

# Corrigé du problème sur les facteurs invariants

## Partie I : Étude du groupe unimodulaire

1°) Il suffit de décomposer, pour  $\{i, j\} \in \{1, \dots, n\}^2$  :  $a_{i,j} = \sum_{k=0}^p b_{i,j,k} X^k$ , où  $p$  est le degré maximal des coefficients non nuls de  $A$ ; on obtient, en posant pour  $k \in \{1, \dots, p\}$   $B_k = (b_{i,j,k})_{1 \leq i, j \leq n}$  :  $A = B_0 + XB_1 + \dots + X^p B_p$  avec  $p = \delta(A)$ .

2°) Tout d'abord,  $I_n \in \mathcal{U}_n$ . Ensuite, le produit de deux matrices de déterminant  $\in U$  a cette même qualité, c'est immédiat par la multiplicativité du déterminant. Enfin, une matrice unimodulaire  $A$  ayant un déterminant non nul, elle est inversible dans  $\mathcal{M}_n(\mathbb{F})$ , et son inverse est  $\frac{1}{\det A} {}^t \text{com}(A)$ , qui appartient à  $\mathcal{A}_n$  puisque  $\frac{1}{\det A} \in R$  et les coefficients de  ${}^t \text{com}(A)$  également. D'où  $A^{-1} \in \mathcal{U}_n$ .

Ainsi,

$\mathcal{U}_n$  est un groupe pour la multiplication des matrices.

3°) Les matrices  $R$ -élémentaires ont un déterminant 1 (pour les transvections) ou dans  $U$  : elles sont donc bien unimodulaires. Il suffit de vérifier que leurs inverses sont  $R$ -élémentaires. Or :  $D_i(\lambda)^{-1} = D_i(\frac{1}{\lambda})$  et  $T_{ij}(\lambda) = T_{ij}(-\lambda)$ .

Donc

$\mathcal{R}_n$  est un sous-groupe de  $\mathcal{U}_n$ .

4°) a) Il s'agit d'une relation d'équivalence car  $\forall (A, B, C), (U_1, V_1, U_2, V_2) \in \mathcal{A}_n^3 \times \mathcal{R}_n^4$  :  $A = I_n A I_n$ ; si  $A = U_1 B V_1$ , alors  $B = U_1^{-1} A V_1^{-1}$ ; enfin si  $A = U_1 B V_1$  et  $B = U_2 C V_2$ , alors  $A = U_1 U_2 C V_1 V_2$ . Le fait que  $\mathcal{R}_n$  est un groupe (multiplicatif) permet de conclure.

b) D'après le cours (qu'il convient de réécrire ici), les lignes de  $T_{i,j}(a)A$  sont les mêmes que celles de  $A$ , sauf la  $i$ -ème, à laquelle on a ajouté  $a$  fois la  $j$ -ème. les lignes de  $T_{1,i}(-1)T_{i,1}(1)A$  sont alors les mêmes que celles de  $A$ , sauf la première qui vaut  $-L_i$  et la  $i$ -ème qui est  $L_i + L_1$ .

c) Soit  $A = (a_{i,j}) \in \mathcal{A}_n$ ; repérons parmi ses coefficients non nuls choisissons-en un,  $a_{i,j}$ , ayant le degré [resp. la valeur absolue] minimal (il n'est peut-être pas unique). Par des transpositions sur les lignes et colonnes on peut l'amener en première ligne et première colonne : en effet, si l'on fait sur les colonnes la même chose que sur les lignes, d'après la question précédente, la matrice  $T_{1,i}(1)T_{i,1}(-1)AT_{1,j}(-1)T_{j,1}(1)$  admet en place  $(1, 1)$  le coefficient  $a_{i,j}$ . Dans le cas particulier où l'on a  $i = 1$  (ou  $j = 1$ ), deux de ces transvections disparaissent et le coefficient obtenu est  $-a_{i,j}$  qui convient aussi bien.

