2019-2020

Algèbre L3B

Correction de l'examen : Janvier 2019

Tout document et appareil électronique (calculatrice, téléphone portable) est interdit.

Barème indicatif : Cours : /1,5, Ex 1 : /5,5, Ex 2 : /7, Ex 3 : /7

Question de cours. Soit E un $\mathbb{R}$-espace vectoriel de dimension finie.

1. Enoncer le théorème de décomposition des noyaux.
2. Soit f un endomorphisme de E. Donner une condition nécessaire et suffisante sur le polynôme minimal μ_f de f pour que f soit diagonalisable.
3. Le démontrer en utilisant le théorème de décomposition des noyaux.

Exercice 1. Soit $\alpha, \beta \in \mathbb{C}$. On considère l'endomorphisme f de $E = \mathbb{R}^4$ dont la matrice dans la base canonique est donnée par

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ -1 & 1 & 1 & 0 \\ -2 & \beta & 2 & \alpha \end{pmatrix}$$

1. (a) Quel est le polynôme caractéristique de f ?
   La matrice étant triangulaire inférieure, on a sans calcul que $\chi_f = X(X-1)^2(X-\alpha)$.

   (b) Donner sans calculs les polynômes minimaux possibles pour f ? (on pourra distinguer les cas où $\alpha = 0$ et $\alpha = 1$.)
   Si $\alpha \neq 0, 1$, alors le polynôme minimal est un diviseur de χ_f ayant les mêmes racines. Il y a donc deux possibilités $X(X-1)(X-\alpha)$ et $X(X-1)^2(X-\alpha)$.
   Si $\alpha = 0$, alors on a 4 possibilités $X(X-1)$, $X^2(X-1)$, $X(X-1)^2$ et $X^2(X-1)^2$.
   Si $\alpha = 1$ on a 3 possibilités qui sont $X(X-1)$, $X(X-1)^2$, et $X(X-1)^3$

(c) Quel est le rang de la matrice $f - \mathrm{Id}_E$?

La matrice de $f - \mathrm{Id}_E$ est donnée par

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ -2 & \beta & 2 & \alpha - 1 \end{pmatrix}$$

Comme les lignes 2 et 3 sont multiples, et que le reste est échelonné, on voit immédiatement que le rang est 2.

2. On suppose tout d'abord que $\alpha \neq 0$ et $\alpha \neq 1$.

(a) Quel est alors le polynôme minimal de f ?

Par la question précédente, on déduit que $\dim \mathrm{Ker}(f - \mathrm{Id}_E)$ est de dimension 2. Comme la multiplicité de la valeur propre 1 dans le polynôme caractéristique est 2 si $\alpha \neq 1$, on a alors que le sous-espace caractéristique E_1 est égale au sous-espace propre V_1, ce qui signifie que la multiplicité de $(X - 1)$ dans μ_f est 1. Puisque $\alpha \neq 0, 1$, le polynôme minimal est donc $X(X - 1)(X - \alpha)$.

(b) L'endomorphisme f est-il diagonalisable ?

Le polynôme minimal étant scindé à racines simples, f est diagonalisable.

3. On suppose dans cette question que $\alpha = 0$. Montrer que f est diagonalisable si et seulement si $\beta = 2$.

Les calculs précédents sont valables pour $\alpha = 0$. On a donc encore $E_1 = V_1$.
La matrice est donc diagonalisable si et seulement si $V_0 = \mathrm{Ker} f$ est de dimension 2 (qui est la multiplicité de 0 dans χ_f), autrement dit si le rang de f est 2, c'est à dire si et seulement si $\beta = 2$.
On peut aussi calculer $P(M) = M^2 - M$ (où $P = X(X - 1)$), et voir que P annule f si et seulement si $\beta = 2$.

4. On suppose maintenant que $\alpha = 1$.

(a) Montrer que f n'est pas diagonalisable.

