

Centrale-Supélec 2019¹

PC - Mathématiques 1

I Exemples de sous-algèbres

I.A Exemples de sous-algèbres de $\mathcal{M}_n(\mathbb{K})$

1. En remarquant que $T_n(\mathbb{K}) = \text{Vect}_{\mathbb{K}}(E_{ij})_{i \leq j}$ et $T_n^+(\mathbb{K}) = \text{Vect}_{\mathbb{K}}(E_{ij})_{i < j}$ on montre immédiatement que ce sont des sous-espaces vectoriels de $\mathcal{M}_n(\mathbb{K})$. Le produit de deux matrices triangulaires étant encore triangulaire, $T_n(\mathbb{K})$ est stable par produit. De plus, si la diagonale de l'une des deux matrices triangulaires est nulle, la diagonale de la matrice produit le sera aussi. Donc $T_n^+(\mathbb{K})$ aussi est stable par produit.

Les ensembles $T_n(\mathbb{K})$ et $T_n^+(\mathbb{K})$ sont des sous-algèbres de $\mathcal{M}_n(\mathbb{K})$.

2. L'ensemble $S_2(\mathbb{K})$ n'est pas une sous-algèbre de $\mathcal{M}_n(\mathbb{K})$ car il n'est pas stable par produit. En effet, les matrices $A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ sont symétriques, mais leur produit $AB = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ ne l'est pas. L'ensemble $A_2(\mathbb{K})$ n'est pas une sous-algèbre car $C = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ est antisymétrique mais $C^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ ne l'est pas.

Les ensembles $S_2(\mathbb{K})$ et $A_2(\mathbb{K})$ ne sont pas des sous-algèbres de $\mathcal{M}_2(\mathbb{K})$.

3. Reprenons les contre-exemples de la question précédente. Les matrices $A' = \text{Diag}(A, O_{k-2})$ et $B' = \text{Diag}(B, O_{k-2})$ sont symétriques de taille k mais leur produit $A'B' = \text{Diag}(AB, O_{k-2})$ ne l'est pas. La matrice $C' = \text{Diag}(C, O_{k-2})$ est antisymétrique de taille k mais $C'^2 = \text{Diag}(C^2, O_{k-2})$ ne l'est pas.

Les ensembles $S_k(\mathbb{K})$ et $A_k(\mathbb{K})$ ne sont pas des sous-algèbres de $\mathcal{M}_k(\mathbb{K})$.

I.B Exemples de sous-algèbres de $\mathcal{L}(E)$

4. L'ensemble $\mathcal{A}_F$ n'est pas vide car l'endomorphisme nul 0_E stabilise F . Soit $u, v \in \mathcal{A}_F$ et $\lambda \in \mathbb{K}$. Alors pour tout $x \in F$, $(u + \lambda v)(x) = u(x) + \lambda v(x) \in F$. Donc $u + \lambda v$ stabilise F et $\mathcal{A}_F$ est stable par combinaison linéaire ce qui fait de $\mathcal{A}_F$ un sous-espace vectoriel de $\mathcal{L}(E)$. Soient $u, v \in \mathcal{A}_F$. Alors $(u \circ v)(F) = u(v(F)) \subset u(F) \subset F$ donc $u \circ v$ stabilise F et $\mathcal{A}_F$ est stable par composition.

L'ensemble $\mathcal{A}_F$ est une sous-algèbre de $\mathcal{L}(E)$.

5. Soit G un supplémentaire de F dans E . Dans une base adaptée à la décomposition $F \oplus G = E$ la matrice d'un endomorphisme stabilisant F est de la forme $\begin{pmatrix} A & B \\ 0_{n-p,p} & C \end{pmatrix}$. Réciproquement une telle matrice est la matrice d'un endomorphisme stabilisant F .

Donc $\mathcal{A}_F$ est isomorphe à $\left\{ \begin{pmatrix} A & B \\ 0_{n-p,p} & C \end{pmatrix} : A \in \mathcal{M}_p(\mathbb{K}), B \in \mathcal{M}_{p,n-p}(\mathbb{K}), C \in \mathcal{M}_{n-p}(\mathbb{K}) \right\}$ qui est de dimension $p^2 + p(n-p) + (n-p)^2 = (n-p+p)^2 - p(n-p)$.

$\dim \mathcal{A}_F = n^2 - np + p^2$.

1. Vous pouvez envoyer vos remarques ainsi que les irréductibles erreurs et fautes de frappes qui se seront glissées dans ce document à l'adresse suivante pierre-amaury.monard@laposte.net. L'auteur vous en sera reconnaissant.

