# Agrégation interne de Mathématiques

(et CAERPA)

## Session 2002

## Première épreuve écrite

# Préambule

On notera $\mathbf{N}$ l'ensemble des nombres entiers naturels, $\mathbf{Z}$ l'anneau des nombres entiers relatifs, $\mathbf{Q}$ le corps des nombres rationnels, $\mathbf{R}$ le corps des nombres réels et $\mathbf{C}$ le corps des nombres complexes. On désignera par $\mathbf{K}$ un des corps $\mathbf{Q}$, $\mathbf{R}$ ou $\mathbf{C}$ et par $\mathbf{E}$ un des anneaux euclidiens $\mathbf{Z}$ ou $\mathbf{K}[X]$, l'anneau $\mathbf{E}$ est donc un anneau intègre. On notera $U(\mathbf{E})$ l'ensemble des *unités* de $\mathbf{E}$, c'est-à-dire l'ensemble des éléments de $\mathbf{E}$ qui sont inversibles dans $\mathbf{E}$ ; on a donc $U(\mathbf{Z}) = \{\pm 1\}$ et $U(\mathbf{K}[X]) = \mathbf{K} \setminus \{0\}$ et enfin, on notera $\mathbf{F}$ le corps des fractions de l'anneau $\mathbf{E}$ ; on a donc $\mathbf{F} = \mathbf{Q}$ si $\mathbf{E} = \mathbf{Z}$, et $\mathbf{F} = \mathbf{K}(X)$ si $\mathbf{E} = \mathbf{K}[X]$.

Le *stathme* de l'anneau euclidien $\mathbf{E}$ est l'application $\mathrm{st} : \mathbf{E} \setminus \{0\} \to \mathbf{N}$ définie par $\mathrm{st}(n) = |n|$ si $\mathbf{E} = \mathbf{Z}$ et par $\mathrm{st}(p) = \deg(p)$ si $\mathbf{E} = \mathbf{K}[X]$. La division euclidienne dans $\mathbf{E}$ peut s'exprimer ainsi :

soient $a$ et $b$ dans $\mathbf{E} \setminus \{0\}$, alors, ou bien $b$ divise $a$, ou bien il existe $q \in \mathbf{E}$ et $r \in \mathbf{N} \setminus \{0\}$ (resp. $r \in \mathbf{E} \setminus \{0\}$) si $\mathbf{E} = \mathbf{Z}$ (resp. si $\mathbf{E} = \mathbf{K}[X]$), tels que $a = bq + r$ et $\mathrm{st}(r) < \mathrm{st}(b)$.

1. Soit $A$ un sous-ensemble de $\mathbf{E}$, fini ou infini, contenant au moins un élément non nul, on appellera *valence* de $A$ le nombre suivant :

$$\mathrm{val}(A) = \inf\{\mathrm{st}(a) \ \mid \ a \in A,\ a \neq 0\}.$$

Montrer que $\mathrm{val}(A)$ est un élément bien défini de $\mathbf{N}$.

2. On appelle *opération élémentaire* sur un sous-ensemble $A$ de $\mathbf{E}$, contenant au moins un élément non nul, l'ajout à $A$ d'un élément non nul $r$ de $\mathbf{E}$ qui est le reste de la division euclidienne d'un élément $a$ non nul de $A$ par un élément $b$ non nul de $A$. Montrer qu'on a l'alternative suivante :

ou bien, il existe un élément $r_1$ de $A$ qui divise tous les éléments de $A$,

ou bien, il existe une opération élémentaire sur $A$ telle que $\mathrm{val}(A \cup \{r\}) < \mathrm{val}(A)$.

3. Montrer qu'un nombre fini d'opérations élémentaires à partir de $A$ conduit à un ensemble $B = A \cup \{r_1, \ldots, r_n\}$ dans lequel $r_n$ divise tous les éléments de $B$.