On a toujours $\dim \mathrm{Ker}(f - \mathrm{Id}_E) = 2$, mais cette fois la multiplicité de 1 dans χ_f est 3, V_1 est donc strictement inclus dans E_1, et f n'est pas diagonalisable.

(b) On suppose $\beta = 0$, donner alors une base de E dans laquelle la matrice de f est

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Un calcul direct donne $\mathrm{Ker} f = \mathrm{vect}(e_2 - e_3 + 2e_4)$,
$\mathrm{Ker}(f - \mathrm{Id}_E) = \mathrm{vect}(e_4, e_1 + e_2 + e_3)$ et
$\mathrm{Ker}(f - \mathrm{Id}_E)^2 = \mathrm{vect}(e_4, e_1 + e_2 + e_3, e_3)$. On pose alors $v_1 = e_2 - e_3 + 2e_4$, $v_4 = e_3$, $v_3 = f(v_4) - v_4 = 2e_4$. Enfin, en posant $v_2 = e_1 + e_2 + e_3$, on obtient que (v_1, v_2, v_3, v_4) est une base cherchée.

5. On suppose toujours que $\alpha = 1$. On pose $g = 2f - f^2$ et $h = f^2 - f$.
   (a) Montrer que $g(g - \mathrm{Id}_E)$ est l'endomorphisme nul. Que peut-on en déduire pour g ?
   On a $g(g - \mathrm{Id}_E) = f(2\mathrm{Id}_E - f)(2f - f^2 - \mathrm{Id}_E) = (f - 2\mathrm{Id}_E)f(f - \mathrm{Id}_E)^2$. Or $X(X-1)^2$ est le polynôme minimal de f, on a donc $g(g - \mathrm{Id}_E) = 0$, autrement dit le polynôme $X(X-1)$ annule g. Comme il est scindé à racines simples, g est diagonalisable.
   (b) Calculer $g + h$ et h^2 en fonction de f.
   On a $g + h = f$, et $h^2 = f^2(f - \mathrm{Id}_E)^2 = 0$.
   (c) En déduire la décomposition de Dunford de f.
   g est diagonalisable, h est nilpotent, $g + h = f$, et enfin ils commutent car ce sont des polynômes en f, la décomposition $f = g + h$ est donc la décomposition de Dunford de f.

Exercice 2. Soit p un nombre entier et $k = \mathbb{Z}/p\mathbb{Z}$. Soit P un polynôme de $k[X]$ irréductible.

1. (Question de cours) Montrer que k est un corps si et seulement si p est un nombre premier.
2. On suppose maintenant que p est premier.
   (a) Montrer que tout polynôme Q de $k[X]$ est soit divisible par P soit premier avec P.
   Si $Q \in k[X]$ n'est pas premier avec P, alors ils ont un diviseur commun (non inversible), or P est irréductible, donc ce diviseur commun est forcément P.
   (b) En déduire que $k[X]/(P)$ est un corps.
   On raisonne comme dans la question 1.. Soit Q un polynôme de $k[X]$ tel que sa classe dans $k[X]/(P)$ est non nulle, ceci veut dire que P ne divise pas Q. Par le (a), on en déduit que Q est premier avec P. Par Bézout, on a donc $AP + BQ = 1$ avec $A, B \in k[X]$. Autrement dit $\bar{B}\bar{Q} = \bar{1}$ dans $k[X]/(P)$. Donc $\bar{Q}$ est inversible. On a donc montré que tout élément non nul de $k[X]/(P)$ est inversible. Ceci montre que c'est un corps.
   NB : on peut aussi utiliser le fait qu'un idéal engendré par un élément irréductible dans un anneau principal est maximal.
   (c) Quelle est sa caractéristique ?
   La caractérisitique est le noyau de l'unique morphisme $\mathbb{Z} \to K$. Remarquons que l'image de p par ce morphisme est nulle, car nulle dans k, donc dans $k[X]$ et donc dans $k[X]/(P)$. Donc la caractéristique de K est un diviseur de p. Comme p est premier, c'est p.

