HEC–ESSEC – Mathématiques I

Mathématiques approfondies

Corrigé du sujet adapté – 2022

Les questions et sous-questions conservent la numérotation de l'énoncé. Les notations $\mathbb{E}$ et $\mathbb{V}$ désignent l'espérance et la variance. La transposée d'une matrice A est notée ${}^tA$.

Partie I – A. Sous-espaces engendrés par les itérés

Pour $e \neq 0$, on note $B(e,k) = (e, u(e), \dots, u^{k-1}(e))$ et $E_u(e) = \mathrm{Vect}(e, u(e), \dots, u^{n-1}(e))$. On étudie la longueur maximale $d(e)$ d'une famille $B(e,k)$ libre.

Corrigé – Partie I – A. Sous-espaces engendrés par les itérés.

1. Une famille liée.

L'espace E est de dimension n. Toute famille de $n+1$ vecteurs de E est liée, donc

$$\boxed{B(e,n+1) \text{ est liée.}}$$

2. Existence de $d(e)$.

Comme $e \neq 0$, $B(e,1)$ est libre. Si $k \geq n+1$, $B(e,k)$ contient la famille liée précédente et est liée. L'ensemble des longueurs libres est donc un ensemble non vide d'entiers compris entre 1 et n ; il possède un maximum :

$$\boxed{d(e) \text{ existe et } 1 \leq d(e) \leq n.}$$

3. Relation et base.

Posons $d = d(e)$. La famille $B(e,d)$ est libre et $B(e,d+1)$ est liée. Dans une relation non triviale sur cette dernière, le coefficient de $u^d(e)$ ne peut être nul, sinon la liberté de $B(e,d)$ annulerait tous les coefficients. On peut donc isoler ce terme :

$$\boxed{u^d(e) = \sum_{i=0}^{d-1} a_i u^i(e).}$$

Posons $H = \mathrm{Vect}(e, u(e), \dots, u^{d-1}(e))$. Les images des $d-1$ premiers générateurs appartiennent à H, et l'image du dernier y appartient par la relation obtenue. La linéarité donne $u(H) \subset H$. Dès lors, une récurrence montre que $u^k(e) \in H$ pour tout $k \geq d$. Ainsi $H = E_u(e)$; la famille génératrice est libre, donc

$$\boxed{B(e,d(e)) \text{ est une base de } E_u(e), \qquad \dim E_u(e) = d(e).}$$

4. Stabilité et minimalité.

Le raisonnement précédent montre

$$\boxed{u(E_u(e)) \subset E_u(e).}$$

Si un sous-espace K contient e et est stable par u, la récurrence $u^0(e) = e \in K$ puis $u^{k+1}(e) = u(u^k(e)) \in K$ donne tous les itérés. Comme K est un sous-espace, il contient leurs combinaisons linéaires :

$$\boxed{e \in K, \quad u(K) \subset K \quad \Longrightarrow \quad E_u(e) \subset K.}$$

5. Vecteurs propres.

Le vecteur non nul e est propre si et seulement si $u(e) = \lambda e$ pour un réel λ. Cette égalité équivaut à la liaison de $(e, u(e))$, alors que (e) est libre. Donc

$$\boxed{e \text{ est propre pour } u \quad \Longleftrightarrow \quad d(e) = 1.}$$

6. Homothéties.

Si $u = \lambda \operatorname{Id}_E$, chaque vecteur non nul est propre, donc $d(e) = 1$. Réciproquement, supposons tous les vecteurs non nuls propres. Pour une base $(b_1, \dots, b_n)$, écrivons $u(b_i) = \lambda_i b_i$. Pour $i \neq j$, $b_i + b_j$ est propre : il existe μ tel que

$$\lambda_i b_i + \lambda_j b_j = \mu(b_i + b_j).$$

La liberté de (b_i, b_j) entraîne $\lambda_i = \mu = \lambda_j$. Tous les λ_i sont donc égaux à un réel λ, et la linéarité donne $u = \lambda \operatorname{Id}_E$. Ainsi

$$\boxed{u \text{ est une homothétie} \quad \Longleftrightarrow \quad \forall e \neq 0,\ d(e) = 1.}$$

7. Endomorphismes cycliques.

Par définition, u est cyclique si et seulement s'il existe $e \neq 0$ avec $E_u(e) = E$. Ce sous-espace a pour dimension $d(e)$; il égale E exactement lorsque sa dimension vaut n. Donc

$$\boxed{u \text{ est cyclique} \quad \Longleftrightarrow \quad \exists e \neq 0,\ d(e) = n.}$$

Partie I – B. Endomorphismes cycliques

On suppose $E = E_u(e)$ et on travaille dans la base $(e, u(e), \dots, u^{n-1}(e))$. On pose $P_A(X) = X^n - \sum_{i=0}^{n-1} a_i X^i$, où $u^n(e) = \sum_{i=0}^{n-1} a_i u^i(e)$.

Corrigé – Partie I – B. Endomorphismes cycliques.

8. Matrice dans la base cyclique.

Pour $0 \leq j \leq n-2$, l'image du j-ième itéré est le suivant. La dernière colonne est donnée par les coefficients de la relation sur $u^n(e)$. Ainsi

$$\boxed{A = \begin{pmatrix} 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & a_{n-2} \\ 0 & \cdots & 0 & 1 & a_{n-1} \end{pmatrix}.}$$

C'est une matrice compagnon, dite aussi de Frobenius.

9. Un polynôme annulateur.

La relation définissant les a_i donne $P_A(u)(e) = 0$. Les puissances de u commutent entre elles, donc $P_A(u)u^k = u^k P_A(u)$. Pour $0 \leq k \leq n-1$,

$$P_A(u)(u^k(e)) = u^k(P_A(u)(e)) = 0.$$

L'application $P_A(u)$ est nulle sur une base de E, donc

$$\boxed{P_A(u)(e) = 0, \qquad P_A(u)(u^k(e)) = 0, \qquad P_A(u) = 0.}$$

10. Liberté des premières puissances.

Si $\sum_{i=0}^{n-1} c_i u^i = 0$, son application à e donne $\sum_i c_i u^i(e) = 0$. La liberté de la base cyclique impose tous les c_i nuls :

$$\boxed{(\mathrm{Id}_E, u, \ldots, u^{n-1}) \text{ est libre.}}$$

11. Degré minimal d'un annulateur non nul.

Le polynôme P_A est unitaire de degré n et annule u. Si un polynôme non nul de degré inférieur à n annulait u, ses coefficients donneraient une relation non triviale entre les puissances précédentes. C'est impossible, d'où

$$\boxed{\min\{\deg Q : Q \neq 0,\ Q(u) = 0\} = n, \qquad \deg P_A = n.}$$

12. Valeurs propres et dimensions des sous-espaces propres.

Écrivons un vecteur x dans la base cyclique, avec coordonnées $(x_0, \ldots, x_{n-1})$. L'égalité $Ax = \lambda x$ équivaut à

$$\lambda x_0 = a_0 x_{n-1}, \qquad x_{j-1} + a_j x_{n-1} = \lambda x_j \quad (1 \leq j \leq n-1).$$

