RÉDUCTION DES ENDOMORPHISMES

OLIVIER DEBARRE

Table des matières

Dans tout ce texte, u désigne un endomorphisme d'un espace vectoriel E de dimension s sur un corps $\mathbf{k}$.

1. Espaces propres et espaces caractéristiques

Pour chaque $\lambda \in \mathbf{k}$, on définit l'*espace propre* de u associé par

$$E_\lambda = \mathrm{Ker}(u - \lambda \,\mathrm{Id}_E)$$

C'est un sous-espace vectoriel de E sur lequel u est une homothétie de rapport λ. Un élément de E_λ s'appelle un *vecteur propre* de u (pour la valeur propre λ). Pour des raisons techniques, on suppose souvent un vecteur propre non nul (de sorte que la valeur propre associée est bien déterminée). Les *valeurs propres* de u sont les éléments de $\mathbf{k}$ pour lesquelles existe un vecteur propre (non nul). Ce sont donc les racines dans $\mathbf{k}$ du *polynôme caractéristique*

$$\chi_u(X) = \mathrm{dét}(X \,\mathrm{Id}_E - u) \in \mathbf{k}[X]$$

un polynôme unitaire de degré s. On donne des définitions analogues pour des matrices carrées à coefficients dans $\mathbf{k}$. On aura souvent besoin de considérer des valeurs

propres dans un corps plus grand que $\mathbf{k}$, ou des vecteurs propres à coeffficients dans un corps plus grand que $\mathbf{k}$ (par exemple, lorsque $\mathbf{k} = \mathbf{R}$, dans le corps des complexes). Il est alors plus facile de raisonner avec des matrices.

Exercices 1. (1) Montrer qu'une matrice carrée M à coefficients dans $\mathbf{k}$ est trigonalisable dans $\mathbf{k}$ (c'est-à-dire semblable à une matrice triangulaire supérieure) si et seulement si son polynôme caractéristique est scindé sur $\mathbf{k}$.

(2) Soit M une matrice carrée à coefficients dans $\mathbf{k}$ dont le polynôme caractéristique est scindé. Soit $P \in \mathbf{k}[X]$. Si $\lambda_1, \ldots, \lambda_m$ sont les valeurs propres de M, les valeurs propres de $P(M)$ sont $P(\lambda_1), \ldots, P(\lambda_m)$.

(3) On dit qu'une matrice carrée M d'ordre s est *nilpotente* s'il existe un entier $r > 0$ tel que $M^r = 0$. Montrer que M est nilpotente si et seulement si $\chi_M(X) = X^s$.

(4) Montrer qu'une matrice $M \in \mathscr{M}_s(\mathbf{C})$ est nilpotente si et seulement si la matrice nulle est dans l'adhérence de la classe de similitude $\mathscr{C}_M = \{PMP^{-1} \mid P \in \mathrm{GL}_s(\mathbf{C})\}$.

Les espaces propres sont en somme directe, mais leur somme directe n'est E que si u est diagonalisable. Par exemple, la seule valeur propre de la matrice carrée

$$U_s = \begin{pmatrix} 0 & 1 & 0 & \cdots & \ldots & 0 \\ 0 & 0 & 1 & 0 & \ldots & 0 \\ \vdots & & \ddots & \ddots & \ddots & \vdots \\ \vdots & & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & \cdots & 0 & 1 \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 \end{pmatrix} \tag{1}$$

est 0, et l'espace propre associé est de dimension 1.

L'espace vectoriel $\mathrm{End}(E)$ des endomorphismes de E étant de dimension finie s^2, la famille $\{\mathrm{Id}_E, u, u^2, \ldots, u^{s^2}\}$ est liée. Il existe donc un polynôme non nul P (de degré au plus s^2) tel que $P(u) = 0$. En d'autres termes, le morphisme d'anneaux

$$\begin{array}{ccc} \mathbf{k}[X] & \longrightarrow & \mathrm{End}(E) \\ Q & \longmapsto & Q(u) \end{array}$$

n'est pas injectif. Son noyau est donc engendré par un polynôme unitaire uniquement déterminé, que l'on appelle le *polynôme minimal* de u, et que l'on notera μ_u.

Remarques 1. (1) Le polynôme minimal de l'homothétie $\lambda \mathrm{Id}_E$ est $X - \lambda$; en particulier, le polynôme minimal de l'endomorphisme nul est X (sauf si $E = 0$, auquel cas le polynôme caractéristique de tout endomorphisme de E est 1 !).

(2) On définit de façon analogue le polynôme minimal d'une matrice carrée M à coefficients dans $\mathbf{k}$. Notons que le polynôme minimal de M reste le polynôme

minimal de la matrice M vue comme matrice à coefficients dans n'importe quel corps contenant $\mathbf{k}$. Cela résulte du fait que le degré du polynôme minimal est le rang de la famille $\{M^r\}_{r\in\mathbf{N}}$.

Lemme 1. *Les valeurs propres de u sont exactement les racines (dans $\mathbf{k}$) de son polynôme minimal.*

Démonstration. Soit $\lambda \in \mathbf{k}$; en substituant u à X dans la division euclidienne $\mu_u(X) = Q(X)(X-\lambda) + \mu_u(\lambda)$, on obtient

$$0 = \mu_u(u) = Q(u) \circ (u - \lambda \operatorname{Id}_E) + \mu_u(\lambda) \operatorname{Id}_E \tag{2}$$

Si λ est valeur propre de u, on a $u(x) = \lambda x$ pour un vecteur propre (non nul) x. Si on applique l'égalité (2) à x, on obtient

$$0 = Q(u)\big((u - \lambda \operatorname{Id}_E)(x)\big) + \mu_u(\lambda)x = \mu_u(\lambda)x$$

de sorte que $\mu_u(\lambda) = 0$.

Inversement, si $\mu_u(\lambda) = 0$, on a $Q(u) \circ (u - \lambda \operatorname{Id}_E) = 0$ grâce à (2). Comme Q est de degré strictement inférieur à μ_u, on a $Q(u) \neq 0$, donc $u - \lambda \operatorname{Id}_E$ n'est pas bijectif : λ est bien valeur propre de u. □

Supposons que le polynôme minimal de u soit *scindé* sur $\mathbf{k}$; il se décompose donc en produit de facteurs linéaires

$$\mu_u(X) = \prod_{\lambda\in\mathbf{k}} (X-\lambda)^{q_\lambda} \qquad \text{avec } q_\lambda \in \mathbf{N}.$$

On définit alors l'*espace caractéristique* associé à λ par

$$E'_\lambda = \operatorname{Ker}(u - \lambda \operatorname{Id}_E)^{q_\lambda}$$

Il contient bien sûr l'espace propre E_λ et est stable par u. Comme, par définition, $\mu_u(u) = 0$, le lemme ci-dessous entraîne que les espaces caractéristiques sont en somme directe, et que leur somme est toujours E :

$$E = \operatorname{Ker} \mu_u(u) = \bigoplus_\lambda \operatorname{Ker}(u - \lambda \operatorname{Id}_E)^{q_\lambda} = \bigoplus_\lambda E'_\lambda$$

De plus, chaque projection $E \to E'_\lambda \subset E$ est un polynôme en u, ce qui nous servira plus tard.

Lemme 2 (Lemme des noyaux)**.** *Soient $P_1, \dots, P_m$ des polynômes premiers entre eux deux à deux. On pose $P = P_1 \cdots P_m$.*

1) *On a* $\operatorname{Ker} P(u) = \operatorname{Ker} P_1(u) \oplus \cdots \oplus \operatorname{Ker} P_m(u)$.
2) *Les projections* $\operatorname{Ker} P(u) \to \operatorname{Ker} P_i(u) \subset \operatorname{Ker} P(u)$ *relatives à cette décomposition en somme directe sont des polynômes en u.*

DÉMONSTRATION. On procède par récurrence sur m. Il suffit donc de traiter le cas $m = 2$. Le théorème de Bézout entraîne l'existence de polynômes A_1 et A_2 tels que

$$1 = A_1P_1 + A_2P_2$$

Si $x \in \operatorname{Ker} P_1(u) \cap \operatorname{Ker} P_2(u)$, on a $P_1(u)(x) = P_1(u)(x) = 0$, d'où

$$x = A_1(u)(x)P_1(u)(x) + A_2(u)(x)P_2(u)(x) = 0$$

D'autre part, $\operatorname{Ker} P_i(u)$ est contenu dans $\operatorname{Ker} P(u)$. Si $x \in \operatorname{Ker} P(u)$, on a

$$x = \underbrace{P_1(u)\big(A_1(u)(x)\big)}_{\in \operatorname{Ker} P_2(u)} + \underbrace{P_2(u)\big(A_2(u)(x)\big)}_{\in \operatorname{Ker} P_1(u)}$$

donc $E = \operatorname{Ker} P_1(u) + \operatorname{Ker} P_2(u)$. Ceci montre 1). De plus, la projection sur $\operatorname{Ker} P_1(u)$ est, sur $\operatorname{Ker} P(u)$, égale à $(A_2P_2)(u)$, et celle sur $\operatorname{Ker} P_2(u)$ à $(A_1P_1)(u)$, ce qui prouve 2). □

Proposition 1. *Les propriétés suivantes sont équivalentes :*
(i) *l'endomorphisme u est diagonalisable sur $\mathbf{k}$;*
(ii) *il existe un polynôme scindé à racines simples dans $\mathbf{k}$ qui annule u ;*
(iii) *le polynôme minimal de u est scindé à racines simples dans $\mathbf{k}$;*
(iv) *pour chaque λ, on a $E_\lambda = E'_\lambda$.*

DÉMONSTRATION. Il est clair que l'on a les implications (i)$\Longrightarrow$(ii)$\Longleftrightarrow$(iii)$\Longrightarrow$(iv). L'implication (iv)$\Longrightarrow$(i) résulte de l'égalité $E = \bigoplus_\lambda E'_\lambda$, conséquence du lemme des noyaux 2. □

Exercices 2. (1) Soient M une matrice inversible complexe et k un entier strictement positif tel que M^k soit diagonalisable. Montrer que M est diagonalisable.

