Agrégation interne de Mathématiques

session 2002

première composition

solution proposée par Dany-Jack Mercier

IUFM de Guadeloupe, Morne Ferret,
BP517, Abymes cedex 97178,
dany-jack.mercier@univ-ag.fr

NB : Le sujet de l'épreuve n'est pas joint à ce document. Il pourra être téléchargé sur le site http ://perso.wanadoo.fr/megamaths/

Préambule

P.1. On sait que $\mathbb{N}$ est un ensemble bien ordonné. Par suite la partie

$$\{\mathrm{st}\,(a)\ /\, a \in A\backslash\{0\}\}$$

de $\mathbb{N}$, qui n'est pas vide car $A\backslash\{0\} \neq \emptyset$, possèdera un plus petit élément.

P.2. Supposons que l'on ne soit pas dans le premier cas, autrement dit qu'il n'existe pas d'élément r_1 de A qui divise tous les éléments de A. Soit $b \in A\backslash\{0\}$ tel que

$$\mathrm{st}\,(b) = \mathrm{Min}\,\{\mathrm{st}\,(a)\ /\, a \in A\backslash\{0\}\} = \mathrm{val}\,(A)\,.$$

L'élément b ne divise pas tous les éléments de A, aussi il existe $a \in A$ tel que

$$a = bq + r \quad \text{avec } r \neq 0 \text{ et } \mathrm{st}\,(r) < \mathrm{st}\,(b) = \mathrm{val}\,(A)\,.$$

Alors $\mathrm{val}\,(A \cup \{r\}) := \mathrm{Min}\,\{\mathrm{st}\,(a)\ /\, a \in (A \cup \{r\}) \setminus \{0\}\} = \mathrm{st}\,(r) < \mathrm{val}\,(A)$, et l'on obtient bien $\mathrm{val}\,(A \cup \{r\}) < \mathrm{val}\,(A)$.

P.3. Si la propriété était fausse, la question **P.2** permettrait de construire une suite $(u_n)_{n\in\mathbb{N}}$ de la façon suivante :

- on choisit r_0 dans $A\backslash\{0\}$ et l'on pose $u_0 = \mathrm{st}\,(r_0)$,
- une fois u_0, ..., u_n construits, on sait l'existence de r_{n+1} tel que

$$\mathrm{val}\,(A \cup \{r_0, ..., r_{n+1}\}) < \mathrm{val}\,(A \cup \{r_0, ..., r_n\})$$

(cf. **P.2**) et l'on pose $u_{n+1} = \mathrm{val}\,(A \cup \{r_0, ..., r_{n+1}\})$.
La suite d'entiers naturels (u_n) est alors strictement décroissante, ce qui est absurde.

P.4. r_n divise tous les éléments de B, donc à fortiori tous les éléments de A, et divisera ainsi le pgcd e de ces éléments. Réciproquement, e divise tous les éléments de A, donc aussi, en procédant de proche en proche, tous les éléments de B (en effet, r_1 s'écrit sous la forme $r_1 = a_1 - b_1 q$ où a_1 et b_1 sont des éléments de A, et e, qui divise a_1 et b_1, divisera nécessairement r_1 ; puis on recommence en écrivant r_2 sous la forme $r_2 = a_2 - b_2 q$ où a_2 et b_2 sont des éléments de $A \cup \{r_1\}$ et en constatant que e, qui divise a_2 et b_2, divisera nécessairement r_2 ; et ainsi de suite jusqu'à arriver à r_n).
Finalement r_n divise e, et e divise r_n, donc r_n et e sont associés (par définition, deux éléments sont associés s'ils sont égaux à une constante multiplicative inversible près).

P.5. L'entier 3 définit une opération élémentaire sur A puisque $15 = 6 \times 2 + 3$ avec 15 et 6 dans A. On a $\mathrm{val}\,(A \cup \{3\}) = 3 < \mathrm{val}\,(A) = 6$. Mais 3 ne divise

pas tous les éléments de $A \cup \{3\}$, donc il faut continuer. Le seul élément de $A \cup \{3\}$ non divisible par 3 est 10, donc on calcule $10 = 3 \times 3 + 1$ et l'on constate que 1 définit une opération élémentaire sur $A \cup \{3\}$. On a

$$\mathrm{val}\,(A \cup \{1;3\}) = 1 < \mathrm{val}\,(A \cup \{3\}) < \mathrm{val}\,(A)\,.$$

On a terminé puisque 1 divise tous les éléments de $A \cup \{1;3\}$.

Première partie

I.1. Si $\det P$ est inversible dans E, alors $\det P \neq 0$ et P est inversible en tant que matrice dans $M_{p,p}(F)$. On sait alors que l'inverse P^{-1} de P dans $M_{p,p}(F)$ est donnée par la formule

$$P^{-1} = \frac{1}{\det P}\,{}^t\mathrm{com}\,P \qquad (*)$$

où la transposée ${}^t\mathrm{com}\,P$ de la comatrice de P appartient à $M_{p,p}(E)$. Comme $\det P$ est inversible dans E, $\frac{1}{\det P} \in E$ et $(*)$ montre que $P^{-1} \in M_{p,p}(E)$, autrement dit que P est inversible dans $M_{p,p}(E)$.

Réciproquement, si P est inversible dans $M_{p,p}(E)$, il existe une matrice P' de $M_{p,p}(E)$ telle que $PP' = P'P = I$, d'où $(\det P)(\det P') = 1 = (\det P')(\det P)$ avec $\det P$ et $\det P'$ dans E. Cela prouve que $\det P$ est inversible dans E, d'inverse $(\det P)^{-1} = \det P'$.

I.2. La relation $\overset{E}{\simeq}$ est réflexive puisque $M = I_p M I_q$, symétrique à partir du moment où $N = PMQ$ entraîne $M = P^{-1}NQ^{-1}$, et transitive puisque, si $N = PMQ$ et $T = P'NQ'$, alors $T = (P'P)\,M\,(QQ')$ avec $P'P$ et QQ' inversibles, soit $T \overset{E}{\simeq} M$.

I.3.i. Posons $A = (a_{ij})$, et notons l_i la i-ème ligne de A et c_j la j-ème colonne de A. On a

$$T_{ij}^{p}(b) = \begin{pmatrix} 1 & 0 & \cdots & & 0 \\ 0 & \ddots & & & \vdots \\ & & \ddots & b & \\ \vdots & & & \ddots & 0 \\ 0 & \cdots & & 0 & 1 \end{pmatrix}$$

où b est dans la i-ème ligne, j-ième colonne, donc

$$T_{ij}^{p}(b)A=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1q} \\ & \ddots & & \\ a_{i1}+ba_{j1} & a_{i2}+ba_{j2} & \ddots & a_{iq}+ba_{jq} \\ & & \ddots & \\ a_{p1} & a_{p2} & \cdots & a_{pq} \end{pmatrix}.$$

Ainsi la multiplication de A par $T_{ij}^{p}(b)$ à gauche conserve toutes les lignes de A sauf la i-ème qui est remplacée par l_i+bl_j. $T_{ij}^{p}(b)$ est une matrice de transvection et calculer $T_{ij}^{p}(b)A$ revient à faire l'opération élémentaire sur les lignes de A symbolisée par $l_i \leftarrow l_i+bl_j$. On vérifie de la même manière que le calcul de $AT_{ij}^{p}(b)$ correspond à une opération élémentaire sur les colonnes de A symbolisée par $c_j \leftarrow c_j+bc_i$. Le tableau ci-dessous récapitule le lien entre les produits de matrices demandées et les opérations sur les lignes ou les colonnes.

Produit matriciel :	Opération élémentaire sur les lignes :
$T_{ij}^{p}(b)A$	$l_i \leftarrow l_i+bl_j$
$S_{ij}^{p}A$	$l_i \longleftrightarrow l_j$
$D(u_1,...,u_p)A$	$\forall i \quad l_i \leftarrow u_i l_i$

Produit matriciel :	Opération élémentaire sur les colonnes :
$AT_{ij}^{q}(b)$	$c_j \leftarrow c_j+bc_i$
AS_{ij}^{q}	$c_i \longleftrightarrow c_j$
$AD(u_1,...,u_q)$	$\forall i \quad c_j \leftarrow u_j c_j$

Remarque : $T_{ij}^{p}(b)$ est une matrice de transvection et S_{ij}^{p} est une matrice de transposition.

I.3.ii. $\star$ Soit f l'endomorphisme de F^p de matrice $T_{ij}^{p}(b)$ dans la base canonique $e=(e_1,...,e_p)$ de F^p. On a

$$\begin{cases} f(e_\alpha)=e_\alpha \text{ si } \alpha \neq j, \\ f(e_j)=e_j+be_i. \end{cases}$$

Il suffit de définir l'endomorphisme $g: F^p \to F^p$ par

$$\begin{cases} g(e_\alpha)=e_\alpha \text{ si } \alpha \neq j, \\ g(e_j)=e_j-be_i, \end{cases}$$

pour obtenir $f\circ g(e_\alpha)=g\circ f(e_\alpha)=e_\alpha$ pour tout vecteur e_α de la base e. Cela signifie que $f\circ g=g\circ f=Id$, autrement dit que f est bijective d'inverse

g. On en déduit que la matrice $T_{ij}^{p}(b)$ est inversible dans $M_{p,p}(F)$ et d'inverse $\left(T_{ij}^{p}(b)\right)^{-1} = T_{ij}^{p}(-b)$. Comme $T_{ij}^{p}(-b) \in M_{p,p}(E)$, la matrice $T_{ij}^{p}(b)$ sera bien inversible dans $M_{p,p}(E)$.

