

Devoir surveillé n°7
CORRECTION

Problème - Décomposition de Froebenius

Dans toute cette partie, on note \mathbb{K} , un corps (qui est \mathbb{R} en première partie).
Pour tout polynôme $\pi \in \mathbb{K}[X]$, on note (π) l'ensemble $\pi \cdot \mathbb{K}[X] = \{\pi \times Q, Q \in \mathbb{K}[X]\}$.

n désigne un entier fixé dans tout le sujet et on fixe $M \in \mathcal{M}_n(\mathbb{R})$, une matrice carrée d'ordre n .
On note $\mathbb{K}[M] = \{T(M), T \in \mathbb{K}[X]\}$, l'ensemble des polynômes en M .

I. Etude de cas particuliers

Dans cette partie, on se concentre sur trois matrices $A, C \in \mathcal{M}_3(\mathbb{R})$ et $B \in \mathcal{M}_4(\mathbb{R})$.
Dans les parties suivantes, elles pourront de nouveau être mobilisées.

$$A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & -3 \\ 0 & 1 & 3 \end{pmatrix} \quad B = \frac{1}{2} \begin{pmatrix} 2 & 1 & -3 & 0 \\ 2 & -2 & -2 & -2 \\ 2 & 0 & -4 & -2 \\ -2 & 2 & 4 & 4 \end{pmatrix} \quad \text{et} \quad C = \begin{pmatrix} -2 & -1 & -10 \\ 2 & 1 & 8 \\ 1 & 1 & 3 \end{pmatrix}$$

1. Etude de A . On considère $X_1 = \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix}$ et $X_2 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$

(a) Les calculs donnent

/1

$$AX_1 = \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix} = X_1 \quad AX_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \quad A^2X_2 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \quad A^3X_2 = \begin{pmatrix} 1 \\ -3 \\ 3 \end{pmatrix}$$

(b) Encore des calculs...

/0,5

$$T_2(A) \times X_2 = A^3X_2 - 3A^2X_2 + 3AX_2 - X_2 = \begin{pmatrix} 1+0+0-1 \\ -3+0+3+0 \\ 3-3+0+0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

(c) On a $AX_1 = X_1$, i.e. $(A - I_3)X_1 = 0$.

/0,5

$$\text{Avec } T_1 = X - 1, \text{ on a } T_1(A) \times X_1 = 0 \text{ (colonne nulle).}$$

(d) On reconnaît : $T_2 = (X - 1)^3$. Donc $T_1|T_2$ et ainsi :

/1

$$T_1 \wedge T_2 = T_1 = (X - 1) \text{ et } T_1 \vee T_2 = T_2 = (X - 1)^3$$

2. Etude de B .

On note $I_B = \{BX, X \in \mathcal{M}_{4,1}(\mathbb{R})\}$ et $K_B = \{X \in \mathcal{M}_{4,1}(\mathbb{R}) \mid BX = 0\}$

(a) • $B \times 0 = 0$, donc $0 \in I_B$ (le zéro de droite) et $0 \in K_B$ (le zéro de gauche).

• Par ailleurs, si $\lambda_1, \lambda_2 \in \mathbb{R}$,

— Pour $Y_1, Y_2 \in I_B$,

Il existe $X_1, X_2 \in \mathcal{M}_{4,1}(\mathbb{R})$ tels que $Y_1 = BX_1$ et $Y_2 = BX_2$,

alors $\lambda_1 Y_1 + \lambda_2 Y_2 = \lambda_1 BX_1 + \lambda_2 BX_2 = B(\lambda_1 X_1 + \lambda_2 X_2) \in I_B$.

— Pour $X_1, X_2 \in K_B$,

$B(\lambda_1 X_1 + \lambda_2 X_2) = \lambda_1 BX_1 + \lambda_2 BX_2 = \lambda_1 0 + \lambda_2 0 = 0$.

Donc $\lambda_1 X_1 + \lambda_2 X_2 \in K_B$.

Les ensembles I_B et K_B sont non vides, stables par combinaisons linéaires :

/1

$$I_B \text{ et } K_B \text{ sont des sous-espaces vectoriels de } \mathcal{M}_{4,1}(\mathbb{R}).$$

(b) On a les équivalences

$$Y \in I_B \iff \exists a, b, c, d \in \mathbb{R} \text{ tels que } Y = B \times \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = a \begin{pmatrix} 1 \\ 1 \\ 1 \\ -1 \end{pmatrix} + b \begin{pmatrix} 1/2 \\ -1 \\ 0 \\ 1 \end{pmatrix} + c \begin{pmatrix} -3/2 \\ -1 \\ -2 \\ 2 \end{pmatrix} + d \begin{pmatrix} 0 \\ -1 \\ -1 \\ 2 \end{pmatrix}$$

$$\iff Y \in \text{vect}(C_1(B), C_2(B), C_3(B), C_4(B))$$

où $C_j(B)$ est la j -ième colonne de B . On a une famille génératrice de I_B . Est-elle libre?

Soient $a, b, c, d \in \mathbb{K}$

$$aC_1(B) + bC_2(B) + cC_3(B) + dC_4(B) = 0 \iff \begin{cases} a + \frac{1}{2}b - \frac{3}{2}c = 0 \\ a - b - c - d = 0 \\ a - 2c - d = 0 \\ -a + b + 2c + 2d = 0 \end{cases} \iff \begin{cases} -a + b + c + d = 0 \\ a + \frac{1}{2}b - \frac{3}{2}c = 0 \\ 0 + b - c = 0 \\ a - b = 0 \end{cases} \begin{array}{l} -L_2 \\ L_1 \\ L_3 - L_2 \\ L_4 + 2L_2 \end{array}$$

$$\iff \begin{cases} -a + b + c + d = 0 \\ 0 - b + c = 0 \\ a - b = 0 \\ a - b = 0 \end{cases} \begin{array}{l} -L_3 \\ L_2 - \frac{3}{2}L_3 \end{array} \iff \begin{cases} a = b \\ c = b \\ d = -b \end{cases}$$

○ **Remarques !**

⚡ On aurait pu à ce stade raisonner uniquement en implication et non en équivalence, mais pour l'étude de K_B , l'équivalence est importante

La famille n'est donc pas libre, il y a une variable libre. On a ainsi par exemple (avec $b = 1$) :

$$C_1(B) + C_2(B) + C_3(B) - C_4(B) = 0$$

Appliquons alors la réduction liée : $C_2(B) = C_4(B) - C_1(B) - C_3(B)$, donc

$$I_B = \text{vect}(C_1(B), C_2(B), C_3(B), C_4(B)) = \text{vect}(C_1(B), C_3(B), C_4(B))$$

On cherche alors à montrer la liberté de $(C_1(B), C_3(B), C_4(B))$, on retrouve alors le même système que précédemment mais avec $b = 0$ et donc nécessairement : $a = c = -d = b = 0$. /2,5

Donc $(C_1(B), C_3(B), C_4(B))$ est une base I_B et $\dim(I_B) = 3$

On étudier maintenant K_B . On fait le calcul et on trouve :

$$X = \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} \in K_B \iff aC_1(B) + bC_2(B) + cC_3(B) + dC_4(B) = 0$$

Or ce système a été étudié :

$$X = \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} \in K_B \iff a = b = c = -d \iff X = b \begin{pmatrix} 1 \\ 1 \\ 1 \\ -1 \end{pmatrix}$$

Donc $K_B = \text{vect}\left(\begin{pmatrix} 1 \\ 1 \\ 1 \\ -1 \end{pmatrix}\right)$ Cette famille composée d'un seul vecteur non nulle est libre, /1,5

donc $\dim(K_B) = 1$.