(2) Montrer qu'une matrice $M \in \mathscr{M}_s(\mathbf{F}_q)$ est diagonalisable sur $\mathbf{F}_q$ si et seulement si $M^q = M$.

(3) Montrer qu'une matrice $M \in \mathscr{M}_s(\mathbf{C})$ est diagonalisable si et seulement si sa classe de similitude $\mathscr{C}_M = \{PMP^{-1} \mid P \in \mathrm{GL}_s(\mathbf{C})\}$ est fermée dans $\mathscr{M}_s(\mathbf{C})$.

(4) Soit M une matrice complexe carrée. Montrer que la série $\sum_{n=0}^{+\infty} \frac{M^n}{n!}$ converge. On appelle sa limite l'*exponentielle* de la matrice M et on la note $\exp(M)$ ou e^M. Montrer dét$(\exp(M)) = \exp(\mathrm{Tr}(M))$. Montrer qu'il existe un polynôme $P \in \mathbf{C}[X]$ tel que $e^M = P(M)$.

2. Décomposition de Dunford

On décompose un endomorphisme en une partie « facile », car diagonalisable, et une partie nilpotente.

Proposition 2 (Décomposition de Dunford)**.** *Supposons le polynôme minimal de u scindé. Il existe une décomposition*

$$u = d + n$$

unique telle que

1) *d est diagonalisable ;*
2) *n est nilpotent ;*
3) *$dn = nd$.*

De plus, d et n sont des polynômes en u.

Démonstration. Comme $\sum \pi_\lambda = \mathrm{Id}_E$, on écrit

$$u = \sum u\pi_\lambda = \underbrace{\sum \lambda\pi_\lambda}_{d} + \underbrace{\sum (u - \lambda \,\mathrm{Id}_E)\pi_\lambda}_{n}$$

et on a toutes les propriétés cherchées.

Montrons l'unicité. Si l'on a une autre décomposition $u = d' + n'$ vérifiant les propriétés 1), 2) et 3), les endomorphismes d' et n' commutent à u, donc à tout polynôme en u, donc à d et n. Donc les endomorphismes diagonalisables d et d' diagonalisent dans une même base et $d - d' = n' - n$ est diagonalisable et nilpotent donc est nul. □

Dans le cas où le polynôme minimal de u n'est pas scindé, on peut toujours se placer sur un corps de décomposition de μ_u. Il faut alors bien sûr, dans l'énoncé de la proposition, comprendre que d est diagonalisable dans une extension convenable de $\mathbf{k}$. Il n'est cependant pas toujours vrai que d et n sont « définis sur $\mathbf{k}$ » (il est plus facile de penser en termes de matrices) : il faut supposer le corps $\mathbf{k}$ *parfait* (*cf.* définition 1 et Théorème 5).

Lorsque $\mathbf{k} = \mathbf{R}$, on peut procéder ainsi : comme $u = d + n$, on a $u = \bar{u} = \bar{d} + \bar{n}$ et les endomorphismes $\bar{d}$ et $\bar{n}$ vérifient encore les propriétés 1), 2) et 3) (de nouveau, il est plus prudent de raisonner avec des matrices, cela évite d'expliquer de quel espace vectoriel $\bar{u}$ est un endomorphisme). Par unicité, on a $\bar{d} = d$ et $\bar{n} = n$, donc d et n sont réels. De plus, si P est un polynôme complexe tel que $d = P(u)$, on a $d = \mathrm{Re}(d) = \mathrm{Re}(P(u)) = (\mathrm{Re}\, P)(u)$ et idem pour n.

Exercices 3. (1) Soit $M = D + N$ la décomposition de Dunford d'une matrice carrée. À quelle condition M est-elle semblable à D ? Si M est inversible, montrer que D l'est aussi.

(2) Soient M une matrice inversible complexe et n un entier strictement positif. Montrer qu'il existe un polynôme $P \in \mathbf{C}[X]$ tel que $P(M)^n = M$ (on pourra d'abord traiter le cas $M = \lambda I + N$, avec $\lambda \neq 0$ et N nilpotente, en utilisant un développement en série entière de $\sqrt[n]{1+x}$).

(3) Soit M une matrice complexe carrée. Montrer qu'il existe un polynôme $P \in \mathbf{C}[X]$ tel que $e^{P(M)} = M$ (procéder comme en (2) ; voir exercice 2(4) pour la définition de l'exponentielle d'une matrice). Si M est réelle, peut-on trouver un tel polynôme dans $\mathbf{R}[X]$?

(4) Soit M une matrice réelle inversible. Montrer qu'il existe une matrice réelle A telle que $M = e^A$ si et seulement si il existe une matrice réelle N telle que $M = N^2$.

(5) Soit M une matrice réelle inversible telle qu'il existe une matrice réelle N telle que $M = N^2$. Montrer que pour tout entier $k \neq 0$, il existe une matrice réelle P telle que $M = P^k$.

3. Structure des endomorphismes nilpotents et réduite de Jordan

Sur chaque espace caractéristique E'_λ, l'endomorphisme u est somme de l'homothétie de rapport λ et d'un endomorphisme nilpotent. Nous allons montrer que dans une base convenable, la matrice d'un endomorphisme nilpotent est diagonale par blocs du type U_r défini en (1). En conclusion, si le polynôme minimal est scindé, on aura trouvé une base dans laquelle la matrice de u est diagonale par blocs du type $\lambda I_r + U_r$.

Attention, le même λ peut intervenir plusieurs fois, comme dans la matrice

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

On considère donc un endomorphisme nilpotent u de l'espace vectoriel E de dimension s.

Soient e_0 un vecteur de E et r le plus petit entier positif tel que $u^r(e_0) = 0$. On pose $e_i = u^i(e_0)$. Les vecteurs $(e_0, \ldots, e_{r-1})$ forment une famille *libre*. Montrons-le par récurrence sur r. C'est évident pour $r = 0$. Si $r \geq 1$ et que l'on a une combinaison linéaire nulle

$$a_0 e_0 + \cdots + a_{r-1} e_{r-1} = 0$$

on applique u et on obtient

$$a_0 e_1 + \cdots + a_{r-2} e_{r-1} = 0$$

Comme le plus petit entier r' tel que $u^{r'}(u(e_0)) = 0$ est $r-1$, l'hypothèse de récurrence dit que la famille $(e_1, \dots, e_{r-1})$ est libre. On a donc $a_0 = \cdots = a_{r-2} = 0$, puis $a_{r-1} = 0$ car $e_{r-1} \neq 0$. On a donc en particulier $r \leq s$. Si $r = s$, on obtient ainsi une base de E dans laquelle la matrice de u est U_s.

Dans le cas général, on note p le plus petit entier tel que $u^p = 0$ et $N_i = \operatorname{Ker} u^i$. On vérifie que l'on a une chaîne d'inclusions strictes

$$\{0\} = N_0 \subsetneq N_1 \subsetneq \cdots \subsetneq N_p = E$$

En particulier, $\dim(N_i) \geq i$ pour $1 \leq i \leq p$, de sorte que $p \leq s$. On va construire par récurrence descendante sur $i \in \{0, \dots, p\}$ des sous-espaces vectoriels M_i de E tels que

$$N_i = N_{i-1} \oplus M_i$$

vérifiant $u(M_i) \subset M_{i-1}$. On a donc

$$\begin{array}{ccccc} N_i & = & N_{i-1} & \oplus & M_i \\ {\scriptstyle u}\downarrow & & {\scriptstyle u}\downarrow & & \downarrow{\scriptstyle u} \\ N_{i-1} & = & N_{i-2} & \oplus & M_{i-1} \end{array}$$

ainsi que

$$E = \underbrace{M_1 \oplus \cdots \oplus M_i}_{N_i} \oplus M_{i+1} \oplus \cdots \oplus M_p$$

La construction se fait de la manière suivante. On prend pour M_p n'importe quel supplémentaire de N_p dans E. Si M_i $(i \geq 2)$ est construit, on remarque que

$$\begin{array}{rcll} u(M_i) & \subset & N_{i-1} & \text{car } u(N_i) \subset N_{i-1} \\ u(M_i) \cap N_{i-2} & = & \{0\} & \text{car } M_i \cap N_{i-1} = \{0\} \end{array}$$

Il suffit de prendre pour M_{i-1} un supplémentaire de N_{i-2} dans N_{i-1} contenant $u(M_i)$. Remarquons enfin que la restriction de u à M_i est injective pour $i \geq 2$, puisque $M_i \cap N_1 = \{0\}$.

On construit alors une base de E de la façon suivante :

$$\begin{array}{ccccccc}
M_p & \overset{u}{\hookrightarrow} & M_{p-1} & \overset{u}{\hookrightarrow} & \cdots & \overset{u}{\hookrightarrow} & M_1 \\
e_{p,1} & & u(e_{p,1}) & & & & u^{p-1}(e_{p,1}) \\
\vdots & & \vdots & & & & \vdots \\
e_{p,m_p} & & u(e_{p,m_p}) & & & & u^{p-1}(e_{p,m_p}) \\
& & e_{p-1,m_p+1} & & & & u^{p-2}(e_{p-1,m_p+1}) \\
& & \vdots & & & & \vdots \\
& & e_{p-1,m_{p-1}} & & & & u^{p-2}(e_{p-1,m_{p-1}}) \\
& & & & & & \vdots \\
& & & & & & e_{1,m_2+1} \\
& & & & & & \vdots \\
& & & & & & \vdots \\
& & & & & & e_{1,m_1}
\end{array}$$

avec $m_i = \dim M_i$. La famille des vecteurs qui apparaissent dans ce tableau forme une base de E que l'on ordonne en partant du coin supérieur droit avec $u^{p-1}(e_{p,1})$, en lisant la première ligne vers la gauche, puis la seconde ligne aussi vers la gauche et ainsi de suite jusqu'à la dernière ligne, qui est donc le seul vecteur e_{1,m_1}.