Remarque : Une autre façon d'arriver à ce résultat est de rappeler que $T_{ij}^{p}(b) A$ correspond à l'opération élémentaire $l_i \leftarrow l_i + bl_j$, si bien que

$$T_{ij}^{p}(-b) T_{ij}^{p}(b) A$$

correspond à l'opération $l_i \leftarrow l_i + bl_j$ suivie de $l_i \leftarrow l_i - bl_j$, autrement dit ne transforme pas les lignes de A. On a donc $T_{ij}^{p}(-b) T_{ij}^{p}(b) A = A$ pour toute matrice A, et en particulier avec $A = I$, ce qui donne $T_{ij}^{p}(-b) T_{ij}^{p}(b) = I$. On recommence dans l'autre sens pour obtenir $T_{ij}^{p}(b) T_{ij}^{p}(-b) = I$ et conclure à l'inversibilité de $T_{ij}^{p}(b)$.

$\star$ Le produit $S_{ij}^{p} A$ correspond à l'opération élémentaire $l_i \longleftrightarrow l_j$ d'échange des i-èmes et j-èmes lignes de A, donc $S_{ij}^{p} S_{ij}^{p} A = A$. Il suffit de remplacer A par I pour obtenir $S_{ij}^{p} S_{ij}^{p} = I$ et constater que S_{ij}^{p} est inversible dans $M_{p,p}(E)$ d'inverse elle-même. La matrice de transposition S_{ij}^{p} est involutive.

$\star$ Le produit $D(u_1, ..., u_p) A$ transforme chacune des lignes l_i de A en $u_i l_i$. Les u_i sont inversibles par hypothèse, et l'on constate que

$$D\left(u_1^{-1}, ..., u_p^{-1}\right) D(u_1, ..., u_p) A = A.$$

Si $A = I$, on obtient $D\left(u_1^{-1}, ..., u_p^{-1}\right) D(u_1, ..., u_p) = I$, et l'on vérifierait de même que $D(u_1, ..., u_p) D\left(u_1^{-1}, ..., u_p^{-1}\right) = I$, donc $D(u_1, ..., u_p)$ est inversible dans $M_{p,p}(E)$ d'inverse $D\left(u_1^{-1}, ..., u_p^{-1}\right)$.

$\star$ Récapitulons :

$$\left(T_{ij}^{p}(b)\right)^{-1} = T_{ij}^{p}(-b) \ ; \ \left(S_{ij}^{p}\right)^{-1} = S_{ij}^{p} \text{ et } \left(D(u_1, ..., u_p)\right)^{-1} = D\left(u_1^{-1}, ..., u_p^{-1}\right).$$

I.3.iii. La propriété est triviale lorsqu'il s'agit de $S_{ij}^{p} A$ ou de $A S_{ij}^{q}$ puisqu'il y a seulement eu permutation de deux lignes ou de deux colonnes. Pour ce qui concerne $D(u_1, ..., u_p) A$, il s'agit de vérifier que le pgcd des coefficients a_{ij} de A coïncide avec celui des mêmes éléments multipliés par l'une quelconque des unités u_1,..., u_p de E. C'est trivial puisque le pgcd et son calcul est défini au produit par une unité de E près (pour deux éléments, cela s'écrit $\text{pgcd}(a, b) = \text{pgcd}(ua, vb)$ où u et v sont des unités de E, et se prouve en écrivant, par exemple, $aE + bE = (au) E + (bv) E$). Le cas $AD(u_1, ..., u_q)$ se traite de la même façon.

Si $b \in E$, alors $\text{pgcd}(x, y) = \text{pgcd}(x, y + bx)$ puisque les diviseurs communs à x et y d'une part, et à x et $y + bx$ d'autre part, coïcident. Donc la propriété est encore vraie pour $T_{ij}^{p}(b) A$ et $A T_{ij}^{q}(b)$.

I.4.i. Si l'un des quatre termes ne divise pas les trois autres, on peut toujours faire des permutations de lignes ou de colonnes pour aboutir à une matrice A telle que $\mathrm{val}(A) = \mathrm{st}(a)$. On envisage alors 2 cas :

a) Si a ne divise pas b ou ne divise pas c, par exemple si a ne divise pas b, la division euclidienne de b par a s'écrit $b = aq + r$ avec $r \neq 0$ et $\mathrm{st}(r) < \mathrm{st}(a)$. L'opération $A \mapsto AT_{1,2}^2(-q)$ sur les colonnes fait passer de A à

$$B = \begin{pmatrix} a & r \\ c & d - cq \end{pmatrix}$$

et l'on obtient $\mathrm{val}(B) \leq \mathrm{st}(r) < \mathrm{st}(a) = \mathrm{val}(A)$.

b) Si a divise b et c, il ne divise pas d et l'on peut écrire $d = aq + r$ avec $r \neq 0$ et $\mathrm{st}(r) < \mathrm{st}(a)$. Posons alors $b = ab'$ et $c = ac'$.

• Si c' est inversible, on utilise les opérations suivantes :

$$\begin{aligned} A &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & ab' \\ ac' & aq + r \end{pmatrix} \\ &\rightsquigarrow AD(1, c') = \begin{pmatrix} a & ab'c' \\ ac' & ac'q + rc' \end{pmatrix} \\ &\rightsquigarrow AD(1, c') T_{12}^2(-q) = \begin{pmatrix} a & ab'c' - qa \\ ac' & rc' \end{pmatrix} \\ &\rightsquigarrow B := D\left(1, \frac{1}{c'}\right) AD(1, c') T_{12}^2(-q) = \begin{pmatrix} a & ab'c' - qa \\ a & r \end{pmatrix} \end{aligned}$$

avec finalement $\mathrm{val}(B) \leq \mathrm{st}(r) < \mathrm{st}(a) = \mathrm{val}(A)$.

• Si c' n'est pas inversible, on utilise l'opération élémentaire $l_2 \leftarrow l_2 + (1 - c')\, l_1$ pour se ramener au cas précédent. On passe ainsi de A à A' :

$$\begin{aligned} A &= \begin{pmatrix} a & b \\ ac' & d \end{pmatrix} \\ &\rightsquigarrow A' = \begin{pmatrix} a & b \\ ac' + (1 - c')\, a & d + (1 - c')\, b \end{pmatrix} = \begin{pmatrix} a & b \\ a & d + (1 - c')\, b \end{pmatrix}, \end{aligned}$$

et l'on peut appliquer le cas précédent à A' puisque le coefficient de la seconde ligne, première colonne, de A' est a et vérifie bien $a = a \times 1$ avec 1 inversible.

I.4.ii. • Les opérations élémentaires sur les lignes et les colonnes de A conservent le pgcd des coefficients des matrices d'après **I.3.iii**, si bien qu'il suffise de prouver qu'il existe une matrice C telle que $C \overset{E}{\simeq} A$ et $C = \begin{pmatrix} e_1 & * \\ * & * \end{pmatrix}$ où e_1

divise les coefficients $*$ pour être assuré d'obtenir l'égalité $e_1 = \text{pgcd}\,(a, b, c, d)$. On construit C en utilisant un nombre fini de fois la question **I.4.i** :

De deux choses l'une :

a) Si A est telle que l'un des coefficients a, b, c, d divise les trois autres, on peut permuter des lignes et des colonnes pour placer ce diviseur commun à la place de a et obtenir C.

b) Sinon, il existe des opérations élémentaires qui nous fassent passer de A à B telle que $\text{val}\,(B) < \text{val}\,(A)$. Comme B n'est pas nulle (sinon $C \overset{E}{\simeq} A$ entraînerait $A = 0$, absurde), on peut appliquer **I.4.i** à nouveau et tomber dans l'un des deux cas a) et b), et ainsi de suite...

Le processus s'arrête en fait nécessairement après un nombre fini de pas sur le cas a) en nous fournissant une matrice $C = \begin{pmatrix} e_1 & * \\ * & * \end{pmatrix}$ équivalente à A dont le coefficient e_1 divise tous les coefficients $*$. En effet, si le processus retombait sans cesse sur le cas b), il permettrait de définir une suite strictement décroissante (u_n) d'entiers naturels formée des valuations des différentes matrices construites en b) : $u_0 = \text{val}\,(A) > u_1 = \text{val}\,(B) > u_2 = \text{val}\,(B_2) > ...$, ce qui est absurde.

• On passe facilement de C à D en utilisant des matrices de transvections :

$$\begin{aligned} C &= \begin{pmatrix} e_1 & e_1 b' \\ e_1 c' & e_1 d' \end{pmatrix} \\ &\rightsquigarrow \begin{pmatrix} e_1 & e_1 b' \\ 0 & e_1 d' - e_1 b' c' \end{pmatrix} \text{ par l'opération élémentaire } l_2 \leftarrow l_2 - c' l_1 \\ &\rightsquigarrow \begin{pmatrix} e_1 & 0 \\ 0 & e_1 d' - e_1 b' c' \end{pmatrix} = D \text{ par l'opération élémentaire } c_2 \leftarrow c_2 - b' c_1. \end{aligned}$$

• On a obtenu une matrice $D = \begin{pmatrix} e_1 & 0 \\ 0 & e_2 \end{pmatrix}$ équivalente à A avec $e_2 \in E$. Supposons $e_2 \neq 0$. Si $E = \mathbb{Z}$, on peut éventuellement diviser la seconde colonne de D par -1, qui est bien inversible dans $\mathbb{Z}$, pour se ramener à $e_2 > 0$. Si $E = K\,[X]$, on peut diviser la seconde colonne de D par le coefficient dominant du polynôme e_2 (coefficient qui est bien inversible dans $K\,[X]$) pour se ramener à un polynôme e_2 unitaire.