On considère dans le reste de l'exercice le cas $p = 2$.

5. (a) Justifier que le polynôme $P(X) = X^3 + X^2 + 1 \in k[X]$ est irréductible, et que donc $K := k[X]/(P)$ est un corps.
   On calcule $P(0) = 1$ et $P(1) = 1$, donc ce polynôme n'a pas de racines. Comme il est de degré 3, s'il était réductible il aurait au moins une racine. K est un corps par la question 2.(b)

   (b) Montrer que le corps K contient exactement 8 éléments.
   Deux polynômes de $k[X]$ ont la même image dans K si et seulement si ils ont même reste par la division euclidienne par P. Comme P est de degré 3, l'ensemble des restes possibles est l'ensemble des polynômes de degré ≤ 2 de $k[X]$. Comme k contient 2 éléments, ceci donne 8 possibilités qui sont

$$0, 1, X, X+1, X^2, X^2+1, X^2+X, X^2+X+1.$$

   (c) Combien de groupe multiplicatif $(K^\times, .)$ contient-il d'éléments ? Est-il cyclique ?
   Comme K est un corps, le groupe des inversibles de K est $K \setminus \{0\}$. On obtient donc 7 éléments. 7 étant premier, le groupe est nécessairement cyclique.

6. On note $\pi : k[X] \to K$ la projection naturelle.

   (a) Montrer que l'on a l'égalité $\pi(X)^2\pi(X+1) = \pi(1)$ dans K.
   On a $\pi(P) = 0$, comme π est un morphisme d'anneau, cela donne $\pi(x)^3 + \pi(X)^2 + \pi(1) = 0$. Enfin comme $\pi(1) = 1 = -1$ (on est dans $\mathbb{Z}/2\mathbb{Z}$), on obtient l'égalité voulue.

   (b) En déduire l'inverse de $\pi(X^2)$, puis l'inverse de $\pi(X^4+1)$.
   On a donc $\pi(X^2)^{-1} = \pi(X+1)$. Pour X^4+1, on doit tout d'abord effectuer la division euclidienne de X^4+1 par P. On obtient $X^4 + 1 = (X+1)P + (X^2+X)$. On a donc $\pi(X^4+1) = \pi(X^2+X)$. Son inverse est alors $\pi(X)$.

7. On définit $Q = X^4 + 1$ dans $k[X]$.

   (a) Calculer le pgcd de P et $Q = X^4+1$ dans $k[X]$.
   On a déjà $X^4 + 1 = (X+1)P + (X^2+X)$. Puis $P = X(X^2+X) + 1$. On obtient alors

$$1 = P - X(X^2+X) = P - X((X^4-1) - (X+1)P)) = (X^2+X+1)P - X(X^4-1),$$

   donc P et Q sont premiers entre eux, leur pgcd est 1. (On peut aussi conclure avec le fait que Q est inversible dans $k[X]/(P)$.)

   (b) En déduire que l'on a un isomorphisme d'anneaux

$$\Phi : k[X]/(PQ) \to k[X]/(P) \times k[X]/(Q).$$

   P et Q étant premiers entre eux, c'est le théorème des restes chinois pour les polynômes.

(c) Calculer l'antécédent de $(\pi(X), \pi_2(X+1))$ par Φ où π_2 est la projection canonique $k[X] \to k[X]/(Q)$.
Un antécédent de $(\pi(X), \pi_2(X+1))$ est donné par $(X+1)AP + XBQ$ où $AP + BQ = 1$. On obtient donc

$$(X+1)(X^5+X+1) - X(X^5-X) = X^5+1$$

8. (a) Montrer que l'application

$$\begin{aligned} K^\times \times K &\longrightarrow K \\ (A, B) &\mapsto AB \end{aligned}$$

définit une action de $K^\times$ sur K.
On a $(AA').B = A.(A'.B)$ car la multiplication est associative, et $1.B = B$. C'est donc une action.