La matrice de u dans cette base est diagonale par blocs de type U_r, avec m_p blocs de type U_p, puis $m_{p-1} - m_p$ blocs de type U_{p-1} et ainsi de suite jusqu'à $m_1 = \dim(\operatorname{Ker} u)$ blocs de type U_1 (c'est-à-dire la matrice carrée d'ordre 1 nulle !).

Nous avons donc démontré l'existence de la forme réduite de la matrice d'un endomorphisme nilpotent annoncée au début de ce numéro. On peut montrer qu'une telle décomposition est unique à l'ordre des blocs près. C'est facile une fois qu'on a réalisé que chaque bloc de taille r donne lieu à $\min(r, i)$ vecteurs libres de N_i. Si n_r est le nombre de blocs U_r, on a donc

$$\dim N_i = \sum_{r=1}^{i} r n_r + i \sum_{r=i+1}^{s} n_r$$

Nous avons montré que si le polynôme minimal d'un endomorphisme u de l'espace vectoriel E est scindé, il existe une base de E dans laquelle la matrice de u est diagonale par blocs du type $\lambda I_r + U_r$. C'est ce qu'on appelle la *réduction de Jordan* de l'endomorphisme u. Il existe bien d'autres approches de la réduction de Jordan. Nous en présentons une dans les numéros suivants basée sur le fait que l'anneau $\mathbf{k}[X]$ est euclidien.

Exercice 1. Soient $M \in \mathscr{M}_s(\mathbf{k})$ et $t \in \mathbf{k} - \{0\}$. Montrer que si M est nilpotente, M est semblable à tM. Réciproquement, si $t \in \mathbf{k}$ n'est pas une racine de l'unité et que M et tM sont semblables, montrer que M est nilpotente.

4. Matrices à coefficients dans un anneau euclidien

On sait qu'une matrice M (pas nécessairement carrée) de rang r à coefficients dans un corps est équivalent à la matrice par blocs

$$\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$$

On a une version de ce résultat pour les matrices à coefficients dans un anneau euclidien.

Théorème 1. *Soit M une matrice à coefficients dans un anneau euclidien A. Il existe des matrices inversibles P et Q à coefficients dans A telles que*

$$PMQ = \begin{pmatrix} d_1 & & & & \\ & \ddots & & 0 & \\ & & d_r & & \\ & & & 0 & \\ & 0 & & & \ddots \\ & & & & & 0 \end{pmatrix}$$

avec $d_1 \mid \cdots \mid d_r$. Les d_i sont uniquement déterminés (à multiplication par une unité de A près).

Cet énoncé est encore vrai lorsque A est un anneau qui n'est que principal (on utilise en particulier pour la démonstration le résultat de l'exercice 4.2) ci-dessous). En revanche, on va voir dans la démonstration que lorsque A est euclidien, on peut choisir P et Q (qui ne sont pas uniquement déterminées !) produits de matrices du type $I + aE_{i,j}$ avec $i \neq j$ et $a \in A$; en d'autres termes, on peut arriver à la forme réduite de M par des opérations élémentaires[1] sur ses lignes et ses colonnes (il existe même un algorithme). Il existe des anneaux principaux pour lesquels cette propriété n'est pas vérifiée.

[1]Par « opération élémentaire » sur les lignes (resp. sur les colonnes), on entend uniquement « ajouter un multiple d'une ligne (resp. d'une colonne) à une autre ».

Avec de telles opérations, on peut aussi échanger deux lignes, l'une d'elles étant changée en son opposé :

$$\begin{pmatrix} L_i \\ L_j \end{pmatrix} \longrightarrow \begin{pmatrix} L_i \\ L_i + L_j \end{pmatrix} \longrightarrow \begin{pmatrix} -L_j \\ L_i + L_j \end{pmatrix} \longrightarrow \begin{pmatrix} -L_j \\ L_i \end{pmatrix}$$

(on ne peut pas juste échanger deux lignes, puisque le déterminant est inchangé par nos opérations élémentaires).

DÉMONSTRATION. Soit $\varphi : A \to \mathbf{N}$ le stathme euclidien, avec la convention $\varphi(a) = 0 \Leftrightarrow a = 0$[2].

On procède tout d'abord par récurrence sur le nombre de lignes + le nombre de colonnes de $M = (a_{i,j})$. On pose $\varphi(M) = \min_{a_{i,j}\neq 0} \varphi(a_{i,j})$ si $M \neq 0$ et $\varphi(0) = 0$ et, pour une taille fixée, on fait une seconde récurrence sur $\varphi(M)$.

Si $\varphi(M) = 0$, on a $M = 0$ et c'est terminé.

On suppose que l'on a $\varphi(M) > 0$. Par des échanges de lignes et de colonnes, on amène un coefficient non nul avec φ minimal dans le coin en haut à gauche. On fait la division $a_{i,1} = a_{1,1}q_i + r_i$, pour $i > 1$. Si $r_i \neq 0$, on fait une opération élémentaire sur les lignes qui remplace $a_{i,1}$ par r_i et on applique l'hypothèse de récurrence. Si $r_i = 0$, la même opération élémentaire remplace $a_{i,1}$ par 0. Il reste donc à considérer le cas où tous les coefficients de la première colonne, sauf le premier, sont nuls. Faisant pareil avec des opérations élémentaires sur les colonnes, on peut aussi supposer que tous les coefficients de la première ligne, sauf le premier, sont nuls. On obtient ainsi une matrice de la forme

$$\begin{pmatrix} a_{1,1} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & N & \\ 0 & & & \end{pmatrix}$$

On applique l'hypothèse de récurrence (sur la taille) à N et on obtient une matrice du type

$$\begin{pmatrix} a_{1,1} & 0 & & & & & \\ 0 & d_2 & & & & 0 & \\ & & \ddots & & & & \\ & & & d_r & & & \\ & & & & 0 & & \\ & 0 & & & & \ddots & \\ & & & & & & 0 \end{pmatrix}$$

avec $d_2 \mid \cdots \mid d_r$. Si l'on ajoute la $2^{\text{ème}}$ ligne à la première, le même raisonnement que ci-dessus montre qu'on peut appliquer l'hypothèse de (la seconde) récurrence, sauf si $a_{1,1}$ divise d_2, auquel cas la démonstration de l'existence est terminée.

---

[2]Cela signifie que pour tout $a \in A$ et $b \in A - \{0\}$, il existe un unique couple (q, r) dans A^2 tel que $a = bq + r$ et $\varphi(r) < \varphi(b)$.

Remarquons que si u est une unité de A, la division de u par u est $u = u \times 1 + 0$, donc comme, pour tout $a \in A$, on a $u = u \times (1 - u^{-1}a) + a$, l'unicité de la division entraîne $\varphi(a) \geq \varphi(u)$. On en déduit $\varphi(u) = \varphi(1) = \min_{a\in A-\{0\}} \varphi(a) > 0$.

Inversement, si $\varphi(u)$ a cette valeur, la division de 1 par u donne $1 = uq + r$ et nécessairement $r = 0$, de sorte que u est inversible dans A.

Pour l'unicité, c'est plus compliqué. Le plus rapide est de considérer

$$\delta_k(M) = \text{pgcd}(k \times k \text{ mineurs de } M)$$

et de montrer que $\delta_i(M)$ divise $\delta_i(PM)$. Lorsque P et Q sont inversibles, on a alors

$$\delta_k(M) = \delta_k(PMQ) = d_1 \cdots d_k$$

ce qui exprime les d_k en fonction d'entiers qui ne dépendent que de M (à multiplication par une unité de A près). Pour démontrer cette propriété, si l'on appelle L_i^k le k-vecteur formé des k premiers coefficients de la $i$ème ligne de M et que l'on note $P = (b_{i,j})_{1 \leq i,j \leq p}$, le premier $k \times k$ mineur de PM est

$$\text{dét}(b_{1,1}L_1^k + \cdots + b_{1,p}L_p^k, \ldots, b_{k,1}L_1^k + \cdots + b_{k,p}L_p^k)$$

qui est une combinaison linéaire des $k \times k$ mineurs extraits des k premières colonnes de M. Il est donc divisible par $\delta_k(M)$. □

Exercice 2. Soit G un sous-groupe de $\mathbf{Z}^n$.

1) Montrer qu'il existe un entier $r \in \{0, \ldots, n\}$ et des vecteurs $x_1, \ldots, x_r$ de $\mathbf{Z}^n$ tels que $G = \mathbf{Z}x_1 \oplus \cdots \oplus \mathbf{Z}x_r$ (on pourra raisonner par récurrence sur n et considérer $G \cap (\mathbf{Z}^{n-1} \times \{0\})$).

2) Montrer qu'il existe des vecteurs $e_1, \ldots, e_n \in \mathbf{Z}^n$ et des entiers strictement positifs $d_1, \ldots, d_r$ vérifiant $d_1 \mid \cdots \mid d_r$ tels que $\mathbf{Z}^n = \mathbf{Z}e_1 \oplus \cdots \oplus \mathbf{Z}e_n$ et $G = \mathbf{Z}d_1e_1 \oplus \cdots \oplus \mathbf{Z}d_re_r$ (appliquer le théorème 1 à la matrice $n \times r$ dont les colonnes sont les (composantes des) vecteurs $x_1, \ldots, x_r$).