4. Dans tout le problème, on appellera *le plus grand commun diviseur* des éléments d'un ensemble $A$ comme ci-dessus celui des plus grands communs diviseurs qui est un nombre positif si $\mathbf{E} = \mathbf{Z}$, ou un polynôme unitaire si $\mathbf{E} = \mathbf{K}[X]$. Soit $e$ le plus grand commun diviseur des éléments de $A$, comparer $e$ et l'élément $r_n$ trouvé en 3.

5. Traiter explicitement l'exemple $A = \{6, 10, 15\}$, dans le cas $\mathbf{E} = \mathbf{Z}$.

# Première partie

*On dira qu'une matrice à $p$ lignes et $q$ colonnes est une* matrice de type $(p, q)$. *Le but de cette partie et de la suivante est de trouver une condition nécessaire et suffisante pour que deux matrices de type $(p, q)$ à coefficients dans $\mathbf{E}$ soient équivalentes en tant que matrices à coefficients dans $\mathbf{E}$. Ce résultat sera utilisé dans la troisième partie pour donner une condition nécessaire et suffisante pour que deux matrices carrées à coefficients dans $\mathbf{K}$ soient semblables.*

On notera $M_{p,q}(\mathbf{E})$ l'ensemble des matrices de type $(p, q)$ à coefficients dans $\mathbf{E}$, c'est-à-dire le sous-ensemble de $M_{p,q}(\mathbf{F})$ formé des matrices dont tous les termes sont dans $\mathbf{E}$. Le *rang*

d'une matrice $A \in M_{p,q}(\mathbf{E})$ est le rang de $A$ considérée comme matrice à coefficients dans $\mathbf{F}$. On dira qu'une matrice $A \in M_{p,p}(\mathbf{E})$ est *inversible* si elle a un inverse dans $M_{p,p}(\mathbf{E})$. Le *déterminant* de $A \in M_{p,p}(\mathbf{E})$, noté $\det(A)$, est le déterminant de $A$ considérée comme matrice à coefficients dans $\mathbf{F}$. On remarquera que $\det(A) \in \mathbf{E}$ et que, si $B \in M_{p,p}(\mathbf{E})$, on a $\det(AB) = \det(A)\det(B)$.

1. Montrer qu'une matrice $P \in M_{p,p}(\mathbf{E})$ est inversible si et seulement si son déterminant est inversible dans $\mathbf{E}$, c'est-à-dire si $\det P \in U(\mathbf{E})$.

2. Deux matrices $M'$ et $M''$ de $M_{p,q}(\mathbf{E})$ sont dites $\mathbf{E}$-*équivalentes* s'il existe des matrices inversibles $P \in M_{p,p}(\mathbf{E})$ et $Q \in M_{q,q}(\mathbf{E})$ telles que $M'' = PM'Q$. On notera cette relation $M' \overset{\mathbf{E}}{\simeq} M''$. Montrer que la relation $\overset{\mathbf{E}}{\simeq}$ est une relation d'équivalence.

3. Soient $i$ et $j$ deux nombres entiers distincts vérifiant $1 \leqslant i \leqslant p$ et $1 \leqslant j \leqslant p$, et $b \in \mathbf{E} \setminus \{0\}$. On note $T^p_{i,j}(b)$ la matrice de $M_{p,p}(\mathbf{E})$ dont les termes diagonaux sont égaux à 1 et dont le seul terme non nul en dehors de la diagonale est sur la $i$-ème ligne et la $j$-ème colonne, et a pour valeur $b$, on note $S^p_{i,j}$ la matrice de $M_{p,p}(\mathbf{E})$ obtenue à partir de la matrice unité en échangeant $i$-ème ligne et $j$-ème ligne et on note $D(u_1, \ldots, u_p)$ la matrice diagonale dont les termes diagonaux sont des unités $u_1, \ldots, u_p$ de $\mathbf{E}$.