6. Pour tout $p \in \{1, \dots, p-1\}$, $n^2 - np + p^2 = (p - \frac{n}{2})^2 + \frac{3n^2}{4}$ donc la dimension de $\mathcal{A}_F$ est maximale quand $|p - \frac{n}{2}|$ est maximale i.e quand $p = 1$ ou $p = n - 1$ auxquels cas elle vaut $n^2 - n + 1$.

$$\max_{1 \leq p \leq n-1} (n^2 - np + p^2) = n^2 - n + 1.$$

I.C exemples de sous-algèbres de $\mathcal{M}_2(\mathbb{K})$ diagonalisables et non diagonalisables

7. Posons $K := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Alors $\Gamma(\mathbb{K}) = \text{Vect}_{\mathbb{K}}(I_2, K)$ ce qui montre que $\Gamma(\mathbb{K})$ est un sous-espace vectoriel de $\mathcal{M}_2(\mathbb{K})$. De plus, $I_2^2 = I_2$, $I_2 K = K I_2 = K$ et $K^2 = -I_2$ donc $\Gamma(\mathbb{K})$ est stable par produit puisque qu'un produit de vecteurs d'une famille génératrice reste dans $\Gamma(\mathbb{K})$.

$$\Gamma(\mathbb{K}) \text{ est une sous-algèbre de } \mathcal{M}_2(\mathbb{K}).$$

8. Si $\Gamma(\mathbb{R})$ était diagonalisable tous ses éléments seraient diagonalisables. En particulier, $K \in \Gamma(\mathbb{R})$ serait diagonalisable. Son polynôme caractéristique $\chi_K = X^2 + 1$ serait alors scindé sur $\mathbb{R}$ ce qui n'est manifestement pas le cas.

$$\Gamma(\mathbb{R}) \text{ n'est pas une sous-algèbre diagonalisable de } \mathcal{M}_2(\mathbb{R}).$$

9. Le polynôme $\chi_K = X^2 + 1 = (X - i)(X + i)$ est scindé à racines simples sur $\mathbb{C}$. D'après le théorème de Cayley-Hamilton, χ_K annule K . Donc K est annulé par un polynôme scindé à racines simples sur $\mathbb{C}$ i.e est diagonalisable sur $\mathbb{C}$.

$$K = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ est diagonalisable sur } \mathbb{C}.$$

Soit $P \in GL_2(\mathbb{C})$ telle que $K = P \text{Diag}(i, -i) P^{-1}$. Soit $M \in \Gamma(\mathbb{C})$ et $a, b \in \mathbb{C}$ tels que $M = aI_2 + bK$. Alors $M = P(aI_2 + b \text{Diag}(i, -i)) P^{-1} = P \text{Diag}(a + ib, a - ib) P^{-1}$. Vrai pour tout $M \in \Gamma(\mathbb{C})$ donc $\Gamma(\mathbb{C})$ est diagonalisable.

$$\Gamma(\mathbb{C}) \text{ est une sous-algèbre diagonalisable de } \mathcal{M}_2(\mathbb{C}).$$

Remarque : On aurait aussi pu montrer que tous les éléments de $\Gamma(\mathbb{C})$ étaient diagonalisables -via leur polynôme caractéristique par exemple- puis que $\Gamma(\mathbb{K})$ est une algèbre commutative ce qui prouverait que les éléments de $\Gamma(\mathbb{C})$ sont co-diagonalisables. L'esprit du sujet voulait cependant que nous passions par la diagonalisabilité de K .

II Une sous-algèbre commutative de $\mathcal{M}_n(\mathbb{R})$

II.A Calcul des puissances de J

10. Sans difficulté. La matrice J envoie e_i sur e_{i+1} et la matrice J^2 envoie e_i sur e_{i+2} où les indices sont pris modulo n .

$$J = \begin{pmatrix} 0 & \cdots & \cdots & 1 \\ 1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 1 & 0 \end{pmatrix} \text{ et } J^2 = \begin{pmatrix} 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \ddots & 0 & 1 \\ 1 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & 0 \\ 0 & \cdots & 1 & 0 & 0 \end{pmatrix}.$$

11. La matrice J^k est la matrice canoniquement associée à l'endomorphisme qui envoie e_i sur e_{i+k} toujours en prenant les indices modulo n . En particulier, J^n est la matrice identité.

$J^n = I_n$. J^k n'a que des 0 sauf sur la k -ième sous-diagonale et la $n - k$ -ième sur-diagonale où il y a des 1.