(b) Combien cette action a-t-elle d'orbites ? Est-elle transitive ?
L'orbite de 0_K est $\{0_K\}$. L'orbite de 1_K contient tous les autres éléments car tous les éléments non nuls sont inversibles donc tout éléments non nul s'écrit $A = A.1_K$ avec $A \in K^\times$. On a donc deux orbites, l'action n'est pas transitive.

(c) L'action est-elle fidèle ?
Soit $A \in K^\times$ tel que pour tout $B \in K$, $AB = B$, alors c'est vrai pour $B = 1_K$, et on en déduit que $A = 1_K$. L'action est donc fidèle.

(d) On note $\varphi : K^\times \to \mathfrak{S}_8$ le morphisme associé à l'action. Montrer que $\varphi(\pi(X))$ est un 7-cycle.
φ est un morphisme de groupe. L'ordre de $\pi(X)$ est 7, car l'ordre du groupe $K^\times$ est 7. L'ordre de $\varphi(\pi(X))$ est donc un diviseur de 7. Ce n'est pas 1, car sinon $\varphi(\pi(X))$ serait dans le noyau, et φ est injective (l'action est fidèle). C'est donc 7. Les seuls éléments d'ordre 7 de $\mathfrak{S}_8$ sont des 7-cycles, on donc la conclusion.

Exercice 3. On rappelle que toute matrice de $O_2(\mathbb{R})$ est de la forme

$$R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}, \text{ avec } \theta \in [0, 2\pi[\quad \text{ou } S_\varphi = \begin{pmatrix} \cos\varphi & \sin\varphi \\ \sin\varphi & -\cos\varphi \end{pmatrix}$$

et qu'on a les relations suivantes pour tous $\theta, \theta', \varphi, \varphi' \in [0n2\pi[$

$$R_\theta R_{\theta'} = R_{\theta+\theta'},\ S_\varphi R_\theta = S_{\varphi-\theta},\ R_\theta S_\varphi = S_{\theta+\varphi} \text{ et } S_\varphi S_{\varphi'} = R_{\varphi-\varphi'}.$$

1. (Question de cours) Montrer que $SO_2(\mathbb{R})$ est un groupe abélien isomorphe à $(\mathcal{U}, .)$ où $\mathcal{U} = \{z \in \mathbb{C}^*, |z| = 1\}$.
On considère l'application $\Phi : SO_2(\mathbb{R}) \to \mathcal{U}$ qui à R_θ associe $e^{i\theta}$. Cette application est clairement une bijection, car l'angle d'une rotation est uniquement défini à 2π-près, ainsi que l'argument d'un nombre complexe. Comme de plus

$$\Phi(R_\theta R_{\theta'}) = \Phi(R_{\theta+\theta'}) = e^{i(\theta+\theta')} = e^{i\theta}e^{i\theta'} = \Phi(R_\theta)\Phi(R_{\theta'}),$$

c'est un morphisme de groupes.

   (a) Montrer que que G est isomorphe au sous-groupe

$$\mathcal{U}_n = \{z \in \mathbb{C}^* |\ z^n = 1\}.$$

   Par le théorème de Lagrange, tous les éléments de G vérifient $R^n = \mathrm{Id}$, donc s'envoie sur des racines n-ième de l'unité par l'isomorphisme Φ. Puisqu'il y a n racines de l'unité distinctes, l'image de G par Φ est exactement $\mathcal{U}_n$.

   (b) En déduire que G est cyclique.
   Le groupe $\mathcal{U}_n$ est engendré par $e^{\frac{2i\pi}{n}}$ car toute racine n-ième de 1 est de la forme $e^{\frac{2ik\pi}{n}}$.

