EPFL

1

Enseignant: Philippe Michel
Examen: Algèbre Linéaire Avancée, MATH-110
Date: Le 25 Janvier 2022, 16h15-19h15
Durée: 3 heures

Student One

SCIPER : **111111**

Signature :

Attendez le début de l'examen avant de tourner la page.

Ce document est imprimé recto-verso, il contient 33 pages.

Ne pas dégrafer.

- Aucun document n'est autorisé.
- Une calculette simple (sans display graphique) est autorisée.
- Pour les questions à choix multiples:
  - entourez la bonne réponse (sans justification) et utilisez un stylo à encre noire ou bleue foncée; en cas d'erreur effacez proprement avec du correcteur blanc.
  - Une réponse incorrecte compte 0 mais n'entraine pas de point négatif.
- Pour les questions ouvertes:
  - Répondre dans l'espace dédié.
  - Vous pouvez utiliser un crayon à papier à condition d'écrire lisiblement;
  - Si vous utilisez des résultats du cours, citez-les explicitement.
  - Sauf mention explicite du contraire on a le droit d'utiliser un résultat d'un autre exercice ou d'une question précédente du même exercice pour répondre à une question même si on ne l'a pas démontré.
- Si une question est erronée, l'enseignant se réserve le droit de l'annuler.
- L'examen est LONG mais il n'est pas nécessaire de le faire correctement intégralement pour obtenir la note maximale.

Formulaire concernant les déterminants

Soit K un corps de caractéristique 2, $d \geqslant 1$, V un K-EV de dimension d et $\mathcal{B} = \{\mathbf{e}_1, \cdots, \mathbf{e}_d\}$ une base de V. On rappelle que l'espace vectoriel $\mathrm{Alt}^{(n)}(V;K)$ des formes multilinéaires alternées en d variables est de dimension 1 (ainsi toute forme multilinéaire alternée est proportioelle a toute autre forme multilinéaire alternée non-nulle). On note $\det_{\mathcal{B}}$ l'unique forme multilinéaire alternée telle que

$$\det_{\mathcal{B}}(\mathbf{e}_1, \cdots, \mathbf{e}_d) = 1.$$

Soit $(v_1, \cdots, v_d) \in V^d$ et $v_i = \sum_{j=1}^d x_{ij}\mathbf{e}_j$. On a alors

$$\det_{\mathcal{B}}(v_1, \cdots, v_d) = \sum_{\sigma \in \mathfrak{S}_d} \mathrm{sign}(\sigma) x_{1\sigma(1)}.\cdots.x_{d\sigma(d)} = \sum_{\sigma \in \mathfrak{S}_d} \mathrm{sign}(\sigma) x_{\sigma(1)1}.\cdots.x_{\sigma(d)d}$$

Pour $\varphi : V \mapsto V$ une application lineaire, on définit son déterminant $\det(\varphi) \in K$ comme l'unique scalaire vérifiant l'une des égalités équivalentes suivantes:

$$\det_{\mathscr{B}}(\varphi(\mathbf{e}_1), \cdots, \varphi(\mathbf{e}_d)) = \det(\varphi)\det_{\mathcal{B}}(\mathbf{e}_1, \cdots, \mathbf{e}_d) = \det(\varphi).$$

$$\forall (v_1, \cdots, v_d) \in V^d,\ \det_{\mathcal{B}}(\varphi(v_1), \cdots, \varphi(v_d)) = \det(\varphi)\det_{\mathcal{B}}(v_1, \cdots, v_d)$$

et si

$$\mathrm{mat}_{\mathcal{B}}(\varphi) = (m_{ij})_{i,j \leqslant d} = M$$

est la matrice de φ dans la base $\mathscr{B}$, alors

$$\det(\varphi) = \det(M) = \sum_{\sigma \in \mathfrak{S}_d} \mathrm{sign}(\sigma) m_{1\sigma(1)}.\cdots.m_{d\sigma(d)} = \sum_{\sigma \in \mathfrak{S}_d} \mathrm{sign}(\sigma) m_{\sigma(1)1}.\cdots.m_{\sigma(d)d}.$$

On a par ailleurs pour $\varphi, \psi \in \mathrm{End}(V)$ et $M, N \in M_d(K)$ et $\lambda \in K$

$$\det(\varphi \circ \psi) = \det(\varphi)\det(\psi),\ \det(M.N) = \det(M)\det(N)$$

$$\det(\lambda\varphi) = \lambda^d \det(\varphi),\ \det(\lambda.M) = \lambda^d \det(M)$$

$$\det(\mathrm{Id}_V) = 1 = \det(\mathrm{Id}_d)$$

Par ailleurs si $M \in M_d(K)$ se décompose en blocs de matrices carrées

$$M = \begin{pmatrix} M_1 & * \\ \mathbf{0} & M_2 \end{pmatrix} \text{ ou bien } M = \begin{pmatrix} M_1 & \mathbf{0} \\ & M_2 \end{pmatrix},\ M_1 \in M_{d_1}(K),\ M_2 \in M_{d_2}(K),\ d = d_1 + d_2,$$

on a

$$\det(M) = \det(M_1)\det(M_2).$$

Exercice 1 (Questions de cours et QCM). .

1. Enoncer deux propriétés de l'application "transposition" sur l'espace des matrices.

2. Soit G un groupe, H un groupe commutatif et $\varphi : G \mapsto H$ un morphisme de groupes alors l'image $\mathrm{Im}(\varphi) = \varphi(G)$ est un sous-groupe de H invariant par conjugaison.

