Décomposition de Frobenius

E désigne un espace vectoriel de dimension finie n sur un corps K.
Un endomorphisme u de E est dit cyclique s'il existe $a \in E$ tel que $(a, u(a), ..., u^{n-1}(a))$ forme une base de E (on dira dans ce cas que a est adapté à u).
Étant donné un endomorphisme u de E, on appelle commutant de u : $\mathcal{C}(u) = \{v \in L(E) | uv = vu\}$.
On rappelle qu'un endomorphisme u est une transvection de E s'il existe une forme linéaire non nulle $\phi \in E^*$, un vecteur $a \in E$ vérifiant $\phi(a) = 0$, tels que, pour tout x, $u(x) = x + \phi(x)a$. Et qu'une dilatation de rapport $\lambda \in K^*$ est un endomorphisme de la forme $u(x) = x + (\lambda - 1)\phi(x)b$, où ϕ est une forme linéaire non nulle, b un vecteur vérifiant $\phi(b) = 1$.
On note $\Omega_{i,j}$ la matrice de $M_n(K)$ dont tous les coefficients sont nuls sauf le coefficient d'indice (i, j) qui vaut 1.
Pour tout $\mu \in K$, $(i, j) \in {\mathbb{N}_n}^2$, $i \neq j$, on pose $T_{i,j}(\mu) = I_n + \mu\Omega_{i,j}$.
Pour tout $\lambda \in K^*$, $i \in \mathbb{N}_n$, on pose $D_i(\lambda) = I + (\lambda - 1)\Omega_{i,i}$.
Soit $u \in L(E)$. On rappelle que si $Q \in K[X]$, $Q = \gamma_0 + \gamma_1 X + ... + \gamma_r X^r$, alors $Q(u)$ vaut, par définition, $Q(u) = \gamma_0 id_E + \gamma_1 u + ... + \gamma_r u^r$ ($u^k = u \circ u \circ ... \circ u$).
Une matrice $A \in M_p(K)$ est dite matrice compagnon si elle est de la forme :

$$\begin{pmatrix} 0 & 0 & ... & 0 & \alpha_0 \\ 1 & 0 & ... & 0 & \alpha_1 \\ 0 & 1 & ... & 0 & \alpha_2 \\ ... & & & & \\ 0 & 0 & ... & 1 & \alpha_{p-1} \end{pmatrix}$$

On définit le polynôme P_A associé à A par $P_A = X^p - (\alpha_0 + \alpha_1 X + ... + \alpha_{p-1} X^{p-1})$.

Première partie

Soit u un endomorphisme non nul de E. On pose $\mathcal{P}(u) = \{Q(u) | Q \in K[X]\}$.

1. Montrer que $\mathcal{C}(u)$ est une sous-algèbre unitaire de $L(E)$, que $\mathcal{P}(u)$ est la plus petite sous-algèbre unitaire de $L(E)$ qui contienne u.
2. On suppose u cyclique. Soit $a \in E$ adapté à u, et $\mathcal{B}$ la base $(a, u(a), ..., u^{n-1}(a))$.
   On pose $u^n(a) = \alpha_0 a + \alpha_1 u(a) + ... + \alpha_{n-1} u^{n-1}(a)$.
   (a) Écrire la matrice A de u dans la base $\mathcal{B}$.
   (b) Soit $v \in \mathcal{C}(u)$. On écrit $v(a)$ dans la base $\mathcal{B}$: $v(a) = \beta_0 a + \beta_1 u(a) + ... + \beta_{n-1} u^{n-1}(a)$. On pose ensuite $w = \beta_0 id_E + \beta_1 u + ... + \beta_{n-1} u^{n-1}$. Établir l'égalité $v = w$.
   (c) Montrer $\mathcal{P}(u) = \mathcal{C}(u)$
3. Montrer que $P_A(u) = 0$, et que $\forall Q \in K_{n-1}[X],\ Q(u) = 0 \Rightarrow Q = 0$. Quelle est la dimension de $\mathcal{C}(u)$?

