Algèbre linéaire et réduction

1 Préliminaires sur les endomorphismes nilpotents

1. Par définition du minimum, on sait que $u^{p-1} \neq 0$, donc :
$$\boxed{\text{Il existe } x_0 \in E \text{ tel que } u^{p-1}(x_0) \neq 0.}$$
2. Fait moins de 100 fois mais déjà plus de 5... On part d'une combinaison linéaire nulle :
$$\lambda_0 x_0 + \lambda_1 u(x_0) + \cdots + \lambda_{p-1} u^{p-1}(x_0) = 0$$
et il s'agit de montrer que tous les λ_k sont nuls. On peut appliquer u^{p-1} pour montrer que $\lambda_0 = 0$ puis lancer une récurrence avec prédécesseurs... ou bien plus directement supposer qu'il existe un k tel que $\lambda_k \neq 0$. En prenant k_0 le plus petit de ces entiers k et en appliquant u^{p-1-k_0} à la combinaison linéaire initiale on obtient $\lambda_{k_0} = 0$, fournissant une absurdité. Ainsi tous les λ_k sont nuls, et donc :
$$\boxed{\text{La famille } \left(x_0, u(x_0), ..., u^{p-1}(x_0)\right) \text{ est libre.}}$$
3. En dimension n, les familles libres ont un cardinal majoré par n, donc d'après la question précédente :
$$\boxed{p \leqslant n, \text{ puis } u^n = u^p \circ u^{\overbrace{n-p}^{\geqslant 0}} = 0.}$$
4. « On sait » qu'un endomorphisme nilpotent est trigonalisable, avec plus précisément des zéros sur la diagonale de la matrice dans une base adaptée ; on en déduit :
$$\boxed{\chi_u = X^n}$$
Autre point de vue : on se place sur $\mathbb{C}$. On considère la matrice M de u dans n'importe quelle base de E : le polynôme caractéristique de u est celui de M, qu'on peut voir comme une matrice complexe. Or la seule valeur propre possible de M est 0 (si $MX = \lambda X$ alors $M^p X = \lambda^p X = 0$...) donc $\mathrm{Sp}(M) = \{0\}$ donc $\chi_M = X^n$.

   Si u était diagonalisable, alors E serait égal à la somme de ses sous-espaces propres ; or il existe un seul sous-espace propre qui est $\mathrm{Ker}\,(u - 0\mathrm{Id}_E) = \mathrm{Ker}\,(u) \neq E$ car $u \neq 0$. Ainsi :
$$\boxed{u \text{ n'est pas diagonalisable.}}$$

2 Étude d'équations du type $X^2 = A$ avec $A \in \mathcal{M}_n(\mathbb{R})$

2.1 Un exemple

1. On calcule χ_A en développant par rapport à la dernière ligne, pour trouver :
$$\boxed{\chi_A = (X-1)(X-2)(X-3) \text{ donc } \mathrm{Sp}(u) = \mathrm{Sp}(A) = \{1, 2, 3\} \text{ et } A \text{ est diagonalisable.}}$$
Au choix : polynôme caractéristique scindé à racines simples ; ou bien trois valeurs propres distinctes en dimension 3, ou bien en revenant à la preuve : il y a trois sous-espaces propres dont les dimensions sont au moins égales à 1, donc la dimension de la somme **directe** *vaut au moins 3...*
2. Chacun des sous-espaces propres est de dimension 1 d'après ce qui précède (toujours cette histoire de la dimension d'une somme directe...). Il suffit donc de trouver un vecteur propre pour chaque valeur propre. Or en notant $\mathcal{E} = (e_1, e_2, e_3)$ la base canonique de $\mathbb{R}^3$:

(a) La matrice de $v = u - \mathrm{Id}$ dans $\mathcal{E}$ est $\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ donc $v(e_1) = v(e_2)$ donc $e_1 - e_2$ appartient à $\mathrm{Ker}\,(u - \mathrm{Id}_E)$ donc le dirige (dimension). Pour respecter la condition sur la deuxième condition, on prend donc $f_1 = -e_1 + e_2$.