○ **Remarques !**

⚡ On vérifie que $\dim(I_B) + \dim(K_B) = 4$ (Théorème du rang...).

⚡ En fait, pour trouver les dimensions, on résout un même système : le nombre de variables libres est la dimension de K_B , quant à la dimension de I_B , il vaut 4 moins le nombre de variables libres.

⚡ D'où le résultat...

⋈

(c) On note $X = \begin{pmatrix} 1 \\ 1 \\ 1 \\ -1 \end{pmatrix}$.

On a vu que $BX = 0$.

Si B était inversible, en multipliant par B^{-1} , on aurait $X = 0$, impossible. /1

La matrice B n'est pas inversible.

(d) Les calculs donnent :

$$B^2 = \frac{1}{2} \begin{pmatrix} 0 & 0 & 2 & 2 \\ 0 & 1 & -1 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 1 & 1 & 2 \end{pmatrix} \quad B^3 = \frac{1}{2} \begin{pmatrix} 0 & 2 & 0 & 2 \\ 0 & -1 & 1 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 1 & 1 & 2 \end{pmatrix} \quad B^4 = \frac{1}{2} \begin{pmatrix} 0 & 0 & 2 & 2 \\ 0 & 1 & -1 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 1 & 1 & 2 \end{pmatrix}$$

/1,5

Donc $B^4 = B^2$.

(e) Si $n \geq 4$, alors

$$B^n = B^{n-4+4} = B^{n-4} \times B^4 = B^{n-4} B^2 = B^{n-2}$$

Notons pour $n \geq 2$, $U_n = B^n - \mathbf{1}_{n \equiv 0[2]} B^2 - \mathbf{1}_{n \equiv 1[2]} B^3$.

- Alors $U_2 = B^2 - B^2 - 0 = 0$ et $U_3 = B^3 - 0 - B^3 = 0$.
- Soit $n \in \mathbb{N}$, $n \geq 4$:

$$U_n = B^n - \mathbf{1}_{n \equiv 0[2]} B^2 - \mathbf{1}_{n \equiv 1[2]} B^3 = B^{n-2} - \mathbf{1}_{n \equiv 0[2]} B^2 - \mathbf{1}_{n \equiv 1[2]} B^3 = U_{n-2}$$

Donc $(U_{2p+2})_{p \in \mathbb{N}}$ et $(U_{2p+3})_{p \in \mathbb{N}}$ sont deux suites (matricielles) constantes.

Donc pour tout $p \in \mathbb{N}$: $U_{2p+2} = U_2 = 0$ et $U_{2p+3} = U_3 = 0$.

$$\forall n \geq 4 : B^n = \mathbf{1}_{n \equiv 0[2]} B^2 + \mathbf{1}_{n \equiv 1[2]} B^3 = \begin{cases} B^2 & \text{si } n \equiv 0[2] \\ B^3 & \text{si } n \equiv 1[2] \end{cases}$$

/1

La formule est vraie pour $n = 3$, mais en revanche : $B^3 \neq B$.

3. Etude de C

(a) Les calculs donnent :

/1

$$C^2 = \begin{pmatrix} -8 & -9 & -18 \\ 6 & 7 & 12 \\ 3 & 3 & 7 \end{pmatrix} \quad \text{et} \quad C^3 = \begin{pmatrix} -20 & -19 & -46 \\ 14 & 13 & 32 \\ 7 & 7 & 15 \end{pmatrix}$$

(b) On note $\pi = X^3 - 2X^2 - X + 2$. On a alors :

$$\pi(C) = C^3 - 2C^2 - C + 2I_3 = \begin{pmatrix} -20 + 16 + 2 + 2 & -19 + 18 + 1 & -46 + 36 + 10 \\ 14 - 12 - 2 & 13 - 14 - 1 + 2 & 32 - 24 - 8 \\ 7 - 6 - 1 & -7 - 6 - 1 & 15 - 14 - 3 + 2 \end{pmatrix}$$

/1

Ainsi $\pi(C) = C^3 - 2C^2 - C + 2I_3 = 0$.

(c) On a alors $C(C^2 - 2C - I_3) = -2I_3$, donc

$$C \times \left(\frac{1}{2}(I_3 + 2C - C^2) \right) = \left(\frac{1}{2}(I_3 + 2C - C^2) \right) \times C = I_3$$

/0,5

Donc la matrice C est inversible et $C^{-1} = \left(\frac{1}{2}(I_3 + 2C - C^2) \right) = \frac{1}{2} \begin{pmatrix} 5 & 7 & -2 \\ -2 & -4 & 4 \\ -1 & -1 & 0 \end{pmatrix}$.

(d) 1 est une (première) racine de π . Le polynôme π se factorise :

$$\pi(X) = (X - 1)(X^2 - X - 2) = (X - 1)(X - 2)(X + 1)$$

Effectuons la division euclidienne de X^n par π .

$\exists !(Q_n, R_n) \in \mathbb{K}[X] \times \mathbb{K}_2[X]$ tel que $X^n = Q_n \times \pi + R_n$.

On a alors en substituant en $-1, 1$ et 2 (les racines de π) :

$$\begin{cases} (-1)^n &= Q_n(-1) \times 0 & + R_n(-1) \\ 1^n &= Q_n(1) \times 0 & + R_n(1) \\ (2)^n &= Q_n(2) \times 0 & + R_n(2) \end{cases}$$

Comme le degré de R_n est inférieur à deux, R_n est le polynôme d'interpolation de LAGRANGE

$$\begin{aligned} R_n &= (-1)^n \frac{(X - 1)(X - 2)}{(-1 - 1)(-1 - 2)} + 1^n \frac{(X + 1)(X - 2)}{(1 + 1)(1 - 2)} + (2)^n \frac{(X + 1)(X - 1)}{(2 + 1)(2 - 1)} \\ &= \frac{(-1)^n}{6} (X^2 - 3X + 2) - \frac{1}{2} (X^2 - X - 2) + \frac{2^n}{3} (X^2 - 1) \\ &= \frac{1}{6} ([-(-1)^n - 3 + 2^{n+1}]X^2 + [-3(-1)^n + 3]X + [2(-1)^n + 6 - 2^{n+1}]) \end{aligned}$$