12. Sans difficulté.

$$J(a_0, \dots, a_{n-1}) = \sum_0^{n-1} a_k J^k.$$

II.B Une base de $\mathcal{A}$

13. D'après la question précédente, $\mathcal{A} = \text{Vect}(J^0, \dots, J^{n-1})$ donc la famille $(I_n, \dots, J^{n-1})$ est génératrice de $\mathcal{A}$ (et $\mathcal{A}$ est un espace vectoriel!). Montrons qu'elle est libre. Soient $a_0, \dots, a_{n-1} \in \mathbb{R}$ tels que $\sum_0^{n-1} a_k J^k = 0$ i.e $J(a_0, \dots, a_{n-1}) = 0$. Étant donné la définition de $J(a_0, \dots, a_{n-1})$ on a $a_0 = \dots = a_{n-1} = 0$. Donc la famille $(J^0, \dots, J^{n-1})$ est libre et c'est une base de $\mathcal{A}$.

$(J^0, \dots, J^{n-1})$ est une base de $\mathcal{A}$.

Remarque : En fait, $\mathcal{A} = \mathbb{R}[J]$ où $\mathbb{R}[J] = \{P(J) : P \in \mathbb{R}[X]\}$ est l'ensemble des polynômes en J . L'application $\varphi : \mathbb{R}[X] \rightarrow \mathcal{M}_n(\mathbb{R})$ définie par $\varphi(P) = P(J)$ est un morphisme d'algèbre. De plus $\text{Im}(\varphi) = \mathbb{R}[J]$ ce qui montre directement que $\mathcal{A}$ est une algèbre.

14. Si M commute avec tous les éléments de $\mathcal{A}$ alors en particulier M commute avec J . Réciproquement, si M commute avec J alors M commute avec $J^0, \dots, J^{n-1}$. Définissons le centre de M comme l'ensemble $\mathcal{C}(M) := \{A \in \mathcal{M}_n(\mathbb{R}) : AM = MA\}$. En remarquant qu'il s'agit du noyau de l'application linéaire $A \mapsto AM - MA$ on prouve que c'est un sous-espace vectoriel de $\mathcal{M}_n(\mathbb{R})$. Donc $\mathcal{C}(M)$ contient $\text{Vect}(J^0, \dots, J^{n-1}) = \mathcal{A}$ donc M commute avec tous les éléments de $\mathcal{A}$.

Une matrice M commute avec J si et seulement si elle commute avec tous les éléments de $\mathcal{A}$.

15. On sait déjà que $\mathcal{A}$ est un sous-espace vectoriel de $\mathcal{M}_n(\mathbb{R})$. Il existe $a_0, \dots, a_{n-1}, b_0, \dots, b_{n-1} \in \mathbb{R}$ tels que $M = J(a_0, \dots, a_{n-1})$ et $N = J(b_0, \dots, b_{n-1})$. Posons $P = \sum_0^{n-1} a_k X^k$ et $Q = \sum_0^{n-1} b_k X^k$ de sorte que $M = P(J)$ et $N = Q(J)$. Soit $R \in \mathbb{R}_{n-1}[X]$ le reste de la division euclidienne de PQ par $X^n - 1$. Il existe $T \in \mathbb{R}[X]$ tel que $PQ = T(X^n - 1) + R$. Alors $PQ(J) = R(J)$ car $J^n - I_n = 0$. Alors $MN = PQ(J) = R(J) = J(c_0, \dots, c_{n-1})$ où l'on a noté $R = \sum_0^{n-1} c_k X^k$. Donc $MN \in \mathcal{A}$ et $\mathcal{A}$ est stable par produit et c'est une sous-algèbre de $\mathcal{M}_n(\mathbb{R})$. De plus, $MN = PQ(J) = QP(J) = NM$ donc les éléments de $\mathcal{A}$ commutent entre eux.

L'ensemble $\mathcal{A}$ est une sous-algèbre commutative de $\mathcal{M}_n(\mathbb{R})$.

Remarque : Puisque φ est un morphisme d'algèbre et que $\mathbb{R}[X]$ est une algèbre commutative, l'algèbre $\mathbb{R}[J]$ est aussi commutative. En règle général deux polynômes en une même matrice/endomorphisme commutent toujours (pour peu que l'anneau de base soit commutatif).