(b) De même $A - 2I_3 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$ donc en notant $w = u - 2\mathrm{Id}$ on a $w(e_1) + w(e_2) = w(e_3)$, et on peut donc prendre $f_2 = e_1 + e_2 - e_3$.

(c) Enfin $A - 3I_3 = \begin{pmatrix} -1 & 1 & 1 \\ 1 & -1 & 1 \\ 0 & 0 & -1 \end{pmatrix}$ donc on peut prendre pour les mêmes raisons : $f_3 = e_1 + e_2$

On note enfin qu'il y a bien unicité des f_i, les sous-espaces propres étant des droites, et au regard de la contrainte sur la deuxième composant.

$$\boxed{f_1 = \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix},\ f_2 = \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix} \text{ et } f_3 = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}}$$

3. Plutôt que la liberté, on va s'intéresser au caractère générateur en vérifiant que le rang de $\mathcal{F}$ vaut 3 :

$$\mathrm{rg}\begin{pmatrix} -1 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & -1 & 0 \end{pmatrix} = \mathrm{rg}\begin{pmatrix} -1 & 1 & 1 \\ 0 & 2 & 2 \\ 0 & -1 & 0 \end{pmatrix} = \mathrm{rg}\begin{pmatrix} -1 & 1 & 1 \\ 0 & 2 & 2 \\ 0 & 0 & 2 \end{pmatrix} = 3$$

Ainsi, $\mathcal{F}$ est génératrice et de cardinal 3, donc :

$$\boxed{\mathcal{F} \text{ est une base de } \mathbb{R}^3}$$

Puisque $u(f_i) = \lambda_i f_i$, la matrice de u dans $\mathcal{F}$ est simple :

$$\boxed{\mathrm{Mat}(u, \mathcal{F}) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}}$$

En prenant P la matrice de passage de $\mathcal{E}$ vers $\mathcal{F}$ on peut appliquer la formule de changement de base :

$$\boxed{\text{En prenant } P = \begin{pmatrix} -1 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & -1 & 0 \end{pmatrix} \text{ on a } P^{-1}AP = D}$$

C'est à ce moment que vous devez convaincre le correcteur que vous savez de quelle matrice de passage on parle !

4. (a) Les matrices de v^2 et u dans la base canonique $\mathcal{E}$ sont respectivement B^2 et A, donc sont égales, donc (injectivité de $w \mapsto \mathrm{Mat}(w, \mathcal{E})$) :

$$\boxed{v^2 = u}$$

De même, les matrices de $v \circ u$ et $u \circ v$ dans $\mathcal{E}$ sont respectivement $BA = B.B^2 = B^3$ et $AB = B^2.B = B^3$ donc :

$$\boxed{v \circ u = u \circ v}$$

(b) Soit $i \in \{1, 2, 3\}$. On a $(u \circ v)(f_i) = (v \circ u)(f_i)$, donc $u\,(v(f_i)) = v\,(u(f_i)) = v(\lambda_i f_i) = \lambda_i v(f_i)$ donc $v(f_i)$ appartient à $\mathrm{Ker}\,(u - \lambda_i \mathrm{Id})$, qui est une droite engendrée par f_i, et ainsi :

$$\boxed{\text{Pour tout } i \in \{1, 2, 3\},\ v(f_i) \text{ est colinéaire à } f_i.}$$

(c) D'après ce qui précède, V est de la forme $\mathrm{Diag}(\alpha_1, \alpha_2, \alpha_3)$. Mais la relation $v^2 = u$ vue dans la base $\mathcal{F}$ nous dit que $\mathrm{Diag}(\alpha_1, \alpha_2, \alpha_3)^2 = \mathrm{Diag}(1, 2, 3)$ donc $\alpha_1^2 = 1$, $\alpha_2^2 = 2$ et $\alpha_3^2 = 3$. Ainsi :

$$\boxed{\text{La matrice } V \text{ de } v \text{ dans la base } \mathcal{F} \text{ vaut } \mathrm{Diag}(\pm 1, \pm\sqrt{2}, \pm\sqrt{3})}$$

Ce qui conclut l'analyse puisque la formule de changement de base pour v nous dit que B (qui est la matrice qu'on cherche) vaut PVP^{-1} : on a confiné les éventuelles solutions dans un ensemble assez restreint.