I.4.iii. • On a vu que les matrices $T_{ij}^p\,(b)$, S_{ij}^p et $D\,(u_1, ..., u_p)$ sont inversibles dans $M_{p,p}\,(E)$ (**I.3.ii**) et cela entraîne que leurs déterminants sont des éléments inversibles de E (**I.1**). Par suite deux matrices équivalentes D et A seront égales à un coefficient multiplicateur u inversible dans E près, i.e. il existe $u \in E$ inversible tel que $\det D = u \times \det A$, et cela s'écrit $e_1 e_2 = u \det A$.

• Comme $e_1 = \operatorname{pgcd}(a,b,c,d)$ et comme le pgcd est conservé par opérations élémentaires (**I.3.iii**), on aura $e_1 = \operatorname{pgcd}(e_1,0,0,e_2)$, ce qui traduit la divisibilité de e_2 par e_1.

• Si $A \overset{E}{\simeq} \begin{pmatrix} e_1 & 0 \\ 0 & e_2 \end{pmatrix} \overset{E}{\simeq} \begin{pmatrix} e'_1 & 0 \\ 0 & e'_2 \end{pmatrix}$ avec $e_1|e_2$ et $e'_1|e'_2$, nécessairement $e_1 = e'_1 = \operatorname{pgcd}(a,b,c,d)$, puis $e_1e_2 = u \det A$ et $e'_1e'_2 = v \det A$ avec u et v inversibles dans E. On en déduit $e_1e_2 = uv^{-1}e'_1e'_2$ puis $e_2 = uv^{-1}e'_2$, et l'on peut seulement affirmer que les éléments e_2 sont e'_2 associés (i.e. égaux à multiplication près par un inversible de E). Comme l'on décide de choisir e_1 positif (resp. unitaire) lorsque $E = \mathbb{Z}$ (resp. $K[X]$) on peut conclure à $e_2 = e'_2$ et à l'unicité du couple (e_1, e_2).

I.4.iv. Si A et A' ont même facteur invariant (e_1, e_2), il existe des matrices inversibles P, Q, P', Q' telles que $D = PAQ = P'A'Q'$, d'où

$$A = P^{-1}P'A'Q'Q^{-1}$$

et A sera équivalente à A'.

I.4.v. • Si $A \overset{E}{\simeq} A'$, il existe des matrices inversibles P, Q telles que $A' = PAQ$. Cela entraîne $\det A' = (\det P)(\det A)(\det Q)$ avec $\det P$ et $\det Q$ inversibles dans E. Par suite les éléments $\det A'$ et $\det A$ sont associés dans E, et il existe u inversible dans E tel que $\det A' = u(\det A)$. Pour conclure à l'égalité des facteurs invariants de A et A' en utilisant le même raisonnement qu'en **I.4.iii.**, il reste seulement à vérifier que les pgcd de A et A' sont égaux (à multiplication près par un inversible de E). Cela provient du Lemme suivant (écrit pour un produit PA mais qui s'applique aussi à un produit AP) :

Lemme : Si $A' = PA$ avec P inversible dans $M_{p,p}(E)$, alors $\operatorname{pgcd}(A') = \operatorname{pgcd}(A)$ où $\operatorname{pgcd}(A)$ désigne le pgcd des coefficients de la matrice A, défini à multiplication par un facteur inversible près.

preuve du lemme : Il suffit de noter que

$$P = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

et $A' = PA = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \alpha a + \beta c & \alpha b + \beta d \\ \gamma a + \delta c & \gamma b + \delta d \end{pmatrix} := \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$.

Tout diviseur w de a, b, c, d sera obligatoirement un diviseur de $a' = \alpha a + \beta c$, $b' = \alpha b + \beta d$, $c' = \gamma a + \delta c$, $d' = \gamma b + \delta d$. Réciproquement, tout diviseur w de a', b', c', d' divisera aussi a, b, c, d pour exactement les mêmes raisons, puisque l'on peut encore écrire $A = P^{-1}A'$ avec P^{-1} à coefficients dans E. ■

I.5. On a la succession d'opérations élémentaires suivantes :

$$\begin{pmatrix} 6 & 10 \\ 10 & 15 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 6 & 10 \\ 4 & 5 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 2 & 5 \\ 4 & 5 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 2 & 3 \\ 4 & 1 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix}$$
$$\rightsquigarrow \begin{pmatrix} 1 & 4 \\ 3 & 2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 4 \\ 0 & -10 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 \\ 0 & -10 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 \\ 0 & 10 \end{pmatrix},$$

puis

$$\begin{pmatrix} 6 & 12 \\ 12 & 15 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 6 & 12 \\ 6 & 3 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 0 & 9 \\ 6 & 3 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 6 & 3 \\ 0 & 9 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 3 & 6 \\ 9 & 0 \end{pmatrix}$$
$$\rightsquigarrow \begin{pmatrix} 3 & 6 \\ 0 & -18 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 3 & 0 \\ 0 & -18 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 3 & 0 \\ 0 & 18 \end{pmatrix}.$$

Remarque : Les facteurs invariants des deux matrices proposées sont $(1, 10)$ et $(3, 18)$. Ils sont distincts donc ces matrices ne sont pas E-équivalentes. On aurait pu le voir plus rapidement en notant que les pgcd des coefficients de ces deux matrices sont différents.

Deuxième partie

II.1.i. On procède comme à la question **I.3.i**. en montrant qu'il existe des opérations élémentaires qui font passer de $A = (a_{ij})_{1\leq i\leq p,\, 1\leq j\leq q}$ à une matrice dont le premier coefficient a_{11} divise tous les autres. On peut toujours supposer que $a_{11} = \mathrm{val}\,(A)$ quitte à permuter des lignes et des colonnes de A. Si a_{11} ne divise pas tous les autres coefficients, il existe i, j tels que a_{11} ne divise pas a_{ij}, et l'on peut toujours utiliser la matrice extraite $\begin{pmatrix} a_{11} & a_{1j} \\ a_{i1} & a_{ij} \end{pmatrix}$ si i et j sont différents de 1, ou n'importe quelle matrice 2×2 contenant a_{11} et a_{ij} si i ou j vaut 1, puis appliquer **I.3.i** pour remplacer cette sous-matrice par une matrice $Q = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ telle que $\mathrm{val}\,(Q) < \mathrm{val}\,(A) = a_{11}$. La matrice A' de type $p \times q$ obtenue à partir de A vérifie alors $\mathrm{val}\,(A') < \mathrm{val}\,(A)$, si bien que l'on ne puisse pas obtenir ce cas une infinité de fois (cela donnerait naissance à une suite de valences de matrices $\mathrm{val}\,(A)$ strictement décroissante dans $\mathbb{N}$, ce qui est absurde). Au bout d'un nombre fini de pas, on tombe donc sur une matrice $A'' = (a_{ij})$ (que l'on notera avec des coefficients non primés pour ne pas surcharger les notations) telle que a_{11} divise tous les autres coefficients.

Puisque a_{11} divise tous les coefficients a_{21}, ..., a_{p1}, un travail sur les lignes de A (avec des opérations élémentaires du style $l_i \longleftarrow l_i + bl_j$) permet de se

ramener à une matrice du type

$$A''' = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1,q+1} \\ 0 & & & \\ \vdots & & & \\ & & & \\ 0 & a_{p,2} & \cdots & a_{p,q+1} \end{pmatrix}$$

où a_{11} divise toujours tous les coefficients. En travaillant ensuite sur les colonnes (et toujours en utilisant des opérations élémentaires $c_i \longleftarrow c_i + bc_j$), on obtient la matrice B désirée.

Clairement $\operatorname{rg}(A') = \operatorname{rg}(A) - 1$.

II.1.ii. On montre le résultat par récurrence sur $m := p + q$ en utilisant la question précédente. La propriété est vraie si $p + q = 1$, et démontrée en **I.4** si $p + q = 2$. Si $p + q \geq 3$, **II.1.i** montre l'existence d'une matrice A' de type $(p-1, q-1)$ telle que

$$A \overset{E}{\simeq} \begin{pmatrix} e_1 & 0 \\ 0 & A' \end{pmatrix}$$

où e_1 divise tous les coefficients de A'. L'hypothèse récurrente appliquée à A' montre l'existence d'un certain nombre d'opérations élémentaires qui transforment A' en $\begin{pmatrix} \mathrm{D}(e_2, ..., e_r) & 0 \\ 0 & 0 \end{pmatrix}$ avec $e_2 | e_3$, ..., $e_{r-1} | e_r$. On passera donc de A à $\begin{pmatrix} \mathrm{D}(e_1, ..., e_r) & 0 \\ 0 & 0 \end{pmatrix}$ en utilisant des opérations élémentaires. Comme e_1 divise le pgcd des coefficients de A', et comme le pgcd des coefficients de A' est égal à celui de $\mathrm{D}(e_2, ..., e_r)$ (en effet, la question **I.3** montre que deux matrices qui se déduisent l'une de l'autre par opérations élémentaires ont des "pgcd" égaux), on obtient aussi $e_1 | e_2$.