3) Montrer que les entiers $r, d_1, \ldots, d_r$ ne dépendent que du groupe G (considérer le rang du $\mathbf{Q}$-sous-espace vectoriel de $\mathbf{Q}^n$ engendré par G, puis compter le nombre de points de l'image de G dans $(\mathbf{Z}/N\mathbf{Z})^n$ pour des entiers N bien choisis).

Les mêmes méthodes permettent de montrer que si A est un anneau principal,

- tout A-sous-module M de A^n est libre, engendré par au plus n éléments, c'est-à-dire qu'il existe un entier $r \in \{0, \ldots, n\}$ et des éléments $x_1, \ldots, x_r$ de A^n tels que $M = Ax_1 \oplus \cdots \oplus Ax_r$;
- tout A-module de type fini est isomorphe à une somme $A^s \oplus A/d_1A \oplus \cdots \oplus A/d_rA$ où $d_1, \ldots, d_r$ sont des éléments de A vérifiant $d_1 \mid \cdots \mid d_r$; les entiers s et r et les idéaux $d_1A, \ldots, d_rA$ sont uniquement déterminés.

Mais il vaut mieux ne pas parler de modules à l'oral d'agrégation...

Bien que ce ne soit pas utile ici, il est important de remarquer qu'une démonstration analogue donne le résultat suivant.

Théorème 2. *Soit M une matrice carrée d'ordre s* inversible *à coefficients dans un anneau euclidien A. Il existe une matrice inversible P à coefficients dans A, produit*

de matrices élémentaires, telle que

$$PM = \begin{pmatrix} 1 & & & 0 \\ & \ddots & & \\ & & 1 & \\ 0 & & & \det M \end{pmatrix}$$

On rappelle qu'une matrice carrée à coefficients dans un anneau A est inversible si et seulement si son déterminant est une unité de A.

Démonstration. On suit la démonstration du théorème 1 : on fait d'abord une récurrence sur la taille de la matrice, puis une deuxième récurrence sur $\min_{a_{i,1}\neq 0} \varphi(a_{i,1})$ (les éléments de la première colonne ne peuvent pas être tous nuls). On arrive ainsi, avec uniquement des opérations élémentaires sur les lignes, à une matrice de la forme

$$\begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,s} \\ 0 & & & \\ \vdots & & N & \\ 0 & & & \end{pmatrix}$$

Comme $\det M = a_{1,1} \det N$ est une unité, $a_{1,1}$ est une unité et N est inversible. On applique l'hypothèse de récurrence (sur la taille) à N et on obtient une matrice diagonale

$$\begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & \cdots & a_{1,s} \\ 0 & 1 & 0 & \cdots & 0 \\ & & \ddots & & \\ & 0 & & 1 & \\ & & & & \det(M)/a_{1,1} \end{pmatrix}$$

puis à la matrice diagonale

$$\begin{pmatrix} a_{1,1} & & & & \\ & 1 & & 0 & \\ & & \ddots & & \\ & 0 & & 1 & \\ & & & & \det(M)/a_{1,1} \end{pmatrix}$$

La séquence suivante d'opérations élémentaires

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & b \\ -a & 0 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & b \\ -a & 0 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & b \\ 0 & ab \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 \\ 0 & ab \end{pmatrix}$$

où a et b sont des unités, permet de conclure. □

Corollaire 1. *Soit A un anneau euclidien. Le groupe $\mathrm{SL}_s(A)$ est engendré par les matrices élémentaires.*

Exercices 4. (1) Montrer que le groupe $\mathrm{SL}_2(\mathbf{Z})$ est engendré par les matrices $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$ et $\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}$.

(2) Soient A un anneau principal et $a_1, \dots, a_s$ des éléments de A. Montrer qu'il existe un matrice carrée d'ordre s à coefficients dans A dont la première ligne est $(a_1, \dots, a_s)$ et dont le déterminant est le pgcd de $a_1, \dots, a_s$ (lorsque A est euclidien, cela résulte facilement du théorème 1 appliqué à la matrice ligne $(a_1, \dots, a_s)$).

5. Facteurs invariants

Il ressort du théorème 1 qu'étant donnée une matrice M carrée d'ordre s à coefficients dans le corps $\mathbf{k}$, il existe des matrices $P(X)$ et $Q(X)$ à coefficients dans $\mathbf{k}[X]$, inversibles donc à déterminant dans $\mathbf{k}^*$, telles que

$$P(X)(XI_s - M)Q(X) = \begin{pmatrix} p_1(X) & & 0 \\ & \ddots & \\ 0 & & p_s(X) \end{pmatrix}$$

où les $p_i(X)$ sont des polynômes unitaires vérifant $p_1 \mid \cdots \mid p_s$. Les p_i sont uniquement déterminés par la donnée de M. On les appelle les *facteurs invariants* de M (en général, on ne considère que ceux qui sont différents de 1). Remarquons que

$$\chi_M(X) = \det(XI_s - M) = \det P(X)(XI_s - M)Q(X) = p_1(X) \cdots p_s(X)$$

Cette définition très abstraite ne semble pas très utile pour la réduction des matrices, problème pour lequel on cherche des matrices *semblables* à M. La proposition suivante montre que c'est tout le contraire !

Proposition 3. *Des matrices carrées M et N à coefficients dans $\mathbf{k}$ sont semblables (dans $\mathscr{M}_s(\mathbf{k})$) si et seulement si les matrices $XI - M$ et $XI - N$ sont équivalentes (dans $\mathscr{M}_s(\mathbf{k}[X])$).*

Démonstration. Il est clair que si M et N sont semblables, $XI - M$ et $XI - N$ sont semblables, donc équivalentes.

Supposons inversement que l'on ait

$$P(X)(XI - M)Q(X) = XI - N$$

c'est-à-dire

$$P(X)(XI - M) = (XI - N)Q(X)^{-1}$$

Il le faut le justifier, mais ce n'est pas difficile de voir qu'on peut effectuer les divisions

$$\begin{aligned} P(X) &= (XI-N)P_1(X)+P_0 \\ Q(X)^{-1} &= \tilde{Q}_1(X)(XI-M)+\tilde{Q}_0 \end{aligned}$$

avec P_0 et $\tilde{Q}_0$ dans $\mathscr{M}_s(\mathbf{k})$ (la difficulté provient du fait qu'on n'est pas dans un anneau commutatif). On obtient en remplaçant

$$((XI-N)P_1(X)+P_0)(XI-M)=(XI-N)(\tilde{Q}_1(X)(XI-M)+\tilde{Q}_0)$$

ou encore

$$(XI-N)(P_1(X)-\tilde{Q}_1(X))(XI-M)=(XI-N)\tilde{Q}_0-P_0(XI-M)$$

Le membre de gauche est donc de degré au plus 1 en X, ce qui n'est possible que si $P_1(X)=\tilde{Q}_1(X)$. On a donc $(XI-N)\tilde{Q}_0=P_0(XI-M)$. L'égalité des coefficients de X donne $\tilde{Q}_0=P_0$, celle des coefficients constants donne $N\tilde{Q}_0=P_0M$. Il reste à montrer que $\tilde{Q}_0$ est inversible. On refait une division

$$Q(X)=Q_1(X)(XI-N)+Q_0$$

et on écrit

$$\begin{aligned} I &= Q(X)^{-1}Q(X) \\ &= (\tilde{Q}_1(X)(XI-M)+\tilde{Q}_0)Q(X) \\ &= \tilde{Q}_1(X)(XI-M)Q(X)+\tilde{Q}_0Q(X) \\ &= \tilde{Q}_1(X)P(X)^{-1}(XI-N)+\tilde{Q}_0(Q_1(X)(XI-N)+Q_0) \\ &= \big(\tilde{Q}_1(X)P(X)^{-1}+\tilde{Q}_0Q_1(X)\big)(XI-N)+\tilde{Q}_0Q_0 \end{aligned}$$

De nouveau, comme $\tilde{Q}_0Q_0$ est constant, le facteur de $XI-N$ est nul et $\tilde{Q}_0Q_0=I$, d'où la conclusion. □

On obtient ainsi les facteurs invariants comme invariants de similitude, mais pas encore de forme réduite pour M.

On verra plus tard (cor. 3) que le polynôme minimal de M est le « plus grand » des facteurs invariants. Le polynôme minimal d'une matrice carrée M à coefficients dans $\mathbf{k}$ reste le polynôme minimal de la matrice M vue comme matrice à coefficients dans n'importe quelle extension de $\mathbf{k}$ (rem. 1.(3)). Plus généralement, les facteurs invariants de M restent aussi les mêmes, que M soit vue comme matrice à coeffcients dans $\mathbf{k}$ ou comme matrice à coefficients dans une extension de $\mathbf{k}$. Cela résulte du théorème 1.

Corollaire 2. *Soit* $\mathbf{K}$ *un corps contenant* $\mathbf{k}$. *Deux matrices dans* $\mathscr{M}_s(\mathbf{k})$ *sont semblables dans* $\mathscr{M}_s(\mathbf{k})$ *si et seulement si elles sont semblables dans* $\mathscr{M}_s(\mathbf{K})$.

Exercices 5. (1) Démontrer directement le corollaire ci-dessus dans le cas où le corps $\mathbf{k}$ est infini (si M et N sont semblables dans $\mathscr{M}_s(\mathbf{K})$, il existe une matrice inversible $P \in \mathscr{M}_s(\mathbf{K})$ telle que $PM = NP$; on pourra écrire $P = e_1P_1 + \cdots + e_rP_r$, où $(e_1, \ldots, e_r)$ est une base de $\mathbf{K}$ sur $\mathbf{k}$ et $P_i \in \mathscr{M}_s(\mathbf{k})$, et montrer que pour $\lambda_1, \ldots, \lambda_r$ convenables dans $\mathbf{k}$, la matrice $\lambda_1P_1 + \cdots + \lambda_rP_r$ est inversible).