d) Si, par les transvections précédentes, on a fait apparaître un coefficient non nul dans  $A'$  dont le degré [resp. la valeur absolue] est  $<$  à celui de  $a'_{1,1}$ , on réapplique le procédé de la question précédente pour l'amener en première ligne, première colonne. Ce processus s'arrête nécessairement après un nombre fini d'itérations (puisque  $\delta \in \mathbb{N}$  diminue strictement à chaque itération) : on aboutit à une matrice  $B = (\beta_{i,j})$ ,  $R$ -équivalente à  $A$  et telle que le coefficient  $\beta_{1,1}$  soit non nul et vérifie  $\beta_{1,1} = \delta(B)$ .

Pour  $1 < k \leq n$ , soit  $q_k$  le quotient et  $r_k$  le reste de la division euclidienne de  $\beta_{k,1}$  par  $\beta_{1,1}$  :  $\beta_{k,1} = q_k \beta_{1,1} + r_k$ . La transvection à gauche  $T_{k,1}(-q_k)$  fait apparaître en  $k$ -ème ligne et première colonne  $r_k$ , qui est nul ou de degré [resp. valeur absolue] strictement inférieur à  $\delta(B)$ . Dans le second cas, on réapplique la question précédente pour obtenir un coefficient en haut à gauche de degré [resp. valeur absolue] strictement plus petit que  $\delta(B)$ .

Ce processus, appliqué pour tous les coefficients de la première ligne et pareillement pour ceux de la première colonne, va s'arrêter après un nombre fini d'itérations (puisque  $\delta$  ne saurait diminuer indéfiniment). A ce moment, toutes les divisions nécessaires vont donner un reste nul et on aboutira à une matrice  $A'' = (a''_{ij})$ , telle que  $a''_{k1} = a''_{1k} = 0$  pour tout  $k > 1$ .

e) Soit, s'il existe, un coefficient non nul  $a''_{k,l}$  avec  $k$  et  $l \geq 2$ . Une transvection  $T_{k,1}(1)$  à gauche amène en première colonne, sur la ligne  $k$ , le coefficient  $a''_{1,1}$  et ne change rien d'autre. Une transvection à droite  $T_{1,l}(p)$  change alors  $a''_{k,l}$  en  $a''_{k,l} - p a''_{1,1}$ . Prenant pour  $p$  le quotient de la division euclidienne de  $a''_{k,l}$  par  $a''_{1,1}$ , on va trouver un coefficient nul ou de degré [resp. valeur absolue]  $< \delta(A'')$ .

Dans le second cas, on répète les étapes antérieures jusqu'à ce que (après un nombre fini d'itérations,  $\delta \in \mathbb{N}$  diminuant strictement à chaque étape...) le coefficient d'indice  $(1, 1)$  divise tous les autres.

Finalement,  $A$  est bien  $R$ -équivalente à une matrice  $A_1 = (\alpha_{i,j})$ , telle que  $\alpha_{k,1} = \alpha_{1,k} = 0$  pour tout  $k > 1$ , et que  $\alpha_{1,1}$  divise tous les  $\alpha_{ij}$  non nuls.

(Il est à noter qu'on ne fait ici que des transvections.)

### 5°) Forme normale de Hermite..

Prouvons le résultat par récurrence. Pour  $n = 1$  il n'y a rien à faire. Admettons que la forme réduite proposée ait lieu en dimension  $n - 1$ . Soit  $A \in \mathcal{A}_n$ . Appliquant la question précédente, on trouve une matrice  $A_1$   $R$ -équivalente à  $A$  et de la forme  $\begin{pmatrix} e_1 & 0 \\ 0 & A_2 \end{pmatrix}$ , et  $A_2 \in \mathcal{A}_{n-1}$ . Une dilatation permet de rendre  $e_1$  unitaire [resp.  $> 0$ ], ce que nous supposons.