i) On appellera *opérations élémentaires sur les lignes et les colonnes* de $A$ la multiplication de $A \in M_{p,q}(\mathbf{E})$ à gauche par une matrice $T^p_{i,j}(b)$, $S^p_{i,j}$ ou $D(u_1, \ldots, u_p)$, ainsi que la multiplication à droite par une matrice $T^q_{i,j}(b)$, $S^q_{i,j}$ ou $D(u_1, \ldots, u_q)$. Exprimer ces opérations en termes de manipulations sur les lignes et les colonnes de $A$. On appellera *suite d'opérations sur les lignes et les colonnes* de $A$ toute composition d'opérations élémentaires sur les lignes et les colonnes de $A$.

ii) Montrer que $T^p_{i,j}(b)$, $S^p_{i,j}$ et $D(u_1, \ldots, u_p)$ sont inversibles et donner leurs inverses.

iii) Les matrices $T^p_{i,j}(b) \cdot A$, $S^p_{i,j} \cdot A$, $D(u_1, \ldots, u_p) \cdot A$, $A \cdot T^q_{i,j}(b)$, $A \cdot S^q_{i,j}$ et $A \cdot D(u_1, \ldots, u_q)$ sont $\mathbf{E}$-équivalentes à $A$ ; montrer que, de plus, le plus grand commun diviseur des termes d'une quelconque de ces matrices est égal au plus grand commun diviseur des termes de $A$.

Soit $A = (a_{i,j})_{1 \leqslant i \leqslant p, 1 \leqslant j \leqslant q} \in M_{p,q}(\mathbf{E})$, supposons la matrice $A$ non nulle, on appellera encore *valence* de $A$ le nombre entier :

$$\mathrm{val}(A) = \min\{\mathrm{st}(a_{i,j}) \mid a_{i,j} \neq 0,\ 1 \leqslant i \leqslant p,\ 1 \leqslant j \leqslant q\}.$$

4. On traite dans cette question le cas des matrices de type $(2,2)$.

i) On considère la matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2,2}(\mathbf{E})$, supposée non nulle. Montrer qu'on a l'alternative suivante :

ou bien, un des quatre termes $a$, $b$, $c$ et $d$ divise les trois autres,

ou bien, il existe une suite d'opérations sur les lignes et les colonnes de $A$ qui transforme $A$ en une matrice $B$ telle que $B \overset{\mathbf{E}}{\simeq} A$ et $\mathrm{val}(B) < \mathrm{val}(A)$.

Pour cela, on pourra d'abord supposer que $\mathrm{val}(A) = \mathrm{st}(a)$ et distinguer deux cas :

si $a$ ne divise pas $b$, ou si $a$ ne divise pas $c$, donner une opération élémentaire qui donne le résultat annoncé ;

si $a$ divise $b$ et $c$ et ne divise pas $d$, donner une suite d'opérations élémentaires qui donne le résultat annoncé.

ii) Montrer qu'il existe une suite d'opérations sur les lignes et les colonnes de $A$ qui transforme $A$ en une matrice $C$ telle que $C \overset{\mathbf{E}}{\simeq} A$ et $C = \begin{pmatrix} e_1 & * \\ * & * \end{pmatrix}$, où $e_1$ est le plus grand commun diviseur de $a$, $b$, $c$ et $d$, et les $*$ désignent des éléments de $\mathbf{E}$ divisibles par $e_1$, puis en une matrice $D$ telle que $D \overset{\mathbf{E}}{\simeq} A$ et $D = \begin{pmatrix} e_1 & 0 \\ 0 & e_2 \end{pmatrix}$. Montrer que l'on peut supposer de plus, dans le cas $e_2 \neq 0$, que $e_2$ est un nombre positif si $\mathbf{E} = \mathbf{Z}$, ou un polynôme unitaire si $\mathbf{E} = \mathbf{K}[X]$. On supposera cette condition réalisée pour le reste de la question 4.