Si $x_{n-1} = 0$, les équations prises de bas en haut donnent toutes les coordonnées nulles. Un vecteur propre doit donc avoir $x_{n-1} \neq 0$. En remontant les équations, on obtient

$$x_j = \left(\lambda^{n-1-j} - \sum_{k=j+1}^{n-1} a_k \lambda^{k-1-j}\right) x_{n-1} \quad (0 \leq j \leq n-2).$$

La première équation devient $P_A(\lambda)x_{n-1} = 0$. Ainsi une valeur propre est nécessairement une racine réelle de P_A. Réciproquement, si $P_A(\lambda) = 0$, on pose $x_{n-1} = 1$ et on définit les autres coordonnées par cette formule : toutes les équations sont vérifiées, et $x \neq 0$. Enfin chaque coordonnée est déterminée par le seul scalaire x_{n-1}. Le sous-espace propre a donc pour base le vecteur obtenu en prenant ce scalaire égal à 1 :

$$\boxed{\lambda \in \mathrm{Sp}(u) \iff P_A(\lambda) = 0, \qquad \lambda \in \mathrm{Sp}(u) \implies \dim E_\lambda(u) = 1.}$$

13. Caractérisation de la diagonalisabilité.

Si u est diagonalisable, E est somme directe de ses sous-espaces propres. Chacun a dimension 1, donc il faut exactement n valeurs propres réelles distinctes. Ce sont autant de racines de P_A. Réciproquement, si P_A admet n racines réelles distinctes, la question 12 donne n valeurs propres distinctes de u. Des vecteurs propres non nuls associés sont libres et forment une base de E. Ainsi

$$\boxed{u \text{ est diagonalisable} \iff P_A \text{ possède } n \text{ racines réelles distinctes.}}$$

Partie I – C. Un exemple en dimension trois

On étudie les matrices $F = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & -1 \\ 1 & -1 & -1 \end{pmatrix}$ et $G = \begin{pmatrix} 1 & -1 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$ et les endomorphismes f, g associés.

Corrigé – Partie I – C. Un exemple en dimension trois.

14. Diagonalisabilité de f.

La matrice F est réelle et symétrique. Le théorème spectral fournit donc une base orthonormale de vecteurs propres ; en particulier,

$$\boxed{f \text{ est diagonalisable.}}$$

15. Une base de diagonalisation.

Pour $v = (x, y, z)$, $Fv = (z, -z, x - y - z)$. Si $Fv = \lambda v$, les deux premières équations sont $z = \lambda x$ et $-z = \lambda y$. Pour $\lambda = 0$, on obtient $z = 0$ et $x = y$: l'espace propre est engendré par $(1, 1, 0)$. Pour $\lambda \neq 0$, on a $y = -x$ et $z = \lambda x$. La troisième équation devient $(2 - \lambda)x = \lambda^2 x$. Un vecteur non nul impose $x \neq 0$, donc

$$\lambda^2 + \lambda - 2 = (\lambda + 2)(\lambda - 1) = 0.$$

Les trois vecteurs suivants sont propres et associés à des valeurs propres distinctes ; ils forment donc une base :

$$\boxed{\begin{array}{c} \lambda_1 = -2, \quad \lambda_2 = 0, \quad \lambda_3 = 1, \\ V_1 = (1, -1, -2), \quad V_2 = (1, 1, 0), \quad V_3 = (1, -1, 1). \end{array}}$$

16. Un vecteur cyclique pour f.

On a $V = V_1 + V_2 + V_3 = (3, -1, -1)$. Supposons $c_0 V + c_1 f(V) + c_2 f^2(V) = 0$. Dans la base propre, les coefficients de V_i sont $c_0 + c_1\lambda_i + c_2\lambda_i^2$. Le polynôme $Q(X) = c_0 + c_1 X + c_2 X^2$ s'annule en $-2, 0, 1$; s'il était non nul, il aurait au plus deux racines. Ainsi $Q = 0$, ce qui établit la liberté. Donc

$$\boxed{d(V) = 3, \qquad f \text{ est cyclique.}}$$

17. Polynôme annulateur de g.

Le calcul donne $G^2 = 2G$, donc $Q(X) = X(X - 2)$ annule g. Aucun polynôme non nul constant ne peut annuler un endomorphisme sur un espace non nul. Si $ag + b\,\mathrm{Id} = 0$ avec $a \neq 0$, g serait une homothétie ; ce n'est pas le cas puisque G possède des coefficients non nuls hors de la diagonale. Il n'y a donc aucun annulateur de degré 1.

$$\boxed{Q(X) = X(X - 2) \text{ est un annulateur non nul de degré minimal 2.}}$$

Un endomorphisme cyclique en dimension 3 n'a aucun annulateur non nul de degré inférieur à 3, d'après la question 11. Par conséquent,

$$\boxed{g \text{ n'est pas cyclique.}}$$

18. Une base propre commune.

On vérifie directement

$$G(1,-1,-2)=(2,-2,-4),\quad G(1,1,0)=0,\quad G(1,-1,1)=(2,-2,2).$$

Donc

$$\boxed{g(V_1)=2V_1,\quad g(V_2)=0,\quad g(V_3)=2V_3.}$$

La famille (V_1,V_2,V_3), déjà reconnue comme base, est donc aussi une base de vecteurs propres de g.

Partie I – D. Tests polynomiaux en Python

Les coefficients des polynômes sont rangés par puissances croissantes. La division euclidienne permet de calculer un pgcd ; les changements de signe fournissent un test suffisant de présence de racines réelles distinctes.

Corrigé – Partie I – D. Tests polynomiaux en Python.

19. Existence d'un pgcd unitaire.

Le polynôme 1 divise P et Q. Le degré d'un diviseur commun non nul est compris entre 0 et $\min(\deg P,\deg Q)$, donc l'ensemble de ces degrés a un maximum. Choisissons un diviseur commun de degré maximal et divisons-le par son coefficient dominant : il reste diviseur des deux polynômes et devient unitaire. Ainsi

$$\boxed{P,Q \text{ admettent un diviseur commun unitaire de degré maximal.}}$$

L'algorithme d'Euclide permet de le calculer. Si $P=AQ+R$, les diviseurs communs de P,Q sont exactement ceux de Q,R, puisque $R=P-AQ$ et $P=AQ+R$. Les degrés des restes non nuls diminuent strictement ; l'algorithme s'arrête, et le dernier reste non nul, rendu unitaire, est un pgcd.