On peut appliquer l'hypothèse de récurrence à  $A_2$ . Si  $A_2$  est nulle, l'algorithme est terminé. Sinon, comme  $e_1$  divise tous les coefficients de  $A_2$ , il garde cette propriété à chaque étape (car on effectue uniquement des transvections, ainsi que des dilatations de rapport  $\in \mathcal{U}$ , qui conservent la divisibilité des coefficients par  $e_1$ ); donc toute matrice  $R$ -équivalente à  $A_2$  a ses coefficients divisibles par  $e_1$ .

On en déduit immédiatement une matrice  $R$ -équivalente de la forme  $S = \begin{pmatrix} e_1 & & & 0 \\ & e_2 & & \\ & & \ddots & \\ 0 & & & e_n \end{pmatrix}$  avec  $e_1|e_2|e_3|\dots|e_{r-1}|e_r|e_j =$

0 pour  $r < j \leq n$  et les  $e_i$  étant unitaires *resp.*  $> 0$ ].

D'autre part, la  $R$ -équivalence entraîne aussi la  $F$ -équivalence, de sorte que  $r$  est le rang de  $A$  en tant que matrice à coefficients dans  $F$ . On n'a  $r = 0$  que si  $A$  est nulle, et  $r = n$  si et seulement si  $A$  est inversible dans  $\mathcal{M}_n(F)$ .

6°) Nous savons déjà que  $\mathcal{R}_n \subset \mathcal{U}_n$ . Prenons une matrice unimodulaire  $A$ . Elle sera  $R$ -équivalente à une matrice  $S$ . On a donc  $A = USV$  et  $\det A = \det U \det S \det V$ . Mais  $\det A \in \mathcal{U}$ , donc  $\det S$  aussi. Comme c'est le produit des termes diagonaux de  $S$ , ceux-ci sont tous dans  $\mathcal{U}$  (dans le cas général d'un anneau euclidien, écrire, si  $s = s_1 \dots s_n \in \mathcal{U}^t: s_1(s_2 \dots s_n s^{-1}) = 1_R$ , ce qui prouve que  $s_1 \in \mathcal{U}$  ainsi que  $s_2 \dots s_n = s_1^{-1}s$ , et ainsi de suite de proche en proche). Ce sont donc des polynômes constants unitaires [*resp. des éléments de*  $\{-1, 1\} > 0$ ], c'est-à-dire 1. Alors  $S = I_n$  et  $A = UV$  appartient à  $\mathcal{R}_n$ .

Finalement, on voit que

les matrices unimodulaires sont les produits de dilatations et transvections, soit  $\mathcal{R}_n = \mathcal{U}_n$ .

7°) a)

Cherchons  $S$  pour  $A = \begin{pmatrix} -10 - X & -4 \\ 26 & 11 - X \end{pmatrix}$ . On peut ramener le coefficient  $-4$  à 1 par dilatation, ou aussi bien multiplier une ligne par 4 (plus simple):  $A \sim \begin{pmatrix} X + 10 & 4 \\ 104 & 44 - 4X \end{pmatrix}$ . Une transvection de coefficient  $X - 11$  sur les lignes amène:  $A \sim \begin{pmatrix} X + 10 & 4 \\ 104 + (X - 11)(X + 10) & 0 \end{pmatrix} = \begin{pmatrix} X + 10 & 4 \\ X^2 - X - 6 & 0 \end{pmatrix}$ . Une certaine transvection sur les colonnes va alors annuler le  $X + 10$ ; une permutation et une dilatation donnent:  $A \sim \begin{pmatrix} 1 & 0 \\ 0 & X^2 - X - 6 \end{pmatrix}$ . ♦

