PREMIÈRE COMPOSITION DE MATHÉMATIQUES

DURÉE : 4 heures

PROBLÈME

Dans ce problème, K est un corps commutatif, K[X] l'anneau des polynômes à coefficients dans K. Si $p \in K[X]$, on note (p) l'idéal de K[X] engendré par p, et si $\alpha \in K[X]/(p)$ admet le polynôme q comme représentant dans K[X], on écrit $\alpha = q \bmod p$.

Si $\lambda_0, \ldots, \lambda_{m-1} \in K$, on note Frob $(\lambda_0, \ldots, \lambda_{m-1})$ la matrice :

$$\text{Frob}(\lambda_0, \ldots, \lambda_{m-1}) = \begin{bmatrix} 0 & 0 & 0 & \ldots & 0 & \lambda_0 \\ 1 & 0 & 0 & \ldots & 0 & \lambda_1 \\ 0 & 1 & 0 & \ldots & 0 & \lambda_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 0 & \lambda_{m-2} \\ 0 & 0 & 0 & \ldots & 1 & \lambda_{m-1} \end{bmatrix}$$

On écrit Diag $(A_1, A_2, \ldots, A_m)$ pour la matrice diagonale :

$$\text{Diag}(A_1, A_2, \ldots, A_m) = \begin{bmatrix} A_1 & 0 & \ldots & 0 \\ 0 & A_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & A_m \end{bmatrix}$$

où les A_i peuvent être des éléments de K, ou encore des matrices carrées à coefficients dans K, auquel cas il s'agit d'une écriture « par blocs ».

Si f est un K-endomorphisme d'un K-espace vectoriel E, on note π_f son polynôme minimal et χ_f son polynôme caractéristique.

Si f est un endomorphisme de l'espace vectoriel E et g un endomorphisme de l'espace vectoriel F, on dit que l'isomorphisme $\varphi : E \longrightarrow F$ *conjugue* f et g si $g = \varphi f \varphi^{-1}$.

I

1° Soit $p = X^m - \sum_{i=0}^{m-1} \lambda_i X^i$ un élément de K[X]. Le quotient $E = K[X]/(p)$ est un espace vectoriel sur K de dimension m. On considère l'endomorphisme u_p de E défini par $u_p(q \bmod p) = (Xq) \bmod p$ si $q \in K[X]$.

Montrer que u_p est bien défini et qu'il est possible de trouver une base de E telle que la matrice de u_p soit Frob $(\lambda_0, \ldots, \lambda_{m-1})$.

On notera aussi Frob $(\lambda_0, \ldots, \lambda_{m-1}) = \Phi\text{rob}(p)$.

Quel est le polynôme caractéristique de u_p ?

Quel est le polynôme minimal de u_p ?

2° Soit $q = X^n - \sum_{i=0}^{n-1} \mu_i X^i$ un autre polynôme; on suppose que p et q sont premiers entre eux. On définit de même $F = K[X]/(q)$ et aussi $G = K[X]/(pq)$ et les endomorphismes u_q, u_{pq}, associés à la multiplication par X sur F et G respectivement. On obtient par somme directe l'endomorphisme $u_p \oplus u_q$ sur l'espace $E \oplus F$.

En s'aidant du théorème de Bezout, montrer qu'il existe un isomorphisme de K-espace vectoriel $\varphi : E \oplus F \longrightarrow G$ qui conjugue $u_p \oplus u_q$ et u_{pq}.

En déduire que les matrices $\Phi\text{rob}(pq)$ et Diag $(\Phi\text{rob}(p), \Phi\text{rob}(q))$ sont semblables.

Donner un exemple montrant que sans l'hypothèse de primalité entre p et q, ce résultat n'est pas nécessairement vrai.

En comparant les polynômes minimaux de $\Phi\text{rob}(pq)$ et de Diag $(\Phi\text{rob}(p), \Phi\text{rob}(q))$, montrer que, en fait, ces deux matrices sont semblables si et seulement si p et q sont premiers entre eux.

Tournez la page S. V. P.

II

1° E est maintenant un espace vectoriel de dimension finie sur K, sans autre précision. On donne un K-endomorphisme f de E. Si $x \in E$ et si $p \in K[X]$, on note $p*x = (p(f))(x)$ l'image de x par l'endomorphisme $p(f)$ de E.

Montrer que $I_x = \{p \in K[X] \text{ tq } p*x = 0\}$ est un idéal. On note P_x son générateur canonique qu'on appelle polynôme minimal de x pour f.

Quelle relation existe-t-il entre P_x et π_f ?

2° Si $x \in E$, soit E_x le sous-espace de E défini par :

$$E_x = \{p*x \text{ tq } p \in K[X]\}.$$

Montrer que E_x est stable par f.

Montrer qu'il existe un isomorphisme de K-espaces vectoriels

$$\varphi : K[X]/(P_x) \longrightarrow E_x$$

conjuguant u_{P_x} et $f|E_x$. Quelle conclusion en tirer pour le degré de P_x et la dimension de E_x ?