20. Racines répétées d'un polynôme scindé sur $\mathbb{R}$.

Supposons P produit de facteurs linéaires réels. Si a est une racine de répétition $r\geq 2$, écrivons $P(X)=(X-a)^rH(X)$ avec $H(a)\neq 0$. La dérivation donne

$$P'(X)=r(X-a)^{r-1}H(X)+(X-a)^rH'(X).$$

Ainsi $X-a$ divise P et P', et leur pgcd a degré au moins 1. Si chaque racine de P n'apparaît qu'une fois, pour toute racine a on écrit $P=(X-a)H$ avec $H(a)\neq 0$; alors $P'(a)=H(a)\neq 0$. Les polynômes P et P' n'ont aucun diviseur commun non constant, puisque tout diviseur non constant de P possède un facteur linéaire réel. Donc

$$\boxed{P \text{ scindé sur } \mathbb{R}:\quad \text{racines toutes simples} \iff \deg \operatorname{pgcd}(P,P')=0.}$$

21. Fonction `rac_simp`.

On supprime les coefficients dominants nuls pour lire correctement le degré. Les tableaux sont en ordre croissant ; les coefficients de la dérivée sont kc_k.

```
import numpy as np

def reduit(c):
    k = len(c)-1
    while k > 0 and c[k] == 0:
        k = k-1
    return c[:k+1]

def rac_simp(c):
    p = reduit(np.array(c))
    q = np.zeros(len(p)-1)
    for k in range(1, len(p)):
        q[k-1] = k*p[k]
    q = reduit(q)
    while len(q) > 1 or q[0] != 0:
        quotient, r = np.polynomial.polynomial.polydiv(p, q)
        p = q
        q = reduit(r)
    return len(p) == 1
```

Le programme s'applique à un polynôme de degré au moins 1. En arithmétique exacte, il renvoie `True` exactement lorsque le pgcd de P et P' est constant. Sous l'hypothèse que P est scindé sur $\mathbb{R}$, la question 20 identifie cela à la simplicité de toutes ses racines. Pour une matrice compagnon, on fournit les coefficients de P_A, à savoir $(-a_0, \dots, -a_{n-1}, 1)$. Il faut aussi savoir que P_A possède uniquement des facteurs linéaires réels : le test du pgcd ne vérifie pas cette condition. Par exemple, $P = X^2 + 1$ a un pgcd constant avec $P' = 2X$, mais aucune racine réelle.

$$\boxed{P_A \text{ scindé sur } \mathbb{R} : \quad A \text{ diagonalisable} \iff \texttt{rac_simp} \text{ renvoie True.}}$$

En calcul flottant, des restes théoriquement nuls peuvent être affectés par des erreurs d'arrondi. Le test ci-dessus traduit l'algorithme exact ; une sortie numérique proche d'un cas de racines répétées demande une vérification supplémentaire.

22. Détection par changements de signe.

Le polynôme est continu. Pour chaque k, le signe strictement opposé en x_k et x_{k+1} donne une racine dans $]x_k, x_{k+1}[$ par le théorème des valeurs intermédiaires. Ces n intervalles sont disjoints, donc on obtient n racines distinctes. Un polynôme non nul de degré n a au plus n racines :

$$\boxed{P \text{ possède exactement } n \text{ racines réelles distinctes.}}$$

23. Borne sur les racines réelles.

Soit $z \in \mathbb{R}$ avec $P(z) = 0$. Si $|z| \leq 1$, la borne demandée est immédiate. Sinon, $|z| > 1$ et

$$|z|^n = \left|\sum_{k=0}^{n-1} a_k z^k\right| \leq \sum_{k=0}^{n-1} |a_k|\,|z|^k \leq |z|^{n-1} \sum_{k=0}^{n-1} |a_k|.$$

On divise par le réel strictement positif $|z|^{n-1}$, d'où

$$\boxed{|z| \leq m := \max\left(1, \sum_{k=0}^{n-1} |a_k|\right).}$$

24. Fonction `rac_simp_approx`.

Pour `pas` > 0, on parcourt une grille couvrant $[-m, m]$ et on compte les intervalles où le produit des valeurs de P est strictement négatif.

```
def valeur(c, x):
    n = len(c)
    p = x ** n
    for k in range(n):
        p = p-c[k]*x**k
    return p

def rac_simp_approx(c, pas):
    n = len(c)
    m = np.max(np.array([1, np.sum(np.abs(c))]))
    x = -m-pas/2
    px = valeur(c, x)
    nombre = 0
    while x < m+pas/2:
        y = x+pas
        py = valeur(c, y)
        if px*py < 0:
            nombre = nombre+1
        x = y
        px = py
    if nombre == n:
        return True
    return 'ind'
```

Chaque intervalle compté contient une racine réelle distincte. Il ne peut donc y en avoir plus de n. La sortie `True` certifie le critère de la question 13.

25. Utilisation et portée du test.

On donne à la fonction la liste $(a_0, \dots, a_{n-1})$ de la dernière colonne de la matrice compagnon, puis un pas positif. Ainsi

$$\boxed{\texttt{True} \implies A \text{ est diagonalisable sur } \mathbb{R}.}$$

La sortie `'ind'` signifie que le programme n'a pas détecté n changements de signe. Cela peut arriver si P_A n'a pas n racines réelles distinctes, mais aussi s'il en a n : une racine peut coïncider avec un point de la grille, ou plusieurs racines peuvent tomber dans un même intervalle. Cette sortie ne permet donc pas de conclure à la non-diagonalisabilité. Par exemple, pour $P = X(X-1)$, des points de grille égaux à 0 ou à 1 empêchent de compter le changement de signe correspondant avec un produit strictement négatif.

$$\boxed{\texttt{'ind'} \text{ est une réponse indécise.}}$$

II. Deux cas particuliers – A. Cas diagonalisable

Un endomorphisme diagonalisable est cyclique exactement lorsqu'il possède autant de valeurs propres distinctes que la dimension de l'espace. On le démontre par l'action des polynômes sur une base propre.

Corrigé – II. Deux cas particuliers – A. Cas diagonalisable.

26. Un polynôme annulateur de degré p.

Posons

$$Q(X) = \prod_{i=1}^{p}(X - \lambda_i).$$

L'endomorphisme u est diagonalisable : il existe donc une base de E formée de vecteurs propres. Si x est l'un de ces vecteurs, associé à λ_j, alors $u^k(x) = \lambda_j^k x$ pour tout $k \geq 0$. Par combinaison linéaire,

$$Q(u)(x) = Q(\lambda_j)x = 0.$$

Ainsi $Q(u)$ est nul sur une base, donc est l'endomorphisme nul. Comme Q est unitaire de degré p, on peut écrire $Q(X) = X^p + \sum_{k=0}^{p-1} b_k X^k$, d'où

$$\boxed{\prod_{i=1}^{p}(u - \lambda_i \mathrm{Id}_E) = 0, \qquad u^p + \sum_{k=0}^{p-1} b_k u^k = 0.}$$