Soit  $A = \begin{pmatrix} 1 - X & 1 & 0 \\ -1 & 2 - X & 1 \\ 3 & -6 & 6 - X \end{pmatrix}$ . On procède de même, repérant un coefficient égal à 1 en première ligne; par

transvection de colonnes on se ramène à  $A \sim \begin{pmatrix} 0 & 1 & 0 \\ -X^2 + 3X - 3 & 2 - X & 1 \\ 9 - 6X & -6 & 6 - X \end{pmatrix}$ . Des transvections de lignes amènent

aussitôt  $A \sim \begin{pmatrix} 0 & 1 & 0 \\ -X^2 + 3X - 3 & 0 & 1 \\ 9 - 6X & 0 & 6 - X \end{pmatrix}$ . Il reste à combiner les deux dernières lignes, puis la troisième colonne avec la première, dilater et permuter:

$$A \sim \begin{pmatrix} 0 & 1 & 0 \\ -X^2 + 3X - 3 & 0 & 1 \\ 9 - 6X + (X - 6)(-X^2 + 3X - 3) & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -(X - 3)^3 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & (X - 3)^3 \end{pmatrix}$$

On a de même pour  $A = \begin{pmatrix} X^3 - X & 2X^2 \\ X^2 + 5X & 3X \end{pmatrix}$ :

$$A \sim \begin{pmatrix} 3X^3 - 3X & 6X^2 \\ X^2 + 5X & 3X \end{pmatrix} \sim \begin{pmatrix} X^3 - 3X - 10X^2 & 0 \\ X^2 + 5X & 3X \end{pmatrix} \sim \begin{pmatrix} X^3 - 10X^2 - 3X & 0 \\ X^2 + 5X & X \end{pmatrix} \sim \begin{pmatrix} X & 0 \\ 0 & X^3 - 10X^2 - 3X \end{pmatrix}.$$

8°) Les  $T_{i,j(a)}$ ,  $a \in \mathbb{Z}$  sont dans  $SL_n(\mathbb{Z})$  (car de déterminant 1); réciproquement, soit  $A \in SL_n(\mathbb{Z})$ : l'algorithme mis en place à la question 4. ne fait intervenir que des transvections, et en renonçant aux dilatations de rapport  $-1$  et appliquant la question 5., on aboutit par transvections à droite et gauche à une matrice  $S$  où les  $e_i$  valent 1 ou  $-1$ .

Cependant les transvections ne modifient pas le déterminant: comme celui de  $A$  vaut 1, les indices  $i \in \{1, \dots, n\}$  tels que  $e_i = -1$  sont en nombre pair; si par exemple  $e_1 = e_2 = -1$ , on multiplie à gauche par  $T_{2,1}(-2)$ , puis par  $T_{1,2}(1)$ , ensuite par  $T_{2,1}(-2)$ , enfin on multiplie à droite par  $T_{1,2}(1)$  (ce qui donne les matrices 2 - 2 successives  $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ ,  $\begin{pmatrix} -1 & 0 \\ 2 & -1 \end{pmatrix}$ ,

$$\begin{pmatrix} 1 & -1 \\ 2 & -1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Ainsi, par produit à droite et à gauche par des transvections, on aboutit à  $I_n$ , ce qui montre de même qu'au 6. que  $A$  est produit de matrices de transvections:

$SL_n(\mathbb{Z})$  est engendré par les transvections.

## Partie II: Unicité de la forme réduite de Hermite

1°) Si  $A$  et  $B$  sont  $R$ -équivalentes, avec  $A = UBV$ , alors le passage de  $B$  à  $UB$  se fait par transvections et dilatations, donc il suffit de considérer ces deux opérations isolément. La dilatation va éventuellement multiplier certains déterminants par un polynôme constant non nul [*resp.*  $-1$ ], ce qui n'altère pas le pgcd. En ce qui concerne la transvection, comme elle opère par combinaisons linéaires, la plupart des  $k$ -mineurs restent inchangés.