   <u>Vrai</u>　　　　Faux

   parce que H est commutatif tout sous-groupe est distingue

3. Le produit de deux corps est un anneau intègre.

   Vrai　　　　<u>Faux</u>

   $(0_K, 1_{K'}) \times (1_K, 0_{K'}) = (0_K, 0_{K'})$.

4. Une application linéaire $\varphi : \mathbb{R}^m \mapsto \mathbb{R}^n$ est surjective si $m \geqslant n$.

   Vrai　　　　<u>Faux</u>

   Prendre l'application identiquement nulle.

5. Soit $B = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \in M_3(\mathbb{R})$ et M vérifiant ${}^tM.B.M = B$; alors M est inversible.

   <u>Vrai</u>　　　　Faux

   $\det({}^tM.B.M) = \det(M)^2 \det(B) = \det(B) = -1$ donc $\det M \neq 0$

6. Soit K un corps et $C = \begin{pmatrix} 2 & 3 & 0 \\ 1 & 3 & 1 \\ 0 & 2 & 1 \end{pmatrix} \in M_3(K)$ alors C est inversible quelque soit la caractéristique de K.

   <u>Vrai</u>　　　　Faux

   $\det(M) = 6 + 0 + 0 - 0 - 4 - 3 = -1$ (Sarrus) n'est jamais nul quelque soit la caracteristique.

Exercice 2. Soit K un corps et

$$A = \begin{pmatrix} 0 & 1 & 4 & 0 & 1 \\ 0 & 1 & 4 & 2 & -5 \\ 2 & 0 & 8 & 0 & -16 \\ 0 & -1 & -4 & 0 & -1 \end{pmatrix} \in M_{4\times 5}(K).$$

1. Déterminer la valeur de $\mathrm{rang}(A)$ en fonction de la caractéristique de K.

2. On suppose que $\mathrm{car}(K) = 0$. Donner une base de $\ker(A)$: on voit A comme la matrice dans les bases canoniques d'une application linéaire de K^5 vers K^4 et on écrira les vecteurs de la base du noyau sous forme de vecteurs lignes.

Réponses aux questions de l'Exercice 2 (répondre à l'intérieur de la boite)
Si $\mathrm{car}(K) = 2$ la matrice devient

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix} \in M_{4\times 5}(K)$$

qui est de rang 1.
Si $\mathrm{car}(K) \neq 2$ on reduit

$$\begin{pmatrix} 1 & 0 & 4 & 0 & -8 \\ 0 & 1 & 4 & 0 & 1 \\ 0 & 1 & 4 & 2 & -5 \\ 0 & -1 & -4 & 0 & -1 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 4 & 0 & -8 \\ 0 & 1 & 4 & 0 & 1 \\ 0 & 0 & 0 & 2 & -6 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 4 & 0 & -8 \\ 0 & 1 & 4 & 0 & 1 \\ 0 & 0 & 0 & 1 & -3 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

et la matrice est de rang 3 et le noyau de dimension 2. Si les coordonnees dans K^5 sont (x, y, z, t, u) les inconnues principales sont x, y, t et les libres sont z et u: Pour avoir une base on pose $z = 1, u = 0$ et on resoud le systeme reduit et puis $z = 0, u = 1$ et on fait pareil:

$$x + 4 = 0,\ \ y + 4 = 0, t = 0 \to (-4, -4, 1, 0, 0)$$

$$x - 8 = 0,\ \ y + 1 = 0, t - 3 = 0 \to (8, -1, 0, 3, 1).$$

Exercice 3. Soit (G, e_G) un groupe noté multiplicativement. Pour $g, h \in G$ des éléments, le commutateur de g et h est le produit

$$[g, h] := g.h.g^{-1}.h^{-1}.$$

Le sous-groupe dérivé de G, noté $D(G)$ ou $[G, G]$ est le sous-groupe de G engendré par les commutateurs:

$$D(G) = [G, G] = \langle [g, h],\ g, h \in G \rangle \subset G.$$

1. Soit $\varphi : G \mapsto G'$ un morphisme de groupes, montrer que

$$\varphi([G, G]) \subset [G', G'].$$

2. Montrer que $[G, G]$ est invariant par conjugaison:

$$\forall g \in G,\ \mathrm{Ad}(g)([G, G]) = g.[G, G].g^{-1} = [G, G].$$

3. Un groupe G est dit parfait si il est égal à son groupe dérivé:

$$G = [G, G].$$

   Soit (G, e_G) un groupe parfait et (C, e_C) un groupe commutatif (toujours noté multiplicativement), montrer que le seul morphisme de groupes $\varphi : G \mapsto C$ est le morphisme trivial.

4. Montrer que pour $n \geqslant 2$ le groupe symétrique $\mathfrak{S}_n$ n'est pas parfait.

Réponses aux questions de l'Exercice 3 (répondre à l'intérieur de la boite)

1. Comme φ est un morphisme on a

$$\varphi([g, h]) = \varphi(g.h.g^{-1}.h^{-1}) = \varphi(g).\varphi(h).\varphi(g)^{-1}.\varphi(h)^{-1} = [\varphi(g), \varphi(h)] \subset [G', G'].$$

   L'image d'un commutateur est le commutateur des images.