Le coefficient de u^p dans cette relation est 1, donc la relation est non triviale. Par conséquent

$$\boxed{(\mathrm{Id}_E, u, \ldots, u^p) \text{ est liée.}}$$

27. Nombre de valeurs propres lorsque u est cyclique.

Les vecteurs propres associés à des valeurs propres distinctes sont linéairement indépendants, donc $p \leq n$. Si u est cyclique, la question 10 montre que $(\mathrm{Id}_E, u, \ldots, u^{n-1})$ est libre. Si $p < n$, la relation non triviale de la question 26 porterait sur une sous-famille de cette famille libre, ce qui est impossible. Ainsi

$$\boxed{u \text{ diagonalisable et cyclique } \implies p = n.}$$

28. Réciproque lorsque $p = n$.

Soit $e = \sum_{i=1}^{n} e_i$. Pour tout $k \geq 0$, la linéarité et les relations $u(e_i) = \lambda_i e_i$ donnent

$$u^k(e) = \sum_{i=1}^{n} \lambda_i^k e_i.$$

Supposons $\sum_{k=0}^{n-1} c_k u^k(e) = 0$ et posons $R(X) = \sum_{k=0}^{n-1} c_k X^k$. Alors

$$0 = \sum_{i=1}^{n} \left(\sum_{k=0}^{n-1} c_k \lambda_i^k \right) e_i = \sum_{i=1}^{n} R(\lambda_i) e_i.$$

La famille (e_i) étant une base, $R(\lambda_i) = 0$ pour tout i. Les n réels λ_i sont distincts et $\deg R \leq n - 1$ si R est non nul. Un polynôme non nul ayant au plus autant de racines

distinctes que son degré, cela impose $R = 0$, puis $c_k = 0$ pour tout k. Donc $B(e, n)$ est libre ; elle comporte n vecteurs dans un espace de dimension n, donc est une base. Ainsi

$$\boxed{B(e,n) \text{ est une base de } E, \qquad u \text{ est cyclique.}}$$

En réunissant les questions 27 et 28,

$$\boxed{\begin{array}{c}\text{Si } u \text{ est diagonalisable, } \quad u \text{ cyclique} \\ \iff \quad u \text{ possède } n \text{ valeurs propres distinctes.}\end{array}}$$

29. Étude de $u_\alpha = g + \alpha f$.

Reprenons la base propre commune de la section C :

$$V_1 = (1, -1, -2), \qquad V_2 = (1, 1, 0), \qquad V_3 = (1, -1, 1).$$

Les valeurs propres de f dans cette base sont $-2, 0, 1$. De plus, un produit direct par G donne

$$g(V_1) = 2V_1, \qquad g(V_2) = 0, \qquad g(V_3) = 2V_3.$$

Par conséquent

$$\begin{aligned} u_\alpha(V_1) &= (2 - 2\alpha)V_1, \\ u_\alpha(V_2) &= 0, \\ u_\alpha(V_3) &= (2 + \alpha)V_3. \end{aligned}$$

Cette base est une base propre pour u_α pour toute valeur de α, même lorsque deux valeurs propres coïncident. Ainsi

$$\boxed{u_\alpha \text{ est diagonalisable pour tout } \alpha \in \mathbb{R}.}$$

Ses trois valeurs propres sont distinctes exactement lorsque

$$2 - 2\alpha \neq 0, \qquad 2 + \alpha \neq 0, \qquad 2 - 2\alpha \neq 2 + \alpha,$$

soit $\alpha \neq 1$, $\alpha \neq -2$ et $\alpha \neq 0$. Le critère précédent donne

$$\boxed{u_\alpha \text{ est cyclique } \iff \alpha \notin \{-2, 0, 1\}.}$$

Pour $\alpha = -2, 0, 1$, les valeurs propres respectives sont $(6, 0, 0)$, $(2, 0, 2)$ et $(0, 0, 3)$; dans chaque cas, il n'y a que deux valeurs propres distinctes.

II. Deux cas particuliers – B. Cas nilpotent

Appliquer une puissance bien choisie à une relation entre les itérés d'un vecteur permet de montrer leur indépendance. L'indice de nilpotence est maximal exactement dans le cas cyclique.

Corrigé – II. Deux cas particuliers – B. Cas nilpotent.

30. Une famille libre de r vecteurs.

Par définition de l'indice, $u^r = 0$ et $u^{r-1} \neq 0$. Il existe donc bien un vecteur e tel que

$u^{r-1}(e) \neq 0$. Considérons une relation

$$\sum_{k=0}^{r-1} c_k u^k(e) = 0.$$

Si un coefficient était non nul, notons j le plus petit indice tel que $c_j \neq 0$. En appliquant u^{r-1-j}, on obtiendrait

$$0 = c_j u^{r-1}(e) + \sum_{k=j+1}^{r-1} c_k u^{r-1-j+k}(e) = c_j u^{r-1}(e).$$

En effet, chaque exposant de la dernière somme est au moins égal à r et $u^\ell = 0$ pour tout $\ell \geq r$. Cela contredit $c_j \neq 0$ et $u^{r-1}(e) \neq 0$. Tous les coefficients sont donc nuls, d'où

$$\boxed{(e, u(e), \dots, u^{r-1}(e)) \text{ est libre.}}$$

Cette preuve comprend aussi le cas $r = 1$, où la famille se réduit au vecteur non nul e.

31. Indice maximal et matrice dans une base cyclique.

La famille libre précédente comporte r vecteurs dans E, de dimension n ; donc $r \leq n$. Si $r = n$, cette famille est une base de E, et u est cyclique. Réciproquement, si u est cyclique, il existe e tel que $B(e, n)$ soit une base. Si $r < n$, le vecteur $u^r(e) = 0$ appartiendrait à cette famille, ce qui contredirait sa liberté. Ainsi

$$\boxed{r \leq n, \qquad r = n \iff u \text{ est cyclique.}}$$

Lorsque $r = n$ et $u^{n-1}(e) \neq 0$, l'image du j-ième vecteur de $B(e, n)$ est le suivant pour $j < n$, et l'image du dernier est $u^n(e) = 0$. Par lecture des colonnes,

$$\boxed{\mathrm{Mat}_{B(e,n)}(u) = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & 0 \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix}.}$$

II. Deux cas particuliers – C. Un opérateur sur les polynômes

Développer des sommes finies de polynômes pour justifier les intégrales. L'intégration par parties relie l'opérateur aux dérivées successives ; l'opérateur $u - \mathrm{Id}_E$ abaisse ensuite le degré d'une unité.

Corrigé – II. Deux cas particuliers – C. Un opérateur sur les polynômes.