iii) Montrer que $e_1$ divise $e_2$ et que $e_1 e_2 = u \det(A)$, où $u$ est une unité de $\mathbf{E}$. En déduire que le couple $(e_1, e_2)$ est déterminé de façon unique par $A$. On appellera *facteur(s) invariant(s)* de $A$ le couple $(e_1, e_2)$, dans le cas $e_2 \neq 0$ ou l'élément $e_1$, dans le cas $e_2 = 0$.

iv) Montrer que si les matrices non nulles $A$ et $A'$ de $M_{2,2}(\mathbf{E})$ ont les mêmes facteurs invariants, alors elles sont $\mathbf{E}$-équivalentes.

v) Montrer réciproquement que deux matrices $\mathbf{E}$-équivalentes $A$ et $A'$ non nulles ont les mêmes facteurs invariants. On pourra montrer que le déterminant et le plus grand commun diviseur des termes d'une matrice $A \in M_{2,2}(\mathbf{E})$ sont conservés par multiplication à droite ou à gauche par une matrice inversible de $M_{2,2}(\mathbf{E})$, à une multiplication près par une unité de $\mathbf{E}$ dans le cas du déterminant.

5. Traiter explicitement les exemples $A = \begin{pmatrix} 6 & 10 \\ 10 & 15 \end{pmatrix}$ et $A = \begin{pmatrix} 6 & 12 \\ 12 & 15 \end{pmatrix}$, dans le cas $\mathbf{E} = \mathbf{Z}$.

# Deuxième partie

1. On traite dans cette partie le cas général : on notera $A$ une matrice de type $(p, q)$ à coefficients dans $\mathbf{E}$ et de rang $r > 0$.

i) Montrer qu'il existe une suite d'opérations sur les lignes et les colonnes de $A$ qui transforme $A$ en une matrice $B$ telle que $A \overset{\mathbf{E}}{\simeq} B$, qui a la décomposition en blocs suivante :

$$B = \begin{pmatrix} e_1 & (0) \\ (0) & A' \end{pmatrix},$$

où $A'$ est une matrice de type $(p-1, q-1)$ à coefficients dans $\mathbf{E}$, $e_1$ divise tous les termes de $A'$, et les $(0)$ désignent des matrices nulles de types appropriés. Donner le rang de $A'$.

ii) Montrer qu'il existe une suite d'opérations sur les lignes et les colonnes de $A$ qui transforme $A$ en une matrice $C$ telle que $A \overset{\mathbf{E}}{\simeq} C$, qui a la décomposition en blocs suivante :

$$C = \begin{pmatrix} D(e_1, \ldots, e_r) & (0) \\ (0) & (0) \end{pmatrix},$$

où $D(e_1, \ldots, e_r)$ est la matrice diagonale d'ordre $r$ dont les termes diagonaux sont $e_1, \ldots, e_r$, avec les conditions : $e_1$ divise $e_2, \ldots, e_{r-1}$ divise $e_r$, $e_1 \neq 0, \ldots, e_r \neq 0$, et où les $(0)$ désignent toujours des matrices nulles de types appropriés.

iii) Soit $P \in M_{p,p}(\mathbf{E})$ une matrice inversible (dans $M_{p,p}(\mathbf{E})$), montrer que $P$ peut s'écrire comme un produit de matrices $T_{i,j}^p(b)$, $S_{i,j}^p$ et $D(u_1, \ldots, u_p)$, où l'on reprend les notations de la question 3. de la première partie, en particulier, $u_1, \ldots, u_p$ sont des unités de $\mathbf{E}$.

iv) Montrer que deux matrices $A$ et $A'$ de $M_{p,q}(\mathbf{E})$ sont $\mathbf{E}$-équivalentes si et seulement si il existe une suite d'opérations sur les lignes et les colonnes de $A$ qui transforme $A$ en $A'$.