Et donc en substituant C dans la relation $X^n = Q_n \times \pi + R_n$, comme $\pi(C) = 0$ /2,5

$$\begin{aligned} \text{pour tout } n \in \mathbb{N}, \quad C^n &= \frac{1}{6} ([-(-1)^n - 3 + 2^{n+1}]C^2 + [-3(-1)^n + 3]C + [2(-1)^n + 6 - 2^{n+1}]I_3) \\ &= \frac{1}{6} ((-1)^n(C^2 - 3C + 2I_3) + (-3C^2 + 3C + 6I_3) + 2^{n+1}(C^2 - I_3)) \\ &= \frac{1}{6} \begin{pmatrix} 24 - 9(2)^{n+1} & -6(-1)^n + 24 - 9(2)^{n+1} & 12(-1)^n + 24 - 18(2)^{n+1} \\ -12 + 6(2)^{n+1} & 6(-1)^n - 12 + 6(2)^{n+1} & -12(-1)^n - 12 + 12(2)^{n+1} \\ -6 + 3(2)^{n+1} & -6 + 3(2)^{n+1} & -6 + 6(2)^{n+1} \end{pmatrix} \end{aligned}$$

$$\text{car } C^2 - 3C + 2I_3 = \begin{pmatrix} 0 & -6 & 12 \\ 0 & 6 & -12 \\ 0 & 0 & 0 \end{pmatrix}, \quad -3C^2 + 3C + 6I_3 = \begin{pmatrix} 24 & 24 & 24 \\ -12 & -12 & -12 \\ -6 & -6 & -6 \end{pmatrix} \text{ et}$$

$$C^2 - I_3 = \begin{pmatrix} -9 & -9 & -18 \\ 6 & 6 & 12 \\ 3 & 3 & 6 \end{pmatrix}.$$

On trouve alors pour $n = -1$:

$$\frac{1}{6} \begin{pmatrix} 24 - 9(2)^0 & -6(-1)^{-1} + 24 - 9(2)^0 & 12(-1)^{-1} + 24 - 18(2)^0 \\ -12 + 6(2)^0 & 6(-1)^{-1} - 12 + 6(2)^0 & -12(-1)^{-1} - 12 + 12(2)^0 \\ -6 + 3(2)^0 & -6 + 3(2)^0 & -6 + 6(2)^0 \end{pmatrix} = \frac{1}{6} \begin{pmatrix} 15 & 21 & -6 \\ -6 & -12 & 12 \\ -3 & -3 & 0 \end{pmatrix}$$

En simplifiant par 3 : /1

on retrouve ainsi C^{-1} (l'inverse de C) ; donc la formule reste vraie pour $n = -1$.

(e) Soit $P = aX^2 + bX + c$, polynôme générique de $\mathbb{R}_2[X]$.

Supposons que $P(C) = 0$, i.e. : $aC^2 + bC + cI_3 = 0$.

On a donc le système (on raisonne par implication, donc si nécessaire, on fera une réciproque) :

$$\begin{cases} -8a & -2b & +c & = & 0 \\ -9a & & & & = & 0 \\ -18a & -10b & & & = & 0 \\ 6a & +2b & & & = & 0 \\ 7a & +b & +c & = & 0 \\ 12a & +8b & & & = & 0 \\ 3a & +b & & & = & 0 \\ 3a & +b & & & = & 0 \\ 7a & +3b & +c & = & 0 \end{cases} \iff \begin{cases} -9a & -b & & = & 0 \\ 3a & +b & & = & 0 \\ 7a & +b & +c & = & 0 \end{cases} \iff \begin{cases} -9a & -b & & = & 0 \\ 6a & & & = & 0 \\ 7a & +b & +c & = & 0 \end{cases}$$

Ainsi, nécessairement $a = 0, b = 0$ et $c = 0$. Ainsi $P = 0$. Par contraposée : /1,5

Pour tout $P \in \mathbb{R}_2[X]$, non nul : $P(C) \neq 0$.

II. Idéaux de $\mathbb{K}[X]$.

/7

1. Soit $\pi \in \mathbb{K}[X]$. On rappelle que $(\pi) = \pi\mathbb{K}[X]$.

— $0 = \pi \times 0$, donc $0 \in (\pi)$

— Soient $T_1, T_2 \in (\pi)$, alors il existe $Q_1, Q_2 \in \mathbb{K}[X]$ tel que $T_1 = \pi Q_1$ et $T_2 = \pi Q_2$.

Donc $T_1 - T_2 = \pi(Q_1 - Q_2)$. Et comme $Q_1 - Q_2 \in \mathbb{K}[X]$, $T_1 - T_2 \in (\pi)$.

— Soit $T \in (\pi)$ et $R \in \mathbb{K}[X]$, alors il existe $Q \in \mathbb{K}[X]$ tel que $T = \pi Q$.

Donc $TR = \pi QR \in (\pi)$ puisque $QR \in \mathbb{K}[X]$.

/1

(π) est un idéal de $\mathbb{K}[X]$.

2. Réciproquement, considérons un idéal \mathcal{I} de $\mathbb{K}[X]$ non réduit à $\{0\}$.

(a) Comme \mathcal{I} est non réduit à $\{0\}$, $\{\deg P, P \in \mathcal{I} \setminus \{0\}\}$ est non vide.

C'est un sous-ensemble de \mathbb{N} . Donc (propriété du cours) :

/0,5

$\{\deg P, P \in \mathcal{I} \setminus \{0\}\}$ admet un plus petit élément, noté r .

(b) Soit $\pi \in \mathcal{I}$ tel que $\deg \pi = r$. Soit $S \in \mathcal{I}$.

Faisons la division euclidienne de S par π :

Il existe un unique couple $(Q, R) \in \mathbb{K}[X] \times \mathbb{K}_{r-1}[X]$ tel que $S = \pi Q + R$.

On a alors $R = S - \pi Q$.

Mais $S \in \mathcal{I}$, $\pi \in \mathcal{I}$, donc par stabilité multiplicative : $\pi Q \in \mathcal{I}$.

Puis par stabilité additive : $R = S - \pi Q \in \mathcal{I}$.

Si $R \neq 0$, on a $\deg R \in \{\deg T, T \in \mathcal{I} \setminus \{0\}\}$ et $\deg R < r$. Impossible.

Donc $R = 0$ et $S = \pi Q$, donc π divise S .

/1,5

Autrement écrit : $S \in (\pi)$.

(c) La question précédente a démontré que $\mathcal{I} \subset (\pi)$.

Réciproquement, comme $\pi \in \mathcal{I}$ et que \mathcal{I} est un idéal : $\pi Q \in \mathcal{I}$ (pour tout $Q \in \mathbb{K}[X]$).

Ainsi $(\pi) \subset \mathcal{I}$.

/0,5

Par double inclusion : $\mathcal{I} = (\pi)$.

On dit que le polynôme π engendre l'idéal \mathcal{I} .

3. Structure $\frac{\mathbb{K}[X]}{(\pi)}$. On fixe $\pi \in \mathbb{K}[X]$. On note $r = \deg \pi$

On note $M_1 \equiv M_2[\pi]$ si et seulement si $M_1 - M_2 \in (\pi)$

(a) Il s'agit de montrer que la relation est réflexive, symétrique, transitive.