Seconde partie

L'objectif de cette partie est de prouver que toute matrice de $M_n(K)$ est semblable à une matrice diagonale par blocs dont chaque bloc diagonal est une matrice compagnon.
Soit $u \in L(E)$, non nul. Un sous-espace F de E est dit u-cyclique (ou simplement cyclique) si F est stable par u et si u induit sur F un endomorphisme cyclique.

1. Montrer l'existence d'un sous-espace cyclique non réduit à 0.

On choisit un tel sous-espace F, de dimension maximale p (parmi les sous-espaces cycliques de E).

2. On considère une base $(e_1, ..., e_p)$ de F, vérifiant $e_{k+1} = u(e_k)$ $(1 \leqslant k \leqslant p-1)$. Soit $(f_1, ..., f_q)$ une famille de vecteurs qui la complète en une base de E $(q = n - p)$. On note C la matrice de l'application induite par u sur F dans la base $(e_1, ..., e_p)$. Que dire de C ? Décrire la matrice A de u dans la base $(e_1, ..., e_p, f_1, ..., f_q)$.
3. On pose, pour toute $B \in M_n(K)$, $\tau^{\mu}_{(i,j)}(B) = T_{(i,j)}(-\mu)BT_{(i,j)}(\mu)$ $(i \neq j,\ \mu \in K)$. Décrire l'application $\tau^{\mu}_{(i,j)}$ en termes d'opérations élémentaires sur les lignes et les colonnes.
4. Montrer l'existence d'une famille $(g_1, g_2, ..., g_q)$ telle que $(e_1, ..., e_p, g_1, g_2, ..., g_q)$ forme une base de E et que, dans cette base, la matrice de u soit de la forme :

$$\left(\begin{array}{ccccc|cccc} & & & & & \beta_1 & \beta_2 & ... & \beta_q \\ & & & & & 0 & 0 & ... & 0 \\ & & C & & & 0 & 0 & ... & 0 \\ & & & & & \vdots & & & \vdots \\ & & & & & 0 & 0 & ... & 0 \\ \hline .... & .... & .... & .... & .... & .... & .... & .... & .... \\ 0 & & ... & & 0 & \gamma_{1,1} & \gamma_{1,2} & \cdots & \gamma_{1,q} \\ 0 & & ... & & 0 & \gamma_{2,1} & \gamma_{2,2} & \cdots & \gamma_{2,q} \\ \vdots & & & & \vdots & \vdots & & & \vdots \\ 0 & & ... & & 0 & \gamma_{q,1} & \gamma_{q,2} & \cdots & \gamma_{q,q} \end{array}\right)$$

Indication : utiliser des transformations du type τ, ainsi que les colonnes de la sous-matrice compagnon, pour "annuler" les coefficients $A_{p,p+1}$, $A_{p,p+2}$, ..., $A_{p,n}$, puis $A_{p-1,p+1}$, ..., $A_{p-1,n}$, etc.

5. Soit $k \in \{1, ..., q\}$. On suppose $\beta_k \neq 0$. Montrer que $(g_k, u(g_k), ..., u^p(g_k))$ est une famille libre. En déduire $\beta_k = 0$.
6. Prouver l'existence d'un supplémentaire G de F, stable par u.
7. Établir l'existence d'une base de E dans laquelle la matrice de u est une matrice diagonale par blocs dont chaque bloc diagonal est une matrice compagnon.
8. Conclure.

Corrigé

Première partie

1. Clair (ou cours).
2. (a) Puisque $(a, u(a), \dots, u^{n-1}(a))$ est une base de E, il existe $\alpha_0, \alpha_1, \dots, \alpha_{n-1}$ tels que
$$u^n(a) = \alpha_0 a + \alpha_1 u(a) + \dots + \alpha_{n-1} u^{n-1}(a)$$
Il est clair que la matrice de u dans cette base est la matrice compagnon C (de format $n \times n$).