II.1.iii. La question **II.1.ii** montre l'existence de deux matrices A et B, qui sont des produits de matrices du type $T_{ij}^p(b)$, S_{ij}^p et $D(u_1, ..., u_p)$, et telles que $APB = C$ où $C = \begin{pmatrix} \mathrm{D}(e_1, ..., e_r) & 0 \\ 0 & 0 \end{pmatrix}$. Comme A, P et C sont inversibles dans $M_{p,p}(E)$, la matrice diagonale C sera inversible dans $M_{p,p}(E)$, et cela signifie que tous ses coefficients diagonaux sont inversibles dans E. Donc $r = p$ et les e_i sont des unités de E. Il suffit d'écrire

$$P = A^{-1} C B^{-1} = A^{-1} \mathrm{D}(e_1, ..., e_r) B^{-1}$$

et de noter que les matrices inverses A^{-1} et B^{-1} sont encore des produits de matrices du type $T_{ij}^p(b)$, S_{ij}^p et $D(u_1, ..., u_p)$ (**I.3.ii**) pour conclure.

II.1.iv. A et A' sont E-équivalentes si et seulement si il existe des matrices inversibles P et Q telles que $A' = PAQ$. La question **II.1.iii** montre que P et Q sont des produits de matrices du type $T_{ij}^{p}(b)$, S_{ij}^{p} et $D(u_1, ..., u_p)$ et l'on sait que le produit à gauche par P (resp. à droite par Q) correspondent à des opérations élémentaires successives sur les lignes (resp. les colonnes) de A.

II.2.i. • A toute matrice A associons l'ensemble $\Lambda_m(A)$ des mineurs d'ordre m extraits de A, et notons $\text{pgcd}(\Lambda_m(A))$ le pgcd des éléments de $\Lambda_m(A)$. Si A' se déduit de A par une suite d'opérations élémentaires, alors il est facile de voir que $\Lambda_m(A') = \Lambda_m(A)$ si l'opération est du type $l_i \longleftrightarrow l_j$ ou $l_i \longleftarrow l_i + bl_j$, et que les éléments de $\Lambda_m(A')$ et $\Lambda_m(A)$ sont deux à deux associés dans E (i.e. pour tout $x \in \Lambda_m(A')$ et $y \in \Lambda_m(A)$ il existe un inversible v de E tel que $x = vy$) si l'opération est $(\forall i \quad l_i \leftarrow u_i l_i)$. Un travail sur les colonnes donnerait les mêmes résultats, et l'on peut en déduire l'égalité $\text{pgcd}(\Lambda_m(A')) = \text{pgcd}(\Lambda_m(A))$.

En effet, l'échange de lignes ou de colonnes n'a aucun effet sur le calcul des mineurs de la matrices. L'opération élémentaire $l_i \longleftarrow l_i + bl_j$ n'a pas plus d'effet sur les mineurs de A puisqu'un déterminant est invariant si l'on remplace une ligne par elle-même additionnée à une combinaison linéaires des autres lignes (le déterminant est une forme multilinéaire alternée). Enfin l'opération $(\forall i \quad l_i \leftarrow u_i l_i)$ correspondant au produit à gauche par $D(u_1, ..., u_p)$ transforme les lignes des matrices d'ordre m extraites de A en des multiples de ces lignes. Comme les nombres u_i sont inversibles dans E, les mineurs d'ordre m de $D(u_1, ..., u_p)A$ seront les produits des mineurs d'ordre m de A par des produits $v := u_{i_1}...u_{i_m}$ d'unités de E.

• Si $A \overset{E}{\simeq} C$, où C donnée en **II.1.ii**, l'égalité $\text{pgcd}(\Lambda_m(A)) = \text{pgcd}(\Lambda_m(C))$ montre qu'il suffit de prouver le résultat suivant : Pour tout $m \in \mathbb{N}_r$, le produit $e_1...e_m$ est un pgcd des mineurs d'ordre m de C. Ce qui s'énonce aussi

$$\forall m \in \mathbb{N}_r \quad e_1...e_m = \text{pgcd}(\Lambda_m(C)).$$

Pour le voir, considérons une matrice carrée $M = (m_{ij})$ d'ordre m extraite de C. Si le premier coefficient m_{11} de cette matrice est 0, alors la première ligne ou la première colonne de C est entièrement nulle et le mineur associé à M est nul. Les seuls mineurs d'ordre m de C et éventuellent non nuls vérifient donc $m_{11} = e_{i_1}$ avec $i_1 \in \mathbb{N}_r$. Mais alors

$$M = \begin{pmatrix} e_{i_1} & 0 & \cdots & 0 \\ 0 & \# & \# & \# \\ \vdots & \# & \# & \# \\ 0 & \# & \# & \# \end{pmatrix}$$

où la matrice $\begin{pmatrix} \# & \# & \# \\ \# & \# & \# \\ \# & \# & \# \end{pmatrix}$ est une matrice carrée d'ordre $m-1$ extraite de C. Le même raisonnement s'applique : le premier coefficient de cette matrice est de la forme e_{i_2} avec $i_1 < i_2 \leq r$ à moins que le déterminant de cette matrice vale zéro. Finalement, on a montré que tous les mineurs d'ordre m extraits de C étaient de la forme $e_{i_1}e_{i_2}...e_{i_r}$, i.e.

$$\Lambda_m(C) = \{e_{i_1}e_{i_2}...e_{i_r} \,/\, 1 \leq i_1 < ... < i_m \leq r\}.$$

Comme $e_1|e_2|....|e_m$ on constate que $e_1e_2....e_m$ divise tous les éléments de $\Lambda_m(C)$, autrement dit que $e_1...e_m = \operatorname{pgcd}(\Lambda_m(C))$.

II.2.ii. Si deux matrices

$$C = \begin{pmatrix} D(e_1,...,e_r) & 0 \\ 0 & 0 \end{pmatrix} \text{ et } C' = \begin{pmatrix} D\left(e'_1,...,e'_{r'}\right) & 0 \\ 0 & 0 \end{pmatrix}$$

satisfont les conditions de la question **II.1.ii**, alors $r = \operatorname{rg} A = r'$. La question **II.2.i** entraîne alors

$$\begin{cases} e_1 = \operatorname{pgcd}(\Lambda_1(A)) = e'_1 \\ e_1e_2 = \operatorname{pgcd}(\Lambda_2(A)) = e'_1e'_2 \\ .... \\ e_1...e_r = \operatorname{pgcd}(\Lambda_r(A)) = e'_1...e'_r \end{cases} \qquad \text{d'où } (e_1,...,e_r) = \left(e'_1,...,e'_{r'}\right).$$

Remarque : L'égalité $e_1 = \operatorname{pgcd}(\Lambda_1(A)) = e'_1$ entraîne en fait seulement l'existence d'un élément inversible u de E tel que $e_1 = ue'_1$, mais les éléments e_i ont tous été normalisés, si bien que l'on obtienne réellement l'égalité $e_1 = e'_1$.

II.2.iii. • Si A et A' ont les mêmes facteurs invariants $(e_1,...,e_r)$, il existe des matrices inversibles P, Q, P', Q' telles que $C = PAQ = P'A'Q'$, d'où $A = P^{-1}P'A'Q'Q^{-1}$ et l'on peut conclure à $A \overset{E}{\simeq} A'$.

• Réciproquement, si $A \overset{E}{\simeq} A'$, notons

$$C = \begin{pmatrix} D(e_1,...,e_r) & 0 \\ 0 & 0 \end{pmatrix} \quad \text{et} \quad C' = \begin{pmatrix} D\left(e'_1,...,e'_{r'}\right) & 0 \\ 0 & 0 \end{pmatrix}$$

où $(e_1,...,e_r)$ et $\left(e'_1,...,e'_{r'}\right)$ désignent les facteurs invariants respectifs de A et A'. On a $C \overset{E}{\simeq} A \overset{E}{\simeq} A' \overset{E}{\simeq} C'$, de sorte que $(e_1,...,e_r)$ et $\left(e'_1,...,e'_{r'}\right)$ soient tous les deux des facteurs invariants de A. L'unicité de la question **II.2.ii** entraîne alors $(e_1,...,e_r) = \left(e'_1,...,e'_{r'}\right)$.

II.3. On trouve par exemple

$$\begin{aligned} A &\rightsquigarrow \begin{pmatrix} 1 & 0 & \alpha - X \\ \alpha - X & 1 & 0 \\ 0 & \alpha - X & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & \alpha - X \\ 0 & 1 & -(\alpha - X)^2 \\ 0 & \alpha - X & 0 \end{pmatrix} \\ &\rightsquigarrow \begin{pmatrix} 1 & 0 & \alpha - X \\ 0 & 1 & -(\alpha - X)^2 \\ 0 & 0 & (\alpha - X)^3 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & (\alpha - X)^3 \end{pmatrix} \\ &\rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & (\alpha - X)^3 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & (X - \alpha)^3 \end{pmatrix} \end{aligned}$$

et les facteurs invariants de A sont $(1, 1, (X-\alpha)^3)$. Par ailleurs

$$\begin{aligned} B &\rightsquigarrow \begin{pmatrix} 0 & \alpha - X & 1 \\ \alpha - X & 0 & 0 \\ 0 & 0 & \alpha - X \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & \alpha - X & 0 \\ 0 & 0 & \alpha - X \\ \alpha - X & 0 & 0 \end{pmatrix} \\ &\rightsquigarrow \begin{pmatrix} 1 & \alpha - X & 0 \\ 0 & 0 & \alpha - X \\ 0 & -(\alpha - X)^2 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & \alpha - X \\ 0 & -(\alpha - X)^2 & 0 \end{pmatrix} \\ &\rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & \alpha - X & 0 \\ 0 & 0 & -(\alpha - X)^2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & X - \alpha & 0 \\ 0 & 0 & (X - \alpha)^2 \end{pmatrix} \end{aligned}$$

montre que les facteurs invariants de B sont $(1, X-\alpha, (X-\alpha)^2)$.