— Pour tout $M \in \mathbb{K}[X]$, $M - M = 0 = \pi \times 0 \in (\pi)$, donc $M \equiv M[\pi]$.

La relation est réflexive.

— Soient $M_1, M_2 \in \mathbb{K}[X]$, tels que $M_1 \equiv M_2[\pi]$. Il existe $Q \in \mathbb{K}[X]$ tel que $M_1 - M_2 = \pi Q$.

Donc $M_2 - M_1 = \pi(-Q) \in (\pi)$ car $-Q \in \mathbb{K}[X]$.

Donc $M_2 \equiv M_1[\pi]$ et la relation est symétrique.

— Soient $M_1, M_2, M_3 \in \mathbb{K}[X]$, tels que $M_1 \equiv M_2[\pi]$ et $M_2 \equiv M_3[\pi]$.

Il existe $Q_1, Q_2 \in \mathbb{K}[X]$ tel que $M_1 - M_2 = \pi Q_1$ et $M_2 - M_3 = \pi Q_2$.

En additionnant : $M_1 - M_3 = \pi(Q_1 + Q_2) \in (\pi)$ car $Q_1 + Q_2 \in \mathbb{K}[X]$.

Donc $M_1 \equiv M_3[\pi]$ et la relation est transitive.

/1

$\equiv [\pi]$ est une relation d'équivalence sur $\mathbb{K}[X]$.

On note \overline{M} , la classe de M pour cette relation d'équivalence et $\frac{\mathbb{K}[X]}{(\pi)}$ l'ensemble de ces classes.

(b) Soit $\varphi_\pi : \begin{array}{ccc} \mathbb{K}[X] & \rightarrow & \mathbb{K}_{r-1}[X] \\ Q & \mapsto & Q \% \pi \end{array}$ (reste de la division euclidienne de Q par π).

Pour tout polynôme de $T \in \mathbb{K}_{r-1}[X]$, $T \in \mathbb{K}[X]$ et $\varphi_\pi(T) = T$ car $\deg T < \deg \pi$.

Donc T admet au moins un antécédent par φ_π .

/1

φ_π est surjective

Soient $M_1, M_2 \in \mathbb{K}[X]$. On a les équivalences

$$\varphi_\pi(M_1) = \varphi_\pi(M_2) \iff M_1 \% \pi = M_2 \% \pi \iff (M_1 - M_2) \% \pi = 0$$

Par linéarité de la division euclidienne. Et comme le reste est nul :

/1

$$\varphi_\pi(M_1) = \varphi_\pi(M_2) \iff \pi | M_1 - M_2 \iff M_1 \equiv M_2[\pi]$$

On en déduit que $\overline{\varphi}_\pi : \begin{array}{ccc} \frac{\mathbb{K}[X]}{(\pi)} & \longrightarrow & \mathbb{K}_{r-1}[X] \\ \overline{Q} & \longmapsto & Q \% \pi \end{array}$ est bien définie et est bijective.

(c) Soient $M_1, N_1, M_2, N_2 \in \mathbb{K}[X]$ tel que $M_1 \equiv N_1[\pi]$ et $M_2 \equiv N_2[\pi]$.

$$\pi|M_1 - N_1 \text{ et } \pi|M_2 - N_2 \implies \pi|(M_1 - N_1) + (M_2 - N_2) = (M_1 + M_2) - (N_1 + N_2)$$

Donc $M_1 + M_2 \equiv N_1 + N_2[\pi]$ ou de manière équivalente : $\overline{M_1 + M_2} = \overline{N_1 + N_2}$.

Et $M_1 \times M_2 - N_1 \times N_2 = M_1(M_2 - N_2) + (M_1 - N_1)N_2$

$$\pi|M_1 - N_1 \text{ et } \pi|M_2 - N_2 \implies \pi|M_1(M_2 - N_2) + (M_1 - N_1)N_2 = M_1 \times M_2 - N_1 \times N_2$$

Donc $M_1 \times M_2 \equiv N_1 \times N_2[\pi]$ ou de manière équivalente : $\overline{M_1 \times M_2} = \overline{N_1 \times N_2}$. /2

Les opérations $\overline{+}$ et $\overline{\times}$ sont bien opérantes : indépendantes des représentants choisis.

On admet qu'ainsi $\left(\frac{\mathbb{K}[X]}{(\pi)}, \overline{+}, \overline{\times}\right)$ est un anneau.

(d) Comme $\left(\frac{\mathbb{K}[X]}{(\pi)}, \overline{+}, \overline{\times}\right)$ est un anneau ; pour montrer que $\left(\frac{\mathbb{K}[X]}{(\pi)}, \overline{+}, \overline{\times}\right)$ est un corps, il faut et il suffit de démontrer que tout élément non nul est inversible.

Supposons que π est irréductible.

Soit $\overline{T} \in \frac{\mathbb{K}[X]}{(\pi)}$ avec $\overline{T} \neq \overline{0}$ i.e. π ne divise pas T .

Comme π est irréductible et que π ne divise pas T : $\pi \wedge T = 1$.

D'après l'identité de Bézout, il existe $U, V \in \mathbb{K}[X]$ tel que $U\pi + VT = 1$.

Donc $\pi|1 - VT$ i.e. $VT \equiv 1[\pi]$, donc $\overline{V \times T} = \overline{V \times Q} = \overline{1}$.

Ainsi \overline{T} est inversible. Ceci est vrai pour tout \overline{T} non nul. Donc $\frac{\mathbb{K}[X]}{(\pi)}$ est un corps. /1,5

Réciproquement, supposons que $\frac{\mathbb{K}[X]}{(\pi)}$ est un corps.

Soit $A, B \in \mathbb{K}[X]$ tel que $A \times B = \pi$, donc $\overline{A \times B} = \overline{\pi} = \overline{0}$.

Supposons que $\deg B > 0$, alors $\deg A = \deg \pi - \deg B < \deg \pi$.

Ainsi $A \notin (\pi)$ et donc $\overline{A} \neq \overline{0}$. \overline{A} est inversible (car $\frac{\mathbb{K}[X]}{(\pi)}$ est un corps).

On multiplie par \overline{A}^{-1} : $\overline{0} = \overline{A}^{-1} \times \overline{0} = \overline{A}^{-1} \times \overline{A \times B} = \overline{B}$.

Donc $\pi|B$ et nécessairement π et B sont associés ($\deg B \in \llbracket 1, \deg \pi \rrbracket$).

On a donc $AB = \pi \implies (\deg B > 0 \text{ et } \pi \text{ et } B \text{ associés}) \text{ ou } (\deg B = 0 \text{ et } \pi \text{ et } A \text{ associés})$.

Ainsi π est irréductible. /1,5

Donc $\left(\frac{\mathbb{K}[X]}{(\pi)}, \overline{+}, \overline{\times}\right)$ est un corps si et seulement si π est irréductible.

Remarques !

On aurait pu faire un raisonnement en contraposée. En supposant π non irréductible et $\pi = A \times B$,

avec $\deg A, \deg B \in \llbracket 1, \deg \pi - 1 \rrbracket$.