Il y a cependant une exception, qui survient lorsqu'on combine la ligne  $i$  et la ligne  $j$  sur la ligne  $i$ , et que le  $k$ -mineur contient la ligne  $i$  et non la ligne  $j$ . La multilinéarité du déterminant assure alors qu'un tel  $k$ -mineur de  $UB$  est combinaison de deux

mineurs de  $B$ , donc est multiple du pgcd de ceux-ci. En conséquence, on a bien  $\Delta_k(B)|\Delta_k(UB)$ . Comme les matrices  $R$ -élémentaires ont des inverses  $R$ -élémentaires, on a aussi  $\Delta_k(UB)|\Delta_k(B)$  d'où  $\Delta_k(B) = \Delta_k(UB)$  puisque ce sont des polynômes unitaires [resp. des nombres  $> 0$ ]. On montre pareillement que  $\Delta_k(B) = \Delta_k(UBV)$ . ♦

En conséquence,

les  $\Delta_k$  sont des invariants par  $R$ -équivalence des matrices.

2°) Soit une matrice  $S = \begin{pmatrix} e_1 & & & 0 \\ & e_2 & & \\ & & \ddots & \\ 0 & & & e_n \end{pmatrix}$  avec  $e_1|e_2, e_2|e_3, \dots, e_{r-1}|e_r, e_j = 0$  pour  $r < j \leq n$ . Les  $k$ -mineurs non nuls de cette matrice ne peuvent se faire qu'avec les mêmes numéros de lignes et de colonnes, car il nous faut au moins un coefficient non nul par ligne et par colonne. Et de ces mineurs le premier (en haut à gauche) divise tous les autres, valant  $\prod_{i=1}^k e_i$ . C'est donc  $\Delta_k$ . Bien entendu, pour  $k > r$  on a  $\Delta_k = 0$ .

Finalement :

$$\Delta_k = \prod_{i=1}^k e_i \text{ pour } k \leq r, 0 \text{ sinon.}$$

### 3°) Les facteurs invariants..

On en déduit aussitôt la valeur des  $e_k$  par :  $e_k = \frac{\Delta_k}{\Delta_{k-1}}$  en posant  $\Delta_0 = 1$ , tant que  $\Delta_{k-1} \neq 0$ . Le rang étant conservé par opérations élémentaires (rappelons qu'il s'agit d'un rang sur le corps  $F$ ), la valeur de  $r$  est bien déterminée. Comme les  $\Delta_k$  sont invariants par  $R$ -équivalence, il en est de même des  $e_k$  qui sont donc parfaitement déterminés par la classe de  $R$ -équivalence de  $A$  et ne dépendent pas de  $P$  et  $Q$  telles que  $A = PSQ$ . ♦

## Partie III : Application aux invariants de similitude.

Dans cette partie on considère un  $K$ -espace vectoriel  $E$ , de dimension  $n$ , et un endomorphisme  $u \in \mathcal{L}(E)$ , ayant une matrice  $A \in \mathcal{M}_n(\mathbb{K})$  dans une base de référence  $(\varepsilon_1, \dots, \varepsilon_n)$ . On examine la matrice  $\hat{A} = XI - A \in \mathcal{A}_n$ .

1°) Soit  $\hat{A} = PSQ$  la réduction de Hermite de  $\hat{A}$ . La matrice  $\hat{A}$  est inversible car son déterminant est le polynôme caractéristique de  $A$  au signe près, donc un polynôme de degré  $n$ , non nul. Son rang (dans  $\mathcal{M}_n(\mathbb{K}(X))$ ) est donc égal à  $n$ , donc c'est le rang de  $S$ . Donc  $r = n$ .

A cause du cas éventuel où certains facteurs invariants seraient égaux à 1 on change de numérotation en posant :  $(e_1, e_2, \dots, e_n) = (1, 1, \dots, 1, d_1, \dots, d_s)$ . ♦