32. Convergence et nature polynomiale de $u(P)$.

Fixons $x \in \mathbb{R}$ et écrivons $P(X) = \sum_{j=0}^{n-1} a_j X^j$. Le binôme de Newton fournit la somme finie

$$P(x+t) = \sum_{j=0}^{n-1} a_j \sum_{\ell=0}^{j} \binom{j}{\ell} x^{j-\ell} t^\ell.$$

Pour tout entier $\ell \geq 0$, l'intégrale $\int_0^{+\infty} t^\ell e^{-t}\,\mathrm{d}t$ converge. En effet, l'intégrande est continue sur $[0,+\infty[$ et les croissances comparées donnent $t^\ell e^{-t/2} \to 0$; pour t assez grand, $0 \leq t^\ell e^{-t} \leq e^{-t/2}$, dont l'intégrale sur $[0,+\infty[$ converge. Par l'inégalité triangulaire appliquée à la somme finie, l'intégrale de $|P(x+t)|e^{-t}$ converge également. Ainsi l'intégrale qui définit $u(P)(x)$ converge absolument. Posons $c_\ell = \int_0^{+\infty} t^\ell e^{-t}\,\mathrm{d}t$. La linéarité d'une somme finie d'intégrales convergentes donne

$$u(P)(x) = \sum_{j=0}^{n-1} a_j \sum_{\ell=0}^{j} \binom{j}{\ell} c_\ell x^{j-\ell}.$$

Les c_ℓ sont des réels indépendants de x. Cette expression est un polynôme de degré au plus $n-1$, d'où

$$\boxed{\forall x \in \mathbb{R}, \quad \int_0^{+\infty} P(x+t)e^{-t}\,\mathrm{d}t \text{ converge}, \quad u(P) \in E.}$$

33. Linéarité de u.

La question 32 montre que u est une application de E dans E. Pour $P, Q \in E$ et $\alpha, \beta \in \mathbb{R}$, les intégrales considérées convergent et leur linéarité donne, pour tout réel x,

$$\begin{aligned} u(\alpha P + \beta Q)(x) &= \int_0^{+\infty} (\alpha P(x+t) + \beta Q(x+t))e^{-t}\,\mathrm{d}t \\ &= \alpha u(P)(x) + \beta u(Q)(x). \end{aligned}$$

Les fonctions sont donc égales, et $\boxed{u \text{ est un endomorphisme de } E.}$

34. Relation avec la dérivée de P.

Fixons $x \in \mathbb{R}$ et $A > 0$. Sur le segment $[0, A]$, les fonctions $a(t) = P(x+t)$ et $b(t) = -e^{-t}$ sont de classe $\mathcal{C}^1$, de dérivées

$$a'(t) = P'(x+t), \qquad b'(t) = e^{-t}.$$

L'intégration par parties sur ce segment donne

$$\int_0^A P(x+t)e^{-t}\,\mathrm{d}t = -P(x+A)e^{-A} + P(x) + \int_0^A P'(x+t)e^{-t}\,\mathrm{d}t.$$

Le terme $P(x+A)e^{-A}$ tend vers 0 lorsque $A \to +\infty$, par croissances comparées. Les deux intégrales impropres convergent par la question 32, appliquée à P et à $P' \in E$. En passant à la limite,

$$\boxed{u(P)(x) = P(x) + u(P')(x).}$$

Cette égalité vaut pour tout x, donc $u(P) = P + u(P')$.

35. Expression par les dérivées successives.

En appliquant successivement la relation précédente à $P, P', \ldots$, on obtient, pour $j \in [\![1, n]\!]$,

$$u(P) = \sum_{k=0}^{j-1} P^{(k)} + u(P^{(j)}).$$

Cette relation se prouve par récurrence : le cas $j = 1$ est la question 34, puis on remplace $u(P^{(j)})$ par $P^{(j)} + u(P^{(j+1)})$. Comme $\deg P \leq n-1$, on a $P^{(n)} = 0$, et la linéarité donne $u(0) = 0$. Pour $j = n$, il vient

$$\boxed{u(P) = \sum_{k=0}^{n-1} P^{(k)}.}$$

36. Changement de variable.

Pour un réel x fixé, le changement $s = x + t$ est donné par une bijection de classe $\mathcal{C}^1$ de $[0, +\infty[$ sur $[x, +\infty[$, de dérivée constante 1. Sur $[0, A]$, il fournit

$$\int_0^A P(x+t)e^{-t}\,\mathrm{d}t = e^x \int_x^{x+A} P(s)e^{-s}\,\mathrm{d}s.$$

La borne $x + A$ tend vers $+\infty$ avec A. Cette identité de changements de variable montre que les deux intégrales impropres sont de même nature ; la première converge d'après la question 32, donc la seconde converge aussi. En passant à la limite,

$$\boxed{u(P)(x) = e^x \int_x^{+\infty} P(s)e^{-s}\,\mathrm{d}s.}$$

37. Dérivation par une primitive sur des segments.

Posons $H(x) = \int_x^{+\infty} P(s)e^{-s}\,\mathrm{d}s$. Toutes ces intégrales convergent, et leur additivité permet d'écrire, pour tout réel x,

$$H(x) = H(0) - \int_0^x P(s)e^{-s}\,\mathrm{d}s.$$

Cette écriture reste valable pour $x < 0$, avec l'orientation usuelle de l'intégrale sur un segment. La fonction $s \mapsto P(s)e^{-s}$ est continue sur $\mathbb{R}$. Le théorème fondamental de l'analyse, appliqué à l'intégrale sur le segment de bornes 0 et x, donne donc

$$\boxed{H'(x) = -P(x)e^{-x}.}$$

L'expression $u(P)(x) = e^x H(x)$ de la question 36 est un produit de deux fonctions dérivables ; ainsi

$$(u(P))'(x) = e^x H(x) + e^x H'(x) = u(P)(x) - P(x).$$

Enfin, la question 34 donne $u(P) - P = u(P')$, d'où

$$\boxed{(u(P))' = u(P) - P = u(P').}$$

38. Matrice et spectre de u.

Pour $j \in [\![0, n-1]\!]$, la question 35 donne

$$u(X^j) = \sum_{k=0}^{j} \frac{j!}{(j-k)!} X^{j-k} = \sum_{i=0}^{j} \frac{j!}{i!} X^i.$$

Dans la base $(1, X, \ldots, X^{n-1})$, en numérotant les lignes et les colonnes de 0 à $n-1$, la matrice A de u vérifie donc

$$\boxed{A_{i,j} = \begin{cases} \dfrac{j!}{i!} & \text{si } i \leq j, \\ 0 & \text{si } i > j. \end{cases}}$$

Elle est triangulaire supérieure et ses coefficients diagonaux valent 1. Pour identifier le spectre observons que $u(1) = 1$, donc 1 est une valeur propre. Si $P \neq 0$ est un vecteur propre associé à λ, notons $m = \deg P$ et $a \neq 0$ son coefficient dominant. Les dérivées d'ordre positif ont un degré strictement inférieur à m ou sont nulles. Dans l'expression $u(P) = P + P' + \cdots$, le coefficient de X^m vaut donc a. Dans λP, il vaut λa. L'égalité $u(P) = \lambda P$ impose $a = \lambda a$, donc $\lambda = 1$. Ainsi

$$\boxed{\mathrm{Sp}(u) = \{1\}.}$$

39. Image de $v = u - \mathrm{Id}_E$.

La question 35 donne

$$v(P) = \sum_{k=1}^{n-1} P^{(k)}.$$

Ainsi v annule les constantes. Si P est de degré $m \geq 1$ et de coefficient dominant a, la première dérivée a pour terme dominant maX^{m-1} ; toutes les suivantes ont un degré au plus égal à $m-2$ ou sont nulles. Par conséquent

$$\deg v(P) = m - 1, \qquad \text{coefficient dominant de } v(P) = ma.$$

En particulier, $\mathrm{Im}(v) \subset \mathbb{R}_{n-2}[X]$. Pour $j \in [\![1, n-1]\!]$, le polynôme $v(X^j)$ a pour degré $j-1$ et pour coefficient dominant j. Les $n-1$ polynômes