Alors $\overline{A \times B} = \overline{A \times B} = \overline{\pi} = \overline{0}$.

Et pourtant \overline{A} et $\overline{B} \neq 0$, sinon $\pi|A$ ou $\pi|B$, donc $A = 0$ car $\deg A < \deg \pi$...

Donc $\frac{\mathbb{K}[X]}{(\pi)}$ n'est pas intègre (il possède des diviseurs de zéros), il ne peut donc pas être un corps.

On admet également que $\overline{\cdot}$ est bien définie sur $\mathbb{K} \times \frac{\mathbb{K}[X]}{(\pi)}$.

(e) On exploite la bijectivité de $\overline{\varphi_\pi}$ (qui est en fait un isomorphisme).

Soit $\overline{Q} \in \frac{\mathbb{K}[X]}{(\pi)}$.

$\varphi_\pi(\overline{Q}) \in \mathbb{K}_{r-1}[X]$. Il existe un r -uplet $(a_0, a_1, \dots, a_{r-1}) \in \mathbb{K}$ tel que

$$\varphi_\pi(\overline{Q}) = \sum_{k=0}^{r-1} a_k X^k = \sum_{k=0}^{r-1} a_k \varphi_\pi(\overline{X^k})$$

d'après la démonstration de la surjectivité en 3.(b).

Puis (par récurrence) : $\sum_{k=0}^{r-1} a_k \overline{X^k} = \overline{\left\{ \sum_{k=0}^{r-1} a_k X^k \right\}}$.

Le reste de la division euclidienne par π de $T = \sum_{k=0}^{r-1} a_k X^k$ est T car $\deg T \leq r-1 < \deg \pi$.

Donc $\overline{\varphi_\pi(\overline{Q})} = T = \overline{\varphi_\pi \left(\overline{\sum_{k=0}^{r-1} a_k X^k} \right)}$.

Par injectivité de $\overline{\varphi}_\pi : \overline{Q} = \overline{\sum_{k=0}^{r-1} a_k X^k} = \sum_{k=0}^{r-1} a_k \overline{X^k}$. Donc $\frac{\mathbb{K}[X]}{(\pi)} \subset \text{vect}(\overline{1}, \overline{X}, \dots, \overline{X^{r-1}})$

Comme chaque $\overline{X^k} \in \frac{\mathbb{K}[X]}{(\pi)}$, on peut affirmer : /1,5

$$\frac{\mathbb{K}[X]}{(\pi)} = \text{vect}(\overline{1}, \overline{X}, \dots, \overline{X^{r-1}})$$

Il reste à montrer que la famille $(\overline{1}, \overline{X}, \dots, \overline{X^{r-1}})$ est libre.

Soient $\lambda_0, \lambda_1, \dots, \lambda_{r-1}$ tel que $\sum_{k=0}^{r-1} \lambda_k \overline{X^k} = \overline{0}$.

On a donc $\sum_{k=0}^{r-1} \lambda_k X^k \equiv 0$ i.e. $\pi \mid \sum_{k=0}^{r-1} \lambda_k X^k$.

Or $\deg \pi > \deg \sum_{k=0}^{r-1} \lambda_k X^k$, donc nécessairement $\sum_{k=0}^{r-1} \lambda_k X^k = 0$.

Puis on applique la liberté de $(1, X, \dots, X^{r-1})$ et donc pour tout $k \in \llbracket 0, r-1 \rrbracket$, $\lambda_k = 0$.
Ainsi la famille $(\overline{1}, \overline{X}, \dots, \overline{X^{r-1}})$ est libre. /1

$\left(\frac{\mathbb{K}[X]}{(\pi)}, \overline{\cdot}, \overline{\cdot} \right)$ est un \mathbb{K} -espace vectoriel de dimension r .
Une base est $(\overline{1}, \overline{X}, \dots, \overline{X^{r-1}})$

III. Polynômes annulateurs

On considère dans cette partie les deux espaces vectoriels $\mathcal{M} = \mathcal{M}_n(\mathbb{K})$ et $E = \mathcal{M}_{n,1}(\mathbb{K})$.

On fixe $M \in \mathcal{M}$ une matrice, on note $\mathcal{I}_M = \{P \in \mathbb{K}[X] \mid P(M) = 0_{\mathcal{M}}\}$ et $\mathbb{K}[M] = \{T(M), T \in \mathbb{K}[X]\}$.

Puis, pour toute matrice colonne $X \in E$, on note également $\mathcal{I}_{M,X} = \{P \in \mathbb{K}[X] \mid P(M) \times X = 0_E\}$ ainsi que $\mathbb{K}[M]X = \{T(M) \times X, T \in \mathbb{K}[X]\}$.

1. Espaces de dimensions finis.

(a) C'est une question de cours, /1

\mathcal{M} et E sont bien des espaces vectoriels et $\dim(\mathcal{M}) = n^2$ et $\dim(E) = n$

(b) Lorsque la famille génératrice est infinie, les éléments de l'ensemble sont les combinaisons linéaires finis de ces éléments.

$$N \in C(M) \iff \exists I \subset \mathbb{N} \text{ fini } \exists (\lambda_i)_{i \in I} \in \mathbb{R}^I \text{ tel que } N = \sum_{i \in I} \lambda_i M^i$$

En prenant $n = \max I$ puis pour tout $i \leq n$, $a_i = \#_I(i) \lambda_i$ puis enfin $T = \sum_{i=0}^n a_i X^i$:

$$N \in C(M) \iff \exists T \in \mathbb{K}[X] \text{ tel que } N = T(M)$$

Donc $C(M) = \mathbb{K}[M]$.

Par définition, $C(M)$ est bien un sous-espace-vectoriel de \mathcal{M} :

tous les éléments $M^k \in \mathcal{M}$; $C(M)$ est le plus petit sous-espace vectoriel les contenant.

Comme \mathcal{M} est de dimension finie, il en est nécessairement de même de $C(M)$: /2

$C(M) = \mathbb{K}[M]$ est un sev de dimension finie de \mathcal{M} et $r_M := \dim(C(M)) \leq \dim \mathcal{M} = n^2$

(c) Soient $N_1, N_2 \in C(M)$. Alors il existe $P_1, P_2 \in \mathbb{K}[X]$ tels que $N_1 = P_1(M)$ et $N_2 = P_2(M)$.

$$N_1 \times N_2 = P_1(M) \times P_2(M) = \left(\underbrace{P_1 \times P_2}_{\text{multiplication de } \mathbb{K}[X]} \right)(M) = (P_2 \times P_1)(M) = P_2(M) \times P_1(M) = N_2 \times N_1$$

/1,5

Tous les éléments de $C(M)$ commutent.

2. Idéaux

(a) Le polynôme nul appartient à \mathcal{I}_M et à $\mathcal{I}_{M,X}$.

Donc ces ensembles sont non vides.

Soit $P, Q \in \mathcal{I}_M$,

$$(P - Q)(M) = P(M) - Q(M) = 0 - 0 = 0$$

Donc $P - Q \in \mathcal{I}_M$.