5. Dans la partie précédente on a montré que si $X^2 = A$, alors X est de la forme $P\mathrm{Diag}(\pm 1, \pm\sqrt{2}, \pm\sqrt{3})P^{-1}$. Mais réciproquement si X est de cette forme, alors

$$X^2 = P\mathrm{Diag}(\pm 1, \pm\sqrt{2}, \pm\sqrt{3})^2 P^{-1} = P\mathrm{Diag}(1, 2, 3)P^{-1} = PDP^{-1} = A$$

Tous les admissibles sont admis !

$\boxed{\text{L'équation } X^2 = A \text{ possède 8 solutions qui sont les matrices } P\mathrm{Diag}(\pm 1, \pm\sqrt{2}, \pm\sqrt{3})P^{-1}}$

Vous sauriez convaincre un sceptique que ces huit matrices sont distinctes ?

2.2 Quelques résultats généraux

1. (a) On a directement :

$$\boxed{v^{2p} = (v^2)^p = u^p = 0 \text{ et } v^{2(p-1)} = (v^2)^{p-1} = u^{p-1} \neq 0}$$

La première relation nous dit que v est nilpotent. Mais la seconde nous dit que l'indice de nilpotence est strictement plus grand que $2(p-1)$. Or cet indice est majoré par n d'après la question 3 des préliminaires. On a donc $2(p-1) < n$ donc (puisqu'il s'agit d'entiers) $2(p-1) \leqslant n-1$ soit encore $2p \leqslant n+1$ puis :

$$\boxed{p \leqslant \frac{n+1}{2}\cdot}$$

(b) Prenons la matrice $N = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$: elle est nilpotente d'indice $p = 2$. Mais d'après la question précédente s'il existait X telle que $X^2 = A$ alors en appliquant la question précédente aux endomorphismes canoniquement associés à A et X on obtiendrait $p \leqslant \dfrac{2+1}{2} < 2$, ce qui est absurde.

$$\boxed{\text{Il n'existe pas de matrice } X \in \mathcal{M}_2(\mathbb{R}) \text{ telle que } X^2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}}$$

2. (a) Trouver b_0 et b_1 vérifiant les deux premières équations ne pose guère de problème. Observons la troisième équation : il s'agit de $2b_0b_2 + b_1^2 = 0$. b_1 étant connu et surtout b_0 étant non nul, il existe bien un (unique) réel b_2 vérifiant cette équation.
Supposant construit les réels $b_0, ..., b_{q-1}$ vérifiant les premières équations (avec $2 \leqslant q-1 < n-1$), on cherche b_q vérifiant $\sum\limits_{k=0}^{q} b_k b_{q-k} = 0$; mais cette équation est $2b_q + \sum\limits_{k=1}^{q-1} b_k b_{q-k} = 0$, qui possède bien une unique solution (les autres b_k intervenant étant liés à cet instant).

$\boxed{\text{On a bien montré l'existence de réels } b_0, ..., b_{n-1} \text{ vérifiant les équations demandées.}}$

(b) On calcule tranquillement (« avec deux index ») :

$$w^2 = \left(\sum_{k=0}^{n-1} b_k u^k\right)^2 = \sum_{q=0}^{n-1}\left(\sum_{i=0}^{q} b_i b_{q-i}\right)u^q = b_0^2 \mathrm{Id}_E + 2b_0b_1 u + \sum_{q=2}^{n-1}\underbrace{\left(\sum_{i=0}^{q} b_i b_{q-i}\right)}_{=0}u^q$$

$$\boxed{w^2 = \mathrm{Id} + u}$$

3. (a) L'existence de x_1 et ce à quoi il sert a déjà été traité dans les préliminaires :

$$\boxed{\big(x_1, u(x_1), ..., u^{n-1}(x_1)\big) \text{ est une base de } E}$$

La suite est alors évidente (mais permettait de fixer les notations) :