$$v(X), v(X^2), \ldots, v(X^{n-1})$$

sont donc libres : dans une relation non triviale, le terme de degré maximal ne pourrait être compensé par les autres polynômes. Ils appartiennent à $\mathbb{R}_{n-2}[X]$, de dimension $n-1$, donc en constituent une base. Puisqu'ils appartiennent tous à $\mathrm{Im}(v)$, cela donne l'inclusion réciproque, puis

$$\boxed{\mathrm{Im}(v) = \mathbb{R}_{n-2}[X].}$$

40. Nilpotence et caractère cyclique de v.

Chaque application de v abaisse d'une unité le degré d'un polynôme non constant, et v annule les constantes. Tout élément de E a un degré au plus égal à $n-1$; il est donc annulé après n applications de v. Ainsi $v^n = 0$. Pour vérifier que l'indice est exactement n, partons de X^{n-1}. La propriété du coefficient dominant établie à la question 39 donne, par récurrence, pour $j \in [\![0, n-1]\!]$,

$$\deg(v^j(X^{n-1})) = n - 1 - j, \qquad \text{coefficient dominant} = \frac{(n-1)!}{(n-1-j)!}.$$

En particulier,

$$v^{n-1}(X^{n-1}) = (n-1)! \neq 0.$$

Donc $v^{n-1} \neq 0$ et

$$\boxed{v \text{ est nilpotent d'indice } n.}$$

La question 31 entraîne alors que v est cyclique. On peut également le voir directement : les n polynômes $v^j(X^{n-1})$, $0 \leq j \leq n-1$, sont de degrés distincts $n-1, n-2, \ldots, 0$, donc sont libres et forment une base de E. Ainsi

$$\boxed{v \text{ est cyclique ; } X^{n-1} \text{ est un vecteur cyclique.}}$$

Partie III – Décomposition de Frobenius

Construction d'une décomposition en sous-espaces stables sur lesquels l'endomorphisme est cyclique, puis applications aux endomorphismes nilpotents et à la similitude d'une matrice avec sa transposée.

Corrigé – Partie III – Décomposition de Frobenius.

A – Cas d'une homothétie

41. Décomposition d'une homothétie.

Supposons $u = \lambda \mathrm{Id}_E$ et choisissons une base $(v_1, \dots, v_n)$ de E. Pour chaque i, posons $F_i = \mathrm{Vect}(v_i)$. Ces sous-espaces sont non nuls et stables, puisque $u(v_i) = \lambda v_i$. De plus, chaque restriction est un endomorphisme d'un espace de dimension 1, donc cyclique. Enfin, la propriété de base donne

$$\boxed{E = F_1 \oplus \cdots \oplus F_n.}$$

Ainsi $\boxed{(R) \text{ est vraie pour une homothétie.}}$

B – Construction d'un premier facteur cyclique

42. Existence d'une chaîne de longueur au moins deux.

D'après la question 6, si $d(x) = 1$ pour tous les vecteurs non nuls x, alors u est une homothétie. Par contraposée, lorsque u n'est pas une homothétie,

$$\boxed{\exists e \in E \setminus \{0\}, \quad d(e) \neq 1, \quad \text{donc } d(e) \geq 2.}$$

Les valeurs possibles de $d(x)$ appartiennent à $[\![1, n]\!]$. Leur ensemble, non vide et fini, possède un maximum. Dans la suite, on choisit e qui réalise ce maximum et l'on pose $d = d(e)$.

43. Cas $d = n$.

Si $d = n$, la base $B(e, n)$ de $E_u(e)$ contient n vecteurs et engendre E. Ainsi u est cyclique sur E. Il suffit de prendre un seul facteur :

$$\boxed{p = 1, \qquad F_1 = E, \qquad (R) \text{ est réalisée.}}$$

On suppose désormais $2 \leq d \leq n - 1$.

44. Forme linéaire de coordonnée.

Dans la base $\mathcal{B} = (e_0, \dots, e_{n-1})$ complétant $B(e, d)$, chaque vecteur x possède une unique écriture $x = \sum_{k=0}^{n-1} x_k e_k$. L'application $\varphi(x) = x_{d-1}$ est donc bien définie. Pour deux vecteurs x, y et deux réels α, β, la coordonnée d'indice $d - 1$ de $\alpha x + \beta y$ est $\alpha x_{d-1} + \beta y_{d-1}$. Ainsi φ est linéaire. Comme $\varphi(e_{d-1}) = 1$,

$$\boxed{\varphi \in \mathcal{L}(E, \mathbb{R}), \qquad \varphi \neq 0.}$$

On a en particulier $\varphi(e_i) = 0$ pour $0 \leq i \leq d - 2$.

45. Linéarité de Φ.

Chaque puissance u^j est linéaire, et la composée $\varphi \circ u^j$ est une forme linéaire. Pour tous $x, y \in E$ et $\alpha, \beta \in \mathbb{R}$, chacune des coordonnées de $\Phi(\alpha x + \beta y)$ est donc la combinaison linéaire correspondante des coordonnées de $\Phi(x)$ et de $\Phi(y)$. Ainsi

$$\boxed{\Phi \in \mathcal{L}(E, \mathbb{R}^d), \qquad G = \operatorname{Ker}\Phi \text{ est un sous-espace de } E.}$$

46. Images des vecteurs de la chaîne.

Comme $e_k = u^k(e)$ pour $0 \leq k \leq d-1$,

$$\Phi(e_0) = (\varphi(e_{d-1}), \varphi(e_{d-2}), \ldots, \varphi(e_0)) = (1, 0, \ldots, 0).$$

L'égalité $u^d(e) = \sum_{i=0}^{d-1} a_i e_i$ donne $\varphi(u^d(e)) = a_{d-1}$, donc

$$\boxed{\Phi(e_0) = (1, 0, \ldots, 0), \qquad \Phi(e_1) = (a_{d-1}, 1, 0, \ldots, 0).}$$

Plus généralement, numérotant les coordonnées de Φ de 0 à $d-1$, la coordonnée d'indice j de $\Phi(e_k)$ est

$$\varphi(u^{d-1-j}(e_k)) = \varphi(u^{d-1-j+k}(e)).$$

Si $j = k$, cette coordonnée vaut $\varphi(e_{d-1}) = 1$. Si $j > k$, l'exposant est compris entre 0 et $d-2$, donc la coordonnée est nulle. Pour $j < k$, notons $\beta_{j,k}$ sa valeur. Ainsi

$$\boxed{\forall k \in [\![1, d-1]\!], \quad \Phi(e_k) = (\beta_{0,k}, \ldots, \beta_{k-1,k}, 1, 0, \ldots, 0).}$$

47. Isomorphisme de F_1 sur $\mathbb{R}^d$.

D'après la question précédente, la matrice de $\widetilde{\Phi} = \Phi_{|F_1}$ dans $B(e, d)$ et la base canonique de $\mathbb{R}^d$ est

$$\boxed{C = \begin{pmatrix} 1 & \beta_{0,1} & \beta_{0,2} & \cdots & \beta_{0,d-1} \\ 0 & 1 & \beta_{1,2} & \cdots & \beta_{1,d-1} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & \beta_{d-2,d-1} \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix}.}$$