Soit $P \in \mathcal{I}_M$ et $Q \in \mathbb{K}[X]$

$$P \times Q(M) = P(M) \times Q(M) = 0 \times Q(M) = 0$$

Donc $P \times Q \in \mathcal{I}_M$.

Soit $P, Q \in \mathcal{I}_{M,X}$,

$$(P - Q)(M) \times X = P(M) \times X - Q(M) \times X = 0 - 0 = 0$$

Donc $P - Q \in \mathcal{I}_{M,X}$.

Soit $P \in \mathcal{I}_M$ et $Q \in \mathbb{K}[X]$

$$P \times Q(M) \times X = Q \times P(M) \times X = Q(M) \times P(M) \times X = Q(M) \times 0 = 0$$

Donc $P \times Q \in \mathcal{I}_{M,X}$.

/1,5

$$\boxed{\mathcal{I}_M \text{ et } \mathcal{I}_{M,X} \text{ sont des idéaux de } \mathbb{K}[X].}$$

Si $P \in \mathcal{I}_M$, alors $P(M) = 0$ et donc $P(M) \times X = 0$, donc $P \in \mathcal{I}_{M,X}$

/1

$$\boxed{\mathcal{I}_M \subset \mathcal{I}_{M,X}}$$

On appelle polynôme minimal de M , noté π_M , le polynôme de $\mathbb{K}[X]$ unitaire tel que $(\pi_M) = \mathcal{I}_M$.

On appelle polynôme conducteur de M en X (ou minimal de (M, X)), noté $\pi_{M,X}$, le polynôme de $\mathbb{K}[X]$ unitaire tel que $(\pi_{M,X}) = \mathcal{I}_{M,X}$.

(b) Soient $\lambda_0, \lambda_1, \dots, \lambda_{\deg \pi_M - 1} \in \mathbb{K}$ tel que $\sum_{k=0}^{\deg \pi_M - 1} \lambda_k M^k = 0$.

Notons T , le polynôme $\sum_{k=0}^{\deg \pi_M - 1} \lambda_k X^k$. On a donc $T(M) = 0$.

Donc $T \in \mathcal{I}_M$, donc $\pi_M | T$. Il existe $Q \in \mathbb{K}[X]$ tel que $T = \pi_M \times Q$.

Ainsi $\deg T = \deg \pi_M + \deg Q$. Or $\deg \pi_M > \deg T$, donc $\deg Q < 0$. Donc $Q = 0$.

Et par suite $T = 0$ et donc pour tout $k \in \llbracket 0, \deg \pi_M - 1 \rrbracket$, $\lambda_k = 0$.

/1

$$\boxed{\text{Ainsi, la famille } (M^0, M^1, \dots, M^{\deg \pi_M - 1}) \text{ est libre.}}$$

(c) Soient $N \in C(M)$. Tout élément de $C(M)$ est un polynôme en M .

Notons alors $P = \sum_{k=0}^n a_k X^k \in \mathbb{K}[X]$ tel que $N = P(M)$.

. Effectuons la division euclidienne de P par π_M .

Il existe donc $(Q, R) \in \mathbb{K}[X]^2$ tel que $P = Q\pi_M + R$ avec $\deg R < \deg \pi_M$.

Puis

$$N = P(M) = (Q\pi_M + R)(M) = Q(M) \times \underbrace{\pi_M(M)}_{=0} + R(M) = R(M)$$

Or $R \in \mathbb{K}_{\deg \pi_M - 1}[X]$, donc il existe $b_0, b_1, \dots, b_{\deg \pi_M - 1} \in \mathbb{K}$ tels que $R = \sum_k b_k X^k$.

Donc $N = \sum_{k=0}^{\deg \pi_M - 1} b_k M^k$.

Ainsi on a démontré : $C(M) \subset \text{vect}(M^0, M^1, \dots, M^{\deg \pi_M - 1})$.

Réciproquement : Pour tout $k \leq \deg \pi_M - 1$, $M^k \in C(M)$.

Et $C(M)$ est un espace vectoriel, donc $\text{vect}(M^0, M^1, \dots, M^{\deg \pi_M - 1}) \subset C(M)$

/2

$$\boxed{C(M) = \text{vect}(M^0, M^1, \dots, M^{\deg \pi_M - 1})}$$

- (d) On a trouvé une base de $C(M)$, elle est composée de $\deg \pi_M - 1 + 1 = \deg \pi_M$ vecteurs.
Or $\dim C(M) = r_M$, par définition en 1.(b).

/1

$$\deg \pi_M = r_M = \dim C(M) \leq n^2 = \dim \mathcal{M}$$

🕒 **Remarques !**

🌀 Dans ces questions, on redémontre ce qu'on a vu en fin de partie précédente.

🌀 Car il y a une bijection assez naturel de $\theta : \frac{\mathbb{K}[X]}{(\pi_M)} \rightarrow \mathbb{K}[M]$, avec $\theta(\bar{S}) = S(M)$.

🌀 Le plus dur est de démontrer l'indépendance par rapport au représentant de la classe d'équivalence choisie.

- (e) Par construction $\mathcal{I}_M = (\pi_M)$, donc $\pi_M \in \mathcal{I}_M$.

Or on a vu que $\mathcal{I}_M \subset \mathcal{I}_{M,X}$, donc $\pi_M \in \mathcal{I}_{M,X} = (\pi_{M,X})$.

/1

$$\text{Donc } \pi_{M,X} | \pi_M$$

IV. Lemme des noyaux

Soit M une matrice de \mathcal{M} et π_M son polynôme minimal.

On suppose que π_M se décompose en produit d'irréductibles :

$$\pi_M = \prod_{i=1}^s P_i^{\alpha_i}$$

où pour tout $i \in \mathbb{N}_s$, P_i est irréductible dans l'anneau euclidien $\mathbb{K}[X]$ et $\alpha_i \in \mathbb{N}$. On note, pour tout $i \in \mathbb{N}_s$, $K_i = \{X \in E \mid P_i^{\alpha_i}(M) \times X = 0\}$

Le but de ces questions est de montrer qu'il existe $X \in \mathcal{M}_{n,1}(\mathbb{K})$ tel que $\mu_M = \mu_{M,X}$ et d'appliquer ce résultat pour obtenir la décomposition de Fröbenius.

1. On démontre maintenant le lemme des noyaux :

$$E = K_1 \oplus K_2 \cdots \oplus K_s$$

Pour cela on note pour tout $i \in \mathbb{N}_s$, $Q_i = \prod_{j \in \mathbb{N}_s \setminus \{i\}} P_j^{\alpha_j}$. On a donc $P_i^{\alpha_i} Q_i = \pi_M$

- (a) On note pour tout $i \in \mathbb{N}_s$, $Q_i = \prod_{j \in \mathbb{N}_s \setminus \{i\}} P_j^{\alpha_j}$.

Soit Δ tel que pour tout $i \in \mathbb{N}_s$, $\Delta | Q_i$. Supposons $\Delta \neq 1$.

Soit R , un facteur irréductible de Δ .