II.C Diagonalisation de J

16. D'après le théorème de Cayley-Hamilton, χ_J annule J autrement dit π_J divise χ_J où π_J désigne le polynôme minimal de J . C'est le polynôme unitaire de plus petit degré qui annule J . On a donc que $\deg \pi_J \leq n$. Si π_J est de degré n alors $\pi_J = \chi_J$. Le polynôme $X^n - 1$ annule J , est de degré n et est unitaire. Par ailleurs puisque la famille $(J^0, \dots, J^{n-1})$ est libre, aucun polynôme de degré inférieur à $n - 1$ ne peut annuler J . Donc $\deg \pi_J \geq n$ et $\deg \pi_J = n$. Donc $\pi_J = X^n - 1$. D'après ce qui vient d'être dit : $\chi_J = X^n - 1$.

$$\chi_J = X^n - 1.$$

17. Dans $\mathbb{C}$, $X^n - 1 = \prod_{k=0}^{n-1} (X - \omega^k)$ où $\omega := e^{i\frac{2\pi}{n}}$. Donc J est annulé par un polynôme scindé à racines simples dans $\mathbb{C}$ donc est diagonalisable sur $\mathbb{C}$.

$$J \text{ est diagonalisable dans } \mathcal{M}_n(\mathbb{C}).$$

18. Pour $n = 2$, le polynôme caractéristique de J est $X^2 - 1$ qui est scindé à racines simples sur $\mathbb{R}$ donc J est diagonalisable dans $\mathcal{M}_n(\mathbb{R})$. Pour $n \geq 3$ le polynôme minimal de J est $X^n - 1$ qui n'est pas scindé à racines simples sur $\mathbb{R}$ donc aucun polynôme scindé à racines simples sur $\mathbb{R}$ n'annule J et J n'est pas diagonalisable dans $\mathcal{M}_n(\mathbb{R})$.

$$J \text{ n'est pas diagonalisable dans } \mathcal{M}_n(\mathbb{R}) \text{ sauf si } n = 2.$$

19. Le spectre de J est l'ensemble des racines de son polynôme caractéristique. Donc $\text{Sp}_{\mathbb{C}}(J) = \{1, \omega, \dots, \omega^{n-1}\}$ où $\omega = e^{i\frac{2\pi}{n}}$. Il y a n valeurs propres donc elles sont toutes de multiplicité (géométrique) 1 : $\dim E_{\omega^k}(J) = 1$ pour $k = 0, \dots, n-1$. Soit $k \in \{0, \dots, n-1\}$. Posons $X_k := \begin{pmatrix} 1 \\ \omega^k \\ \vdots \\ \omega^{k(n-1)} \end{pmatrix}$. Alors $JX_k = \begin{pmatrix} \omega^k \\ \omega^{2k} \\ \vdots \\ \omega^{kn} \end{pmatrix} = \omega^k X_k$. Donc X_k est un vecteur propre de J associé à la valeur propre ω^k et (X_k) est une base de $E_{\omega^k}(J)$.

$$\text{Sp}_{\mathbb{C}}(J) = \{1, \omega, \dots, \omega^{n-1}\} \text{ et } E_{\omega^k}(J) = \mathbb{C} \begin{pmatrix} 1 \\ \omega^k \\ \vdots \\ \omega^{k(n-1)} \end{pmatrix}.$$

II.D Diagonalisation de $\mathcal{A}$

20. L'ensemble $\mathcal{A}$ n'est pas un $\mathbb{C}$ -espace vectoriel car il n'est pas stable par multiplication par un scalaire **complexe**. Par exemple, $iJ \notin \mathcal{M}_n(\mathbb{R})$ donc $iJ \notin \mathcal{A}$.

$$\text{Non, } \mathcal{A} \text{ n'est pas une sous-algèbre de } \mathcal{M}_n(\mathbb{C}).$$

21. Soit $P \in GL_n(\mathbb{C})$ telle que $PJP^{-1} = \text{Diag}(1, \dots, \omega^{n-1})$. Soit $A \in \mathcal{A}$. Il existe $Q \in \mathbb{R}_{n-1}[X]$ tel que $A = Q(J)$. Alors $PAP^{-1} = PQ(J)P^{-1} = Q(PJP^{-1}) = Q(\text{Diag}(1, \dots, \omega^{n-1})) = \text{Diag}(Q(1), \dots, Q(\omega^{n-1}))$ et la matrice PAP^{-1} est diagonale.

$$\text{Pour tout } A \in \mathcal{A}, PAP^{-1} \text{ est diagonale.}$$

L'égalité $PQ(J)P^{-1}$ vient du fait que $PJ^kP^{-1} = (PJP^{-1})^k$ pour tout $k \in \mathbb{N}$.