(2) Montrer qu'une matrice carrée à coefficients dans $\mathbf{k}$ est semblable à sa transposée.

Exemples 1. (1) Les facteurs invariants de la matrice λI_s sont tous égaux à $X - \lambda$ (ce sont d'ailleurs les seules matrices carrées d'ordre s qui ont s facteurs invariants non constants). En particulier, les facteurs invariants de la matrice nulle sont tous égaux à X.

(2) Si $\lambda_1, \ldots, \lambda_s$ sont des scalaires distincts deux à deux, la matrice diagonale de diagonale $(\lambda_1, \ldots, \lambda_s)$ a pour seul facteur invariant non constant $(X-\lambda_1) \ldots (X-\lambda_s)$.

(3) Les facteurs invariants de la matrice

$$\begin{pmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \mu \end{pmatrix}$$

(où $\lambda \neq \mu$), sont

$$(X - \lambda) \ , \quad (X - \lambda)(X - \mu)$$

6. Matrices compagnons

Par ce qui précède, il suffit pour prouver que deux matrices sont semblables qu'elles ont mêmes facteurs invariants. Nous allons pour chaque polynôme

$$P(X) = X^s + a_{s-1}X^{s-1} + \cdots + a_0$$

construire une matrice de facteur invariant P. Il s'agit de la matrice carrée d'ordre s

$$C_P = \begin{pmatrix} 0 & \cdots & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 & -a_{s-1} \end{pmatrix}$$

dite « compagnon » de P (la matrice compagnon du polynôme constant 1 est donc vide).

Proposition 4. 1) *Le seul facteur invariant (non constant) de C_P est P.*

2) *Le polynôme minimal de C_P est P.*

DÉMONSTRATION. On a remarqué à la fin de la démonstration du théorème 1 que l'on a

$$p_1(X)\dots p_k(X) = \text{pgcd}(k \times k \text{ mineurs de } XI - M)$$

On vérifie que pour C_P, on a pour chaque $k < s$ un tel mineur triangulaire supérieur avec des 1 sur la diagonale. On a donc $p_1(X) = \cdots = p_{s-1}(X) = 1$ et $p_s(X) = \chi_{C_P}(X) = P(X)$. Cela montre 1).

Soit maintenant u l'endomorphisme de $\mathbf{k}^s$ de matrice C_P dans la base canonique $(e_1, \dots, e_s)$. Cette base n'est autre que $(e_1, u(e_1), \dots, u^{s-1}(e_1))$, de sorte que $Q(u)(e_1)$ n'est nul pour aucun polynôme de degré $< s$. Le polynôme minimal est donc de degré au moins s. Comme $P(u)(e_1) = 0$, on a $P(u)(u^i(e_1)) = u^i(P(u)(e_1)) = 0$ donc $P(u) = 0$ et $P = \mu_u$. Cela montre 2). □

Maintenant que l'on sait réaliser un facteur invariant, on montre comment en réaliser n'importe quel nombre.

Proposition 5. *Soient P et Q des polynômes. Les facteurs invariants de la matrice par blocs*

$$\begin{pmatrix} C_P & 0 \\ 0 & C_Q \end{pmatrix}$$

sont $\text{pgcd}(P, Q)$ *et* $\text{ppcm}(P, Q)$.

DÉMONSTRATION. Vu la proposition 4, il suffit de calculer les deux facteurs invariants dans $\mathbf{k}[X]$ de la matrice 2×2

$$\begin{pmatrix} P(X) & 0 \\ 0 & Q(X) \end{pmatrix}$$

Comme on l'a rappelé ci-dessus, le premier est le pgcd des coefficients, et le produit des deux est le déterminant, c'est-à-dire $P(X)Q(X)$. □

Corollaire 3. *Soient M une matrice carrée à coefficients dans $\mathbf{k}$ et $p_1 \mid \cdots \mid p_r$ ses facteurs invariants (non constants). La matrice M est semblable à la matrice par blocs*

$$\begin{pmatrix} C_{p_1} & & 0 \\ & \ddots & \\ 0 & & C_{p_r} \end{pmatrix}$$

Le polynôme minimal de M est p_r.

DÉMONSTRATION. D'après la proposition 5 (par récurrence sur r), les facteurs invariants de cette matrice sont ceux de M. Elles sont donc semblables.

Posons

$$C_M = \begin{pmatrix} C_{p_1} & & 0 \\ & \ddots & \\ 0 & & C_{p_r} \end{pmatrix}$$

Si Q est un polynôme, on a

$$Q(C_M) = \begin{pmatrix} Q(C_{p_1}) & & 0 \\ & \ddots & \\ 0 & & Q(C_{p_r}) \end{pmatrix}$$

Cette matrice est nulle si et seulement si Q est divisible par le polynôme minimal de chaque C_{p_i}. Par la proposition 4.2), cela est équivalent à $p_r \mid Q$. Le polynôme minimal de M, qui est celui de C_M, est donc p_r. □

Corollaire 4 (Hamilton–Cayley)**.** *On a* $\chi_M(M) = 0$.

DÉMONSTRATION. En effet, $\chi_M = p_1 \cdots p_r$. □

Exemple 2. Les matrices compagnons qui interviennent dans la forme réduite de la matrice λI_s sont d'ordre 1, égales à (λ).

D'un point de vue plus intrinsèque, le fait que la matrice d'un endomorphisme u d'un espace vectoriel E soit semblable à une matrice par blocs du type ci-dessus signifie qu'il existe une décomposition de E en somme directe

$$E = E_1'' \oplus \cdots \oplus E_r'' \tag{3}$$

de sous-espaces vectoriels stables par u, tels que la restriction de u à chaque E_i'' soit *cyclique* de polynôme minimal p_i.

Qu'est-ce qu'un endomorphisme cyclique ? Un endomorphisme u d'un espace vectoriel E est dit *cyclique* s'il existe un vecteur $e \in E$ tel que la famille $(u^m(e))_{m\in\mathbf{N}}$ engendre E.

Faisons une petite remarque. Soit x un point de E. On désigne par E_x le plus petit sous-espace vectoriel de E contenant x et stable par u. C'est le sous-espace vectoriel de E engendré par la famille $(u^m(x))_{m\in\mathbf{N}}$.

Lemme 3. *Soit r le plus grand entier tel que la famille $(x, u(x), \ldots, u^{r-1}(x))$ soit libre. Cette famille est une base de E_x.*

Démonstration. Il suffit de montrer que cette famille engendre E_x. Par définition de r, le vecteur $u^r(x)$ est combinaison linéaire des vecteurs de cette famille et on voit facilement, par récurrence sur m, qu'il en est de même pour tous les $u^m(x)$. □

Le lemme 3 entraîne que si u est cyclique, $(e, u(e), \dots, u^{s-1}(e))$ est une base de E. Dans cette base, la matrice de u est une matrice compagnon. La réciproque étant évidente, on voit qu'un endomorphisme est cyclique si et seulement si sa matrice dans une base convenable est une matrice compagnon.

Proposition 6. *L'endomorphisme u est cyclique si et seulement si $\chi_u = \mu_u$.*

Démonstration. Si u est cyclique, sa matrice dans une base convenable est une matrice compagnon, donc son polynôme caractéristique et son polynôme minimal sont égaux (proposition 4.2)).

Inversement, si $\chi_u = \mu_u$, l'endomorphisme u a un seul facteur invariant, χ_u. Elle est donc semblable à C_{χ_u} (corollaire 3) et u est cyclique. □

Exemples 3. (1) Tout endomorphisme de E de matrice $\begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ dans une base (e_1, e_2, e_3) est cyclique : son polynôme caractéristique et son polynôme minimal sont $(X-2)^2(X-1)$. Il est engendré par n'importe quel vecteur qui n'est dans aucun sous-espace stable à part E, comme par exemple $e_2 + e_3$.

(2) Un endomorphisme de matrice $\begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$ n'est pas cyclique : son polynôme caractéristique est $(X-2)^3$, son polynôme minimal $(X-2)^2$.

(3) Un endomorphisme de matrice $\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$ n'est pas cyclique : son polynôme caractéristique est $(X-1)^4$, son polynôme minimal $(X-1)^2$.

7. Lien avec la réduction de Jordan

Le lien entre la réduction sous forme de matrice par blocs de type « compagnon » obtenue au corollaire 3 et la réduction de Jordan expliquée au §3 sous forme de matrice par blocs du type $\lambda I + U$ n'est pas clair. Notons que la réduction du corollaire 3 ne nécessite pas que le polynôme minimal soit scindé, alors que la réduction de Jordan, c'est vraiment nécessaire, puisque celui de la forme réduite l'est.

Pour relier les deux réductions, décomposons chaque facteur invariant en produit de polynômes irréductibles

$$p_i = \pi_1^{q_{i,1}} \cdots \pi_m^{q_{i,m}}$$

Comme les $\pi_j^{q_{i,j}}$ (souvent appelés *diviseurs élémentaires)* sont premiers entre eux deux à deux, la proposition 5 entraîne que la matrice compagnon C_{p_i} est semblable à la matrice par blocs

$$\begin{pmatrix} C_{\pi_1^{q_{i,1}}} & & 0 \\ & \ddots & \\ 0 & & C_{\pi_m^{q_{i,m}}} \end{pmatrix} \tag{4}$$

C'est particulièrement utile lorsque μ_M est scindé, puisque chaque π_j est alors de degré 1, c'est-à-dire de la forme $X - \lambda$. On est donc amené à étudier les matrices $C_{(X-\lambda)^n}$.

