Devoir Surveillé n° 9 (3h)

La présentation, la lisibilité, l'orthographe, la qualité de la rédaction, la clarté, la précision et la concision des raisonnements entreront pour une part importante dans l'appréciation des copies.

Les candidats sont invités à encadrer dans la mesure du possible les résultats de leurs calculs.

L'usage de tout document et de tout matériel électronique est interdit. Notamment, les téléphones portables doivent être éteints *et* rangés.

Problème – Invariants de similitude et réduction de Frobenius

Le but de ce problème est de définir une suite (finie) de polynômes associée à une matrice ou à une endomorphisme, permettant de répondre au problème de la similitude, dans le sens où cette suite caractérise la classe de similitude. En d'autres termes, deux matrices vont avoir des suites égales, si et seulement si elles sont équivalentes. Cette suite de polynômes est appelée suite des invariants de similitude.

Après avoir défini la suite des invariants de similitude, on montrera le rapport qui existe entre cette suite et certains représentants particuliers des classes de similitude : les réduites de Frobenius et les réduites de Jordan.

Dans tout le problème, $\mathbb{K}$ *désigne un corps,* n *désigne un entier strictement positif, et* E *un* $\mathbb{K}$*-espace vectoriel de dimension* n*. On se donne également* $u \in \mathcal{L}(E)$ *un endomorphisme non nul de* E*.*

On note, pour tout $x \in E$, $E_{u,x}$ *le sous-ensemble de* E *défini par :*

$$E_{u,x} = \{P(u)(x) \mid P \in \mathbb{K}[X]\}.$$

Ainsi, il s'agit de l'image de x *par tous les polynômes de l'endomorphisme* u*.*

Question préliminaire

Montrer que pour tout $x \in E$, $E_{u,x}$ est un sous-espace vectoriel de E.

Partie I – Lemme des noyaux

Soit P et Q deux polynômes premiers entre eux.

1. À l'aide d'une relation de Bézout, montrer que la somme $\mathrm{Ker}(P(u)) + \mathrm{Ker}(Q(u))$ est directe.
2. Soit $x \in \mathrm{Ker}(PQ(u))$. Justifier que $P(u)(x) \in \mathrm{Ker}(Q(u))$.
3. Montrer que $\mathrm{Ker}(PQ(u)) = \mathrm{Ker}(P(u)) \oplus \mathrm{Ker}(Q(u))$ (lemme des noyaux)
4. Généraliser à $\mathrm{Ker}(P_1 \cdots P_n(u))$ lorsque $P_1, \dots, P_n$ sont deux à deux premiers entre eux.

Partie II – Polynôme minimal ponctuel et polynôme minimal

1. Soit $\mathrm{Ann}(u)$ le sous-ensemble de $\mathbb{K}[X]$ constitué des polynômes P tels que $P(u) = 0$.
   (a) Montrer que $\mathrm{Ann}(u) \neq \{0\}$.
   (b) Montrer que $\mathrm{Ann}(u)$ est un idéal de $\mathbb{K}[X]$ et en déduire l'existence d'un polynôme unitaire non nul de degré minimal Q_u tel que $Q_u(u) = 0$, appelé polynôme minimal de u.