2. On appelle *mineur d'ordre $m$* d'une matrice $A$ tout déterminant d'une matrice carrée d'ordre $m$ extraite de $A$. On admet que toute opération élémentaire sur les lignes ou les colonnes de $A \in M_{p,q}(\mathbf{E})$ conserve le plus grand commun diviseur des mineurs d'ordre $m$, ceci pour tout $m$, $1 \leqslant m \leqslant \min(p, q)$.

i) On suppose que l'on a transformé par une suite d'opérations sur les lignes et les colonnes la matrice $A$ en une matrice $C$ qui a la forme indiquée en 1.ii), avec les conditions $e_1 \mid e_2, \ldots, e_{r-1} \mid e_r$. Montrer que, pour tout $m$, $1 \leqslant m \leqslant r$, le produit $e_1 \cdots e_m$ est un plus grand commun diviseur des mineurs d'ordre $m$ de $A$.

ii) Avec les mêmes notations, on supposera de plus que $e_1, \ldots, e_r$ sont des entiers positifs si $\mathbf{E} = \mathbf{Z}$, ou des polynômes unitaires si $\mathbf{E} = \mathbf{K}[X]$ : ceci est loisible, quitte à multiplier la matrice $C$ par une matrice $D(u_1, \ldots, u_p)$ bien choisie. Montrer que, la matrice $A$ étant donnée, les $e_1, \ldots, e_r$ calculés en 1.ii), ainsi normalisés, sont définis de façon unique. On appellera *facteurs invariants* de $A$ ce $r$-uplet $(e_1, \ldots, e_r)$.

iii) Montrer que deux matrices $A$ et $A'$ de $M_{p,q}(\mathbf{E})$ sont $\mathbf{E}$-équivalentes si et seulement si elles ont les mêmes facteurs invariants.

3. Soit $\alpha \in \mathbf{K}$, calculer les facteurs invariants des matrices de $M_{3,3}(\mathbf{K}[X])$ suivantes :

$$A = \begin{pmatrix} \alpha - X & 1 & 0 \\ 0 & \alpha - X & 1 \\ 0 & 0 & \alpha - X \end{pmatrix} \text{ et } B = \begin{pmatrix} \alpha - X & 0 & 0 \\ 0 & \alpha - X & 1 \\ 0 & 0 & \alpha - X \end{pmatrix}.$$

# Troisième partie

*Le but de cette partie est de donner une condition nécessaire et suffisante pour que deux matrices carrées d'ordre $p$ à coefficients dans le corps $\mathbf{K}$ soient semblables, c'est-à-dire représentent un même endomorphisme de $\mathbf{K}^p$ dans des bases différentes. On obtiendra de plus une méthode de calcul du polynôme minimal d'un endomorphisme de $\mathbf{K}^p$.*

1. Soit $M \in M_{p,p}(\mathbf{K})$, on note dans toute cette partie $(e_1^M(X), \ldots, e_r^M(X))$ les facteurs invariants de la matrice $M - XI \in M_{p,p}(\mathbf{K}[X])$, où $I$ désigne la matrice unité de $M_{p,p}(\mathbf{K})$. On vient de voir qu'il existe des matrices inversibles $P$ et $Q$ dans $M_{p,p}(\mathbf{K}[X])$ telles que :

$$M - XI = P \cdot \begin{pmatrix} e_1^M(X) & \cdots & 0 & (0) \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & e_r^M(X) & (0) \\ (0) & \cdots & (0) & (0) \end{pmatrix} \cdot Q.$$

Montrer, en calculant le déterminant de $M - XI$, que le rang $r$ de $M - XI$ est égal à $p$. Comparer le polynôme caractéristique de $M$ et le produit $e_1^M(X) \cdots e_p^M(X)$.

2. Soient $M_1$ et $M_2$ deux matrices de $M_{p,p}(\mathbf{K})$, on suppose que ces deux matrices sont semblables, montrer que les deux matrices $M_1 - XI$ et $M_2 - XI$ sont $\mathbf{K}[X]$-équivalentes. En déduire que $M_1 - XI$ et $M_2 - XI$ ont les mêmes facteurs invariants.