Si $CX = 0$, la dernière ligne impose que la dernière coordonnée de X soit nulle. La ligne précédente impose alors que l'avant-dernière coordonnée soit nulle ; en remontant ainsi les lignes, toutes les coordonnées sont nulles. Donc C est injective, et par égalité des dimensions elle est inversible. Ainsi

$$\boxed{\widetilde{\Phi} : F_1 \longrightarrow \mathbb{R}^d \text{ est bijective.}}$$

48. Supplémentaire stable de F_1.

Somme directe. Pour $x \in E$, la bijectivité de $\widetilde{\Phi}$ fournit un unique $z \in F_1$ tel que $\Phi(z) = \Phi(x)$. Le vecteur $x - z$ appartient alors à G, donc $E = F_1 + G$. Si $z \in F_1 \cap G$, alors $\widetilde{\Phi}(z) = 0$, et son injectivité impose $z = 0$. Par conséquent,

$$\boxed{E = F_1 \oplus G, \qquad \dim G = n - d.}$$

Stabilité de G. Soit $x \in G$. Par définition,

$$\varphi(u^j(x)) = 0 \qquad \text{pour } j \in [\![0, d-1]\!].$$

Nous allons montrer que $\varphi(u^d(x)) = 0$ également. Supposons au contraire que $b = \varphi(u^d(x)) \neq 0$. En particulier $x \neq 0$. Considérons une relation linéaire

$$\sum_{i=0}^{d} c_i u^i(x) = 0.$$

En appliquant φ, tous les termes sauf celui d'indice d s'annulent ; on obtient $c_d b = 0$, donc $c_d = 0$. Appliquons ensuite $\varphi \circ u$ à la relation restante : les indices $i \leq d-2$ donnent des valeurs $\varphi(u^{i+1}(x))$ nulles ; il reste $c_{d-1} b = 0$, donc $c_{d-1} = 0$. Plus généralement, lorsque $c_d, \dots, c_{d-j+1}$ ont été annulés, l'application de $\varphi \circ u^j$ impose $c_{d-j} b = 0$: les exposants des autres termes sont strictement inférieurs à d. On obtient ainsi successivement $c_{d-2} = \cdots = c_0 = 0$. La famille $B(x, d+1)$ serait donc libre, ce qui donnerait $d(x) \geq d+1$, contrairement au choix maximal de d.

Ainsi $\varphi(u^d(x)) = 0$. Pour tout $j \in [\![0, d-1]\!]$, on a alors $\varphi(u^j(u(x))) = \varphi(u^{j+1}(x)) = 0$, et donc $u(x) \in G$. Finalement,

$$\boxed{u(G) \subset G.}$$

49. Restriction cyclique au premier facteur.

Le sous-espace $F_1 = E_u(e)$ est stable par u, d'après la question 4. La famille $B(e, d)$ en est une base. Ses termes sont les d premiers itérés de e par l'endomorphisme $u_{|F_1}$, puisque $e \in F_1$ et que ce sous-espace est stable. Par définition,

$$\boxed{u_{|F_1} \text{ est cyclique.}}$$

50. Longueur des chaînes dans G.

Le nombre $d = d(e)$ a été choisi maximal parmi les valeurs $d(x)$ pour $x \neq 0$ dans E. En particulier,

$$\boxed{\forall e' \in G \setminus \{0\}, \quad d(e') \leq d.}$$

La stabilité de G assure aussi que tous les itérés de e' appartiennent à G, donc leur famille libre comporte au plus $\dim G$ vecteurs.

51. Preuve de la propriété (R).

On raisonne par récurrence sur la dimension de l'espace. En dimension 1, l'espace lui-même est un unique facteur cyclique : la propriété est vraie. Supposons-la vraie en toute dimension strictement inférieure à n, et considérons un endomorphisme d'un espace de dimension n. Si c'est une homothétie, la question 41 donne la décomposition. Sinon, on choisit e de longueur maximale $d \geq 2$. Si $d = n$, la question 43 s'applique. Dans le cas restant, les questions 48 et 49 fournissent

$$E = F_1 \oplus G,$$

où les deux sous-espaces sont stables, $u_{|F_1}$ est cyclique et $1 \leq \dim G = n - d < n$. L'hypothèse de récurrence, appliquée à $u_{|G}$, donne des sous-espaces non nuls $F_2, \dots, F_p$ tels que

$$G = F_2 \oplus \cdots \oplus F_p,$$

stables par $u_{|G}$, et dont les restrictions sont cycliques. Comme ces sous-espaces sont inclus dans G, leur stabilité par $u_{|G}$ est exactement leur stabilité par u. En ajoutant le facteur F_1, on obtient donc

$$\boxed{E = F_1 \oplus \cdots \oplus F_p, \quad u(F_i) \subset F_i, \quad u_{|F_i} \text{ cyclique.}}$$

Chaque facteur étant de dimension au moins 1, la somme de leurs dimensions est n et impose $1 \leq p \leq n$. Ainsi

(R) est vraie pour tout endomorphisme d'un espace réel de dimension finie.

Corrigé – Partie III – Application aux endomorphismes nilpotents.

52. Matrice dans une décomposition en sous-espaces stables.

Notons A_k la matrice de $u_{|F_k}$ dans $\mathcal{B}_{F_k}$. Lorsque ces bases sont concaténées, les images des vecteurs de F_k restent dans F_k ; leurs coordonnées dans tous les autres facteurs sont donc nulles. La matrice de u est ainsi diagonale par blocs :

$$\begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & A_p \end{pmatrix}.$$

53. Matrice d'un endomorphisme nilpotent.

Appliquons (R) à u, qui est nilpotent. Pour éviter de confondre le nombre de facteurs avec l'indice de nilpotence de l'énoncé, notons q le nombre de facteurs, et $r_i = \dim F_i$. La restriction $u_i = u_{|F_i}$ est nilpotente, puisque toute puissance annulant u annule aussi u_i. Elle est également cyclique. Par la question 31, son indice de nilpotence vaut donc r_i. Il existe $v_i \in F_i$ tel que $B(v_i, r_i)$ soit une base de F_i. Dans cette base, u_i envoie chaque vecteur sur le suivant, sauf le dernier dont l'image est nulle. Sa matrice est donc

$$N_{r_i} = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 1 & 0 & \ddots & \vdots \\ 0 & \ddots & \ddots & 0 \\ 0 & \cdots & 1 & 0 \end{pmatrix},$$

avec $N_1 = (0)$ si $r_i = 1$. En concaténant ces bases, la question 52 donne $T = \operatorname{diag}(N_{r_1}, \ldots, N_{r_q})$. Cette matrice est triangulaire inférieure ; les seuls coefficients éventuellement non nuls sont ceux immédiatement sous la diagonale. Ils valent 1 à l'intérieur d'un bloc et 0 entre deux blocs. Ainsi

$$t_{i,i} = 0, \qquad t_{i,i-1} \in \{0, 1\} \ (i \geq 2), \qquad t_{i,j} = 0 \text{ dans tous les autres cas.}$$

Corrigé – Partie III – Une matrice est semblable à sa transposée.