2. Soit $x \in E$.
   (a) Montrer de même qu'il existe un polynôme unitaire non nul $Q_{u,x}$, de degré minimal, tel que $Q_{u,x}(u)(x) = 0$. Le polynôme $Q_{u,x}$ est appelé polynôme minimal ponctuel de u en x.
   (b) Justifier que $\deg(Q_{u,x}) \leqslant n$.
   (c) Justifier que $Q_{u,x}$ divise Q_u.
3. Soit $a_1, \ldots, a_p$ des éléments de E tels que la somme $\bigoplus_{i=1}^{k} E_{u,a_i}$ soit directe. On pose $a = \sum_{i=1}^{k} a_i$.
   (a) Montrer que pour tout $i \in [\![1, p]\!]$, Q_{u,a_i} divise $Q_{u,a}$.
   (b) En déduire que $Q_{u,a} = \bigvee_{i=1}^{p} Q_{u,a_i}$ (cette notation désignant le ppcm unitaire des Q_{u,a_i}).
4. On montre dans cette question que le polynôme minimal de u peut être réalisé comme polynôme minimal ponctuel en un certain vecteur a.
   Soit $Q_u = P_1^{a_1} \cdots P_r^{\alpha_r}$ la décomposition du polynôme minimal Q_u en facteurs irréductibles ($r \geqslant 1$, $\alpha_i \geqslant 1$).
   (a) Montrer que $\mathrm{Ker}(P_i^{\alpha_i - 1}(u)) \subsetneq \mathrm{Ker}(P_i^{\alpha_i}(u))$.
   (b) Soit $a_i \in \mathrm{Ker}(P_i^{\alpha_i}(u)) \setminus \mathrm{Ker}(P_i^{\alpha_i - 1}(u))$. Montrer que $Q_{u,a_i} = P_i^{\alpha_i}$.
   (c) Montrer qu'il existe $a \in E$ tel que $Q_u = Q_{u,a}$. Qu'en déduit-on sur le degré de Q_u ?

Partie III – Endomorphismes cycliques, sous-espaces u-monogènes

Soit F un sous-espace vectoriel de E. On dit que :
- *u est cyclique s'il existe $x \in E$ tel que $E = E_{u,x}$*
- *u est F-cyclique, ou F est u-monogène, s'il existe $x \in E$ tel que $F = E_{u,x}$*

1. Soit u un endomorphisme cyclique de E et x tel que $E_{u,x} = E$. On note $d = \deg(Q_{u,x})$.
   (a) Justifier que $d = n$ (on pourra montrer que $(x, u(x), \cdots, u^{d-1}(x))$ est une famille génératrice de E)
   (b) En déduire que $Q_{u,x} = Q_u$.
   (c) Montrer qu'il existe une base $\mathcal{B} = (b_1, \ldots, b_n)$ de E tel que
$$\mathrm{Mat}_{\mathcal{B}}(u) = \begin{pmatrix} 0 & \cdots & \cdots & 0 & -a_0 \\ 1 & 0 & & \vdots & -a_1 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{n-2} \\ 0 & \cdots & 0 & 1 & -a_{n-1} \end{pmatrix},$$
   où $Q_u = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$. Cette matrice est appelée matrice compagnon du polynôme unitaire Q_u.
2. Soit F un sous-espace vectoriel u-monogène.
   (a) Montrer que F est stable par u.
   (b) Soit u_F l'endomorphisme de F induit par u. Justifier que u_F est cyclique.

Partie IV – Théorème des invariants de similitude

On montre dans cette partie le théorème des invariants de similitude affirmant qu'il existe des sous-espaces $F_1, \ldots, F_r$ stables par u tels que

- $E = \bigoplus_{i=1}^{r} F_i$
- *F_i est u-monogène pour tout $i \in [\![1, r]\!]$*
- *$P_r \mid P_{r-1} \mid \cdots \mid P_1$, où P_i désigne le polynôme minimal de l'endomorphisme innduit u_{F_i}.*

Par ailleurs, la suite de polynômes $(P_1, \dots, P_r)$ est indépendante du choix de la décomposition $(F_1, \dots, F_r)$. Les polynômes P_i de cette suite sont appelés les invariants de similitude de u.