   Comme $[G, G]$ est engendre par les commutateurs tout element de $[G, G]$ est un produit de puissances de commutateurs et son image est un produit de puissances des commutateurs des images qui sont des commutateurs dans G' et donc $\varphi([G, G]) \subset [G', G']$.

2. Comme $\mathrm{Ad}(g) : G \mapsto G$ est un morphisme de groupes on a par la question precedente que

$$\mathrm{Ad}(g)[G, G] = g[G, G]g^{-1} \subset [G, G]$$

   Replacant g par g^{-1} on a

$$g^{-1}[G, G]g \subset [G, G] \Longrightarrow g.g^{-1}[G, G]g.g^{-1} \subset g[G, G]g^{-1}$$

   et donc

$$[G, G] \subset g[G, G]g^{-1}$$

   et donc par double inclusion

$$[G, G] = g[G, G]g^{-1}$$

3. On a

$$\varphi([g, h]) = [\varphi(g), \varphi(h)] = \varphi(g).\varphi(h).\varphi(g)^{-1}.\varphi(h)^{-1}$$

   et comme C est commutatif

$$\varphi(g).\varphi(h).\varphi(g)^{-1}.\varphi(h)^{-1} = \varphi(g).\varphi(g)^{-1}.\varphi(h).\varphi(h)^{-1} = e_C.$$

   L'image de tout commutateur est donc triviale et donc l'image d'un produit de puissances de commutateurs est un produit de puissances de commutateurs des images et est donc trivial. Comme tout element de G est un produit de puissances de commutateurs son image par φ est e_C et $\varphi = \underline{e_C}$ est le morphisme trivial.

4. Le groupe symetrique n'est pas parfait car il possede un morphisme non-trivial a valeurs dans un groupe commutatif: la signature (a valeurs dans $\{\pm 1\}$).

Exercice 4. Soit K un corps et

$$\mathrm{SL}_3(K) = \{M \in \mathrm{GL}_3(K),\ \det M = 1\} \subset \mathrm{GL}_3(K)$$

le groupe special lineaire des matrices 3×3 de determinant 1. On rappelle que comme

$$\det : \mathrm{GL}_3(K) \mapsto K^\times$$

est un morphisme de groupes $SL_3(K)$ est un sous-groupe distingue (invariant par conjugaison). On va étudier le structure de ce groupe.
Pour cela on a recours aux matrices de transformations élémentiares suivantes: pour $i \neq j \in \{1, \cdots 3\}$ et $\mu \in K^\times$, on pose

$$C_{ij,\mu} = \mathrm{Id}_3 + \mu.E_{ij} \tag{4.1}$$

où $E_{i'j'},\ i', j' \in \{1, \cdots, 3\}$ désignent les matrices élémentaires et Id_3 est la matrice identité.

1. Soit $M \in M_3(K)$ une matrice. Rappelez (sans preuve) a quelle opération sur M correspond la multiplication a gauche $M \mapsto C_{ij,\mu}.M$?
2. Montrer que $\det(C_{ij,\mu}) = 1$ de sorte que les $C_{ij,\mu}$ appartiennent a $\mathrm{SL}_3(K)$. On va montrer que quand $i \neq j$ parcourent $\{1, \cdots, 3\}$ et μ parcourt $K^\times$ les matrices $C_{ij,\mu}$ engendrent $\mathrm{SL}_3(K)$.
3. Soit
$$M = (m_{ij})_{i,j \leqslant 3} = \begin{pmatrix} m_{11} & m_{12} & m_{13} \\ m_{21} & m_{22} & m_{23} \\ m_{31} & m_{32} & m_{33} \end{pmatrix} \in \mathrm{SL}_3(K)$$
une matrice de déterminant 1: on veut donc montrer que M peut s'écrire comme un produit de matrices (4.1). Montrer que quitte à remplacer M par sa multipliée à gauche par une (des) matrice(s) $C_{ij,\mu}$ convenable, on peut supposer succéssivement que
   (a) $m_{21} \neq 0$,
   (b) puis que $m_{11} = 1$,
   (c) et enfin que M est une matrice par blocs
   $$M = \begin{pmatrix} 1 & m_{12} & m_{13} \\ 0 & m_{22} & m_{23} \\ 0 & m_{32} & m_{33} \end{pmatrix}$$
   avec $m_{22}m_{33} - m_{23}m_{32} = 1$
4. Ensuite montrer qu'on peut se ramener au cas où M est de la forme:
$$M = \begin{pmatrix} 1 & m_{12} & m_{13} \\ 0 & 1 & m_{23} \\ 0 & 0 & 1 \end{pmatrix}$$
5. Et finalement, montrer que cette dernière matrice est un produit de matrices de la forme (4.1). Ainsi vous avez montré que $\mathrm{SL}_d(K)$ est engendré par les matrices de la forme (4.1).
6. Soient $i, j, k \in \{1, \cdots, 3\}$ tous distincts et $\mu \in K^\times$. Montrer l'égalité
$$[C_{ik,\mu}, C_{kj,1}] = C_{ij,\mu}$$
(ici pour A et B deux matrices inversibles on a noté $[A, B] := A.B.A^{-1}.B^{-1}$ leur commutateur; cf Exercice 3). Pour effectuer ce calcul on pourra par exemple considérer les endomorphismes
$$\mathcal{C}_{ij,\mu} : K^3 \mapsto K^3$$
dont les matrices dans la base canonique de K^3 sont les matrices $C_{ij,\mu}$ et regarder comment les $\mathcal{C}_{ij,\mu}$ transforment les vecteurs de cette base $\mathbf{e}_1^0 = (1, 0, 0),\ \mathbf{e}_2^0 = (0, 1, 0),\ \mathbf{e}_3^0 = (0, 0, 1)$.