On vérifie que le seul facteur invariant non constant de la matrice $\lambda I_n + U_n$ est $(X - \lambda)^n$. On a ainsi bien redémontré l'existence d'une forme réduite de Jordan.

Inversement, il est utile de savoir passer de la forme de Jordan aux facteurs invariants. La forme de Jordan est composée de blocs du type $\lambda I_r + U_r$. À chaque tel bloc est associé le polynôme $(X - \lambda)^r$. Pour chaque valeur propre λ, on classe en ordre décroissant les blocs qui apparaissent, et on écrit en colonne les polynômes correspondants

$$\begin{array}{cccc} (X-\lambda_1)^{q_{1,1}} & (X-\lambda_2)^{q_{1,2}} & \cdots \\ (X-\lambda_1)^{q_{2,1}} & (X-\lambda_2)^{q_{2,2}} & \cdots \\ \vdots & \vdots \end{array}$$

avec $q_{i+1,j} \leq q_{i,j}$. On lit alors sur les lignes (en partant de la dernière) les facteurs invariants p_1, p_2, etc.

Exemples 4. (1) Les diviseurs élémentaires de la réduite de Jordan

$$\begin{pmatrix} \lambda & 1 & 0 & 0 & 0 & 0 \\ 0 & \lambda & 0 & 0 & 0 & 0 \\ 0 & 0 & \lambda & 1 & 0 & 0 \\ 0 & 0 & 0 & \lambda & 0 & 0 \\ 0 & 0 & 0 & 0 & \lambda & 0 \\ 0 & 0 & 0 & 0 & 0 & \mu \end{pmatrix}$$

(où $\lambda \neq \mu$), sont

$$\begin{array}{cc} (X-\lambda)^2 & (X-\mu) \\ (X-\lambda)^2 & \\ (X-\lambda) & \end{array}$$

Les facteurs invariants sont donc

$$(X-\lambda)\ , \quad (X-\lambda)^2\ , \quad (X-\lambda)^2(X-\mu)$$

(2) Si $M = \begin{pmatrix} 0 & 4 & 2 \\ -1 & -4 & -1 \\ 0 & 0 & -2 \end{pmatrix}$, on a

$$XI - M = \begin{pmatrix} X & -4 & -2 \\ 1 & X+4 & 1 \\ 0 & 0 & X+2 \end{pmatrix}$$

Faisons des opérations élémentaires selon l'algorithme plus ou moins décrit dans la démonstration du théorème 1 :

$$\begin{pmatrix} X & -4 & -2 \\ 1 & X+4 & 1 \\ 0 & 0 & X+2 \end{pmatrix} \xrightarrow{L_1 \leftrightarrow L_2} \begin{pmatrix} 1 & X+4 & 1 \\ X & -4 & -2 \\ 0 & 0 & X+2 \end{pmatrix}$$

$$\xrightarrow{L_2 \to L_2 - XL_1} \begin{pmatrix} 1 & X+4 & 1 \\ 0 & -4-X(X+4) & -2-X \\ 0 & 0 & X+2 \end{pmatrix} \xrightarrow[C_3 \to C_3 - C_1]{C_2 \to C_2 - (X+4)C_1} \begin{pmatrix} 1 & 0 & 0 \\ 0 & (X+2)^2 & -2-X \\ 0 & 0 & X+2 \end{pmatrix}$$

$$\xrightarrow{L_2 \to L_2 + L_3} \begin{pmatrix} 1 & 0 & 0 \\ 0 & (X+2)^2 & 0 \\ 0 & 0 & X+2 \end{pmatrix} \xrightarrow[L_1 \leftrightarrow L_2]{C_1 \leftrightarrow C_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & X+2 & 0 \\ 0 & 0 & (X+2)^2 \end{pmatrix}$$

Les facteurs invariants sont donc $X+2$ et $(X+2)^2$ et la réduite de Jordan est $\begin{pmatrix} -2 & 1 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & -2 \end{pmatrix}$. Un endomorphisme de matrice M n'est pas cyclique.

(3) Si $M = \begin{pmatrix} 3 & 1 & 0 & 0 \\ -4 & -1 & 0 & 0 \\ 6 & 1 & 2 & 1 \\ -14 & -5 & -1 & 0 \end{pmatrix}$, on obtient comme réduite pour $XI - M$ la matrice

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

Les facteurs invariants sont $(X-1)^2$ et $(X-1)^2$ et la réduite de Jordan est $\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$. Un endomorphisme de matrice M n'est pas cyclique.

(4) Un endomorphisme est cyclique si et seulement si, pour chaque valeur propre, il n'y a qu'un seul bloc de Jordan.

Certains arguments employés dans la méthode ci-dessus semblent peu naturels. Ils ne prennent tout leur sens que lorsqu'on utilise le langage des modules. Le point de départ est le suivant :

1) l'endomorphisme u permet de munir le $\mathbf{k}$-espace vectoriel E d'une structure de $\mathbf{k}[X]$-module en posant
$$X \cdot x = u(x)$$
2) tout $\mathbf{k}[X]$-module de type fini dans lequel tout élément est de torsion (c'est-à-dire qu'il existe un polynôme non nul avec lequel la multiplication donne 0) est isomorphe à une somme directe
$$\mathbf{k}[X]/(p_1) \oplus \cdots \oplus \mathbf{k}[X]/(p_r)$$
où les p_i sont des polynômes unitaires vérifiant $p_1 \mid \cdots \mid p_r$. Ils sont uniquement déterminés[3].

Ces polynômes sont bien sûr les facteurs invariants de u tels qu'ils ont été définis plus haut, et la décomposition de E en somme directe de sous-espaces vectoriels correspondant à l'isomorphisme
$$E \simeq \mathbf{k}[X]/(p_1) \oplus \cdots \oplus \mathbf{k}[X]/(p_r)$$
est la décomposition (3) en somme de sous-espaces stables cycliques. On retrouve ainsi la forme réduite du corollaire 3.

Le lemme chinois donne ensuite
$$\mathbf{k}[X]/(p_i) \simeq \mathbf{k}[X]/(\pi_1^{q_{i,1}}) \oplus \cdots \oplus \mathbf{k}[X]/(\pi_m^{q_{i,m}})$$
On obtient ainsi la forme réduite décrite en (4). Le passage à la réduite de Jordan proprement dite est similaire : dans le sous-espace vectoriel de E image de $\mathbf{k}[X]/(X-\lambda)^r$, on prend comme base e, image de 1, puis $(u-\lambda\,\mathrm{Id})(e), \ldots, (u-\lambda\,\mathrm{Id})^{r-1}(e)$.

Au prix d'un peu plus d'abstraction, on obtient donc de façon plus naturelle les résultats précédents. Bien sûr, il faut démontrer le théorème de structure des modules de type fini de torsion sur un anneau euclidien (on peut le déduire du théorème 1 mais ce n'est pas trivial). La méthode précédente a aussi l'avantage de fournir un algorithme pour la recherche des facteurs invariants.

8. Quelques applications

8.1. **Commutant et bicommutant.** Posons

$$\begin{aligned} \mathrm{Com}(u) &= \{v \in \mathrm{End}(E) \mid uv = vu\} \\ \mathscr{P}(u) &= \{P(u) \mid P \in \mathbf{k}[X]\} \end{aligned}$$

[3]La notation (p) désigne l'idéal de $\mathbf{k}[X]$ engendré par un polynôme p, c'est-à-dire l'ensemble des mutliples de p.

Il est clair que la dimension du sous-espace vectoriel $\mathscr{P}(u)$ de $\mathrm{End}(E)$ est le degré du polynôme minimal de u. Plus généralement, on définit, pour toute partie A de $\mathrm{End}(E)$, le *commutant* de A comme étant

$$\mathrm{Com}(A) = \bigcap_{w\in A} \mathrm{Com}(w) = \{v \in \mathrm{End}(E) \mid \forall w \in A \quad wv = vw\}$$

On a $A \subset \mathrm{Com}(\mathrm{Com}(A))$ et si $A \subset B$, on a $\mathrm{Com}(B) \subset \mathrm{Com}(A)$.

On a une autre caractérisation des endomorphismes cycliques.

Proposition 7. *L'endomorphisme u est cyclique si et seulement si* $\mathrm{Com}(u) = \mathscr{P}(u)$.

Démonstration. Il est clair que $\mathscr{P}(u)$ est toujours contenu dans le commutant de u.

Supposons u cyclique. Soit e un élément de E tel que $E_e = E$. Si v commute avec u, il est entièrement déterminé par $v(e)$, puisque $v(u^m(e)) = u^m(v(e))$. Si $v(e) = a_0e + a_1u(e) + \cdots + a_{s-1}u^{s-1}(e)$, on a donc $v = a_0\,\mathrm{Id}_E + a_1u + \cdots + a_{s-1}u^{s-1}$.

Pour la réciproque, remarquons la chose suivante : s'il y a au moins deux facteurs invariants non constants, la projection sur le sous-espace vectoriel E_1'' de E correspondant au premier (voir (3)) n'est pas un polynôme en u, bien qu'elle commute avec u. En effet, si la projection s'écrit $P(u)$, alors $P(u)$ est nul sur E_2'', donc P est divisible par le polynôme minimal de la restriction de u à E_2'', à savoir p_2. De la même façon, $P(u) - u$ est aussi nul sur E_1'', donc p_1 divise $P - 1$, ce qui est absurde puisque p_1 divise p_2. □

On a un résultat plus complet, mais plus technique, dont il est plus facile (mais pas indispensable) de présenter la démonstration avec le langage des $\mathbf{k}[X]$-modules.