2°) Soit une famille  $(v_1, \dots, v_p)$  de vecteurs de  $E$  et une matrice  $B = (B_{ij}) \in \mathcal{A}_n$ . On appelle *image de  $(v_i)$  par  $B$*  la famille de vecteurs  $(v_j^B)$  définie par  $v_j^B = \sum_{i=1}^p B_{ij}(u)(v_i)$ . Soient  $B$  et  $C$  appartenant à  $\mathcal{A}_n$ . On a

$$(v_j^B)^C = \sum_{l=1}^p C_{lj}(u) \sum_{i=1}^p B_{il}(u)(v_i) = \sum_{l=1}^p \sum_{i=1}^p C_{lj}(u) B_{il}(u)(v_i)$$

mais on se souvient que les polynômes agissent sur l'algèbre des endomorphismes, en commutant entre eux, donc

$$(v_j^B)^C = \sum_{i=1}^p \sum_{l=1}^p B_{il} C_{lj}(u)(v_i) = \sum_{i=1}^p \left( \sum_{l=1}^p B_{il} C_{lj} \right) (u)(v_i) = \sum_{i=1}^p BC_{ij}(u)(v_i) = v_j^{(BC)}$$

3°) Nous dirons qu'une famille  $(v_1, \dots, v_p)$  de  $p$  vecteurs de  $E$  (avec  $p \leq n$ ) est  $u$ -génératrice si la famille de vecteurs  $(u^q(v_i))_{\substack{i \leq p \\ q \in \mathbb{N}}}$  est génératrice de  $E$ . Si  $B$  appartient à  $\mathcal{U}_n$  et que  $(v_i)$  est  $u$ -génératrice, alors la famille  $(v_i^B)$  est constituée de combinaisons linéaires des vecteurs initiaux, donc s'inscrit dans le sous-espace vectoriel engendré. Lorsqu'on applique les puissances de  $u$ , on décrit a priori un sous-espace plus restreint à partir des  $(v_i^B)$ . Soit :  $\text{Vect}(u^q(v_i^B)) \subset \text{Vect}(u^q(v_i))$ . Mais on a aussi  $(v_j^B)^{B^{-1}} = v_j^{B B^{-1}} = v_j$ . Il en résulte, par le même raisonnement, que  $\text{Vect}(u^q(v_i)) \subset \text{Vect}(u^q(v_i^B))$ , d'où égalité. ♦

4°) Cette question est facile mais délicate. En effet, on ne peut pas remplacer directement  $X$  par  $u$  et obtenir  $A - A = 0$ . Il faut procéder plus attentivement, en écrivant :  $(XI - A)_{jj}(u) = u - a_{jj} \text{id}$  et pour  $i \neq j$  :  $(XI - A)_{ij}(u) = 0 - a_{ij} \text{id}$  d'où

$$\sum_{i=1}^n \hat{A}_{ij}(u)(\varepsilon_i) = u(\varepsilon_j) - a_{jj} \varepsilon_j - \sum_{i \neq j} a_{ij} \varepsilon_i = u(\varepsilon_j) - \sum_i a_{ij} \varepsilon_i = 0$$

ce qui montre que  $(\varepsilon_j^{\hat{A}}) = (0, \dots, 0)$ . ♦

5°) a) Considérons à nouveau  $\hat{A} = PSQ$ . La base  $(\varepsilon_1, \dots, \varepsilon_n)$  est génératrice donc  $u$ -génératrice. Soit  $v_i = \varepsilon_i^P$ . D'après la question 2b cette famille de vecteurs est encore  $u$ -génératrice. De plus,  $v_i^S = (\varepsilon_i^P)^S = \varepsilon_i^{\hat{A}Q^{-1}} = (\varepsilon_i^{\hat{A}})^{Q^{-1}} = 0$  d'après la question précédente.

Soit  $m$  le nombre de vecteurs non nuls de cette famille ; on peut renuméroter les  $v_i$  pour mettre en tête ceux qui sont non nuls, et noter  $v_1, \dots, v_m$  les vecteurs non nuls de cette famille, les suivants étant nuls. ♦

b) Examinons concrètement l'action de  $S$  sur les  $v_i$ . On a  $0 = v_j^S = \sum_{i=1}^p S_{ij}(u)(v_i) = S_{jj}(u)(v_j) = v_j$  lorsque  $d_j = 1$ , et  $0 = v_j^S = d_j(u)(v_j)$  lorsque  $d_j \neq 1$ . Ainsi,  $v_j \neq 0$  entraîne  $d_j \neq 1$ . Comme il y a exactement  $s$  facteurs invariants  $d_j$  différents de 1, le nombre  $m$  de vecteurs non nuls vérifie  $m \leq s$ .