$\boxed{\text{On peut décomposer le vecteur } g(x_1) \in E \text{ dans cette base !}}$

(b) Sans trop forcer :

$$g\circ u = g\circ(g-\mathrm{Id}) = g^3 - g = (g^2-\mathrm{Id})\circ g = u\circ g$$

$$\boxed{g\circ u = u\circ g}$$

On va utiliser ceci pour montrer que g et l'endomorphisme $h=\alpha_0\mathrm{Id}_E+\alpha_1 u+\cdots+\alpha_{n-1}u^{n-1}$ coïncident sur une base de E. Oui : celle à laquelle on peut penser !

*Et ceux qui n'ont pas **nommé** h (la majorité hélas) auront une rédaction bien plus pénible à lire.*

C'est parti :

— Tout d'abord, g et h coïncident en x_1 : les α_i ont été choisis pour ça.

— Si maintenant on applique u à la relation fixant les α_i on trouve :

$$(u\circ g)(x_1) = \alpha_0 u(x_1)+\alpha_1 u^2(x_1)+\cdots+\alpha_{n-1}u^n(x_1)$$

ou encore par commutation de u et g :

$$g\left(u(x_1)\right) = u\left(\alpha_0 x_1+\alpha_1 u(x_1)+\cdots+\alpha_{n-1}u^{n-1}(x_1)\right) = h\left(u(x_1)\right)$$

donc g et h coïncident en $u(x_1)$.

— En réitérant le procédé (bref : par récurrence immédiate) on obtient que g et h coïncident sur tous les $u^k(x_1)$.

Les applications g et h coïncident sur une base donc sont égales.

$$\boxed{g=\sum_{k=0}^{n-1}\alpha_k u^k}$$

(c) Si on part d'une combinaison linéaire nulle des u^k (et à vrai dire faire autre chose est proscrit, puisqu'on veut montrer une liberté !) puis qu'on applique ces endomorphismes en x_1, on trouve une combinaison linéaire nulle des $u^k(x_1)$... or les $u^k(x_1)$ (pour $0\leqslant k\leq n-1$) constituent une famille libre de E, donc les scalaires impliqués sont nuls : c'est ce qu'on voulait montrer !

$$\boxed{\text{La famille }(\mathrm{Id},u,...,u^{n-1})\text{ est libre.}}$$

Vous n'avez pas compris la preuve bien que vous ayez plissé les yeux ? Et si vous preniez un crayon et que partiez effectivement d'une combinaison linéaire nulle des u^k ?

Des calculs déjà faits (question 2.b) nous assurent que $g^2=\sum\limits_{k=0}^{n-1}\beta_k u^k$, avec $\beta_0=\alpha_0^2$, $\beta_1=2\alpha_0\alpha_1$ et $\beta_q=\sum\limits_{k=0}^{q}\alpha_k\alpha_{q-k}$ pour $2\leqslant q\leqslant n-1$. Mais par ailleurs $g^2=1\times\mathrm{Id}+1\times u$. On peut conclure par unicité de la décomposition dans la base $(\mathrm{Id},u,....,u^{n-1})$:

$$\boxed{\alpha_0^2=1,\ 2\alpha_0\alpha_1=1,\text{ et }\sum_{k=0}^{q}\alpha_k\alpha_{q-k}=0\text{ pour tout }q\in[\![2,n-1]\!]\text{ (si }n\geqslant 3).}$$

(d) Puisque $\alpha_0^2=1$, on sait que $\alpha_0=\pm1$. On va fixer $\varepsilon=\alpha_0$ une bonne fois pour toute, et montrer que $\alpha_k=\varepsilon b_k$ pour tout $k\in[\![0,n-1]\!]$.