22. D'après la question précédente, la matrice $J(a_0, \dots, a_{n-1}) = Q(J)$ est semblable à la matrice diagonale $D = \text{Diag}(Q(1), \dots, Q(\omega^{n-1}))$.

$$\text{Sp}_{\mathbb{C}}(Q(J)) = \{Q(1), \dots, Q(\omega^{n-1})\}.$$

III Sous-algèbre stricte de $\mathcal{M}_n(\mathbb{R})$ de dimension maximale

III.A Un produit scalaire sur $\mathcal{M}_n(\mathbb{R})$

23. • Notons $b : \mathcal{M}_n(\mathbb{R}) \times \mathcal{M}_n(\mathbb{R})$ l'application définie par $b(A, B) = (A|B) = \text{Tr}({}^tAB)$.
 • Soit $B \in \mathcal{M}_n(\mathbb{R})$ fixé. Alors l'application partielle $b(A, \cdot) : M \mapsto (M|B)$ est la composée de $M \mapsto {}^tAM$ et de la $\text{Tr} : M \mapsto \text{Tr}(M)$ qui sont linéaires. Donc b est linéaire à droite.
 • La trace étant invariante par transposition : $\text{Tr}({}^tAB) = \text{Tr}({}^t({}^tAB)) = \text{Tr}({}^tBA)$ donc $(A|B) = (B|A)$ et b est symétrique.
 • Soit $A \in \mathcal{M}_n(\mathbb{R})$. On a $b(A, A) = \text{Tr}({}^tAA) = \sum_1^n ({}^tAA)_{ii} = \sum_1^n \sum_1^n a_{ji}^2 \geq 0$ donc b est positive.
 • Si $b(A, A) = 0$ alors $\sum_{i,j} a_{ji}^2 = 0$ donc $a_{ji} = 0$ pour tout $i, j = 1, \dots, n$ i.e $A = 0$. Donc b est définie positive.

$b : (A, B) \mapsto \text{Tr}({}^tAB)$ est un produit scalaire sur $\mathcal{M}_n(\mathbb{R})$.

24. En dimension finie, un sous-espace vectoriel et son orthogonal sont supplémentaires. Ici, $\mathcal{M}_n(\mathbb{R})$ est de dimension finie, donc $\dim \mathcal{A} + \dim \mathcal{A}^\perp = \dim \mathcal{M}_n(\mathbb{R})$.

$$\boxed{d + r = n^2.}$$

25. Pour F un sous-espace vectoriel de E un espace euclidien, $x \in F^\perp$ si et seulement si x est orthogonal à n'importe quelle famille génératrice de F . En dimension finie, $F = F^{\perp\perp}$. Donc $M \in \mathcal{A}$ si et seulement si $M \in \mathcal{A}^{\perp\perp}$ si et seulement si M est orthogonal à la famille $(A_1, \dots, A_r)$ qui est bien génératrice de $\mathcal{A}^\perp$.

$M \in \mathcal{A}$ si et seulement si $(A_k|M) = 0$ pour tout $k = 1, \dots, r$.

26. Soit $i, j \in \llbracket 1, r \rrbracket$. Soit $M \in \mathcal{A}$. On a $(M|{}^tNA_i) = \text{Tr}({}^tM{}^tNA_i) = (NM|A_i) = 0$ car $NM \in \mathcal{A}$. Vrai pour tout $M \in \mathcal{A}$:

Pour tout $i = 1, \dots, r$, ${}^tNA_i \in \mathcal{A}^\perp$.

27. L'application ${}^t : A \mapsto {}^tA$ est linéaire donc ${}^t\mathcal{A}$ est un sous-espace vectoriel de $\mathcal{M}_n(\mathbb{R})$ en tant qu'image d'un sous-espace vectoriel par une fonction linéaire. De plus, si $A, B \in \mathcal{A}$, ${}^tA{}^tB = {}^t(BA) \in {}^t\mathcal{A}$ et ${}^t\mathcal{A}$ est stable par produit.

${}^t\mathcal{A}$ est une sous-algèbre de $\mathcal{M}_n(\mathbb{R})$.

La transposée étant involutive, elle est bijective donc injective. La transposition réalise donc un isomorphisme de $\mathcal{A}$ sur ${}^t\mathcal{A}$ et $\dim \mathcal{A} = \dim({}^t\mathcal{A})$.

$$\boxed{\dim \mathcal{A} = \dim({}^t\mathcal{A}).}$$

28. Soit $N \in \mathcal{A}$. Montrons que F est stable par tN . Soit $i \in \llbracket 1, r \rrbracket$. Alors, ${}^tNA_i \in \mathcal{A}^\perp$ d'après la question 26. Donc il existe $c_1, \dots, c_r \in \mathbb{R}$ des coefficients tels que ${}^tNA_i = \sum_1^r c_j A_j$. D'où ${}^tNA_i X = \sum_1^r c_j A_j X \in F$. Vrai pour tout $i = 1, \dots, r$ donc F est stable par tN . Vrai pour tout $N \in \mathcal{A}$ donc :

F est stable par tous les endomorphismes de ${}^t\mathcal{A}$.

