et donc Π_{u_i} est de la forme $P_i^{s_i}$, avec $s_i \leq m_i$. Si x est quelconque dans E, on peut alors écrire $x = \sum_{k=1}^{r} x_k e_k$.

Alors, par linéarité, on obtient que $(\prod_{k=1}^{r} P_i^{s_i})(u)$ annule x. Comme c'est vrai pour tout x, Π_u divise $\prod_{k=1}^{r} P_i^{s_i}$. Nécessairement, on a donc pour tout $i \in [\![1, r]\!]$, $s_i = m_i$.

Revenons à un endomorphisme u_i. Il vérifie donc $\Pi_{u_i} = P_i^{m_i}$. En application de la question précédente, on peut trouver $x_i \in E_i - \{0\}$ tel que $\Pi_{u_i,x_i} = P_i^{m_i}$. On choisit un tel x_i pour tout $i \in [\![1, n]\!]$ et on pose $x = \sum_{i=1}^{r} x_i$.

On veut montrer que $\Pi_{u,x} = \Pi_u = P_1^{m_1} \dots P_r^{m_r}$. On sait déjà que $\Pi_{u,x}$ divise Π_u ; il existe donc $t_1, \dots, t_r$ tels que $\Pi_{u,x} = P_1^{t_1} \dots P_r^{t_r}$, avec $t_i \leq m_i$. De plus,

$$0 = \Pi_{u,x}(u)(x) = \sum_{i=1}^{r} \Pi_{u,x}(u)(x_i)$$

par linéarité. Comme chaque E_i est stable par u, on a aussi $\Pi_{u,x}(u)(x_i) \in E_i$. Comme la somme des E_i est directe, on en déduit que pour tout $i \in [\![1, r]\!]$, $\Pi_{u,x}(u)(x_i) = 0$. Cette égalité ayant lieu dans E_i, on peut la réécrire $\Pi_{u,x}(u_i)(x_i) = 0$. Par définition de Π_{u_i,x_i}, on a donc $\Pi_{u_i,x_i} \mid \Pi_{u,x}$. Or, $\Pi_{u_i,x_i} = P_i^{m_i}$. Ainsi, $\Pi_{u,x}$ est divisible par $P_i^{m_i}$, pour tout $i \in [\![1, r]\!]$. On a donc $\Pi_{u,x} = \prod_{i=1}^{r} P_i^{m_i} = \Pi_u$. Ce qui conclut.

3 Décomposition de Frobenius

12. Comme $p = \deg \Pi_{u,x}$, on sait que la famille $(x, u(x), \dots, u^{p-1}(x))$ est libre. On peut la compléter par des vecteurs $v_1, \dots, v_s$ en une base de E. On définit alors une unique forme linéaire ϕ en décidant que :

$$\forall i \in [\![0, p-2]\!], \phi(u^i(x)) = 0,\ \phi(u^{p-1}(x)) = 1 \text{ et} \forall k \in [\![1, s]\!], \phi(v_k) = 0.$$

Cette forme linéaire ϕ convient par construction.

13. Montrons que $E_x \cap F = \{0\}$. Soit $y \in E_x \cap F$. On peut écrire $y = \sum_{k=0}^{p-1} a_k u^k(x)$. En appliquant la forme linéaire ϕ, on a

$$0 = \phi(y) = \sum_{k=0}^{p-1} a_k \phi(u^k(x)) = a_{p-1}.$$

En effet, $\phi(y) = 0$ car $y \in F$. Ainsi, $a_{p-1} = 0$ et $y = \sum_{k=0}^{p-2} a_k u^k(x)$. On applique maintenant $\phi \circ u$ et, par un calcul analogue, on obtient $a_{p-2} = 0$. On continue de proche en proche, en appliquant successivement $\phi \circ u^i$, pour $i \in [\![0, p-1]\!]$ et on obtient (par récurrence finie) que tous les a_i sont nuls. Donc $y = 0$ et $E_x \cap F = \{0\}$.

Montrons maintenant que les formes linéaires $\phi \circ ui$, pour $i \in [\![0, p-1]\!]$ forment une famille libre. Soient $\lambda_0, \dots, \lambda_{p-1} \in \mathbb{K}$ tels que $\sum_{i=0}^{p-1} \lambda_i \phi \circ u^i = 0$.

En appliquant x, l'égalité se simplifie en $\lambda_{p-1} = 0$. Puis on applique en $u(x)$, pour trouver $\lambda_{p-2} = 0$, etc. Par récurrence finie immédiate, on trouve que tous les λ_i sont nuls, ce qui conclut ce point.

Par une propriété du cours (*qu'il faudrait redémontrer à un écrit, car hors-programme*), $F = \bigcap_{i=0}^{p-1} \mathrm{Ker}(\phi \circ u^i)$ est donc de dimension $\dim E - p$. Comme E_x est de dimension p et qu'on a déjà montré que $E_x \cap F = \{0\}$, on a finalement $E = E_x \bigoplus F$.

Addendum. Il n'y a en fait pas besoin de montrer que les formes linéaires $\phi \circ u_i$ forment une famille libre. On a montré que $E_x \cap F$ sont en somme directe. De plus, $\dim E_x = n_x$ et $\dim F \geq \dim E - n_x$ (car F est l'intersection de n_x noyaux de formes linéaires). La formule de Grassmann donne alors $\dim(E_x + F) \geq \dim E$ et donc l'égalité $E_x + F = E$.

14. Soit $y \in F$, soit $i \in [\![0, p-1]\!]$. On veut montrer que $u(y) \in \mathrm{Ker}(\phi \circ u^i)$, c'est-à-dire que $y \in \mathrm{Ker}(\phi \circ u^{i+1})$. Si $i \leq p-2$, c'est clair, par définition de F. Reste donc à démontrer que $y \in \mathrm{Ker}(\phi \circ u^p)$.

    Comme x est u-maximal, on a $\Pi_{u,x} = \Pi_u$. Donc Π_u est de degré p et u^p est combinaison linéaire des u_i pour $i \leq p-1$. En particulier, on peut trouver $\mu_0, \ldots, \mu_{p-1}$ tels que $u^p(y) = \sum_{k=0}^{p-1} \mu_k u^k(y)$. Donc, $\phi(u^p(y)) = \sum_{k=0}^{p-1} \mu_k \phi(u^k(y)) = 0$.
    Donc, F est stable par u.

15. Résumons la situation. Étant donnés un espace vectoriel E de dimension finie et $u \in \mathscr{L}(E)$, on a montré qu'il existe x_1 un vecteur u-maximal et F_1 un supplémentaire de E_{x_1}, qui est u-stable. On a $\Pi_{u,x_1} = \Pi_u$. De plus, en notant u_{F_1} l'endomorphisme induit par u sur F_1, on a $\Pi_{u_{F_1}} \mid \Pi_u$.

    On peut alors recommencer, avec l'endomorphisme u_{F_1} sur F_1. Il existe un vecteur $x_2 \in F_1$ tel que $\Pi_{u,x_2} = \Pi_{u_{F_1},x_2} = \pi_{u_{F_1}}$, donc $\Pi_{u,x_2} \mid \Pi_{u,x_1}$. De plus, on peut définir un supplémentaire F_2 de E_{x_2} dans F_1, etc. On continue jusqu'à arriver à un x_i tel que $E_{x_i} = F_{i-1}$ (ce qui arrive un moment puisque la dimension de F_i décroit strictement à chaque étape).

Une démonstration plus formelle peut être écrite par récurrence sur la dimension de E.