7. En déduire que le groupe $\mathrm{SL}_3(K)$ est parfait: c'est a dire (cf. Exercice 3) qu'il est engendré par les commutateurs de ses éléments, ou en d'autres termes

$$\mathrm{SL}_3(K) = [\mathrm{SL}_3(K), \mathrm{SL}_3(K)] = \langle [A, B],\ A, B \in \mathrm{SL}_3(K)\rangle.$$

8. Soit $\rho : \mathrm{SL}_3(K) \mapsto \mathrm{GL}(V)$ un morphisme non-trivial (c'est à dire différent du morphisme constant $\underline{\mathrm{Id}_V}$) de $\mathrm{SL}_3(K)$ dans le groupe des automorphismes linéaires d'un K-espace vectoriel de dimension finie. Montrer qu'alors $\dim_K(V) > 1$. On pourra raisonner par l'absurde et utiliser l'hypothèse de dimension 1 pour construire un morphisme de $\mathrm{SL}_3(K)$ vers $K^\times$ et on pourra utiliser l'Exercice 3.

Remarque. Par la même méthode on peut montrer que pour $d \geqslant 3$, $\mathrm{SL}_d(K)$ est engendré par les matrices

$$C_{ij,\mu} = \mathrm{Id}_d + \mu.E_{ij},\ i \neq j \in \{1, \cdots, d\},\ \mu \in K^\times$$

et que ce groupe est parfait. Si $d = 2$ le groupe $\mathrm{SL}_2(K)$ est encore parfait sauf si $K = \mathbb{F}_2$ ou $\mathbb{F}_3$.

Réponses aux questions de l'Exercice 4 (répondre à l'intérieur de la boite)

1. On ajoute a la i-ieme ligne μ fois la j-ieme

2. La matrice $C_{ij,\mu}$ est soit triangulaire superieure soit triangulaire inferieure (suivant que $i < j$ ou $j < i$) et avec des 1 sur la diagonale. Son determinant vaut donc 1 (determinant des matrices de 3 blocs de tailles 1)

3. (a) La matrice M etant inversible sa premiere colonne est non-nulle. Si $m_{21} \neq 0$ on a fini. Si $m_{21} = 0$ on peut ajouter a la second ligne la premiere ou la troisieme suivant que m_{11} ou m_{31} est non-nul: cela veut dire multiplier par $C_{21,1}$ ou $C_{23,1}$
   (b) On multiplie par $C_{12,\mu}$ avec μ tel que $m_11 + \mu.m_{21} = 1$ (possible si $m_{21} \neq 0$)
   (c) On elimine m_{21} et m_{31} en multipliant par $C_{21,-m_{21}}$ et $C_{31,-m_{31}}$ (car $m_{11} = 1$). La nouvelle matrice est de determinant 1 (car on a multipliee l'originale par des matrices de determinant 1) et comme elle est sous forme de blocs $3 = 1 + 2$ on a

$$1 = 1 \times (m_{22}m_{33} - m_{23}m_{32})$$

4. La premiere colonne de la matrice $\begin{pmatrix} m_{22} & m_{23} \\ m_{32} & m_{33} \end{pmatrix}$ n'est pas identiquement nulle (a cause du determinant qui vaut 1). On recommence ce qu'on a fait a l'etape precedente en multipliand par des matrices de la forme $C_{ij,\mu}$ avec $i, j \in \{2, 3\}$: cela ne change pas la premiere colonne ni la premiere ligne.

5. On fait la remontada en mettant a zero m_{23} (on multiplie par $C_{23,-m_{23}}$) puis m_{13} et enfin sur la matrice obtenue on elimine m_{12} (on multiplie par $C_{12,-m_{12}}$) et on arrive a la matrice identite Id_3

6. Pour eviter un calcul a partir des relations de produits de matrices elementaires $E_{ij}.E_{kl}$ on suit l'indication. On suppose $i \neq j \neq k$ On a

$$C_{ij,\mu}\mathbf{e}^0_k = \mathbf{e}^0_k,\ k \neq j, C_{ij,\mu}\mathbf{e}^0_j = \mathbf{e}^0_j + \mu.\mathbf{e}^0_i$$

On a donc

$$C^{-1}_{ij,\mu} = C_{ij,-\mu}$$

Car

$$C_{ij,-\mu}\mathbf{e}^0_k = \mathbf{e}^0_k,\ k \neq j,\ C_{ij,-\mu}(\mathbf{e}^0_j + \mu.\mathbf{e}^0_i) = \mathbf{e}^0_j - \mu.\mathbf{e}^0_i + \mu.\mathbf{e}^0_i = \mathbf{e}^0_j.$$

On a

$$[C_{ik,\mu}, C_{kj,1}] = C_{ik,\mu}C_{kj,1}C_{ik,-\mu}C_{kj,-1}$$

On calcule l'image des trois vecteurs de la base canonique:

$$C_{ik,\mu}C_{kj,1}C_{ik,-\mu}C_{kj,-1}\mathbf{e}_i^0 = \mathbf{e}_i^0 = C_{ij,\mu}\mathbf{e}_i^0$$