Alors $R | Q_1$, donc comme R et P_2, \dots, P_s irréductible,

alors nécessairement R est un de ces nombres.

Donc il existe $s_0 \in [2, s]$ tel que $R = P_{s_0}$.

Mais R divise aussi Q_{s_0} , qui est premier avec P_{s_0} . Impossible

Donc $\Delta = 1$.

/2

Les polynômes Q_i sont premiers entre eux, on peut appliquer la relation de Bézout

$$\forall i \in \mathbb{N}_s, \exists U_i \in \mathbb{K}[X] \text{ tel que } 1 = \sum_{i=1}^s U_i Q_i$$

On applique alors cette relation en M :

/1

$$\forall i \in \mathbb{N}_s, \exists U_i \in \mathbb{K}[X] \text{ tel que } I_n = \sum_{i=1}^s U_i(M) Q_i(M)$$

- (b) Soit $X \in E$.

Si l'on multiplie cette matrice (de la questions précédente) par X , on a

$$X = I_n X = \sum_{i=1}^s U_i(M) Q_i(M) X$$

Notons pour tout $i \in \mathbb{N}_s$, $N_i := U_i(M)Q_i(M)X$, on a donc $X = \sum_{i=1}^s N_i$ et

$$P_i^{\alpha_i}(M) \times N_i = P_i^{\alpha_i}(M)U_i(M)Q_i(M)X = U_i(M) \underbrace{P_i^{\alpha_i}Q_i(M)}_{\pi_M(M)=0} X = 0$$

Donc $N_i \in K_i$

/2

Pour tout $X \in E$, il existe $(N_i)_{i \in \mathbb{N}_s} \in K_1 \times K_2 \cdots \times K_s$ tel que : $X = \sum_{i=1}^s N_i$.

(c) Cela signifie que (l'inclusion réciproque est évidente : $K_i \subset E$) :

/1

$K_1 + K_2 + \cdots + K_s = E$

(d) On considère maintenant $(x_1, x_2, \cdots, x_s) \in K_1 \times K_2 \cdots \times K_s$ tel que $\sum_{i=1}^s x_i = 0$.

Notons que pour $i \neq j$, comme $P_i^{\alpha_i} | Q_j$, alors

$$Q_j(M)x_i = \prod_{k \neq i, j} P_k^{\alpha_k}(M) \underbrace{P_i^{\alpha_i}(M)x_i}_{=0, x_i \in K_i} = 0$$

Alors en multipliant à gauche la relation $0 = \sum_{i=1}^s x_i$ par $Q_j(M)$, on trouve

$$0 = Q_j(M) \times 0 = \sum_{i=1}^s Q_j(M)x_i = Q_j(M)x_j$$

(car les autres termes sont nuls).

Et de même, si on reprend la relation $I_n = \sum_{i=1}^s U_i(M)Q_i(M)$.

$$x_j = I_n \times x_j = \sum_{i=1}^s U_i(M)Q_i(M)x_j \underbrace{=}_{Q_i(M)x_j=0} U_j(M)Q_j(M)x_j \underbrace{=}_{Q_j(M)x_j=0} 0$$

/2,5

Ainsi pour tout $i \in \mathbb{N}_s$, $x_i = 0$

(e) On en déduit que la somme est directe

/1

$K_1 \oplus K_2 \oplus \cdots \oplus K_s$

2. On admet que si une matrice $A \in \mathcal{M}$ n'est pas inversible, alors il existe $X \in E$ tel que $AX = 0$ (colonne nulle) - résultat démontré en cours mardi.

(a) Supposons que $\pi_M = P_1 \times P_2$ avec $\deg P_1 > 0$, donc $\deg P_2 < \deg \pi_M$. On a donc

$$\pi_M(M) = 0 = P_1(M) \times P_2(M)$$

Supposons que $P_1(M)$ soit inversible, alors en multipliant par $(P_1(M))^{-1}$, à gauche :

$$0 = (P_1(M))^{-1} \times 0 = P_1(M)^{-1}P_1(M)P_2(M) = P_2(M)$$

Donc $P_2(M) = 0$, $P_2 \in \mathcal{I}_M$ et donc $\pi_M | P_2$, alors que $\deg \pi_M > \deg P_2$.

La seule possibilité est que $P_2 = 0$ et donc $\pi_M = 0$, faux. Donc

/1,5

$P_1(M) \text{ n'est pas inversible.}$

(b) D'après la question précédente (de la partie précédente), $P_i^{\alpha_i}(M)$ n'est pas inversible. Et d'après le résultat admis : il existe $X_i \in E$ tel que $P_i^{\alpha_i}(M)X_i = 0$

/1

Donc pour tout $i \in \mathbb{N}_s$, $K_i \neq \emptyset$.

(c) Si pour tout $X \in E$ tel que $P_i^{\alpha_i}(M) \times X = 0$, on a $P_i^{\alpha_i-1}(M) \times X = 0$.

D'après le lemme des noyaux : on a vu que pour tout $X \in E$: $X = \sum_{h=1}^s N_h$ avec $N_h \in K_h$.

Notons $\bar{\pi} = \frac{\pi_M}{P_i} = P_i^{\alpha_i-1} \prod_{j \neq i} P_j^{\alpha_j}$.

Alors pour tout $X \in E$: $\pi(M)X = \sum_{h=1}^s \pi(M)N_h$.

Or pour $h \neq i$,

$$\pi(M)N_h = P_i^{\alpha_i-1}(M) \times \prod_{j \neq i, h} P_j^{\alpha_j}(M) \times \underbrace{P_h^{\alpha_h}(M)N_h}_{=0} = 0$$

Et de même, comme $N_i \in K_i$, on a donc $P_i^{\alpha_i}(M) \times N_i = 0$, donc $P_i^{\alpha_i-1}(M) \times N_i = 0$ d'après notre hypothèse.

Ainsi, on a aussi :

$$\pi(M)N_i = \prod_{j \neq i} P_j^{\alpha_j}(M) \times \underbrace{P_i^{\alpha_i-1}(M)N_i}_{=0} = 0$$

Donc pour tout $X \in E$, $\pi(M)X = 0$. Alors $\pi(M) = 0$ (il suffit de prendre $X = E_i$, on trouve alors $C_i(\pi(M)) = 0$ colonne i)

Mais π est de degré strictement plus petit que π_M , on a une contradiction avec la minimalité de π_M . Donc on n'a pas $P_i^{\alpha_i}(M) \times X = 0 \iff P_i^{\alpha_i-1}(M) \times X = 0$. /2

Il existe donc $X \in E$ tel que $P_i^{\alpha_i}(M) \times X = 0$ et $P_i^{\alpha_i-1}(M) \times X \neq 0$.

On note, pour tout $i \in \mathbb{N}_s$, $X_i \in K_i$ tel que $P_i^{\alpha_i-1}(M) \times X \neq 0$

3. On montre maintenant qu'il existe $X \in \mathcal{M}_{n,1}(\mathbb{K})$ tel que $\pi_M = \pi_{M,X}$

(a) Soit π_{M,X_i} le polynôme conducteur de M en X_i .