Proposition 8. *La dimension du $\mathbf{k}$-espace vectoriel* $\mathrm{Com}(u)$ *est*

$$\sum_{i=1}^{r}(2r - 2i + 1)\deg p_i$$

Démonstration. Un endomorphisme v de E est dans $\mathrm{Com}(u)$ si et seulement si le morphisme induit

$$\mathbf{k}[X]/(p_1) \oplus \cdots \oplus \mathbf{k}[X]/(p_r) \longrightarrow \mathbf{k}[X]/(p_1) \oplus \cdots \oplus \mathbf{k}[X]/(p_r)$$

est un morphisme de $\mathbf{k}[X]$-module. Or un tel morphisme est défini par les

$$\begin{array}{rccc} v_{i,j}: & \mathbf{k}[X]/(p_i) & \longrightarrow & \mathbf{k}[X]/(p_j) \\ & 1 & \longmapsto & p_{i,j} \end{array}$$

avec $p_j \mid p_ip_{i,j}$. Si $i \geq j$, on a $p_j \mid p_i$ et $p_{i,j}$ est quelconque, ce qui donne un espace vectoriel de dimension $\deg p_j$.

Si $i < j$, on a $p_i \mid p_j$ et p_j/p_i divise $p_{i,j}$, ce qui donne un espace vectoriel de dimension $\deg p_i$. La dimension de $\mathrm{Com}(u)$ est donc

$$\sum_{i=1}^{r}\Big((r-i)\deg p_i + \sum_{j=1}^{i}\deg p_j\Big)$$

ce qui donne le résultat. □

Proposition 9. *On a* $\mathrm{Com}(\mathrm{Com}(u)) = \mathscr{P}(u)$.

Démonstration. Par définition, $\mathscr{P}(u) \subset \mathrm{Com}(\mathrm{Com}(u))$. Soit $E = E_1'' \oplus \cdots \oplus E_r''$ la décomposition de E correspondant aux facteurs invariants (voir (3). Comme ces sous-espaces sont stables par u, les projections sur les facteurs sont dans $\mathrm{Com}(u)$. Tout élément v de $\mathrm{Com}(\mathrm{Com}(u))$ commute avec ces projections donc laisse stable chaque E_i''. Comme la restriction de u à E_i'' est cyclique, il existe par la proposition 7 un polynôme Q_i tel que $v|_{E_i} = Q_i(u|_{E_i})$.

Notons $e_i \in E_i''$ un vecteur tel que les $(u^m(e))_{m\in\mathbf{N}}$ engendrent E_i''. Pour chaque j, on définit comme dans la démonstration de la proposition 8 un endomorphisme v_j de $\mathrm{Com}(u)$ en posant

$$v_j(e_k) = \begin{cases} 0 & \text{si } \ k \neq r \\ e_j & \text{si } \ k = r \end{cases}$$

On a alors $v \circ v_j = v_j \circ v$, c'est-à-dire

$$\begin{array}{rcl} v\circ v_j(e_r) & = & v_j \circ v(e_r) \\ \| & & \| \\ v(e_j) & & v_j \circ Q_r(u)(e_r) \\ \| & & \| \\ Q_j(u)(e_j) & & Q_r(u)\circ v_j(e_r) \\ \| & & \| \\ Q_j(u)(e_j) & & Q_r(u)(e_j) \end{array}$$

de sorte que $Q_j(u)|_{E_j} = Q_r(u)|_{E_j}$, c'est-à-dire $v|_{E_j} = Q_r(u)|_{E_j}$. On en déduit $v = Q_r(u)$. □

8.2. **Sous-espaces stables.** On s'intéresse ici aux sous-espaces vectoriels de E stables par u.

Proposition 10. *Si* $\mathbf{k}$ *est infini, les propriétés suivantes sont équivalentes :*
(i) u *est cyclique ;*
(ii) $\chi_u = \mu_u$ *;*
(iii) $\mathrm{Com}(u) = \mathscr{P}(u)$ *;*
(iv) E *n'a qu'un nombre fini de sous-espaces vectoriels stables par* u *.*

Démonstration. L'équivalence des propriétés (i), (ii) et (iii) a déjà été vue et est valable en général, sans condition sur le corps $\mathbf{k}$.

Si u est cyclique, on a $E \simeq \mathbf{k}[X]/(\mu_u)$. Les sous-espaces stables sont les $\mathbf{k}[X]/(P)$, avec P unitaire divisant μ_u : il n'y en a qu'un nombre fini.

Inversement, s'il n'y a qu'un nombre fini de sous-espaces stables et si $\mathbf{k}$ est infini, on peut prendre e hors de la réunion des sous-espaces stables autres que E et $E_e = E$. □

Exemples 5. Reprenons certains des exemples 3.

(1) Les sous-espaces stables de la matrice (cyclique) $\begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ sont, en notant (e_1, e_2, e_3) la base canonique,

$$\langle 0 \rangle \ , \quad \langle e_1 \rangle \ , \quad \langle e_3 \rangle \ , \quad \langle e_1, e_2 \rangle \ , \quad \langle e_1, e_3 \rangle \ , \quad \langle e_1, e_2, e_3 \rangle$$

Ils correspondent aux diviseurs unitaires de son polynôme minimal $(X-2)^2(X-1)$, à savoir

$$(X-2)^2(X-1) \ , \quad (X-2)(X-1) \ , \quad (X-2)^2 \ , \quad (X-1) \ , \quad (X-2) \ , \quad 1$$

(2) Les sous-espaces stables de la matrice (non cyclique) $\begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$ sont, en notant (e_1, e_2, e_3) la base canonique,

$$\langle 0 \rangle \ , \quad \langle \lambda e_1 + \mu e_3 \rangle \ , \quad \langle e_1, e_2 \rangle \ , \quad \langle \lambda e_1 + \mu e_3, e_2 \rangle \ , \quad \langle e_1, e_2, e_3 \rangle \ ,$$

pour tout $(\lambda, \mu) \in \mathbf{P}^1_{\mathbf{k}}$.

8.3. **Endomorphismes simples et semi-simples.**

Théorème 3. *L'endomorphisme* u *est simple, c'est-à-dire que les seuls* $\mathbf{k}$*-sous-espaces vectoriels de* E *stables par* u *sont* E *et* $\{0\}$*, si et seulement si* χ_u *est irréductible.*

Lorsque $\mathbf{k}$ est algébriquement clos, cela n'arrive qu'en dimension $s = 1$. Lorsque $\mathbf{k} = \mathbf{R}$, cela n'arrive qu'en dimension 1 ou 2 (c'est le cas par exemple des rotations générales dans le plan).

DÉMONSTRATION. Si χ_u est irréductible et que $F \subset E$ est stable, on a $\chi_{u|_F} \mid \chi_u$ donc $F{=}E$ ou $\{0\}$.

Inversement, supposons u simple. Pour tout x non nul dans E, l'espace vectoriel E_x engendré par les $(u^m(x))_{m\in\mathbf{N}}$ est stable donc égal à E. En particulier (lemme 3), pour tout polynôme P de degré $< s$, on a $P(u)(x) \neq 0$. L'endomorphisme $P(u)$ est ainsi injectif, donc bijectif. Supposons $\chi_u = QR$. Le théorème de Hamilton–Cayley (corollaire 4) entraîne

$$0 = \chi_u(u) = Q(u) \circ R(u)$$

de sorte que $Q(u)$ et $R(u)$ ne peuvent être tous deux bijectifs. L'un des polynômes Q ou R est donc de degré $\geq s$ par ce qui précède, ce qui montre que χ_u est irréductible. □

Théorème 4. *L'endomorphisme u est semi-simple, c'est-à-dire que tout sous-espace vectoriel de E stable admet un supplémentaire stable, si et seulement si μ_u n'est pas divisible par un carré non constant dans $\mathbf{k}[X]$.*

DÉMONSTRATION. Supposons $\mu_u = P^2Q$ avec P non constant. Alors le sous-espace vectoriel $F = \mathrm{Ker}(PQ(u))$ de E est stable. S'il admet un supplémentaire stable G dans E, et si $x \in G$, on a $P(u)(x) \in F \cap G$, donc $P(u)(x) = 0$. L'endomorphisme u est donc annulé ar PQ sur F, et par P sur G, donc par PQ sur E, ce qui est absurde.

Inversement, supposons μ_u produit de facteurs irréductibles distincts $\pi_1, \ldots, \pi_m$. Soit F un sous-espace vectoriel stable. La projection sur chaque $F_i = \mathrm{Ker}(\pi_i(u))$ étant un polynôme en u (lemme 2 des noyaux), on a

$$F = \bigoplus_i (F \cap F_i)$$

Mais $\mu_{u|_{F_i}} = \pi_i$ étant irréductible, $\mathbf{k}[u|_{F_i}] \simeq \mathbf{k}[X]/(\pi_i)$ est un corps. Les $\mathbf{k}$-sous-espaces vectoriels stables de F_i sont exactement ses $\mathbf{k}[u|_{F_i}]$-sous-espaces vectoriels. Ils admettent donc tous des supplémentaires. □

Corollaire 5. *L'endomorphisme u de E est semi-simple si et seulement s'il existe une décomposition $E = E_1 \oplus \cdots \oplus E_m$ en somme directe de sous-espaces vectoriels stables par u telle que u induise par restriction un endomorphisme simple de chaque E_i.*

DÉMONSTRATION. Si u est semi-simple, son polynôme minimal est produit de polynômes irréductibles distincts $\pi_1, \dots, \pi_m$. Posons $E_i = \mathrm{Ker}(\pi_i(u))$. Le lemme des noyaux 2 entraîne $E = E_1 \oplus \cdots \oplus E_m$. Le polynôme minimal de l'endomorphisme u_i de E_i induit par u est π_i, de sorte que u_i est simple par le théorème 3. La réciproque découle aussi des théorèmes 3 et 4. □

Remarque 2. En général, si on décompose le polynôme minimal μ_u en produit de facteurs irréductibles

$$\mu_u = \pi_1^{q_1} \cdots \pi_m^{q_m}$$

et que l'on pose

$$E_i' = \mathrm{Ker}(\pi_i(u)^{q_i})$$

(ce sont les espaces caractéristiques !), le lemme des noyaux donne une décomposition $E = E_1' \oplus \cdots \oplus E_m'$ en somme directe de sous-espaces vectoriels stables par u, chaque projection étant un polynôme en u. Le polynôme minimal de l'endomorphisme u_i de E_i' induit par u est $\pi_i^{q_i}$.