54. Produit d'une matrice compagnon par une matrice symétrique.

On suppose u cyclique, et l'on travaille dans la base $B(e, n)$. Pour alléger les formules, on convient qu'une somme dont la borne supérieure est négative est vide et vaut 0. La colonne d'indice $j+1$ de S, pour $0 \leq j \leq n-1$, donne

$$f(u^j(e)) = u^{n-j-1}(e) - \sum_{k=0}^{n-j-2} a_{k+j+1} u^k(e).$$

En particulier,

$$f(e) = u^{n-1}(e) - \sum_{k=0}^{n-2} a_{k+1} u^k(e).$$

En appliquant u puis en utilisant la relation $u^n(e) = \sum_{k=0}^{n-1} a_k u^k(e)$, on obtient

$$u(f(e)) = u^n(e) - \sum_{k=0}^{n-2} a_{k+1} u^{k+1}(e) = a_0 e.$$

De même,

$$f(u(e)) = u^{n-2}(e) - \sum_{k=0}^{n-3} a_{k+2} u^k(e),$$

$$u(f(u(e))) = u^{n-1}(e) - \sum_{k=0}^{n-3} a_{k+2} u^{k+1}(e).$$

Plus généralement,

$$\boxed{\begin{array}{c} u(f(e)) = a_0 e, \\ u(f(u^j(e))) = u^{n-j}(e) - \displaystyle\sum_{k=0}^{n-j-2} a_{k+j+1} u^{k+1}(e) \quad (1 \leq j \leq n-2). \end{array}}$$

Enfin $f(u^{n-1}(e)) = e$, et donc

$$\boxed{u(f(u^{n-1}(e))) = u(e).}$$

La matrice de la composée $u \circ f$ est AS. Sa première colonne est $(a_0, 0, \ldots, 0)$; toutes les autres colonnes ont une première coordonnée nulle. Pour une colonne d'indice $\ell = j+1 \geq 2$ et une ligne $i \geq 2$, les formules précédentes donnent le coefficient $-a_{i+\ell-2}$ lorsque $i + \ell \leq n+1$, le coefficient 1 lorsque $i + \ell = n+2$, et le coefficient 0 au-delà. Ce sont exactement les coefficients de la matrice S_1 de l'énoncé. Comme ces coefficients ne dépendent que de la somme des indices, S_1 est symétrique, et

$$\boxed{AS = S_1, \qquad {}^tS_1 = S_1.}$$

55. Inversibilité de S et factorisation de A.

Soit $X = (x_1, \ldots, x_n)$ un vecteur colonne tel que $SX = 0$. La dernière ligne de S impose $x_1 = 0$; la ligne précédente donne ensuite $x_2 = 0$. Plus généralement, la ligne d'indice $n - r + 1$ a un coefficient 1 en colonne r, des coefficients éventuellement non nuls dans les colonnes précédentes, et des coefficients nuls dans les colonnes suivantes. Une fois $x_1, \ldots, x_{r-1}$ annulés, cette ligne impose $x_r = 0$. On obtient ainsi $X = 0$, donc S est injective et, comme elle est carrée, inversible. Posons $S_2 = S^{-1}$. Puisque S est symétrique,

$${}^tS_2 = {}^t(S^{-1}) = ({}^tS)^{-1} = S^{-1} = S_2.$$

En multipliant $AS = S_1$ à droite par S^{-1},

$$\boxed{A = S_1 S_2, \qquad {}^tS_1 = S_1, \qquad {}^tS_2 = S_2, \qquad S_2 \text{ inversible.}}$$

56. Transport de la factorisation dans la base canonique.

Avec la matrice de passage P de l'énoncé, $M = PAP^{-1}$. En insérant ${}^tP({}^tP)^{-1} = I_n$, la factorisation précédente donne

$$\boxed{M = PS_1{}^tP\,({}^tP)^{-1}S_2P^{-1}.}$$

Posons

$$V = PS_1{}^tP, \qquad W = ({}^tP)^{-1}S_2P^{-1}.$$

La transposition d'un produit renverse l'ordre de ses facteurs, et S_1, S_2 sont symétriques. Ainsi

$${}^tV = P{}^tS_1{}^tP = V, \qquad {}^tW = ({}^tP)^{-1}{}^tS_2P^{-1} = W.$$

La matrice W est inversible, puisqu'elle est un produit de matrices inversibles. On a donc

$$\boxed{M = VW, \qquad V, W \text{ symétriques}, \qquad W \text{ inversible.}}$$

La propriété (S) est démontrée dans le cas cyclique.

57. Similitude avec la transposée dans le cas cyclique.

La factorisation $M = VW$ avec V, W symétriques donne ${}^tM = WV$. Prenons $Q = W^{-1}$. Cette matrice est inversible et symétrique, puisque l'inverse d'une matrice symétrique inversible est symétrique. On a

$$Q^{-1}MQ = W(VW)W^{-1} = WV = {}^tM.$$

Comme $W = ({}^tP)^{-1}S^{-1}P^{-1}$, on peut écrire explicitement

$$\boxed{Q = W^{-1} = PS{}^tP, \qquad {}^tM = Q^{-1}MQ.}$$

Ainsi M est semblable à sa transposée.

58. Similitude avec la transposée dans le cas général.

Par (R), il existe une base de E dans laquelle la matrice de u est

$$A = \operatorname{diag}(A_1, \ldots, A_p),$$

chaque bloc A_i représentant une restriction cyclique. Pour chaque bloc de taille au moins 2, la question 57 donne une matrice symétrique inversible Q_i telle que ${}^tA_i = Q_i^{-1}A_iQ_i$. Pour un bloc de taille 1, on choisit simplement $Q_i = (1)$: la même identité est vraie. En posant $Q_0 = \operatorname{diag}(Q_1, \ldots, Q_p)$, les produits par blocs donnent

$${}^tA = Q_0^{-1}AQ_0.$$

La matrice Q_0 est symétrique et inversible. Soit P la matrice de passage telle que $M = PAP^{-1}$. Posons $Q = PQ_0{}^tP$, qui est également symétrique et inversible. Alors

$$\begin{aligned} Q^{-1}MQ &= ({}^tP)^{-1}Q_0^{-1}P^{-1}(PAP^{-1})PQ_0{}^tP \\ &= ({}^tP)^{-1}Q_0^{-1}AQ_0{}^tP \\ &= ({}^tP)^{-1}{}^tA{}^tP = {}^t(PAP^{-1}) = {}^tM. \end{aligned}$$

Finalement,

$$\boxed{\forall M \in M_n(\mathbb{R}), \quad \exists Q \text{ symétrique et inversible}, \quad {}^tM = Q^{-1}MQ.}$$

En particulier, toute matrice réelle est semblable à sa transposée.