29. Notons p la dimension de F . Comme F est un sous-espace vectoriel de $\mathbb{R}^n$, on a nécessairement $p \leq n$. Si $p = n$ alors $r \geq n$ et $d = n^2 - r \leq n^2 - n < n^2 - n + 1$ ce qui démontre le résultat.
 Si $p < n$. Alors, comme $\mathcal{A}$ est une sous-algèbre stricte de $\mathcal{M}_n(\mathbb{R})$, $r = n^2 - d > 0$ et donc $p \geq 1$ puisque $F \neq \{0\}$. D'où $1 \leq p \leq n - 1$. D'après la question précédente, ${}^t\mathcal{A} \subset \mathcal{A}_F$ où $\mathcal{A}_F$ a été introduit à la partie I.B. D'après la question 6, $\dim \mathcal{A}_F \leq n^2 - n + 1$ donc $\dim({}^t\mathcal{A}) \leq n^2 - n + 1$. D'après la question 27, $\dim({}^t\mathcal{A}) = \dim \mathcal{A} = d$. Dans ce cas aussi on a $d \leq n^2 - n + 1$.

$$d \leq n^2 - n + 1.$$

Soit F une droite vectorielle de $\mathbb{R}^n$. Alors $\mathcal{A}_F$ est une sous-algèbre de $\mathcal{M}_n(\mathbb{R})$ de dimension $n^2 - n + 1 < n^2$ d'après la partie I.B et c'est donc une sous-algèbre stricte pour laquelle on a l'égalité $d = n^2 - n + 1$.

La dimension maximale d'une sous-algèbre stricte de $\mathcal{M}_n(\mathbb{R})$ est $n^2 - n + 1$.

IV. Réduction d'une algèbre nilpotente

30. Si $n = 1$, les matrices nilpotentes sont les matrices nulles qui sont trigonalisables dans toute base.

Le résultat est vrai pour $n = 1$.

31. S'il n'existe aucun tel sous-espace vectoriel alors $\mathcal{A}$ est irréductible. Or E est un $\mathbb{C}$ -espace vectoriel, donc $\mathcal{A} = \mathcal{L}(E)$ d'après le théorème de Burnside. En particulier, $\text{id}_E \in \mathcal{A}$ mais id_E n'est pas nilpotent ce qui est contradictoire.

Il existe un sous-espace vectoriel V de E distinct de E et $\{0\}$ stable par les éléments de $\mathcal{A}$.

32. Soit W un supplémentaire de V dans E et $\mathcal{B}$ une base adaptée à la décomposition $V \oplus W = E$. Pour tout $u \in \mathcal{A}$, la matrice de u dans la base $\mathcal{B}$ est de la forme $\begin{pmatrix} A & B \\ 0 & D \end{pmatrix}$ où A est de taille $r \times r$, B de taille $r \times s$ et D de taille $s \times s$.

Il existe une base $\mathcal{B}$ telle que $\text{mat}_{\mathcal{B}} u = \begin{pmatrix} A & B \\ 0 & D \end{pmatrix}$ où $A \in \mathcal{M}_r(\mathbb{C})$, $B \in \mathcal{M}_{r,s}(\mathbb{C})$ et $D \in \mathcal{M}_s(\mathbb{C})$.

33. Un calcul matriciel par blocs montre que $\begin{pmatrix} A(u + \lambda v) & B(u + \lambda v) \\ 0 & D(u + \lambda v) \end{pmatrix} = \begin{pmatrix} A(u) & B(u) \\ 0 & D(u) \end{pmatrix} + \lambda \begin{pmatrix} A(v) & B(v) \\ 0 & D(v) \end{pmatrix}$ et $\begin{pmatrix} A(uv) & B(uv) \\ 0 & D(uv) \end{pmatrix} = \begin{pmatrix} A(u)A(v) & * \\ 0 & D(u)D(v) \end{pmatrix}$. Ceci montre que $\{A(u) : u \in \mathcal{A}\}$ est une partie non vide (car $\mathcal{A}$ est non vide) stable par combinaison linéaire et stable par produit. C'est donc une sous-algèbre de $\mathcal{M}_r(\mathbb{C})$. De même pour $\{D(u) : u \in \mathcal{A}\}$.

Les ensembles $\{A(u) : u \in \mathcal{A}\}$ et $\{D(u) : u \in \mathcal{A}\}$ sont des sous-algèbres de $\mathcal{M}_r(\mathbb{C})$ et $\mathcal{M}_s(\mathbb{C})$.