De plus, comme chaque  $d_j$  divise  $d_s$ , on a pour tout  $j$   $d_s(u)(v_j) = 0$ , d'où  $d_s(u)(u^q(v_j)) = 0$  par commutation des polynômes d'endomorphismes. Comme la famille  $(v_i)$  est  $u$ -génératrice, l'endomorphisme  $d_s(u)$  est nul. C'est dire que  $d_s$  est un multiple du polynôme minimal de  $u$ . ♦

6°) Soit alors  $n_i$  le degré du polynôme  $d_i$ . Notons d'abord que  $\prod_{i=1}^s d_i(x) = \Delta_n(X) = \det(XI - A)$  - c'est le *polynôme caractéristique* de  $A$ . Donc, en prenant le degré, il vient  $\sum_{i=1}^s n_i = n$ . Considérons alors la famille de vecteurs  $(u^j(v_i)) / 1 \leq i \leq s, 0 \leq j \leq n_i - 1$ ; le nombre de vecteurs de cette famille est exactement  $n$  d'après ce qu'on vient de voir. Pour que cette famille soit une base, il suffit de montrer qu'elle est génératrice. Or, la famille  $(v_i)$  était  $u$ -génératrice, ce qui signifie que la famille de vecteurs  $((u^j(v_i)) / 1 \leq i \leq s, j \in \mathbb{N})$  est génératrice. Si  $j \geq n_i$  alors on peut diviser  $X^j$  par  $d_i$ :  $X^j = qd_i + r$  avec  $\deg r < n_i$ . Alors

$$u^j(v_i) = q(u)d_i(u)(v_i) + r(u)(v_i) = r(u)(v_i) \in \text{Vect}(u^j(v_i) / 0 \leq j \leq n_i - 1)$$

ce qui prouve le caractère générateur. Il en résulte aussi qu'aucun de ces vecteurs n'est nul, donc que les  $v_i$  sont non nuls pour  $1 \leq i \leq s$ , donc  $m = s$ .

Dans cette base, la plupart des vecteurs ont pour image le vecteur suivant, sauf pour ceux qui sont en fin de liste ( $j = n_i - 1$ ) dont l'image est une combinaison des  $u^j(v_i)$  pour  $j \leq n_i - 1$ . On a donc une matrice diagonale par blocs  $\text{Diag}(\lambda_1, \dots, \lambda_p, D_1, \dots, D_s)$ , où les  $\lambda_i$  sont ce qu'on appellera bientôt des *valeurs propres* de  $u$  (correspondant aux facteurs

invariants égaux à 1), et les  $D_i$  sont des matrices dites *de Frobenius*: 
$$\begin{pmatrix} 0 & \cdots & a_1 \\ 1 & & \vdots \\ \vdots & \ddots & 0 \\ 0 & & 1 & a_{n_i} \end{pmatrix}$$
. Les coefficients  $a_k$  qui apparaissent

dans la dernière colonne de ce bloc sont les opposés des coefficients non dominants du polynôme  $d_i$ . La matrice réduite ainsi obtenue ne dépend que des  $d_i$ , elle a donc un caractère d'unicité. ♦

On note, au passage, que les  $n_i$  forment une suite croissante puisque les  $d_i$  se divisent « en chaîne »; par conséquent, les tailles des blocs successifs augmentent.