Troisième partie

III.1. Les matrices P et Q sont inversibles donc

$$\operatorname{rg}(M - XI) = rg \begin{pmatrix} e_1^M(X) & \cdots & 0 & 0 \\ \vdots & & \vdots & \vdots \\ 0 & \cdots & e_r^M(X) & 0 \\ 0 & & 0 & O \end{pmatrix} = r.$$

Si $r < p$, et si $\chi_M(X) := \det(M - XI)$ désigne le polynôme caractéristique de M, alors $\chi_M(X) = 0$. Cela signifie que le polynôme caractéristique de M est identiquement nul, ce qui est impossible (c'est un polynôme de $K[X]$ degré n). Donc $r = p$ et

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

Puisque P et Q sont inversibles dans $M_{p,p}(K[X])$, leurs déterminants $\det P$ et $\det Q$ sont des unités de $K[X]$, et l'on obtient

$$\chi_M(X) = \det(M - XI) = (\det P) \times (\det Q) \times \left(e_1^M(X) ... e_p^M(X)\right).$$

Il existe donc une unité de $K[X]$, c'est-à-dire une constante non nulle u de K^*, telle que $\chi_M(X) = u\left(e_1^M(X) ... e_p^M(X)\right)$.

III.2. Deux matrices M_1 et M_2 de $M_{p,p}(K)$ sont semblables si et seulement si il existe une matrice P inversible dans $M_{p,p}(K)$ telle que $M_2 = P^{-1}M_1P$. Dans ce cas

$$M_2 - XI = P^{-1}M_1P - XI = P^{-1}(M_1 - XI)P$$

avec P et P^{-1} à fortiori inversibles dans $K[X]$ (leurs déterminants seront en effet des constantes non nulles dans K) Cela signifie que $M_2 - XI$ et $M_1 - XI$ sont $K[X]$-équivalentes, et ont mêmes facteurs invariants (d'après **II.2.iii**).

III.3.i. L'application $\varphi : (K[X])^p \mapsto K^p$ est clairement linéaire. En effet, si λ appartient à K et si $\overrightarrow{a}(X) = \overrightarrow{a}_0 + ... + \overrightarrow{a}_n X^n$ et $\overrightarrow{b}(X) = \overrightarrow{b}_0 + ... + \overrightarrow{b}_n X^n$ désignent deux vecteurs de $(K[X])^p$, alors

$$\begin{aligned}
\varphi\left(\overrightarrow{a}(X) + \lambda\overrightarrow{b}(X)\right) &= \varphi\left((\overrightarrow{a}_0 + \lambda\overrightarrow{b}_0) + ... + (\overrightarrow{a}_n + \lambda\overrightarrow{b}_n)X^n\right) \\
&= (\overrightarrow{a}_0 + \lambda\overrightarrow{b}_0) + ... + f^n(\overrightarrow{a}_n + \lambda\overrightarrow{b}_n) \\
&= \overrightarrow{a}_0 + ... + f^n(\overrightarrow{a}_n) + \lambda\left[\overrightarrow{b}_0 + ... + f^n(\overrightarrow{b}_n)\right] \\
&= \varphi(\overrightarrow{a}_0 + ... + \overrightarrow{a}_n X^n) + \lambda\varphi(\overrightarrow{b}_0 + ... + \overrightarrow{b}_n X^n).
\end{aligned}$$

La surjectivité de φ est évidente : si $\overrightarrow{y} = (y_1, ..., y_p) \in K^p$, il suffit de voir que $\overrightarrow{y} \in K^p \subset (K[X])^p$ et que $\varphi(\overrightarrow{y}) := \overrightarrow{y}$ pour constater que $\overrightarrow{y} \in \operatorname{Im}\varphi$.

III.3.ii. L'application f étendue à $(K[X])^p$ est K-linéaire, donc

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

et la formule demandée sera montrée si l'on prouve que

$$f(\lambda(X)\overrightarrow{a}(X)) = \lambda(X) f(\overrightarrow{a}(X)).$$

Notons

$$\begin{cases} \lambda(X) = \lambda_0 + \lambda_1 X + ... + \lambda_m X^m \in K[X] \\ \overrightarrow{a}(X) = \overrightarrow{a}_0 + \overrightarrow{a}_1 X + ... + \overrightarrow{a}_n X^n \in (K[X])^p. \end{cases}$$

Par définition

$$\lambda(X)\overrightarrow{a}(X) = \sum_i \left(\sum_{u+v=i} \lambda_u \overrightarrow{a}_v\right) X^i$$

donc

$$\begin{aligned} f\left(\lambda\left(X\right)\overrightarrow{a}\left(X\right)\right) &= \sum_{i} f\left(\sum_{u+v=i}\lambda_u\overrightarrow{a}_v\right)X^i \\ &= \sum_{i}\left(\sum_{u+v=i}\lambda_u f\left(\overrightarrow{a}_v\right)\right)X^i = \lambda\left(X\right)f\left(\overrightarrow{a}\left(X\right)\right). \end{aligned}$$

III.3.iii. Par définition $\varphi\left(\overrightarrow{u}X\right) = f\left(\overrightarrow{u}\right)$.

III.3.iv. Le vecteur $\overrightarrow{v}\left(X\right) = \overrightarrow{v}_0 + \overrightarrow{v}_1 X + ... + \overrightarrow{v}_n X^n \in \left(K\left[X\right]\right)^p$ appartient à $\operatorname{Ker}\varphi$ si et seulement si

$$\varphi\left(\overrightarrow{v}\left(X\right)\right) = \overrightarrow{v}_0 + ... + f^n\left(\overrightarrow{v}_n\right) = \overrightarrow{0}. \qquad \left(\overline{1}\right)$$

Par ailleurs,

$$\begin{aligned} \overrightarrow{v}\left(X\right) = \left(f - XId\right)\left(\overrightarrow{w}\left(X\right)\right) &\Leftrightarrow \overrightarrow{v}\left(X\right) = \sum_{i=0}^{n} f\left(\overrightarrow{w}_i\right)X^i - X\sum_{i=0}^{n}\overrightarrow{w}_i X^i \\ &\Leftrightarrow \overrightarrow{v}\left(X\right) = f\left(\overrightarrow{w}_0\right) + \sum_{i=1}^{n}\left(f\left(\overrightarrow{w}_i\right) - \overrightarrow{w}_{i-1}\right)X^i - \overrightarrow{w}_n X^{n+1} \end{aligned}$$

donc l'existence de $\overrightarrow{w}\left(X\right)$ tel que $\overrightarrow{v}\left(X\right) = \left(f - XId\right)\left(\overrightarrow{w}\left(X\right)\right)$ équivaut à l'existence d'au moins une solution $\overrightarrow{w}_0$, ..., $\overrightarrow{w}_n$ au système

$$\left(\overline{2}\right)\begin{cases} \overrightarrow{v}_0 = f\left(\overrightarrow{w}_0\right) \\ \overrightarrow{v}_1 = f\left(\overrightarrow{w}_1\right) - \overrightarrow{w}_0 \\ ..... \\ \overrightarrow{v}_n = f\left(\overrightarrow{w}_n\right) - \overrightarrow{w}_{n-1} \\ \overrightarrow{0} = -\overrightarrow{w}_n \end{cases}, \text{ qui s'écrit } \left(\overline{3}\right)\begin{cases} \overrightarrow{v}_0 = f\left(\overrightarrow{w}_0\right) \\ \overrightarrow{v}_1 = f\left(\overrightarrow{w}_1\right) - \overrightarrow{w}_0 \\ ..... \\ \overrightarrow{v}_{n-1} = f\left(\overrightarrow{w}_{n-1}\right) - \overrightarrow{w}_{n-2} \\ \overrightarrow{v}_n = -\overrightarrow{w}_{n-1}. \end{cases}$$