On notera les éléments de $\mathbf{K}^p$ sous la forme $\overrightarrow{v} = (v_1, \ldots, v_p)$, en particulier,

$$\overrightarrow{\varepsilon_1} = (1, \ldots, 0), \ldots, \overrightarrow{\varepsilon_p} = (0, \ldots, 1)$$

désigneront les éléments de la base canonique $\mathcal{E}$ de $\mathbf{K}^p$. On va considérer le $\mathbf{K}$-espace vectoriel $(\mathbf{K}[X])^p$, dont les éléments sont les $p$-uplets $(a_1(X), \ldots, a_p(X))$, où $a_i(X) \in \mathbf{K}[X]$ pour $1 \leqslant i \leqslant p$. On considérera les éléments de $\mathbf{K}^p$ comme des éléments particuliers de $(\mathbf{K}[X])^p$ «indépendants de $X$» . On définit de plus le produit d'un élément de $(\mathbf{K}[X])^p$ par un polynôme $b(X) \in \mathbf{K}[X]$ par la formule :

$$b(X)\big(a_1(X), \ldots, a_p(X)\big) = \big(b(X)a_1(X), \ldots, b(X)a_p(X)\big) \in (\mathbf{K}[X])^p.$$

Si $a_1(X), \ldots, a_p(X)$ s'écrivent

$$a_1(X) = a_{10} + \cdots + a_{1j}X^j + \cdots + a_{1n}X^n, \ldots, a_p(X) = a_{p0} + \cdots + a_{pj}X^j + \cdots + a_{pn}X^n,$$

on utilisera les notations suivantes :

$$(a_1(X), \ldots, a_p(X)) = a_1(X)\overrightarrow{\varepsilon_1} + \cdots + a_p(X)\overrightarrow{\varepsilon_p} = \overrightarrow{a}(X) = \overrightarrow{a_0} + \cdots + \overrightarrow{a_j}X^j + \cdots + \overrightarrow{a_n}X^n,$$

où $\overrightarrow{a_j} = (a_{1j}, \ldots, a_{pj})$. On a donc avec ces notations :

$$X(\overrightarrow{a_0} + \cdots + \overrightarrow{a_j}X^j + \cdots + \overrightarrow{a_n}X^n) = \overrightarrow{a_0}X + \cdots + \overrightarrow{a_j}X^{j+1} + \cdots + \overrightarrow{a_n}X^{n+1}.$$

3. On considère un endomorphisme $f$ de $\mathbf{K}^p$, dont la matrice par rapport à la base $\mathcal{E}$ est $M = (m_{i,j})_{1\leqslant i\leqslant p, 1\leqslant j\leqslant p}$. On étend $f$ en l'endomorphisme, encore noté $f$, du $\mathbf{K}$-espace vectoriel $(\mathbf{K}[X])^p$, défini par :

$$f(\overrightarrow{a_0} + \cdots + \overrightarrow{a_j}X^j + \cdots + \overrightarrow{a_n}X^n) = f(\overrightarrow{a_0}) + \cdots + f(\overrightarrow{a_j})X^j + \cdots + f(\overrightarrow{a_n})X^n.$$

On définit enfin une application $\varphi : (\mathbf{K}[X])^p \to \mathbf{K}^p$ en posant :

$$\varphi(\overrightarrow{a_0} + \cdots + \overrightarrow{a_j}X^j + \cdots + \overrightarrow{a_n}X^n) = \overrightarrow{a_0} + \cdots + f^j(\overrightarrow{a_j}) + \cdots + f^n(\overrightarrow{a_n}),$$

où $f^j = f \circ \cdots \circ f$ ($j$ fois).

i) Vérifier que $\varphi$ est un homomorphisme surjectif de $\mathbf{K}$-espaces vectoriels.