(car l'indice i n'est jamais en seconde position dans $C_{ik,\pm\mu},\ C_{kj,\pm 1}$ et donc reste invariant). On a

$$\begin{aligned} C_{ik,\mu}C_{kj,1}C_{ik,-\mu}C_{kj,-1}\mathbf{e}_k^0 &= C_{ik,\mu}C_{kj,1}C_{ik,-\mu}\mathbf{e}_k^0 = C_{ik,\mu}C_{kj,1}(\mathbf{e}_k^0 - \mu\mathbf{e}_i^0) \\ &= C_{ik,\mu}(\mathbf{e}_k^0 - \mu\mathbf{e}_i^0) = \mathbf{e}_k^0 - \mu\mathbf{e}_i^0 + \mu\mathbf{e}_i^0 = \mathbf{e}_k^0 \\ &= C_{ij,\mu}\mathbf{e}_k^0 \end{aligned}$$

On a

$$\begin{aligned} C_{ik,\mu}C_{kj,1}C_{ik,-\mu}C_{kj,-1}\mathbf{e}_j^0 &= C_{ik,\mu}C_{kj,1}C_{ik,-\mu}(\mathbf{e}_j^0 - \mathbf{e}_k^0) = C_{ik,\mu}C_{kj,1}(\mathbf{e}_j^0 - (\mathbf{e}_k^0 - \mu\mathbf{e}_i^0)) \\ &= C_{ik,\mu}(\mathbf{e}_j^0 + \mathbf{e}_k^0 - \mathbf{e}_k^0 + \mu\mathbf{e}_i^0) = C_{ik,\mu}(\mathbf{e}_j^0 + \mu\mathbf{e}_i^0) = \mathbf{e}_j^0 + \mu\mathbf{e}_i^0 \\ &= C_{ij,\mu}\mathbf{e}_j^0 \end{aligned}$$

7. Le groupe $\mathrm{SL}_3(K)$ est engendre par les $C_{ij,\mu}$ et les $C_{ij,\mu}$ sont des commutateurs donc $\mathrm{SL}_3(K)$ est engendre par des commutateurs et donc contenu dans le sous-groupe des commutateur $[\mathrm{SL}_3(K), \mathrm{SL}_3(K)] \subset \mathrm{SL}_3(K)$.

8. Par l'absurde: soit $V = K\mathbf{e}_1$ un K-ev de dimension 1 ($\{\mathbf{e}_1\}$ est non-nul et defini une base de V)et $\rho : \mathrm{SL}_3(K) \to \mathrm{GL}(V)$ un morphisme de groupes. On a pour $g \in \mathrm{SL}_3(K)$

$$\rho(g)(\mathbf{e}_1) = \lambda(g)\mathbf{e}_1,\ \lambda(g) \in K$$

car comme V est de dimension 1, $\rho(g)(\mathbf{e}_1)$ est un multiple de $\mathbf{e}_1$. De plus $\lambda(g) \neq 0$ car $\rho(g)$ est inversible et $\lambda(g^{-1}) = \lambda(g)^{-1}$. Comme ρ est un morphisme de groupe, l'application

$$\lambda : \mathrm{SL}_3(K) \to K^\times$$

est un morphisme de groupes et comme $K^\times$ est commutatif et que $\mathrm{SL}_3(K)$ est parfait λ doit etre trivial: Exo 3. Ainsi pour que ρ soit non-trivial on doit avoir $\dim V > 1$.

Exercice 5. [Quaternions de Hamilton] Soit $\mathbb{C} = \mathbb{R} + \mathbb{R}.i,\ i^2 = -1$ le corps des nombres complexes et $M_2(\mathbb{C})$ l'espace des matrices 2×2 a coefficients dans $\mathbb{C}$; on note $\mathbf{0}$ la matrice nulle et Id la matrice identité. On considère dans $M_2(\mathbb{C})$, le $\mathbb{R}$-espace vectoriel

$$\mathbb{H} = \mathbb{R}.\mathrm{Id} + \mathbb{R}.I + \mathbb{R}.J + \mathbb{R}.K$$

avec

$$\mathrm{Id} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},\ J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

C'est l'espace des <u>quaternions de Hamilton</u> et un élément de cet ensemble

$$Z = t\mathrm{Id} + xI + yJ + zK,\ x, y, z, t \in \mathbb{R}$$

est appelé un quaternion. Le sous-espace $\mathbb{R}.\mathrm{Id}$ est appelle espace des <u>quaternions scalaires</u>.
Si Z est un quaternion (donc une matrice) on note $\mathrm{tr}(Z)$ sa trace et $\det(Z)$ son déterminant:

$$Z = \begin{pmatrix} a & b \\ c & d \end{pmatrix},\ \mathrm{tr}(Z) = a + d,\ \det(Z) = ad - bc.$$

1. Montrer que $\{\mathrm{Id}, I, J, K\}$ forme une base du $\mathbb{R}$-EV $\mathbb{H}$

2. Calculer
$$I^2,\ J^2,\ K^2,\ I.J,\ J.I,\ I.K,\ K.I,\ J.K,\ K.J.$$

3. En déduire que $\mathbb{H}$ est stable par produit dans $M_2(\mathbb{C})$; c'est donc une $\mathbb{R}$-algèbre. Montrer que $\mathbb{H}$ n'est pas commutative.