Que peut-on dire du polynôme minimal d'un élément de E_x ?

3° Soient $x, y \in E$; montrer que si $E_x \cap E_y = 0$, alors $P_{x+y} = \text{ppcm}(P_x, P_y)$. Comment peut-on généraliser ce résultat à plus de deux éléments $x_1, \ldots, x_m$ de E ?

4° Montrer que si P_x et P_y sont premiers entre eux, alors $E_{x+y} = E_x \oplus E_y$. Généraliser.

III

E et f sont comme en II.

1° Si x est un vecteur propre de f, que sont P_x et E_x ?

2° On suppose que f est diagonalisable et que son polynôme caractéristique χ_f est à racines simples. Montrer qu'il existe $x \in E$ tel que $E = E_x$, et qu'il existe un isomorphisme $\varphi : E \longrightarrow K[X]/(\chi_f)$ conjuguant f et u_{x_f}.

3° On suppose maintenant f diagonalisable sans hypothèse sur son polynôme caractéristique. Montrer qu'il existe $x_1, \ldots, x_p \in E$ vérifiant :

a. $E = E_{x_1} \oplus \ldots \oplus E_{x_p}$;

b. $P_{x_{i-1}}$ divise P_{x_i} pour $2 \leqslant i \leqslant p$.

En déduire qu'il existe une base de E telle que la matrice de f soit :

$$f = \text{Diag}(\Phi\text{rob}(P_{x_1}), \ldots, \Phi\text{rob}(P_{x_p})).$$

On dit qu'un endomorphisme f pour lequel il existe $x_1, \ldots, x_p$ vérifiant *a* et *b* est un *endomorphisme à diviseurs*.

Tournez la page S. V. P.

E.N.S. de LYON
Option Math-Math 1
page 41
1987

IV

1° On suppose maintenant f nilpotent. Que peut-on dire de P_x si $x \in E$?

2° On suppose d'abord $f^2 = 0$. Montrer qu'il existe E_2 et E_1, des sous-espaces de E tels que :

a. $f|E_2$ est injectif;

b. $f|E_1 = 0$;

c. $E = E_1 \oplus E_2 \oplus f(E_2)$.

En déduire que f est un endomorphisme à diviseurs.

3° On suppose maintenant $f^3 = 0$. Montrer que f est un endomorphisme à diviseurs.

La même méthode permet évidemment de démontrer que tout endomorphisme nilpotent est un endomorphisme à diviseurs. La démonstration du cas général *n'est pas demandée.*

V

1° On suppose ici que π_f, le polynôme minimal de f, est irréductible; quel est le polynôme minimal P_x quand $0 \neq x \in E$?

Montrer que si F est un sous-espace de E stable par f, et si $x \in E$, alors ou bien $E_x \subset F$, ou bien $E_x \cap F = 0$.

Montrer que f est alors un endomorphisme à diviseurs, et que, dans une base de E, f s'écrit :

$$f = \text{Diag}\,(\Phi\text{rob}\,(\pi_f), \ldots, \Phi\text{rob}\,(\pi_f)).$$

En déduire que la dimension de E est nécessairement un multiple du degré de π_f.

2° On suppose maintenant que $\pi_f = P^2$ où P est un polynôme irréductible.

Soit $F = \ker P(f)$; montrer que F est stable par f, et que le 1° s'applique à $(\ker P(f), f|\ker P(f))$.

On peut définir aussi $E' = E/F$ et par passage au quotient (pourquoi ?), f induit un endomorphisme f' de E'; montrer que le 1° s'applique à (E', f')

Montrer qu'il existe une base de E telle que f s'écrive :

$$f = \text{Diag}\,(\Phi\text{rob}\,(P), \ldots, \Phi\text{rob}\,(P), \Phi\text{rob}_2\,(P), \ldots, \Phi\text{rob}_2\,(P))$$

où $\Phi\text{rob}_2(P)$ est la matrice :

$$\Phi\text{rob}_2(P) = \begin{bmatrix} & & 0 & \ldots & 0 & 1 \\ & & 0 & \ldots & 0 & 0 \\ \Phi\text{rob}\,(P) & & \vdots & \ddots & \vdots & \vdots \\ & & 0 & \ldots & 0 & 0 \\ 0 & & & \Phi\text{rob}\,(P) & & \end{bmatrix}$$

Indication : on pourra utiliser une décomposition de E en somme directe $E = E_1 \oplus E_2 \oplus P(f)(E_2)$ avec $E_1 \subset \ker P(f)$ et $P(f)|E_2$ injectif.

Montrer que $\Phi\text{rob}_2\,(P)$ et $\Phi\text{rob}\,(P^2)$ sont semblables.

En déduire que (E, f) est un endomorphisme à diviseurs.

3° Généraliser au cas où π_f est une puissance quelconque d'un polynôme irréductible.

VI

Montrer que tout endomorphisme d'un espace vectoriel est un endomorphisme à diviseurs.

page 42 E.N.S. de LYON
1987 Option Math—Math 1