   (b) On a, pour tout $k \in [\![, 0, n-1]\!]$, $w(u^k(a)) = \beta_0 u^k(a) + \beta_1 u(u^k(a)) + ... + \beta_{n-1} u^{n-1}(u^k(a)) = u^k(\beta_0 a + \beta_1 u(a) + ... + \beta_{n-1} u^{n-1}(a)) = u^k(v(a)) = v(u^k(a))$ (car u et v commutent). Ainsi, w et v coïncident sur une base de E d'où $w = v$.

   (c) $\mathcal{P}(u) \subset \mathcal{C}(u)$ est immédiat, et on vient de prouver l'inclusion réciproque.
3. On a, vu la relation $u^n(a) = \alpha_0 a + \alpha_1 u(a) + \dots + \alpha_{n-1} u^{n-1}(a)$, $P_A(u)(a) = 0$ donc, pour tout $k \in \mathbb{N}$, $P_A(u)(u^k(a)) = u^k(P_A(u)(a)) = 0$ et, par conséquent, $P_A(u) = 0$. P_A est donc un polynôme annulateur de u. C'est en fait le polynôme minimal de u car, vu la liberté de $(a, u(a), \dots, u^{n-1}(a))$, $(e, u, \dots, u^{n-1})$ est libre (ce qui montre bien $\forall Q \in K_{n-1}[X],\ Q(u) = 0 \Rightarrow Q = 0$). Ainsi $\mathcal{C}(u) = \mathcal{P}(u) = \text{Vect}(e, u, \dots, u^{n-1})$ est de dimension n.

Seconde partie

1. Soit $a \in E \setminus \{0\}$, et k le plus petit entier tel que $u^k(a) \in \text{Vect}(a, u(a), \dots, u^{k-1}(a))$. Alors $F = \text{Vect}(a, u(a), \dots, u^{k-1}(a))$ est un sous-espace stable par u. On vérifie aisément que $(a, u(a), \dots, u^{k-1}(a))$ est libre, c'est une base de F, qui est donc u-cyclique.
2. F est stable par u, et u induit sur cet espace un endomorphisme cyclique auquel la base $(e_1, e_2, \dots, e_p)$ est adaptée. Donc A va être de la forme $\left(\begin{array}{c|c} C & B \\ .... & .... \\ 0 & D \end{array}\right)$, où $C \in M_p(K)$ est une matrice compagnon, $B \in M_{p,q}(K)$, $D \in M_q(K)$.
3. Calculer $\tau_{i,j}^{\mu}(B)$ revient à appliquer à B successivement les opérations $C_j \leftarrow C_j + \mu C_i$ et $L_i \leftarrow L_i - \mu L_j$. Notons que ces deux opérations commutent (car multiplier à droite par $T_{i,j}(\mu)$ puis à gauche par $T_{i,j}(-\mu)$ sont deux opérations qui commutent !). Il est essentiel de noter que, puisque $T_{i,j}(-\mu) = T_{i,j}(\mu)^{-1}$, B et $\tau_{i,j}^{\mu}(B)$ sont semblables.
4. On a $C_{p,p-1} = 1$. Donc les opérations
$$\begin{cases} C_{p+1} \leftarrow C_{p+1} - B_{p,1} C_{p-1} \\ C_{p+2} \leftarrow C_{p+2} - B_{p,2} C_{p-1} \\ \dots \\ C_n \leftarrow C_n - B_{p,q} C_{p-1} \end{cases}$$
permettent de "remplacer" la dernière ligne de B par des zéros. Les opérations "duales", sur les lignes,
$$\begin{cases} L_{p-1} \leftarrow L_{p-1} + B_{p+1,1} L_{p+1} \\ \dots \\ L_{p-1} \leftarrow L_{p-1} - B_{n,1} L_n \end{cases}$$

ne modifient pas C puisque, en-dessous de C, ne se trouvent que des 0. Ces opérations reviennent à calculer

$$\tau_{p-1,n}(B_{p+1,q}) \circ \ldots \circ \tau_{p-1,p+2}(B_{p+1,2}) \circ \tau_{p-1,p+1}(B_{p+1,1})(A)$$