Soit $u \in \mathcal{A}$. Il existe $N \in \mathbb{N}$ tel que $u^N = 0_n$. Un calcul matriciel par blocs montre que $u^N = \begin{pmatrix} A(u)^N & * \\ 0 & D(u)^N \end{pmatrix}$. Donc $A(u)^N = 0_r$ et $D(u)^N = 0_s$.

Les éléments de $\{A(u) : u \in \mathcal{A}\}$ et $\{D(u) : u \in \mathcal{A}\}$ sont nilpotents.

34. Le sous-espace vectoriel V étant distinct de $\{0\}$ et de E , sa dimension r vérifie $1 \leq r \leq n - 1$. De même pour s la dimension de W . D'après l'hypothèse de récurrence, il existe $P \in GL_r(\mathbb{C})$ et $Q \in GL_s(\mathbb{C})$ telles que pour tout $u \in \mathcal{A}$, les matrices $PA(u)P^{-1}$ et $QD(u)Q^{-1}$ sont triangulaires supérieures.

Posons $T = \begin{pmatrix} P & 0 \\ 0 & Q \end{pmatrix}$. Alors T est inversible d'inverse $T^{-1} = \begin{pmatrix} P^{-1} & 0 \\ 0 & Q^{-1} \end{pmatrix}$. Alors $T \text{mat}_{\mathcal{B}}(u) T^{-1} = \begin{pmatrix} PA(u)P^{-1} & * \\ 0 & QD(u)Q^{-1} \end{pmatrix} \in T_n^+(\mathbb{C})$. Donc $\mathcal{A}$ est trigonalisable.

L'algèbre $\mathcal{A}$ est trigonalisable.

35. La matrice T est inversible. Elle envoie donc la base $\mathcal{B}$ sur une autre base $\mathcal{B}'$ de E . Dans la base $\mathcal{B}'$, la matrice de u est $T \text{mat}_{\mathcal{B}} T^{-1} \in T_n^+(\mathbb{C})$.

Il existe une base de E dans laquelle les éléments de $\mathcal{A}$ sont triangulaires supérieures.

V. Le théorème de Burnside

V.A Recherche d'un élément de rang 1

36. Posons $F := \{u(x) : u \in \mathcal{A}\}$. Considérons le morphisme d'évaluation en x , $\text{Eval}_x : \mathcal{A} \rightarrow E$ défini par $\text{Eval}_x(u) := u(x)$. L'application Eval_x est linéaire et son image est exactement F ce qui prouve que F est un sous-espace vectoriel de E .

Montrons F est stable par $\mathcal{A}$. Soit $z \in F$. Il existe $u \in \mathcal{A}$ tel que $z = u(x)$. Soit $v \in \mathcal{A}$. Alors $v(z) = (v \circ u)(x) \in \mathcal{A}$. Vrai pour tout $z \in F$ et $v \in \mathcal{A}$, donc F est stable par $\mathcal{A}$. Puisque $\mathcal{A}$ est irréductible, $F = \{0\}$ ou $F = E$.

Si $F = \{0\}$ alors $u(x) = 0$ pour tout $u \in \mathcal{A}$. Donc $x \in G := \bigcap_{u \in \mathcal{A}} \ker u$. Si $z \in G$ alors $v(z) = 0 \in G$ pour tout $v \in \mathcal{A}$ donc G est stable par $\mathcal{A}$. Donc $G = \{0\}$ ou $G = F$ par irréductibilité de $\mathcal{A}$. Or $x \in G$ est non nul donc $G \neq \{0\}$ et $G = E$. Donc $\ker(u) = E$ pour tout $u \in \mathcal{A}$ i.e $\mathcal{A} = \{0_{\mathcal{L}(E)}\}$. Or $n \geq 2$, il existe donc H un sous-espace vectoriel de E strict non réduit à $\{0\}$. Alors H est stable par $\mathcal{A} = \{0\}$ ce qui contredit l'irréductibilité de $\mathcal{A}$.

Donc $F = E$ et $y \in F$. Il existe donc $u \in \mathcal{A}$ tel que $y = u(x)$.

Il existe $u \in \mathcal{A}$ tel que $u(x) = y$.

37. Notons r le rang de v . Puisque $r \geq 2$ il existe une famille libre à deux éléments de $\text{Im}(v)$. Notons x et y leurs antécédents par v ; alors $v(x), v(y)$ est libre. Nécessairement, $v(x), v(y) \neq 0$. D'après la question précédente, il existe $u \in \mathcal{A}$ tel que $u(v(x)) = y$.