4. On note $\mathbb{H}^\times$ le groupe multiplicatif des quaternions inversibles. Soit $Z = t\mathrm{Id} + xI + yJ + zK$ un quaternion. Calculer $\det(Z)$ en fonction de t, x, y, z et montrer que $Z \in \mathbb{H}$ est inversible (comme matrice) si et seulement si $Z \neq \mathbf{0}$: on a donc $\mathbb{H}^\times = \mathbb{H} - \{\mathbf{0}\}$

   Remarque. Bien que tout élément non-nul soit inversible, $\mathbb{H}$ n'est PAS commutative et ce n'est donc pas un corps. On dit que $\mathbb{H}$ est une <u>algèbre à divisions</u>.

5. Les quaternions sont munis d'une "conjugaison complexe"
$$Z \mapsto \overline{Z} = t\mathrm{Id} - xI - yJ - zK$$
qui est $\mathbb{R}$-lineaire (admis). Montrer que
$$\ker(\mathrm{tr}) = \{Z \in \mathbb{H},\ Z + \overline{Z} = \mathbf{0}\} = \mathbb{R}.I + \mathbb{R}.J + \mathbb{R}.K.$$
Le sous-espace
$$\mathbb{H}_0 = \mathbb{R}.I + \mathbb{R}.J + \mathbb{R}.K$$
est appelé espace des quaternions <u>imaginaires</u>.

6. Montrer que pour tout quaternion Z on a
$$Z.\overline{Z} = \det(Z)\mathrm{Id}$$
et que pour Z' un autre quaternion, on a
$$\overline{Z.Z'} = \overline{Z'}.\overline{Z}.$$

7. Montrer que pour tout $Z \in \mathbb{H}$ il existe $b = b(Z), c = c(Z) \in \mathbb{R}$ tels que
$$Z^2 + b.Z + c\mathrm{Id} = \mathbf{0}$$
(on pourra par exemple exprimer $\overline{Z}$ comme combinaison linéaire a coefficients réels de Id et Z).

8. En déduire que le $\mathbb{R}$-EV
$$\mathbb{R}.\mathrm{Id} + \mathbb{R}.Z \subset \mathbb{H}$$
est un sous-anneau commutatif de $\mathbb{H}$ qu'on notera $\mathbb{R}[Z]$. Montrer que tout élément non-nul de $\mathbb{R}[Z]$ a son inverse contenu dans $\mathbb{R}[Z]$. Ainsi $\mathbb{R}[Z]$ est un corps (commutatif) de $\mathbb{H}$.

9. Que vaut $\dim_{\mathbb{R}}(\mathbb{R}[Z])$ si Z est un quaternion scalaire ? si Z n'est pas un quaternion scalaire?

10. Comme $\mathbb{R}[Z]$ est un corps contenu dans $\mathbb{H}$, ce dernier est un $\mathbb{R}[Z]$-espace vectoriel (la multiplication "par les scalaires" étant donnée par la multiplication dans $\mathbb{H}$).

    (a) Que vaut $\dim_{\mathbb{R}[Z]}(\mathbb{H})$ si Z est un quaternion scalaire ?

    (b) Montrer que si Z n'est pas un quaternion scalaire, il existe $I' \in \{I, J, K\}$ tel que $\{\mathrm{Id}, I'\}$ forme une $\mathbb{R}[Z]$-base de $\mathbb{H}$.

11. Le <u>centralisateur</u> de Z dans $\mathbb{H}$ est defini comme le sous-ensemble des éléments de $\mathbb{H}$ qui commutent avec Z:
$$\mathrm{Cent}(Z) := \{C \in \mathbb{H},\ C.Z = Z.C\}.$$
Montrer que $\mathrm{Cent}(Z)$ est un sous-anneau (non-nul) de $\mathbb{H}$ et que c'est également un $\mathbb{R}[Z]$-EV.

12. Montrer que si Z n'est pas un quaternion scalaire on a
$$\mathrm{Cent}(Z) = \mathbb{R}[Z].$$
Pour cela on pourra (si on veut) montrer que, pour $C \in \mathrm{Cent}(Z)$ un élément non-nul du centralisateur le $\mathbb{R}[Z]$-EV
$$\mathbb{R}[Z] + \mathbb{R}[Z].C \subset \mathbb{H}$$
est un anneau commutatif; on en déduira que $\mathbb{R}[Z] + \mathbb{R}[Z].C = \mathbb{R}[Z]$.

Réponses aux questions de l'Exercice 5 (répondre à l'intérieur de la boite)

1. Soit
$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = t\mathrm{Id} + xI + yJ + zK = \begin{pmatrix} t+ix & y+iz \\ -y+iz & t-ix \end{pmatrix},\ x, y, z, t \in \mathbb{R}$$
On a
$$t + ix = 0 \Rightarrow t = x = 0,\ y + iz \Rightarrow y = z = 0.$$
La famille est libre et par definition elle engendre $\mathbb{H}$ c'est donc une base.

2. On calcule
$$I^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -\mathrm{Id},\ J^2 = -\mathrm{Id},\ K^2 = -\mathrm{Id},$$
$$IJ = -JI = K,\ I.K = I^2.J = -J,\ K.I = IJI = -JI^2 = J = -IK,$$
$$JK = JIJ = -J^2I = I,\ KJ = IJJ = -I = -JK$$

3. Les produits des generateurs de $\mathcal{H}$ sont encore dans $\mathcal{H}$ donc (par distributivite) un produit de CL de ces generateurs est encore un CL d'element de $\mathbb{H}$. ainsi $\mathbb{H}$ est stable par produit. Comme $IJ = -JI$ l'agebre $\mathbb{H}$ n'est pas commutative.