2. Soit G est sous-groupe abélien de $O_2(\mathbb{R})$ qui n'est pas entièrement contenu dans $SO_2(\mathbb{R})$.

   (a) Montrer qu'il existe φ tel que $G = \langle S_\varphi \rangle$ ou $G = \langle R_\pi, S_\varphi \rangle$.
   Soit G non inclus dans SO_2, alors G contient un S_φ pour un certain φ. Si $G = G = \langle S_\varphi \rangle$, alors G est bien abélien car cyclique et fini car l'ordre de S_φ est 2. Si G contient un R_θ, $\theta \neq 0$, alors comme G est abélien, R et S doivent commuter, c'est à dire que l'on doit avoir

$$\varphi - \theta = \varphi + \theta \ \mathrm{mod} 2\pi$$

   Ceci implique que $\theta = \pi$. Comme R_π a ordre 2, ainsi que S_φ et qu'ils commutent, on en déduit que $G = \langle R_\pi, S_\varphi \rangle$ a 4 éléments qui sont $\{\mathrm{Id}, R, S, RS\}$ et qu'il est commutatif.
   Enfin, si G contient deux éléments S_φ et $S_{\varphi'}$ distincts, alors il contient leur produit donc une rotation d'angle non nul, et on est ramené au cas précédent, ce qui est une contradiction.

   (b) Le groupe $G = \langle R_\pi, S_\varphi \rangle$ est-il cyclique ? Montrer qu'il est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
   Le groupe $G = \langle R_\pi, S_\varphi \rangle$ n'est pas cyclique, en effet il contient 4 éléments qui sont tous d'ordre ≤ 2 puisqu'on a $R_\pi S_\varphi = S_{\varphi+\pi}$. Comme R et S commutent, tout élément de de G s'écrit de la forme $R^k S^\ell$. L'application $f : G \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ qui envoie $R^k S^\ell$ sur $(\bar{k}, \bar{\ell})$ est un morphisme de groupes. En effet, $f(R^k S^\ell R^i S^j) = f(R^{k+i} S^{\ell+j}) = (\overline{k+i}, \overline{\ell+j}) = (\bar{k}, \bar{\ell}) + (\bar{i}, \bar{j})$. Elle est clairement surjective. Par ailleurs comme R, S et RS ont ordre 2, elle est injective. C'est donc un isomorphisme de groupes.

Dans la suite de l'exercice, E désigne un $\mathbb{R}$-espace vectoriel de dimension 3.

4. Soit f une isométrie positive de E.

   (a) Montrer que si F est un sous-espace stable par f, alors $F^\perp$ est aussi stable par f.

   Soit $x \in F^\perp$, et soit $y \in F$. Comme f est une isométrie, elle est en particulier inversible, donc $y = f(y')$ pour un certain y' dans F. Alors on a $\langle f(x), y\rangle = \langle f(x), f(y')\rangle = \langle x, y'\rangle = 0$. Donc $f(x)$ est dans $F^\perp$.

   (b) Montrer que si λ est une valeur propre de f, alors $\lambda = \pm 1$.

   Soit Λ un valeur propre de f, notons x un vecteur propre associé. On a alors $\langle x, x\rangle = \langle f(x), f(x)\rangle = \lambda^2\langle x, x\rangle$. Comme x est non nul, $\langle x, x\rangle \neq 0$ on a donc $\lambda^2 = 1$, ce qui implique $\lambda = \pm 1$.

5. On suppose de plus que $f^2 \neq \mathrm{Id}_E$.

   (a) Montrer que f a une valeur propre (réelle) et notons $V = \mathrm{vect}(v)$ le sous-espace engendré par un vecteur propre associé.

   Le polynôme caractéristique de f est un polynôme à coefficient réels de degré 3, il a donc au moins une racine réelle. Il a donc au moins une valeur propre réelle.

   (b) Montrer que f restreint au sous-espace $V^\perp$ est une isométrie de $V^\perp$.

   Comme V est stable par f, on en déduit par la question précédente que $V^\perp$ est stable par f. Par ailleurs pour tout x, y dans $V^\perp$, on a $\langle f(x), f(y)\rangle = \langle x, y\rangle$ donc l'endomorphisme restreint est aussi une isométrie.