— Un petit coup d'œil à la définition des b_k nous rappelle que $b_0=1$, donc $\alpha_0=\varepsilon=\varepsilon b_0$.

— On a $\alpha_1=\dfrac{1}{2\alpha_0}=\dfrac{1}{2\varepsilon b_0}=\varepsilon\dfrac{1}{2b_0}=\varepsilon b_1$.

— Vous l'aurez compris : on itère le procédé ! Il s'agit d'une récurrence avec prédécesseurs rédigée ici de façon rapide : si on suppose que $\alpha_i=\varepsilon b_i$ pour tout $i\in[\![0,k-1]\!]$ (avec $q\geqslant 2$ fixé) on montre que $\alpha_q=\varepsilon b_q$ en écrivant

$$2\alpha_q\underbrace{\alpha_0}_{\varepsilon} = -\sum_{k=1}^{q-1}\underbrace{\alpha_k\alpha_{q-k}}_{\varepsilon b_k\varepsilon b_{q-k}=b_kb_{q-k}} = -\sum_{k=1}^{q-1}b_k\varepsilon b_{q-k} = 2\underbrace{b_0}_{1}b_q$$

donc $\alpha_q=\dfrac{b_q}{\varepsilon}=\varepsilon b_q$.

Finalement on a bien pour tout $k \in [\![0, n-1]\!]$, $\alpha_k = \varepsilon b_k$, et donc :

$$\boxed{g = \sum_{k=0}^{n-1} \alpha_k u^k = \varepsilon \sum_{k=0}^{n-1} b_k u^k = \varepsilon w}$$

Les questions 2 et 3 nous montrent que l'équation $f^2 = \mathrm{Id} + u$ possède exactement deux solutions.

4. Notons $A = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ et $N = A - I_4$, de sorte qu'il s'agit de résoudre $X^2 = I_4 + N$. Si on note u l'endomorphisme canoniquement associé à N (qui est nilpotente d'indice 4), les matrices X recherchées seront exactement celles représentant les $f \in \mathcal{L}(R^4)$ telles que $f^2 = \mathrm{Id} + u$, problème qui a été résolu précédemment : il s'agit de l'application $\sum_{k=0}^{3} b_k u^k$ et de son opposée. Il n'y a plus qu'à revenir aux matrices, après avoir noté/calculé que $b_0 = 1$, $b_1 = 1/2$, $b_2 = -1/8$ et $b_3 = 1/16$:

$$\boxed{\text{Les solutions de } X^2 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \text{ sont les deux matrices } \pm \begin{pmatrix} 1 & 1/2 & -1/8 & 1/16 \\ 0 & 1 & 1/2 & -1/8 \\ 0 & 0 & 1 & 1/2 \\ 0 & 0 & 0 & 1 \end{pmatrix}}$$

5. *La décomposition admise dans l'énoncé est ce qu'on appelle la décomposition de Dunford d'un endomorphisme trigonalisable.*
J'ai bien noté que nommer « n » un objet est quasiment discutable... dans un contexte où n désigne la dimension de l'espace de travail depuis le début. Toutes mes confuses !

   (a) C'est du cours (et de preuve quasi-automatique) :

   $$\boxed{\text{Quand deux endomorphismes commutent, les sous-espaces propres de l'un sont stables par l'autre.}}$$

   Ensuite, la relation $n^p = 0$ nous dit que pour tout $x \in E$, $n^p(x) = 0$. C'est a fortiori vrai pour tout $x \in E_\lambda$, et ainsi :

   $$\boxed{\text{L'endomorphisme } n_\lambda \text{ induit par } n \text{ sur } E_\lambda \text{ est nilpotent.}}$$

   (b) Soit $\lambda \in \mathrm{Sp}(d)$. Puisque n_λ est nilpotente, elle est non injective, donc il existe $x \in E_\lambda$ non nul tel que $n_\lambda(x) = 0$. On a alors $u(x) = d(x) + n(x) = \lambda x + n_\lambda(x) = \lambda x$ et puisque $x \neq 0$ on vient de montrer que $\lambda \in \mathrm{Sp}(u)$.