ii) Vérifier qu'on a la relation suivante, pour tous $\lambda(X)$ et $\mu(X)$ de $\mathbf{K}[X]$, et pour tous $\overrightarrow{a}(X)$ et $\overrightarrow{b}(X)$ de $(\mathbf{K}[X])^p$ :

$$f\big(\lambda(X)\overrightarrow{a}(X) + \mu(X)\overrightarrow{b}(X)\big) = \lambda(X)f\big(\overrightarrow{a}(X)\big) + \mu(X)f\big(\overrightarrow{b}(X)\big).$$

iii) Soit $\overrightarrow{u} \in \mathbf{K}^p$, on peut aussi considérer $\overrightarrow{u}$ comme un élément «indépendant de $X$» de $(\mathbf{K}[X])^p$, comparer $f(\overrightarrow{u})$ et $\varphi(\overrightarrow{u}X)$.

iv) Montrer que $\overrightarrow{v}(X) = \overrightarrow{v_0} + \overrightarrow{v_1}X + \cdots + \overrightarrow{v_n}X^n \in (\mathbf{K}[X])^p$ est dans le noyau de $\varphi$ si, et seulement si, il existe $\overrightarrow{w}(X) = \overrightarrow{w}_0 + \overrightarrow{w}_1 X + \cdots + \overrightarrow{w}_n X^n \in (\mathbf{K}[X])^p$ tel que, en notant id l'application identique de $(\mathbf{K}[X])^p$ dans lui-même :

$$\overrightarrow{v}(X) = (f - X\mathrm{id})(\overrightarrow{w}(X)) = \sum_{j=0}^{j=n} \big[f(\overrightarrow{w_j})X^j - \overrightarrow{w_j}X^{j+1}\big].$$

4. On appellera $\mathbf{K}[X]$-*base* de $(\mathbf{K}[X])^p$ une famille $\big(\overrightarrow{\beta_1}, \ldots, \overrightarrow{\beta_p}\big)$ d'éléments de $(\mathbf{K}[X])^p$ telle que tout élément $\overrightarrow{a}(X)$ de $(\mathbf{K}[X])^p$ s'écrive de façon unique sous la forme

$$\overrightarrow{a}(X) = b_1(X)\overrightarrow{\beta_1} + \cdots + b_p(X)\overrightarrow{\beta_p},$$

où $b_1(X), \ldots, b_p(X) \in \mathbf{K}[X]$. Ainsi, $\big(\overrightarrow{\varepsilon_1}, \ldots, \overrightarrow{\varepsilon_p}\big)$ est une $\mathbf{K}[X]$-base de $(\mathbf{K}[X])^p$. De même, on appellera $\mathbf{K}[X]$-base de $\ker(\varphi)$ une famille $\big(\overrightarrow{\gamma_1}, \ldots, \overrightarrow{\gamma_p}\big)$ d'éléments de $\ker(\varphi)$ telle que tout élément $\overrightarrow{a}(X)$ de $\ker(\varphi)$ s'écrive de façon unique sous la forme

$$\overrightarrow{a}(X) = c_1(X)\overrightarrow{\gamma_1} + \cdots + c_p(X)\overrightarrow{\gamma_p},$$

où $c_1(X), \ldots, c_p(X) \in \mathbf{K}[X]$.

i) Vérifier que $\big(f(\overrightarrow{\varepsilon_1}) - X\overrightarrow{\varepsilon_1}, \ldots, f(\overrightarrow{\varepsilon_p}) - X\overrightarrow{\varepsilon_p}\big)$ est une $\mathbf{K}[X]$-base de $\ker(\varphi)$ : on trouve ainsi que les colonnes de la matrice $M - XI$ donnent une $\mathbf{K}[X]$-base de $\ker(\varphi)$ en fonction de la $\mathbf{K}[X]$-base $\big(\overrightarrow{\varepsilon_1}, \ldots, \overrightarrow{\varepsilon_p}\big)$ de $(\mathbf{K}[X])^p$.

ii) Montrer que les opérations sur les lignes et les colonnes de la matrice $M - XI$ correspondent à des changements de $\mathbf{K}[X]$-base de $(\mathbf{K}[X])^p$ et de $\ker(\varphi)$.

iii) En déduire qu'il existe une $\mathbf{K}[X]$-base $\big(\overrightarrow{\beta_1}, \ldots, \overrightarrow{\beta_p}\big)$ de $(\mathbf{K}[X])^p$ telle que

$$\big(e_1^M(X)\overrightarrow{\beta_1}, \ldots, e_p^M(X)\overrightarrow{\beta_p}\big)$$

soit une $\mathbf{K}[X]$-base de $\ker(\varphi)$.