   (c) Montrer qu'il existe une base orthonormée directe $\mathcal{B}$ et un unique $\theta \in]0, \pi[\cup]\pi, 2\pi[$ tels que la matrice de f dans $\mathcal{B}$ est de la forme :

$$\begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

   Soit (v_1, v_2) une base orthonormée de $V^\perp$. Soit $v_3 \in \mathrm{vect}(v)$ de norme 1. Alors la base (v_1, v_2, v_3) est une base orthonormée. Quitte à changer le sens de v_3, on peut supposer qu'elle est directe. Comme les sous-espaces $\mathrm{vect}(v_1, v_2)$ et $\mathrm{vect}(v_3) = V$ sont stables, la matrice de f dans cette base est de la forme :

$$\begin{pmatrix} A & & 0 \\ & & 0 \\ 0 & 0 & \lambda \end{pmatrix}$$

   avec A de la forme R_θ si $f_{|_{V^\perp}}$ est positif, ou S_φ s'il est négatif. Si $\lambda = -1$, alors comme f est positif, on a forcément $A = S_\varphi$. Mais alors la matrice est d'ordre 2 ce qui est contraire à l'hypothèse. On a donc $\lambda = 1$ et alors $A = R_\theta$. Enfin, comme $f^2 \neq \mathrm{Id}_E$, on a $R_\theta^2 \neq I_2$, ce qui exclut $\theta = 0$ et $\theta = \pi$.

(d) En déduire que $V = V_1(f)$ est le sous-espace propre associé à la valeur propre 1 et que la seule droite vectorielle stable par f est V.

Le polynôme caractéristique de la matrice est $(X-1)(X^2+2\cos\theta+1)$ avec $\theta \neq 0, \pi$, il a donc une unique racine réelle. La multiplicité de 1 étant 1, on a $V_1(f) = V$. De plus avoir une droite stable par f équivaut à avoir un vecteur propre. Les seuls vecteurs propres sont les vecteurs non nuls de V.

6. Soit H un sous-groupe abélien fini non réduit à $\{\mathrm{Id}_E\}$ de $SO(E)$ n'ayant aucun élément d'ordre 2. On fixe $f \neq \mathrm{Id}_E$ un élément de H. On note $V = V_1(f)$ et $W = V^\perp$.

(a) Montrer que pour tout $h \in H$, V et W sont stables par h.

Soit $v \in V$, alors $f(h(v)) = h(f(v)) = h(v)$, donc $h(v)$ est dans V. Comme V est stable, W est aussi stable par h.

(b) En déduire que si $h \neq \mathrm{Id}_E$, alors $V = V_1(h)$.

Comme $h^2 \neq \mathrm{Id}_E$, par la question précédente, on en déduit que $V = V_1(h)$ car h a une unique droite stable.

(c) Montrer que l'ensemble H_W des $h_{|_W}$ où $h \in H$ est un sous-groupe abélien fini de $SO(W)$.

Par la question 4.(c), pour tout h, $h_{|_W}$ est une isométrie positive de W. L'ensemble H_W est donc un sous groupe fini de $SO(W)$. Comme H est abélien, H_W aussi.

(d) En utilisant la question 1., déduire que H est cyclique.

Par la question 1., on en déduit que H_W est cyclique. Notons g un générateur. Alors il existe $h \in H$ avec $h_{|_W} = g$. Soit h' un élément de H. Alors il existe $n \in \mathbb{Z}$ tel que $h'_{|_W} = g^n$. Soit $x \in E$, on a alors $x = v + w$ avec $v \in V$ et $w \in W$. De plus comme $V \subset V_1(h)$ pour tout h' (ils sont égaux pour $h' \neq \mathrm{Id}_E$ et strictement inclus pour $h' = \mathrm{Id}_E$), on a alors

$$h^n(x) = h^n(v) + h^n_{|_W}(w) = v + h'_{|_W}(w) = h'(v+w) = h'(x),$$

autrement dit $h^n = h'$, et H est cyclique.