4. On a
$$\det(Z) = \det \begin{pmatrix} t+ix & y+iz \\ -y+iz & t-ix \end{pmatrix} = (t+ix)(t-ix) - (y+iz)(-y+iz)$$
$$= |t+ix|^2 + |y+iz|^2 = t^2 + x^2 + y^2 + z^2.$$
ainsi (comme x, y, z, t sont des reels)
$$\det Z = 0 \Longleftrightarrow x = y = z = t = 0 \Longleftrightarrow Z = \mathbf{0}$$
et si $Z \neq 0$ est inversible dans $M_2(\mathbb{C})$car son determinant est non-nul:
$$\mathbb{H}^{\times} = \mathbb{H} - \{\mathbf{0}\}$$

5.
$$\ker(\mathrm{tr}) = \{Z = \begin{pmatrix} t+ix & y+iz \\ -y+iz & t-ix \end{pmatrix},\ \mathrm{tr}(Z) = t+ix+t-ix = 2t = 0\}$$
$$= \mathbb{R}.I + \mathbb{R}.J + \mathbb{R}.K$$

On a aussi
$$Z + \overline{Z} = t\mathrm{Id} + xI + yJ + zK + t\mathrm{Id} - xI - yJ - zK = 2t\mathrm{Id} = \mathbf{0} \Longleftrightarrow t = 0.$$

6. soit $Z = t\mathrm{Id} + Z_0$ avec $Z_0 = xI + yJ + zK \in \mathbb{H}_0$. On a
$$Z\overline{Z} = (t\mathrm{Id} + Z_0)(t\mathrm{Id} - Z_0) = t^2\mathrm{Id} + t(Z_0 - Z_0) - Z_0^2$$
$$= t^2\mathrm{Id} - (-x^2\mathrm{Id} - y^2\mathrm{Id} - z^2\mathrm{Id} + xy(IJ + JI) + xz(IK + KI) + yz(JK + KJ))$$
$$= (t^2 + x^2 + y^2 + z^2)\mathrm{Id} + \mathbf{0} = \det(Z)\mathrm{Id}$$
car $IJ = -JI$ etc... La relation
$$\overline{ZZ'} = \overline{Z}'\overline{Z}$$
est obtenue par un calcul similaire.

7. Si $Z = \mathbf{0}$ on prend $b = c = 0$. Sinon on a
$$\overline{Z} = t\mathrm{Id} - (Z - t\mathrm{Id}) = 2t\mathrm{Id} - Z.$$
Comme
$$\det(Z)\mathrm{Id} = Z\overline{Z} = Z(2t\mathrm{Id} - Z) = 2tZ - Z^2$$
et donc
$$Z^2 - 2tZ + \det(Z)\mathrm{Id} = \mathbf{0}$$
$$b(Z) = -2t,\ c(Z) = \det(Z) = t^2 + x^2 + y^2 + z^2.$$

8. On a
$$\mathrm{Id}^2 = \mathrm{Id},\ \mathrm{Id}.Z = Z.\mathrm{Id} = Z, Z^2 = -\det(Z)\mathrm{Id} + 2tZ.$$
tous ces produits sont contenus dans $\mathbb{R}\mathrm{Id} + \mathbb{R}Z$ et un produits de deux CL de ces elements est encore contenu dans $\mathbb{R}\mathrm{Id} + \mathbb{R}Z$. De plus Id et Z commutent entre eux et avec eux memes donc les CLs de ces elements commutent entre elles. L'anneau est donc commutatif.

Soit $Z' = x\mathrm{Id} + yZ \in \mathbb{R}\mathrm{Id} + \mathbb{R}Z$ non nul. Alors $\det(Z') \neq 0$ et on a
$$\mathrm{Id} = -\frac{1}{\det Z'}(Z'^2 + b'Z') = -\frac{1}{\det Z'}(Z' + b'\mathrm{Id}).Z'$$
et donc
$$Z'^{-1} = -\frac{1}{\det Z'}(Z' + b'\mathrm{Id}) \in \mathbb{R}\mathrm{Id} + \mathbb{R}\mathbb{Z}.$$

9. Si Z est un scalaire ssi $Z = \alpha\mathrm{Id}$ est proportionnel a la matrice identite et $\mathbb{R}[Z] = \mathbb{R}\mathrm{Id}$ est de dimension 1. Sinon Z n'est pas proportionel a Id et la famille $\{\mathrm{Id}, Z\}$ est libre et $\mathbb{R}[Z]$ est un $\mathbb{R}$-ev de dimension 2.

10. Si Z est un scalaire $\mathbb{R}[Z] = \mathbb{R}.\mathrm{Id} \simeq \mathbb{R}$ et la dimension est 4.

Sinon $Z = t\mathrm{Id} + xI + yJ + zK$ avec x, y, z non-tous nuls. Soit $I' \in \{I, J, K\}$ tel que $I' \not\in \mathbb{R}\mathrm{Id} + \mathbb{R}Z$ (si I' n'existe pas $\mathbb{H}$ serait contenu dans $\mathbb{R}\mathrm{Id} + \mathbb{R}Z$ et de $\mathbb{R}$-dimension 2). Supposons qu'il existe $U, V \in \mathbb{R}[Z]$ tel que
$$U\mathrm{Id} + V.I' = U + V.I' = \mathbf{0}.$$
Si $U = 0$ alors on a $V.I' = \mathbf{0}$ et donc $V.I'.I' = -V = \mathbf{0}$ et $V = \mathbf{0}$.