De la même manière, on peut utiliser $C_{p-1,p-2} = 1$ pour "éliminer" les coefficients $B_{p-1,1}$ à $B_{p-1,q}$. Notons que ces opérations sur les colonnes n'altèrent par le travail déjà effectué, d'une part parce que $C_{p-1,p-2}$ est le seul coefficient non nul de la colonne $p-2$ de C, d'autre part parce que les opérations sur les lignes ne vont modifier que la ligne L_{p-1}. On poursuit par récurrence, remplaçant ainsi, à la $k$ieme étape, la ligne numéro $p-k+1$ de B par 0. Après $p-1$ étapes, on obtient une matrice de la forme souhaitée.

Chaque transformation $\tau_{i,j}(\mu)$ revient à effectuer un changement de base dont la matrice de passage est $T_{i,j}(\mu)$ (seul le j^{ieme} vecteur de base est changé, qui est remplacé par lui-même plus μ fois le i^{ieme} vecteur de base). Puisqu'à chaque fois, l'indice j est plus grand que $p+1$, ce changement de base ne modifie pas les p premiers vecteurs de la base, qui restent $(e_1, e_2, \ldots, e_p)$. Il existe donc $(g_1, g_2, \ldots, g_q)$ telle que $(e_1, e_2, \ldots, e_p, g_1, g_2, \ldots, g_q)$ forme une base de E et telle que, dans cette base, la matrice de u soit de la forme souhaitée.

5. Notons $F_k = \text{Vect}(e_1, e_2, \ldots, e_k, g_1, g_2, \ldots, g_q)$. On a, pour $0 \leqslant k < p$, $u(F_k) \subset F_{k+1}$, d'où

$$\begin{aligned}
&u(g_k) \in \beta_k e_1 + F_0 \subset F_1,\\
&u^2(g_k) \in \beta_k e_2 + F_1 \subset F_2,\\
&\ldots,\\
&u^j(g_k) \in \beta_k e_j + F_{j-1} \subset F_j,\\
&\ldots,\\
&u^p(g_k) \in \beta_k e_p + F_{p-1} \subset F_p
\end{aligned}$$

   Supposons l'existence de λ_0 à λ_p, non tous nuls, tels que $\lambda_0 g_k + \lambda_1 u(g_k) + \ldots + \lambda_p u^p(g_k) = 0$. Soit j le plus grand indice tel que $\lambda_j \neq 0$ ($j \geqslant 1$ puisque $g_k \neq 0$). Alors on voit que $u^j(g_k) \in \text{Vect}(g_k, \ldots, u^{j-1}(g_k)) \subset F_{j-1}$, d'où, puisque $u^j(g_k) \in \beta_k e_j + F_{j-1}$ et $\beta_k \neq 0$, $e_j \in F_{j-1}$: contradiction. Ainsi, la famille $(g_k, u(g_k), \ldots, u^p(g_k))$ est une famille libre. Ceci contredit la maximalité de la dimension de F. Donc $\beta_k = 0$.

6. Ainsi, la matrice de u dans la base $(e_1, e_2, \ldots, e_p, g_1, \ldots, g_q)$ est composée de deux blocs diagonaux, ce qui entraîne que $G = \text{Vect}(g_1, \ldots, g_p)$ est stable par u : c'est un supplémentaire stable de F.

7. Par récurrence sur $n = \dim(E)$. Si $F \subsetneq E$, on applique l'hypothèse de récurrence à l'endomorphisme induit par u sur le sous-espace stable G mis en évidence ci-dessus.

8. Matriciellement, cela signifie que toute matrice est semblable à une matrice diagonale par blocs $\text{Diag}(C_1, C_2, \ldots, C_r)$, dont chaque bloc diagonal C_j est une matrice compagnon.