Tout revient donc à prouver que $\left(\overline{1}\right)$ est équivalent à l'existence d'un n-uplet $\left(\overrightarrow{w}_0, ..., \overrightarrow{w}_{n-1}\right)$ qui vérifie le système $\left(\overline{3}\right)$. S'il existe un tel n-uplet, le système $\left(\overline{3}\right)$ entraîne

$$\begin{cases} \overrightarrow{v}_0 = f\left(\overrightarrow{w}_0\right) \\ \overrightarrow{v}_1 + \overrightarrow{w}_0 = f\left(\overrightarrow{w}_1\right) \\ ..... \\ \overrightarrow{v}_{n-1} + \overrightarrow{w}_{n-2} = f\left(\overrightarrow{w}_{n-1}\right) \\ \overrightarrow{v}_n + \overrightarrow{w}_{n-1} = \overrightarrow{0} \end{cases}$$

puis

$$\begin{cases} \overrightarrow{v}_0 = f\left(\overrightarrow{w}_0\right) \\ f\left(\overrightarrow{v}_1\right) + f\left(\overrightarrow{w}_0\right) = f^2\left(\overrightarrow{w}_1\right) \\ ..... \\ f^{n-1}\left(\overrightarrow{v}_{n-1}\right) + f^{n-1}\left(\overrightarrow{w}_{n-2}\right) = f^n\left(\overrightarrow{w}_{n-1}\right) \\ f^n\left(\overrightarrow{v}_n\right) + f^n\left(\overrightarrow{w}_{n-1}\right) = \overrightarrow{0} \end{cases}$$

en appliquant plusieurs fois f aux deux membres de chacune des lignes. Il suffit d'additionner les lignes du dernier système écrit pour obtenir

$$\overrightarrow{v}_0 + ... + f^n(\overrightarrow{v}_n) = \overrightarrow{0},$$

ce qui prouve $\left(\overline{1}\right)$. Réciproquement, si $\left(\overline{1}\right)$ est satisfait, les n dernières lignes du système $\left(\overline{3}\right)$ définissent un unique n-uplet $(\overrightarrow{w}_0, ..., \overrightarrow{w}_{n-1})$ (en opérant de proche en proche à partir du bas). Ce n-uplet vérifie

$$\begin{cases} \overrightarrow{v}_1 + \overrightarrow{w}_0 = f(\overrightarrow{w}_1) \\ \overrightarrow{v}_2 + \overrightarrow{w}_1 = f(\overrightarrow{w}_2) \\ ..... \\ \overrightarrow{v}_{n-1} + \overrightarrow{w}_{n-2} = f(\overrightarrow{w}_{n-1}) \\ \overrightarrow{v}_n + \overrightarrow{w}_{n-1} = \overrightarrow{0} \end{cases}$$

donc

$$\begin{cases} f(\overrightarrow{v}_1) + f(\overrightarrow{w}_0) = f^2(\overrightarrow{w}_1) \\ f^2(\overrightarrow{v}_2) + f^2(\overrightarrow{w}_1) = f^3(\overrightarrow{w}_2) \\ ..... \\ f^{n-1}(\overrightarrow{v}_{n-1}) + f^{n-1}(\overrightarrow{w}_{n-2}) = f^n(\overrightarrow{w}_{n-1}) \\ f^n(\overrightarrow{v}_n) + f^n(\overrightarrow{w}_{n-1}) = \overrightarrow{0}. \end{cases}$$

En additionnant membres à membres, on obtient

$$f(\overrightarrow{v}_1) + ... + f^n(\overrightarrow{v}_n) + f(\overrightarrow{w}_0) = \overrightarrow{0},$$

d'où $-\overrightarrow{v}_0 + f(\overrightarrow{w}_0) = \overrightarrow{0}$ (en tenant compte de $\left(\overline{1}\right)$), c'est-à-dire la première ligne de $\left(\overline{3}\right)$. Cela achève la démonstration.

Remarque : On vient de prouver que $\operatorname{Ker}\varphi = \operatorname{Im}(f - XId)$ ce qui possède bien un sens puisque $\varphi : (K[X])^p \mapsto K^p$ et $f - XId : (K[X])^p \mapsto (K[X])^p$.

III.4.i. La question précédente montre que

$$\overrightarrow{v}(X) \in \operatorname{Ker}\varphi \Leftrightarrow \exists\, \overrightarrow{w}(X) \in (K[X])^p \quad \overrightarrow{v}(X) = (f - XId)(\overrightarrow{w}(X)). \quad (1)$$

Comme $(\overrightarrow{\varepsilon}_1..., \overrightarrow{\varepsilon}_p)$ est une $K[X]$-base de $(K[X])^p$, tout vecteur $\overrightarrow{w}(X)$ de $(K[X])^p$ s'écrit sous la forme $\overrightarrow{w}(X) = b_1(X)\overrightarrow{\varepsilon}_1 + ... + b_p(X)\overrightarrow{\varepsilon}_p$, et (1) équivaut à

$$\exists\, b_1(X), ..., b_p(X) \quad \overrightarrow{v}(X) = \sum_{i=0}^{p} b_i(X)(f - XId)(\overrightarrow{\varepsilon}_i),$$

soit

$$\exists\, b_1(X), ..., b_p(X) \quad \overrightarrow{v}(X) = \sum_{i=0}^{p} b_i(X)(f(\overrightarrow{\varepsilon}_i) - X\overrightarrow{\varepsilon}_i)$$

Cela prouve que le système $(f(\overrightarrow{\varepsilon}_1) - X\overrightarrow{\varepsilon}_1, ..., f(\overrightarrow{\varepsilon}_p) - X\overrightarrow{\varepsilon}_p)$ engendre le $K[X]$-module $(K[X])^p$. Pour vérifier que c'est une base de ce $K[X]$-module, il suffit maintenant de prouver que c'est un système libre, autrement dit que

$$\sum_{i=0}^{p} b_i(X)(f(\overrightarrow{\varepsilon}_i) - X\overrightarrow{\varepsilon}_i) = \overrightarrow{0} \Rightarrow \forall i \quad b_i(X) = 0.$$

On raisonne par l'absurde : s'il existait un polynôme-coefficient $b_i(X)$ non nul, on pourrait poser

$$m = \text{Max}\{\deg b_i(X) \ / \ i \in \mathbb{N}_p \text{ et } b_i(X) \neq 0\}$$

et $I = \{i \in \mathbb{N}_p \,/\, \deg b_i(X) = m\}$. Si $b_i(X)$ est de degré m, notons simplement $b_i(X) = \xi_i X^m + ...$ Il suffit alors d'égaler les coefficients des monômes de degrés $m+1$ dans l'égalité $\sum_{i=0}^{p} b_i(X)(f(\overrightarrow{\varepsilon}_i) - X\overrightarrow{\varepsilon}_i) = \overrightarrow{0}$ pour obtenir $\sum_{i\in I} b_i(X)\overrightarrow{\varepsilon}_i = \overrightarrow{0}$, d'où $b_i(X) = 0$ pour tout $i \in I$, ce qui est absurde.

III.4.ii. Les opérations élémentaires sur les lignes ou les colonnes de $M - XI$ reviennent à effectuer des produits de matrices du style $P(M - XI)Q$, avec $P, Q \in \left\{T_{ij}^p(b), S_{ij}^p, D(u_1, ..., u_p)\right\}$, donc reviennent exactement à effectuer des changements de bases sur les espaces $\text{Ker}\,\varphi$ et $(K[X])^p$, puisque

$$M - XI = \begin{array}{c} \begin{matrix} f(\overrightarrow{\varepsilon}_1) - X\overrightarrow{\varepsilon}_1 & \cdots & f(\overrightarrow{\varepsilon}_p) - X\overrightarrow{\varepsilon}_p \end{matrix} \\ \begin{pmatrix} \# & \cdots & \# \\ \# & & \# \\ \# & \cdots & \# \end{pmatrix} \end{array} \begin{matrix} \\ \overrightarrow{\varepsilon}_1 \\ \vdots \\ \overrightarrow{\varepsilon}_p. \end{matrix}$$

La matrice carrée P correspond à un changement de base de l'espace de départ $(K[X])^p$, tandis que la matrice Q correspond à un changement de base de l'espace d'arrivée $\text{Ker}\,\varphi$.

III.4.iii. Il suffit d'utiliser la question **III.1** et de mettre en oeuvre toutes les opérations élémentaires nécessaires pour aboutir à une matrice équivalente à $M - XI$ et de la forme

$$\begin{pmatrix} e_1^M(X) & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & e_p^M(X) \end{pmatrix}.$$

Cette matrice est celle de l'application linéaire de $(K[X])^p$ dans $\text{Ker}\,\varphi$ de matrice $M - XI$ dans les bases $(\overrightarrow{\varepsilon}_1..., \overrightarrow{\varepsilon}_p)$ de $(K[X])^p$, et

$$(f(\overrightarrow{\varepsilon}_1) - X\overrightarrow{\varepsilon}_1, ...f(\overrightarrow{\varepsilon}_p) - X\overrightarrow{\varepsilon}_p)$$

de $\operatorname{Ker}\varphi$. Par conséquent, il existe une base $(\overrightarrow{\beta}_1 ..., \overrightarrow{\beta}_p)$ de $(K[X])^p$ telle que

$$(e_1^M(X)\overrightarrow{\beta}_1 ..., e_p^M(X)\overrightarrow{\beta}_p)$$

soit une base de $\operatorname{Ker}\varphi$.