Alors $P_i^{\alpha_i} \in \mathcal{I}_{M,X_i} = (\pi_{M,X_i})$. Donc $\pi_{M,X_i} | P_i^{\alpha_i}$.

Or P_i est irréductible, donc $\pi_{M,X_i} = P_i^{a_i}$ avec $a_i \leq \alpha_i$.

Mais par ailleurs, $P_i^{\alpha_i-1}(M)X_i \neq 0$, donc $\pi_{M,X_i} = P_i^{a_i}$ ne divise pas $P_i^{\alpha_i-1}$.

Donc $a_i > \alpha_i$. Au final : $a_i = \alpha_i$ et /2

le polynôme conducteur de M en X_i est $\pi_{M,X_i} = P_i^{\alpha_i}$.

(b) Soit $Y \in \mathbb{K}[M]X_i$. Il existe $T \in \mathbb{K}[X]$ tel que $Y = T(M)X_i$.

On a alors, par commutation des polynômes en M :

$$P_i^{\alpha_i}(M)Y = P_i^{\alpha_i}(M)T(M)X_i = T(M) \underbrace{P_i^{\alpha_i}(M)X_i}_{=0} = 0$$

Donc $Y \in K_i$. /1

$\mathbb{K}[M]X_i \subset K_i$

(c) Soient $Y_1, Y_2 \dots Y_s$ tel que $\forall i \in \mathbb{N}_s$, $Y_i \in \mathbb{K}[M]X_i$ et $\sum_{i=1}^s Y_i = 0$.

Alors comme Y_i est aussi élément de K_i , on a une somme d'éléments de K_i , nulle.

On sait que la somme des espaces K_i est directe, donc nécessairement pour tout i , $Y_i = 0$. /1,5

On a donc $\bigoplus_{h \in \mathbb{N}_s} \mathbb{K}[M]X_h$.

(d) On commence par montrer que $\pi_{M,X}$ est un multiple de chaque π_{M,X_h} .

Il s'agit donc de montrer que pour tout $h \in \mathbb{N}_s$ $\pi_{M,X_h} | \pi_{M,X}$, i.e. $\pi_{M,X} \in \mathcal{I}_{M,X_h}$. Or

$$0 = \pi_{M,X}(M) \times X = \pi_{M,X}(M) \left(\sum_{h=1}^s X_h \right) = \sum_{h=1}^s \pi_{M,X}(M)X_h$$

Or $\pi_{M,X}$ est un polynôme, donc $\forall h \in H$, $\pi_{M,X}(M)X_h \in \mathbb{K}[M]X_h$.

Mais on a la somme directe $\bigoplus_{h \in \mathbb{N}_s} \mathbb{K}[M]X_h$, donc :

$$\sum_{h=1}^s \pi_{M,X}(M)(X_h) = 0 \implies \forall h \in \mathbb{N}_s, \pi_{M,X}(M)(X_h) = 0 \implies \forall h \in \mathbb{N}_s, \pi_{M,X_h} | \pi_{M,X}$$

Ainsi $\pi_{M,X}$ est un multiple de chaque π_{M,X_h} . /1,5
 Montrons maintenant que c'est le plus petit. Soit $T \in \mathbb{K}[X]$:

$$\forall h \in \mathbb{N}_s, \pi_{M,X_h}|T \iff \forall h \in \mathbb{N}_s, T(M) \times X_h = 0 \implies T(M) \times X = \sum_{h=1}^s T(M) \times X_h = \sum_{h=1}^s 0 = 0$$

Donc $T \in \mathcal{I}_{M,X}$ et ainsi $\pi_{M,X}|T$. /1,5

Ainsi $\pi_{M,X}$ divise tous les multiples des π_{M,X_h}

$$\boxed{\pi_{M,X} = \bigvee_{h \in \mathbb{N}_s} \pi_{M,X_h}}$$

- (e) De même qu'on a démontré que $\mathbb{K}[M]$ était un espace vectoriel de dimension $\deg \pi_M$, sous-espace vectoriel de \mathcal{M} , donc $\deg \pi_M \leq n^2$ (a priori), on démontre que pour tout X , $\mathbb{K}[M]X$ est un espace vectoriel de dimension $\deg \pi_{M,X}$, sous-espace vectoriel de E , donc $\deg \pi_{M,X} \leq n$ (a priori), Or il existe X tel que $\pi_M = \pi_{M,X}$, donc /1,5

$$\boxed{\deg \pi_M \leq n}$$

4. Pré-décomposition de Fröbenius.

On fixe $i \in \mathbb{N}_s$ et on note $d_i = \deg P_i^{\alpha_i}$.

- (a) Soient $\lambda_0, \lambda_1 \dots \lambda_{d_i-1} \in \mathbb{K}$ tel que $\sum_{h=0}^{d_i-1} \lambda_h M^h X_i = 0$.

Alors le polynôme $T = \sum_{h=0}^{d_i-1} \lambda_h X^h$ vérifie $T(M)X_i = 0$, donc $\pi_{M,X_i}|T$.

Mais $\deg T < \deg \pi_{M,X_i} = d_i$. Donc nécessairement $T = 0$.

Par conséquent, pour tout $h \in \llbracket 0, \alpha_i - 1 \rrbracket$, $\lambda_h = 0$. /1

$$\boxed{(X_i, MX_i, \dots, M^{d_i-1}X_i) \text{ est une famille libre.}}$$

En fait c'est une base de $\mathbb{K}[M]X_i$.

- (b) On note R_i , la matrice de $\mathcal{M}_{n,d_i}(\mathbb{K})$ tel que pour tout $j \in \mathbb{N}_{\alpha_i}$, $C_j(R_i) = M^{j-1}X_i$. Le produit par blocs donne : /1

$$\boxed{M \times R_i = M \times (X_i \ MX_i \ M^2X_i \ \dots \ M^{d_i-1}X_i) = (MX_i \ M^2X_i \ M^3X_i \ \dots \ M^{d_i}X_i)}$$

- (c) $d_i = \deg(P_i^{\alpha_i})$. On a P_i unitaire. On suppose $P_i^{\alpha_i} = X^{d_i} + a_{d_i-1}X^{d_i-1} + \dots + a_1X + a_0$. On a alors $P_i^{\alpha_i}(M)X_i = 0$, donc $M^{d_i}X_i = -a_{d_i-1}M^{d_i-1}X_i - \dots - a_1MX_i - a_0X_i$.

On a alors /2

$$\boxed{R_i \times \underbrace{\begin{pmatrix} 0 & \dots & \dots & 0 & -a_0 \\ 1 & \ddots & & \vdots & -a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{d_i-2} \\ 0 & \dots & 0 & 1 & -a_{d_i-1} \end{pmatrix}}_{=F_i} = (MX_i \ M^2X_i \ M^3X_i \ \dots \ M^{d_i}X_i) = M \times R_i}$$

F_i s'appelle la matrice compagnon du polynôme $P_i^{\alpha_i}$.

En combinant bien toutes les matrices F_i , on obtient la décomposition de Fröbenius de M .