1. Soit $d = \deg(Q_u)$. Justifier qu'il existe un sous-espace F de dimension d et u-monogène.
2. Soit $(e_1, \dots, e_d)$ une base de F, complétée en une base $(e_1, \dots, e_n)$ de E. On note, pour $i \in [\![1, n]\!]$, $e_i^* \in E^*$ l'unique forme linéaire telle que pour tout $j \in [\![1, n]\!]$, $e_i^*(e_j) = \delta_{i,j}$.
   (a) Soit $G = \bigcap_{i \in \mathbb{N}} \mathrm{Ker}(e_d^* \circ u^i)$. Montrer que G est un sous-espace vectoriel de E, stable par u.
   (b) Montrer que $(e_d^* \circ u^i)_{i \in [\![0, d-1]\!]}$ est une famille libre.
   (c) En déduire que $\dim F = n - d$.
   (d) Montrer que $E = F \oplus G$.
   (e) Soit u_F et u_G les endomorphismes induits par u sur F et G respectivement, et P_1 et P_2 leur polynôme minimal. Montrer que $P_2 \mid P_1$.
3. Montrer à l'aide de la question précédente le théorème des invariants de similitude énoncé en début de partie. On ne s'intéressera pour le moment pas à l'unicité des P_i, qui fait l'objet de la question suivante.
4. Soit $(F_1, \dots, F_r)$ et $(G_1, \dots, G_s)$ deux suites de sous-espaces u-monogènes vérifiant les conditions du théorème des invariants de similitude, et $P_1, \dots, P_r$, $Q_1, \dots, Q_s$ les deux suites de polynômes associées. On suppose qu'elles ne sont pas égales, et on note j le plus grand indice tel que $P_i = Q_i$ pour tout $i \in [\![1, j-1]\!]$.
   (a) Montrer que $\sum_{i=1}^{r} \deg(P_i) = \sum_{j=1}^{s} \deg(Q_j) = n$.
   (b) En déduire que $j \leqslant r$ et $j \leqslant s$.
   (c) Montrer que
   $$P_j(u)(E) = \bigoplus_{i=1}^{j-1} P_j(u)(F_i) = \bigoplus_{i=1}^{s} P_j(u)(G_i).$$
   (d) Justifier que $\dim(P_j(u)(F_i)) = \dim(P_j(u)(G_i))$, pour tout $i \in [\![1, j-1]\!]$ (on pourra comparer les matrices de u_{G_1} et de u_{G_2} dans des bases bien choisies, et en déduire une relation entre u_{G_1} et u_{G_2})
   (e) Montrer que pour tout $i \in n[\![j, s]\!]$, $\dim(P_j(u)(G_i)) = 0$.
   (f) Montrer que $P_j = Q_j$ et conclure.

Partie V – Quelques applications

On donne dans cette partie quelques applications du théorème des invariants de similitude. On retrouve en particulier la forme réduite de Jordan, déjà vue en DM, lorsque le polynôme Q_u est scindé (par exemple lorsque $\mathbb{K}$ est algébriquement clos)

1. Réduction de Frobenius.
   Soit $(P_1, \dots, P_r)$ les invariants de similitude de u, et $C(P_1), \dots, C(P_n)$ les matrices compagnons associées (voir partie III). Montrer qu'il existe une base $\mathcal{B}$ de E dans laquelle la matrice de u est la matrice diagonale par blocs définie de la manière suivante :
   $$\mathrm{Mat}_{\mathcal{B}}(u) = \begin{pmatrix} C(P_1) & & 0 \\ & \ddots & \\ 0 & & C(P_r) \end{pmatrix}.$$

2. Réduction de Jordan.

   On suppose que le polynôme minimal Q_u est scindé. Montrer qu'il existe une base $\mathcal{C}$ de E dans laquelle la matrice de u est :

$$\mathrm{Mat}_{\mathcal{C}}(u) = \begin{pmatrix} J_1 & & 0 \\ & \ddots & \\ 0 & & J_s \end{pmatrix},$$

   où les J_i sont des blocs de Jordan :

$$J_i = \begin{pmatrix} \lambda_i & 1 & 0 & 0 \\ 0 & \ddots & \ddots & 0 \\ \vdots & \ddots & \ddots & 1 \\ 0 & \cdots & 0 & \lambda_i \end{pmatrix}$$

   On pourra commencer par étudier le cas où u est nilpotent, en décrivant dans cette situation la matrice de Frobenius obtenue dans la question précédente.

3. Caractérisation des classes de similitude.

   Montrer que deux matrices A et B de $\mathcal{M}_n(\mathbb{K})$ sont semblables si et seulement les endomorphismes canoniquement associés ont mêmes invariants de similitude.

4. Invariance de la similitude par restriction du corps de base.

   Soit $\mathbb{K}$ un sous-corps d'un corps $\mathbb{L}$. Soit A et B dans $\mathcal{M}_n(\mathbb{K})$. Montrer que A et B sont semblables dans $\mathcal{M}_n(\mathbb{K})$ si et seulement si elles sont semblables dans $\mathcal{M}_n(\mathbb{L})$.