III.5.i. Comme $(e_1^M(X)\overrightarrow{\beta}_1 ..., e_p^M(X)\overrightarrow{\beta}_p)$ est une base de $\operatorname{Ker}\varphi$, on sait que

$$\forall i \quad \varphi(e_i^M(X)\overrightarrow{\beta}_i) = \overrightarrow{0}. \qquad (2)$$

En particulier, si $n_i = 0$, alors $e_i^M(X) = 1$ et $\varphi(\overrightarrow{\beta}_i) = \overrightarrow{0}$. Supposons maintenant que $n_i > 0$, et montrons que

$$\varphi(\overrightarrow{\beta}_i X^j) = f^j(\overrightarrow{\delta}_i).$$

Posons $\overrightarrow{\beta}_i = \overrightarrow{a}_0 + ... + \overrightarrow{a}_n X^n$. Alors $\varphi(\overrightarrow{\beta}_i) = \overrightarrow{a}_0 + ... + f^n(\overrightarrow{a}_n) := \overrightarrow{\delta}_i$ et l'on a, par définition de φ,

$$\begin{aligned}
\varphi(\overrightarrow{\beta}_i X^j) &= \varphi\left((\overrightarrow{a}_0 + ... + \overrightarrow{a}_n X^n) X^j\right) \\
&= \varphi\left(\overrightarrow{a}_0 X^j + ... + \overrightarrow{a}_n X^{n+j}\right) \\
&= f^j(\overrightarrow{a}_0) + ... + f^{n+j}(\overrightarrow{a}_n) \\
&= f^j[\overrightarrow{a}_0 + ... + f^n(\overrightarrow{a}_n)] \\
&= f^j(\varphi(\overrightarrow{\beta}_i)) := f^j(\overrightarrow{\delta}_i).
\end{aligned}$$

III.5.ii. • La famille $(\overrightarrow{\beta}_1 ..., \overrightarrow{\beta}_p)$ est une base de $(K[X])^p$ (**III.4.iii**), donc tout vecteur $\overrightarrow{a}(X)$ de $(K[X])^p$ s'exprime de façon unique sous la forme

$$\overrightarrow{a}(X) = b_1(X)\overrightarrow{\beta}_1 + ... + b_p(X)\overrightarrow{\beta}_p \qquad (3)$$

où $b_i(X) \in K[X]$. Par division euclidienne de $b_i(X)$ par $e_i^M(X)$, il existe deux polynômes $q_i(X)$ et $r_i(X)$ tels que

$$b_i(X) = e_i^M(X)\,q_i(X) + r_i(X) \quad \text{avec } \deg r_i \leq n_i.$$

L'application $\varphi : (K[X])^p \to K^p$ est K-linéaire surjective, donc tout élément de K^p s'exprimera sous la forme $\varphi(\overrightarrow{a}(X))$ avec

$$\begin{aligned}
\varphi(\overrightarrow{a}(X)) &= \varphi(b_1(X)\overrightarrow{\beta}_1 + ... + b_p(X)\overrightarrow{\beta}_p) \\
&= \varphi(b_1(X)\overrightarrow{\beta}_1) + ... \\
&= \varphi(e_1^M(X)\,q_1(X)\overrightarrow{\beta}_1) + \varphi(r_1(X)\overrightarrow{\beta}_1) + ...
\end{aligned}$$

Si l'on pose $q_1(X) = q_{1,0} + ... + q_1, m_1 X^{m_1}$, on obtient

$$\begin{aligned}\varphi(e_1^M(X)\, q_1(X)\, \overrightarrow{\beta}_1) &= \varphi((q_{1,0} + ... + q_{1,m_1} X^{m_1})\, e_1^M(X)\, \overrightarrow{\beta}_1) \\ &= \sum_{j=1}^{m_1} q_{1,j} \varphi(X^j e_1^M(X)\, \overrightarrow{\beta}_1),\end{aligned}$$

et le même calcul qu'en **III.5.i** montre que

$$\varphi(X^j e_1^M(X)\, \overrightarrow{\beta}_1) = f^j(\varphi(e_1^M(X)\, \overrightarrow{\beta}_i)) = f^j(0) = 0,$$

puisque $e_1^M(X)\, \overrightarrow{\beta}_i \in \operatorname{Ker}\varphi$ (d'après **II.4.iii**). Donc $\varphi(e_1^M(X)\, q_1(X)\, \overrightarrow{\beta}_1) = 0$ et

$$\varphi(\overrightarrow{a}(X)) = \varphi(r_1(X)\, \overrightarrow{\beta}_1) + ... + \varphi(r_p(X)\, \overrightarrow{\beta}_p).$$

Il suffit d'utiliser la K-linéarité de φ et d'écrire les polynômes $r_i(X)$ in extenso dans l'expression précédente, pour constater que la famille

$$\mathcal{B} = \left\{ \overrightarrow{\beta}_i X^j \,/\, 1 \leq i \leq p,\ 0 \leq j \leq n_i - 1 \right\}$$

est bien une famille K-génératrice de K^p.

• Montrons que $\mathcal{B}$ est une famille libre de K^p. Pour cela, considérons une combinaison liéaire nulle de la forme

$$\sum_{\substack{1 \leq i \leq p \\ 0 \leq j \leq n_i - 1}} \lambda_{ij}\, \overrightarrow{\beta}_i X^j = \overrightarrow{0}$$

avec $\lambda_{ij} \in K$. Cette combinaison s'écrit $\sum_{1 \leq i \leq p} \left(\sum_{0 \leq j \leq n_i - 1} \lambda_{ij} X^j \right) \overrightarrow{\beta}_i = \overrightarrow{0}$, ce qui entraîne $\sum_{0 \leq j \leq n_i - 1} \lambda_{ij} X^j = 0$ pour tout i (puisque $(\overrightarrow{\beta}_1 ..., \overrightarrow{\beta}_p)$ est une base de $(K[X])^p$). Par suite $\lambda_{ij} = 0$ pour tous i, j.

III.6.i. Il suffit de calculer les images des vecteurs de la base

$$\mathcal{B} = \left\{ \overrightarrow{\beta}_i X^j \,/\, 1 \leq i \leq p,\ 0 \leq j \leq n_i - 1 \right\} = (\overrightarrow{\delta}_{i_0}, ..., f^{n_{i_0}-1}(\overrightarrow{\delta}_{i_0}), ...)$$

par f en fonction des vecteurs de $\mathcal{B}$ pour obtenir le résulat. En effet

$$\begin{cases} f\left(f^j(\overrightarrow{\delta}_{i_0})\right) = f^{j+1}(\overrightarrow{\delta}_{i_0}) \text{ si } 0 \leq j \leq n_{i_0} - 2 \\ f\left(f^{n_{i_0}-1}(\overrightarrow{\delta}_{i_0})\right) = f^{n_{i_0}}(\overrightarrow{\delta}_{i_0}) = d_{i_0,0}\, \overrightarrow{\delta}_{i_0} + ... + d_{i_0,n_{i_0}-1} f^{n_{i_0}-1}(\overrightarrow{\delta}_{i_0}) \quad (*) \end{cases}$$

où la dernière égalité $(*)$ est justifiée par le raisonnement suivant. On sait que $(e_1^M(X)\, \overrightarrow{\beta}_1 ..., e_p^M(X)\, \overrightarrow{\beta}_p)$ est une base de $\operatorname{Ker}\varphi$, donc $\varphi(e_i^M(X)\, \overrightarrow{\beta}_i) = \overrightarrow{0}$, et cela s'écrit

$$\varphi\left(\left(X^{n_i} - d_{i,n_i-1} X^{n_i-1} - ... - d_{i,0}\right) \overrightarrow{\beta}_i\right) = \overrightarrow{0}$$

$$\varphi(X^{n_i}\overrightarrow{\beta}_i) - d_{i,n_i-1}\varphi(X^{n_i-1}\overrightarrow{\beta}_i)... - d_{i,0}\varphi(\overrightarrow{\beta}_i) = \overrightarrow{0},$$

ou encore, en appliquant **III.5.i**

$$f^{n_i}(\overrightarrow{\delta}_i) - d_{i,n_i-1}f^{n_i-1}(\overrightarrow{\delta}_i)... - d_{i,0}\overrightarrow{\delta}_i = \overrightarrow{0}$$

soit $f^{n_i}(\overrightarrow{\delta}_i) = d_{i,0}\overrightarrow{\delta}_i + ... + d_{i,n_i-1}f^{n_i-1}(\overrightarrow{\delta}_i)$ comme voulu.

III.6.ii. On a déjà vu en **II.2** que si M et N étaient semblables, alors $M-XI$ et $N-XI$ possédaient les mêmes facteurs invariants. Réciproquement, si $M-XI$ et $N-XI$ possèdent les mêmes facteurs invariants $e_1^M(X)$, ..., $e_p^M(X)$, la question **III.6.i** montre l'existence de deux bases "adaptées" à M et à N, dans lesquelles les matrices des applications linéaires f et g - de matrices M et N dans la base canonique de K^p - sont égales (en effet, les seuls coefficients qui interviennent dans la matrice bloc exhibée en **III.6.i** sont ceux des facteurs invariants $e_1^M(X)$, ..., $e_p^M(X)$). Cela signifie que les matrices M et N sont semblables.