Corollaire 6. *Si* $\mathbf{k}$ *est algébriquement clos, l'endomorphisme* u *est semi-simple si et seulement s'il est diagonalisable.*

DÉMONSTRATION. Si u est diagonalisable, son polynôme minimal μ_u est scindé à racines simples dans $\mathbf{k}$ (prop. 1) donc u est semi-simple par le théorème 4. Réciproquement, si $\mathbf{k}$ est algébriquement clos, le polynôme minimal de u est scindé sur $\mathbf{k}$. Si u est de plus semi-simple, μ_u est à racines simples par le théorème 4, donc u est diagonalisable par la proposition 1. Ceci montre le premier point. □

Pour avoir un énoncé valable sur des corps plus généraux que les corps algébriquement clos, on introduit la définition suivante.

Définition 1. *Un corps* $\mathbf{k}$ *est* parfait *s'il est soit de caractéristique* 0*, soit de caractéristique* $p > 0$ *avec* $\mathbf{k}^p = \mathbf{k}$.

Un corps algébriquement clos est parfait. Un corps fini est parfait. Un corps parfait est aussi caractérisé par le fait que les racines de tout polynôme irréductible de $\mathbf{k}[X]$ dans un corps de décomposition sont simples (si $\alpha \in \mathbf{k} - \mathbf{k}^p$, le polynôme $X^p - \alpha$ est irréducible dans $\mathbf{k}[X]$, mais a une racine de multiplicité p, dans un corps de décomposition).

Corollaire 7. *Soit* $\mathbf{k}$ *un corps parfait. Une matrice* $M \in \mathscr{M}_s(\mathbf{k})$ *est semi-simple si et seulement si elle est diagonalisable dans une extension finie de* $\mathbf{k}$*. Elle est alors semi-simple dans toute extension de* $\mathbf{k}$.

DÉMONSTRATION. Soit $M \in \mathscr{M}_s(\mathbf{k})$ et soit $\mathbf{K}$ une extension finie de $\mathbf{k}$ sur laquelle μ_M est scindé. Si la matrice M est semi-simple, μ_M est produit de facteurs irréductibles distincts dans $\mathbf{k}[X]$ (théorème 4), donc aussi dans $\mathbf{K}[X]$ puisque $\mathbf{k}$ est parfait. Comme le polynôme minimal de M sur $\mathbf{K}$ divise ${\mu_M}^4$, il est scindé à racines simples et M est diagonalisable sur $\mathbf{K}$ par la proposition 1.

Réciproquement, si M est diagonalisable sur une extension $\mathbf{K}'$ de $\mathbf{k}$, le polynôme minimal de M sur $\mathbf{K}'$, qui est encore μ_M, est scindé à racines simples sur $\mathbf{K}'$ donc n'a pas de facteur carré sur $\mathbf{k}$. La matrice M est donc semi-simple par le théorème 4. □

Théorème 5 (Décomposition de Dunford sur un corps parfait)**.** *On suppose* $\mathbf{k}$ *parfait. Il existe une décomposition*

$$u = d + n$$

unique telle que

1) *d est semi-simple ;*
2) *n est nilpotent ;*
3) *$dn = nd$.*

De plus, d et n sont des polynômes en u.

Démonstration. La remarque 2 montre qu'il suffit de traiter le cas où le polynôme minimal de u est une puissance π^q d'un polynôme π irréductible dans $\mathbf{k}[X]$.

Dans un corps de décomposition K de π, on écrit $\pi(X) = \prod_\lambda (X-\lambda)$ (où λ décrit l'ensemble des racines (simples) de π dans K). La démonstration de la proposition 2 montre que la décomposition de Dunford sur K est donnée par

$$d = \sum_\lambda \lambda \pi_\lambda \qquad , \qquad n = u - d$$

Il s'agit de montrer que d et n (il est plus sage de les considérer comme matrices) sont à coefficients dans $\mathbf{k}$. Rappelons que les projections π_λ avaient été obtenues via le lemme des noyaux comme polynômes en u, en partant du théorème de Bézout. Plus précisément, si on écrit

$$1 = \sum_\lambda Q_\lambda(X) \prod_{\mu \neq \lambda} (X-\mu)^q \tag{5}$$

avec $Q_\lambda \in K[X]$, alors $\pi_\lambda = Q_\lambda(u) \prod_{\mu\neq\lambda}(u - \mu \operatorname{Id})^q$ et $d = Q(u)$, où

$$Q(X) = \sum_\lambda \lambda Q_\lambda(X) \prod_{\mu \neq \lambda} (X-\mu)^q \tag{6}$$

[4]Il lui est en fait égal par la remarque 1.(2).

Or les équations (5) et (6) s'écrivent aussi

$$\frac{1}{\pi(X)^q} = \sum_\lambda \frac{Q_\lambda(X)}{(X-\lambda)^q} \qquad , \qquad \frac{Q(X)}{\pi(X)^q} = \sum_\lambda \frac{\lambda Q_\lambda(X)}{(X-\lambda)^q}$$

Il s'agit de montrer que Q est à coefficients dans $\mathbf{k}$. Une façon de faire est d'introduire des indéterminées $Y_1, \dots, Y_r$ et d'ecrire une décomposition

$$\frac{1}{(X-Y_1)^q \cdots (X-Y_r)^q} = \sum_{i=1}^{r} \sum_{j=1}^{q} \frac{F_{i,j}(Y_1, \dots, Y_r)}{(X-Y_i)^j} \tag{7}$$

en éléments simples sur le corps $\mathbf{k}(Y_1, \dots, Y_r)$. Par unicité de cette décomposition, on a pour toute permutation σ de $\{1, \dots, r\}$

$$F_{i,j}(Y_{\sigma(1)}, \dots, Y_{\sigma(r)}) = F_{\sigma(i),j}(Y_1, \dots, Y_r)$$

Si on écrit

$$\sum_{i=1}^{r} \sum_{j=1}^{q} \frac{Y_i F_{i,j}(Y_1, \dots, Y_r)}{(X-Y_i)^j} = \frac{Q(X, Y_1, \dots, Y_r)}{\pi(X)^q}$$

avec $Q \in \mathbf{k}(Y_1, \dots, Y_r)[X]$, cela entraîne que Q est symétrique en $Y_1, \dots, Y_r$. En particulier, si on substitue les racines de π aux Y_i, on obtient que les coefficients de Q sont des fractions rationnelles en les coefficients de π : ils sont en particulier dans $\mathbf{k}$[5]. □

[5]Il vaut mieux vérifier que l'on n'obtient pas de dénominateur nul en faisant la substitution. On peut pour cela préciser la décomposition (7) : si on fait le changement de variables $X' = X - Y_1$ et la division *selon les puissances croissantes* en X' à l'ordre m du polynôme 1 par le polynôme $P = (X' - Y_2')^q \cdots (X' - Y_r')^q$, on obtient (par récurrence sur m)

$$1 = \frac{PA_m + X'^m B_m}{(Y_2' \cdots Y_r')^{mq}}$$

où A_m et B_m sont des polynômes en $X', Y_2', \dots, Y_r'$ à coefficients entiers, vérifiant $\deg_{X'} A_m < m$. On en déduit

$$\frac{1}{X'^q (X'-Y_2')^q \cdots (X'-Y_r')^q} = \frac{A_q(X', Y_2', \dots, Y_r')}{X'^q (Y_2' \cdots Y_r')^{q^2}} + \text{ termes sans pôle en } X' = 0$$

En substituant $X' = X - Y_1$ et $Y_k' = Y_k - Y_1$, on obtient

$$\frac{1}{\prod_{i=1}^r (X-Y_i)^q} = \sum_{i=1}^{r} \sum_{j=1}^{q} \frac{A_{q,j}(Y_1 - Y_i, \dots, Y_r - Y_i)}{(X-Y_i)^j \prod_{1 \le k \le r,\ k \ne i} (Y_k - Y_i)^{q^2}}$$

On voit ainsi que les $F_{i,j}$ de la preuve sont tels que $F_{i,j} \prod_{1 \le i < j \le r} (Y_i - Y_j)^{2q^2}$ est un polynôme (symétrique) en $Y_1, \dots, Y_r$. Il en est de même pour Q, donc on peut substituer les racines de π aux Y_i sans problème.

Références

[G] Gantmacher, F. R., *Théorie des matrices. Tome 1 : Théorie générale.* Traduit du russe par Ch. Sarthou. Collection Universitaire de Mathmatiques **18**, Dunod, Paris, 1966.

[J] Jacobson, N., *Basic algebra. I.* Deuxième édition. W. H. Freeman and Company, New York, 1985.

[N] Newman, M., *Integral matrices.* Pure and Applied Mathematics **45**. Academic Press, New York-London, 1972.

Olivier DEBARRE
Institut de Recherche Mathématique Avancée – UMR 7501
UFR de Mathématiques et Informatique
7 rue René Descartes
Université Louis Pasteur
67084 Strasbourg Cedex – France

e-mail : debarre@math.u-strasbg.fr