5. On pose, pour $1 \leqslant i \leqslant p$, $e_i^M(X) = X^{n_i} - d_{i,n_i-1}X^{n_i-1} - \cdots - d_{i,1}X - d_{i,0}$.

i) Montrer que, si $n_i = 0$, on a $\varphi(\overrightarrow{\beta_i}) = \overrightarrow{0}$. Si $n_i > 0$, on pose $\varphi(\overrightarrow{\beta_i}) = \overrightarrow{\delta_i}$, montrer que, pour tout entier positif $j$, on a $\varphi(\overrightarrow{\beta_i}X^j) = f^j(\overrightarrow{\delta_i})$.

ii) Montrer que la famille $\mathcal{B}$ suivante est une base de $\mathbf{K}^p$ :

$$\mathcal{B} = \big(f^j(\overrightarrow{\delta_i}) \mid 1 \leqslant i \leqslant p,\ 0 \leqslant j \leqslant n_i - 1\big).$$

On pourra pour cela étudier l'image par $\varphi$ de la famille $\big(\overrightarrow{\beta_i}X^j \mid 1 \leqslant i \leqslant p,\ 0 \leqslant j\big)$.

6. Si $n_i > 0$, on appelle *matrice compagnon* du polynôme $e_i^M(X)$ la matrice carrée d'ordre $n_i$ suivante :

$$C_i^M = \begin{pmatrix} 0 & 0 & \cdots & 0 & d_{i,0} \\ 1 & 0 & \cdots & 0 & d_{i,1} \\ 0 & 1 & \cdots & 0 & d_{i,2} \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & d_{i,n_i-1} \end{pmatrix}.$$

i) Soit $i_0$ le plus petit $i$ tel que $n_i > 0$, montrer que la matrice de $f$ dans la base $\mathcal{B} = \left(\overrightarrow{\delta_{i_0}}, \ldots, f^{n_{i_0}-1}(\overrightarrow{\delta_{i_0}}), \overrightarrow{\delta_{i_0+1}}, \ldots\right)$ est la matrice $M_{\mathcal{B}}(f)$ diagonale par blocs dont les blocs diagonaux sont les matrices $C_{i_0}^M, \ldots, C_p^M$.

ii) Montrer que deux matrices $M$ et $N$ de $M_{p,p}(\mathbf{K})$ sont semblables si, et seulement si les deux matrices $M - XI$ et $N - XI$ ont les mêmes facteurs invariants. Ces polynômes $e_1^M(X), \ldots, e_p^M(X)$ sont appelés *les invariants de similitude* de la matrice $M$.

iii) On rappelle que les invariants de similitude de $M$ vérifient par construction : $e_i^M(X)$ divise $e_{i+1}^M(X)$, pour $1 \leqslant i \leqslant p-1$. Montrer que $e_p^M(X)$ est le polynôme minimal de l'endomorphisme $f$.

7. Soit $\alpha \in \mathbf{K}$, calculer les invariants de similitude des matrices $M$ et $N$ suivantes. Ces matrices sont-elles semblables ?

$$M = \begin{pmatrix} \alpha & 1 & 0 & 0 \\ 0 & \alpha & 0 & 0 \\ 0 & 0 & \alpha & 1 \\ 0 & 0 & 0 & \alpha \end{pmatrix} \text{ et } N = \begin{pmatrix} \alpha & 0 & 0 & 0 \\ 0 & \alpha & 0 & 0 \\ 0 & 0 & \alpha & 1 \\ 0 & 0 & 0 & \alpha \end{pmatrix}.$$