III.6.iii. On démontre les deux résultats suivants :

Lemme 1 : Le polynôme caractéristique et le polynôme minimal de la matrice

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

sont respectivement $\chi(X) = (-1)^n e_i^M(X)$ et $m(X) = e_i^M(X)$, où

$$e_i^M(X) = X^{n_i} - d_{i,n_i-1}X^{n_i-1} - ... - d_{i,0}.$$

Preuve du Lemme 1 : Pour simplifier, notons C au lieu de C_i^M et n, d_j au lieu de n_i, $d_{i,j}$. On démontre que $\chi(X) = (-1)^n\left(X^n - d_{n-1}X^{n-1} - ... - d_0\right)$ par récurrence sur n. La propriété est triviale au rang $n = 2$. Au rang n, on calcule

$$\chi(X) = \det(C - XI) = \begin{vmatrix} -X & 0 & \cdots & 0 & d_0 \\ 1 & -X & \cdots & 0 & d_1 \\ & 1 & & & \\ \vdots & \vdots & \ddots & -X & \\ 0 & 0 & \cdots & 1 & d_{n-1} - X \end{vmatrix}$$

$$= -X\begin{vmatrix} -X & \cdots & 0 & d_1 \\ 1 & & & \\ \vdots & \ddots & -X & \\ 0 & \cdots & 1 & d_{n-1} - X \end{vmatrix} + (-1)^{n+1}d_0\begin{vmatrix} 1 & -X & \cdots & 0 \\ & 1 & & \\ \vdots & \vdots & \ddots & -X \\ 0 & 0 & \cdots & 1 \end{vmatrix}.$$

L'hypothèse récurrente appliquée au rang $n-1$ permet d'obtenir

$$\begin{aligned}\chi(X) &= -X(-1)^{n-1}\left(X^{n-1}-d_{n-1}X^{n-1}-...-d_1\right)+(-1)^{n+1}d_0\\ &= (-1)^n\left(X^n-d_{n-1}X^{n-1}-...-d_0\right)\end{aligned}$$

et de conclure.

Le polynôme minimal $m(X)$ de C est, par définition, l'unique polynôme unitaire de plus petit degré P qui est annulé par C, autrement dit qui satisfait $P(C)=0$.
On sait que $m(X)$ est un générateur de l'idéal $\{P\in K[X]\ /\ P(C)=0\}$, que $\chi(X)$ appartient à cet idéal (Théorème de Cayley-Hamilton) et que $m(X)$ divise $\chi(X)$. Pour démontrer que $m(X)=(-1)^n\chi(X)$, il suffira donc de prouver qu'aucun polynôme $P(X)$ non nul de degré $d<n$ ne vérifie $P(C)=0$.

Notons f l'endomorphisme de matrice C dans la base canonique $(e_1,...,e_n)$ de K^n. On a

$$C=\begin{pmatrix}0&0&\cdots&0&d_0\\1&0&\cdots&0&d_1\\&1&&&\\\vdots&\vdots&\ddots&0&\\0&0&\cdots&1&d_{n-1}\end{pmatrix}$$

donc

$$\begin{cases}f(e_1)=e_2\\ f^2(e_1)=f(e_2)=e_3\\ \cdots\\ f^{n-1}(e_1)=f(e_{n-1})=e_n\\ f^n(e_1)=f(e_n)=d_0e_1+d_1e_2+...+d_{n-1}e_n\end{cases}$$

et en particulier $f^j(e_1)=e_{n+j}$ pour tout $j\in\{1,...,n-1\}$. Si

$$P(X)=X^d-a_{d-1}X^{d-1}-...-a_0$$

était un polynôme de degré $d<n$ et tel que $P(f)=0$, on aurait

$$f^d=a_{d-1}f^{d-1}+...+a_1f+a_0Id,$$

donc a fortiori $f^d(e_1)=a_{d-1}f^{d-1}(e_1)+...+a_1f(e_1)+a_0e_1$, ce qui s'écrit encore $e_{d+1}=a_{d-1}e_d+...+a_1e_2+a_0e_1$, ce qui est absurde puisque $(e_1,...,e_n)$ est une base de K^n. ■

Lemme 2 : Soit f l'endomorphisme de matrice

$$M_{\mathcal{B}}(f)=\begin{pmatrix}C_{i_0}^M&&0\\&\ddots&\\0&&C_p^M\end{pmatrix}.$$

Le polynôme caractéristique de f est $\chi_f(X) = (-1)^p e_1^M(X)...e_p^M(X)$ et le polynôme minimal de f est $m_f(X) = e_p^M(X)$.

Preuve du Lemme 2 : Le calcul du polynôme caractéristique de f a déjà été fait en **III.2**, et il est facile à retrouver en calculant un déterminant par blocs et en appliquant le Lemme 1. Soit P un polynôme de $K[X]$. On a

$$\begin{array}{rcl} P(f)=0 & \Leftrightarrow & P(M_{\mathcal{B}}(f))=0 \\ & \Leftrightarrow & \left\{\begin{array}{l} P\left(C_{i_0}^M\right)=0 \\ \cdots \\ P\left(C_p^M\right)=0 \end{array}\right. \Leftrightarrow \left\{\begin{array}{l} m_{i_0}|P \\ \cdots \\ m_{i_p}|P \end{array}\right. \Leftrightarrow \text{ppcm}\left(m_{i_0},...,m_{i_p}\right)|P \end{array}$$

où $m_i(X)$ désigne le polynôme minimal de C_i^M, et cela montre que le polynôme minimal de f est $m_f(X) = \text{ppcm}\left(m_{i_0},...,m_{i_p}\right)$. Puisque $m_i = e_i^M(X)$ (Le Lemme 1), la chaîne ascendante de divisibilité $e_{i_0}^M(X)|e_{i_0+1}^M(X)|...|e_p^M(X)$ permet d'écrire $m_f(X) = \text{ppcm}\left(e_{i_0}^M(X),...,e_p^M(X)\right) = e_p^M(X)$. ■

III.7. Les matrices suivantes sont équivalentes :

$$\left(\begin{array}{cccc} \alpha-X & 1 & 0 & 0 \\ 0 & \alpha-X & 0 & 0 \\ 0 & 0 & \alpha-X & 1 \\ 0 & 0 & 0 & \alpha-X \end{array}\right); \left(\begin{array}{cccc} 1 & \alpha-X & 0 & 0 \\ \alpha-X & 0 & 0 & 0 \\ 0 & 0 & \alpha-X & 1 \\ 0 & 0 & 0 & \alpha-X \end{array}\right)$$

$$\left(\begin{array}{cccc} 1 & \alpha-X & 0 & 0 \\ 0 & -(\alpha-X)^2 & 0 & 0 \\ 0 & 0 & \alpha-X & 1 \\ 0 & 0 & 0 & \alpha-X \end{array}\right); \left(\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & -(\alpha-X)^2 & 0 & 0 \\ 0 & 0 & \alpha-X & 1 \\ 0 & 0 & 0 & \alpha-X \end{array}\right)$$

$$\left(\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -(\alpha-X)^2 \\ 0 & 1 & \alpha-X & 0 \\ 0 & \alpha-X & 0 & 0 \end{array}\right); \left(\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 1 & \alpha-X & 0 \\ 0 & 0 & 0 & -(\alpha-X)^2 \\ 0 & \alpha-X & 0 & 0 \end{array}\right)$$

$$\left(\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 1 & \alpha-X & 0 \\ 0 & 0 & 0 & -(\alpha-X)^2 \\ 0 & 0 & -(\alpha-X)^2 & 0 \end{array}\right); \left(\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -(\alpha-X)^2 \\ 0 & 0 & -(\alpha-X)^2 & 0 \end{array}\right)$$

$$\left(\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -(\alpha-X)^2 & 0 \\ 0 & 0 & 0 & -(\alpha-X)^2 \end{array}\right); \left(\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & (X-\alpha)^2 & 0 \\ 0 & 0 & 0 & (X-\alpha)^2 \end{array}\right)$$

et les invariants de similitude de M sont $\left(1, 1, (X-\alpha)^2, (X-\alpha)^2\right)$. On recommence avec N. Les matrices suivantes sont équivalentes :

$$\begin{pmatrix} \alpha-X & 0 & 0 & 0 \\ 0 & \alpha-X & 0 & 0 \\ 0 & 0 & \alpha-X & 1 \\ 0 & 0 & 0 & \alpha-X \end{pmatrix} ; \begin{pmatrix} 0 & 0 & 0 & \alpha-X \\ 0 & \alpha-X & 0 & 0 \\ 1 & 0 & \alpha-X & 0 \\ \alpha-X & 0 & 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & \alpha-X & 0 \\ 0 & \alpha-X & 0 & 0 \\ 0 & 0 & 0 & \alpha-X \\ \alpha-X & 0 & 0 & 0 \end{pmatrix} ; \begin{pmatrix} 1 & 0 & \alpha-X & 0 \\ 0 & \alpha-X & 0 & 0 \\ 0 & 0 & 0 & \alpha-X \\ 0 & 0 & -(\alpha-X)^2 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \alpha-X & 0 & 0 \\ 0 & 0 & 0 & \alpha-X \\ 0 & 0 & -(\alpha-X)^2 & 0 \end{pmatrix} ; \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \alpha-X & 0 & 0 \\ 0 & 0 & \alpha-X & 0 \\ 0 & 0 & 0 & -(\alpha-X)^2 \end{pmatrix}$$

et l'on obtient finalement

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & X-\alpha & 0 & 0 \\ 0 & 0 & X-\alpha & 0 \\ 0 & 0 & 0 & (X-\alpha)^2 \end{pmatrix}.$$

Les invariants de similitude de N sont donc $\left(1, X-\alpha, X-\alpha, (X-\alpha)^2\right)$. Ils sont différents de ceux de M, donc M et N ne sont pas semblables.

Remarque : Les matrices M et N sont données sous a forme de Jordan, et laissent voir des espaces propres associés à α de dimensions respectives 2 et 3, ce qui suffit pour affirmer qu'elles ne sont pas semblables.

That's all folks !