On a $(v \circ u)(\text{Im } v) \subset \text{Im } v$ donc on peut considérer $\tilde{f}$ l'endomorphisme induit par $v \circ u$ sur $\text{Im } v$. Tout endomorphisme admet au moins une valeur propre complexe en dimension finie. Il existe donc $\lambda \in \mathbb{C}$ tel que $\tilde{f} - \lambda \text{id}_{\text{Im } v}$ soit non inversible. En particulier, $\text{rg}(\tilde{f} - \lambda \text{id}_{\text{Im } v}) < r$. Posons $f := \tilde{f} \circ v$ qui est bien défini si l'on voit v comme un élément de $\mathcal{L}(E, \text{Im } v)$. Alors $f = v \circ u \circ v - \lambda v$ et $\text{rg } f \leq \text{rg } \tilde{f} < \text{rg } v$ d'après ce qui vient d'être dit. De plus, $f(x) = v(u \circ v(x)) - \lambda v(x) = v(y) - \lambda v(x)$ est non nul par liberté de $(v(x), v(y))$ donc $\text{rg } f > 0$. D'où le résultat.

Il existe $u \in \mathcal{A}$ et $\lambda \in \mathbb{C}$ tels que $0 < \text{rg}(v \circ u \circ v - \lambda v) < \text{rg } v$.

38. Rappelons que $\mathcal{A} \neq \{0\}$ car l'algèbre $\{0\}$ n'est pas irréductible dès que $n \geq 2$. Soit donc $v_0 \in \mathcal{A}$ non nul. Si $\text{rg } v_0 = 1$ c'est terminé. Si $\text{rg } v_0 \geq 2$ on construit alors $v_1 = v_0 \circ u \circ v_0 - \lambda v_0$ comme dans la question précédente. Alors v_1 est encore un élément de l'algèbre $\mathcal{A}$ et de plus, $1 \leq \text{rg } v_1 \leq \text{rg } v_0$. En itérant, on construit ainsi une suite d'éléments $v_0, v_1, v_2, \dots$ de $\mathcal{A}$ de rangs strictement décroissants. Comme il n'existe pas de suite infinie strictement décroissante d'entiers naturels, ce processus s'arrête à v_k de rang 1.

Il existe $v \in \mathcal{A}$ de rang 1.

V.B Conclusion

39. Posons $x = u(\varepsilon_0)$. Puisque u_0 n'est pas l'endomorphisme nul, il existe $v_i \in \mathcal{A}$ tel que $v_i(x) = \varepsilon_i$ d'après la question 36. On pose alors $u_i := v_i \circ u_0$. D'une part, $u_i \in \mathcal{A}$. D'autre part, le noyau de u_i contient $\varepsilon_2, \dots, \varepsilon_n$ donc u_i est de rang 0 ou 1. De plus, $u_i(\varepsilon_1) = v_i(x) = \varepsilon_i$. Donc u_i est de rang 1 et vérifie bien $u_i(\varepsilon_1) = \varepsilon_i$.

Il existe $u_1, \dots, u_n \in \mathcal{A}$ de rang 1 tels que $u_i(\varepsilon_1) = \varepsilon_i$ pour tout $i \in \llbracket 1, n \rrbracket$.

40. Soient $i, j \in \llbracket 1, n \rrbracket$. D'après la question 36, il existe $w_j \in \mathcal{A}$ tel que $w_j(\varepsilon_j) = \varepsilon_1$. Posons $f_{ij} = u_i \circ w_j$. Alors $f_{ij}(\varepsilon_j) = \varepsilon_i$. De plus f_{ij} est de rang 1 donc $f_{ij}(\varepsilon_k) = 0$ si $k \neq j$. Donc la matrice de f_{ij} est la matrice élémentaire E_{ij} . Puisque $(E_{ij})_{i,j}$ est une base de $\mathcal{M}_n(\mathbb{C})$, la famille $(f_{ij})_{i,j}$ est une base de $\mathcal{L}(E)$. Donc l'algèbre $\mathcal{A}$ contient $\mathcal{L}(E)$ et $\mathcal{A} = \mathcal{L}(E)$.

Si E est un $\mathbb{C}$ -ev alors la seule sous-algèbre irréductible de $\mathcal{L}(E)$ est $\mathcal{L}(E)$.

Remarque : Ce n'est plus vrai si E est un $\mathbb{R}$ -espace vectoriel. En effet, l'existence du scalaire λ de la question 37 vient du fait que tout polynôme non constant de $\mathbb{C}[X]$ admet au moins une racine dans $\mathbb{C}$. Dans un $\mathbb{R}$ -espace vectoriel il n'existe pas forcément de valeur propre.

*** FIN ***