   $$\boxed{\mathrm{Sp}(d) \subset \mathrm{Sp}(u)}$$

   On a donc $\mathrm{Sp}(d) \subset \mathbb{R}_+^*$, donc 0 n'est pas valeur propre de d, donc :

   $$\boxed{d \text{ est bijective.}}$$

   Il faut réécrire ce raisonnement tant qu'il ne va pas de soi : λ est valeur propre de f si et seulement si $f - \lambda \mathrm{Id}$ est non bijective ; en particulier pour $\lambda = 0$.

   (c) Déjà, d est diagonalisable donc l'espace est la somme (directe) de ses sous-espaces propres :

   $$\boxed{E = \bigoplus_{k=1}^{r} E_{\lambda_k}}$$

   La décomposition $x = x_1 + \cdots + x_r \in E_{\lambda_1} \oplus \cdots \oplus E_{\lambda_r}$ nous donne directement (puisque chaque x_i est dans $\mathrm{Ker}\,(d - \lambda_i \mathrm{Id})$) :

   $$\boxed{d(x) = \lambda_1 x_1 + \cdots + \lambda_r x_r}$$

   (d) On va construire δ par sa restriction à chaque E_λ. Fixons donc $\lambda \in \mathrm{Sp}(d)$: puisque la restriction d_λ de d à E_λ vaut $\lambda \mathrm{Id}_{\mathbb{E}_\lambda}$ et $\lambda > 0$, on a directement $d_\lambda = \left(\sqrt{\lambda}\mathrm{Id}_{E_\lambda}\right)^2$.

   On définit donc δ l'unique endomorphisme de E tel que la restriction à chaque E_λ vaut $\sqrt{\lambda}\mathrm{Id}$ (c'est possible d'après le cours car la somme des E_λ vaut E). On a alors :

   $$\boxed{\delta^2 = d}$$

Pour la relation $n \circ \delta = \delta \circ n$, il suffit de vérifier que ces deux endomorphismes de E coïncident sur chaque E_λ. Mais ceci est clair puisque sur chaque λ la restriction de δ est une homothétie donc commute avec n.

$$\boxed{n \circ \delta = \delta \circ n}$$

(e) Si on regarde par exemple la matrice de δ à une base adaptée aux E_λ, on voit que cette matrice est inversible. On peut aussi noter que $\delta^2 = d$ puis regarder le déterminant, qui est non nul...

$$\boxed{\delta \text{ est bijective}}$$

Si on prend ensuite un entier p tel que $n^p = 0$, alors puisque n commute avec δ donc δ^{-2} : $\left(n \circ \delta^{-2}\right)^p = n^p \delta^{-2p} = 0$.

$$\boxed{n \circ \delta^{-2} \text{ est nilpotent.}}$$

(f) D'après la question 2 de cette partie :

$$\boxed{\text{Si on note } P = \sum_{k=0}^{n-1} b_k X^k \text{ alors } w = P(n \circ \delta^{-2}) \text{ vérifie } w^2 = \mathrm{Id} + n \circ \delta^{-2}.}$$

Il est alors tentant de considérer $v = w \circ \delta$! En effet si w et δ commutent alors

$$v^2 = w^2 \circ \delta^2 = (\mathrm{Id} + n \circ \delta^{-2}) \circ \delta^2 = \delta^2 + n = d + n = u$$

Et de fait, puisque n et δ commutent :

$$w \circ \delta = \sum_{k=0}^{n-1} b_k (n \circ \delta^{-2})^k \circ \delta = \sum_{k=0}^{n-1} b_k n^k \circ \delta^{-2k+1} = \sum_{k=0}^{n-1} b_k \delta \circ (n \circ \delta^{-2})^k = \delta \circ w$$

$$\boxed{\text{On a construit } v \in \mathcal{L}(E) \text{ tel que } v^2 = u.}$$