Sinon on a $V.I' = U$ et donc $-V = V.I'.I' = U.I'$: on a donc $V \neq \mathbf{0}$ car $U \in \mathbb{R}[Z]$ etant non-nul doit etre inversible et I' est une matrice inversible donc $-V$ est inversible.

On a vu qu'alors $V^{-1} \in \mathbb{R}[Z]$ et donc

$$I' = V^{-1}.U \in \mathbb{R}[Z]$$

car $\mathbb{R}[Z]$ est un anneau. Cela contredit le choix de I'. La famille $\{\mathrm{Id}, I'\}$ est donc $\mathbb{R}[Z]$-libre.

Le $\mathbb{R}[Z]$-ev engendre par $\{\mathrm{Id}, I'\}$ est egal a

$$\mathbb{R}[Z]\mathrm{Id} + \mathbb{R}[Z]I' = \mathbb{R}[Z] + \mathbb{R}[Z]I' = \mathbb{R}.\mathrm{Id} + \mathbb{R}.Z + \mathbb{R}.I' + \mathbb{R}.Z.I'.$$

c'est egalement un $\mathbb{R}$-ev de $\mathbb{H}$ engendre par $\{\mathrm{Id}, Z, I', Z.I'\}$. Montrons que $\{\mathrm{Id}, Z, I', Z.I'\}$ est libre: cela montrera que cet espace est de $\mathbb{R}$ dimension 4 et donc egal a $\mathbb{H}$. Supposons que

$$t\mathrm{Id} + xZ + yI' + z.Z.I' = \mathbf{0},\ t, x, y, z \in \mathbb{R}.$$

On a alors

$$U.\mathrm{Id} + V.I' = \mathbf{0},\ U = t\mathrm{Id} + xZ,\ V = yI' + z.Z \in \mathbb{R}[Z].$$

Comme $\{\mathrm{Id}, I'\}$ est $\mathbb{R}[Z]$-libre on doit avoir $U = V = \mathbf{0}$ et comme Z n'est pas sclaire cela implique que $t = x = y = z = 0$.

11. Soient $C, C' \in \mathrm{Cent}(Z)$, on a

$$(C - C')Z = CZ - C'Z = ZC - ZC' = Z(C - C'),\ C.C'.Z = CZC' = ZCC'$$

et de plus $\mathrm{Id} \in Cent(Z)$ et donc le critere de sous-anneau est satisfait: $Cent(Z)$ est un sous-anneau de $\mathbb{H}$.

De plus

$$\mathbb{R}[Z] = \mathbb{R}\mathrm{Id} + \mathbb{R}.Z \subset Cent(Z)$$

car Id et Z commutent avec Z. Cette inclusion fait de $Cent(Z)$ un $\mathbb{R}[Z]$-EV.

12. Supposons que Z ne soit pas un scalaire (sinon $Cent(Z) = \mathbb{H}$).

Soit $C \in Cent(Z) - \{0\}$ alors comme C commute avec Id et Z, il commute avec toute element de $\mathbb{R}[Z]$; considerons

$$\mathbb{R}[Z] + \mathbb{R}[Z]C \subset \mathbb{H}.$$

C'est un $\mathbb{R}[Z]$-ev de $\mathbb{H}$.

Soit $U + VC, U' + V'C \in \mathbb{R}[Z] + \mathbb{R}[Z]C$ par commutativite on a

$$(U + VC)(U' + V'C) = UU' + UV'C + VCU' + VCV'C = UU' + VV'C^2 + (UV' + VU')C$$

et on a vu que $C^2 \in \mathbb{R} + \mathbb{R}C$ et donc $VV'C^2 \in \mathbb{R}[Z]C$. On en deduit que $\mathbb{R}[Z] + \mathbb{R}[Z]C$ est stable par produit et c'est donc un sous-anneau de $\mathbb{H}$.

De plus il est commutatif car $\mathbb{R}[Z]$ etant commutatif U, U', V, V' commutent et donc

$$(U + VC)(U' + V'C) = (U' + V'C)(U + VC).$$

Le $\mathbb{R}[Z]$-ev $\mathbb{R}[Z] + \mathbb{R}[Z]C$ est un sous-$\mathbb{R}[Z]$-ev de dimension au moins 1 (car il contient $\mathbb{R}[Z]$ qui est de $\mathbb{R}[Z]$-dimension 1) est contenu dans le $\mathbb{R}[Z]$-ev $\mathbb{H}$ qui est de dimension 2. Si il etait de dimension 2 on aurait

$$\mathbb{R}[Z] + \mathbb{R}[Z]C = \mathbb{H}$$

et $\mathbb{H}$ serait commutatif ce qui n'est pas le cas.

Ainsi $\mathbb{R}[Z] + \mathbb{R}[Z]C$ est de dimension 1 et doit donc etre egal a $\mathbb{R}[Z]$: cela implique que

$$C \in \mathbb{R}[Z]$$

et donc que

$$Cent(Z) = \mathbb{R}[Z].$$