7°) En particulier, la famille  $(v_s, u(v_s), \dots, u^{n_s-1}(v_s))$  est libre, donc aucun polynôme annulateur ne peut avoir de degré inférieur à  $n_s$  (il établirait une relation de dépendance entre ces vecteurs). Dès lors,

$$\boxed{d_s \text{ est le polynôme minimal de } u \text{ et } \Delta_n = \Delta_s \text{ est le polynôme caractéristique de } u.}$$

8°) Soient  $A$  et  $B$  deux matrices de  $\mathcal{M}_n(\mathbb{K})$ . La  $R$ -équivalence de  $\hat{A} = XI - A$  et de  $\hat{B} = XI - B$  signifie qu'elles ont mêmes polynômes  $d_i$ , donc que les endomorphismes associés  $u$  et  $v$  ont la même matrice réduite dans une base telle qu'indiquée à la question 4, c'est-à-dire que  $u$  et  $v$  sont conjugués, ou que  $A$  et  $B$  sont semblables. ♦

## Partie IV : Applications

1°) **Première application..**

Les matrices  $A = \begin{pmatrix} 1 & 1 & 0 \\ -1 & 2 & 1 \\ 3 & -6 & 6 \end{pmatrix}$  et  $B = \begin{pmatrix} 1 & 1 & 0 \\ -4 & 5 & 0 \\ -6 & 3 & 3 \end{pmatrix}$  ne sont pas semblables. En effet, on trouve que les formes normales

de Hermite de  $\hat{A} = XI - A$  et de  $\hat{B} = XI - B$  sont respectivement  $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & (X-3)^3 \end{pmatrix}$  et  $\begin{pmatrix} 1 & 0 & 0 \\ 0 & (X-3) & 0 \\ 0 & 0 & (X-3)^2 \end{pmatrix}$ . v

2°) **Seconde application..**

$$\boxed{\text{Toute matrice est semblable à sa transposée,}}$$

car  $XI - A = PSQ$  avec  $S$  diagonale, donc  $XI - {}^tA = {}^tQS^tP$  car  $S$  est diagonale. Et  $XI - A$  a mêmes facteurs invariants que  $XI - {}^tA$ ; on applique enfin la question III.6. ♦

3°) **Troisième application..**

Soient deux matrices  $A$  et  $B$  appartenant à  $\mathcal{M}_n(\mathbb{L})$ ,  $\mathbb{L}$  étant un sous-corps de  $K$ . On suppose qu'elles sont semblables dans  $K$ . Les matrices  $XI - A$  et  $XI - B$  sont donc  $K[X]$ -équivalentes, pourvues des mêmes facteurs invariants. Or, ces facteurs invariants se calculent à partir des pgcd des coefficients de ces deux matrices, et appartiennent donc à  $\mathbb{L}[X]$ . Ainsi,  $XI - A$  et  $XI - B$  sont  $\mathbb{L}[X]$ -équivalentes, ce qui nous assure que  $A$  et  $B$  sont semblables dans  $\mathbb{L}$ . ♦

4°) **Quatrième application..**

Ici, les polynômes  $d_i$  sont de la forme  $X^{n_i}$  (puisque le polynôme minimal divise  $X^n$ , qui annule  $u$ ), donc la matrice obtenue est triangulaire inférieure, à coefficients tous nuls sauf ceux situés immédiatement en-dessous de la diagonale, qui valent 0 ou 1: c'est la *réduction de Jordan* d'un endomorphisme nilpotent.

**5°) Cinquième application.**

Si  $M$  est semblable à  $2M$ , la seule valeur propre (sur  $\mathbb{C}$ ) de  $M$  est 0 : le polynôme caractéristique de  $M$  est  $X^n$  et d'après le théorème de Cayley-Hamilton  $M$  est nilpotente ; réciproquement, si elle est nilpotente, un exemple vu en cours montre que chaque bloc de Jordan  $J_m$  (triangulaire avec des coefficients tous nuls sauf ceux situés strictement au-dessus (resp. en dessous] de la diagonale, qui valent 1) est semblable à  $2J_m$  : la question précédente assure que  $M$  est semblable (sur  $\mathbb{C}$ , donc aussi sur  $K$ ) à une matrice diagonale par blocs, avec des blocs de Jordan sur la diagonale ;  $M$  est ainsi semblable à  $2M$ .