DS7 Corrigé

Exercice 1

$$L_i \leftarrow L_i - L_n \quad i = 1, \dots, n-1$$

$$D_n = \begin{vmatrix} a_1 & a_2 & \cdots & a_n \\ a_1 & a_1 & \ddots & \vdots \\ \vdots & & \ddots & a_2 \\ a_1 & \cdots & & a_1 \end{vmatrix} = \begin{vmatrix} 0 & a_2-a_1 & \cdots & a_n - a_1 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & a_2-a_1 \\ a_1 & \cdots & & a_1 \end{vmatrix} = (-1)^{n+1} a_1 \begin{vmatrix} a_2-a_1 & \cdots & a_n-a_1 \\ 0 & \ddots & \vdots \\ 0 & \cdots \; 0 & a_2-a_1 \end{vmatrix}$$

$$= (-1)^{n+1} a_1 (a_2-a_1)^{n-1} = \boxed{a_1 (a_1-a_2)^{n-1}}$$

Exercice 2

$\omega = e^{\frac{2i\pi}{n}}$, $S_p = a_0 + a_1 \omega^p + \dots + a_{n-1} (\omega^p)^{n-1}$ (et non $a_2 (\omega^p)^{n-1}$).

A est une matrice circulante (une ligne est déduite de la précédente par permutation circulaire).

a) pour $1 \leq i,j \leq n$, on a $M_{ij} = \omega^{(i-1)(j-1)}$ donc $(M^2)_{ij} = \sum_{k=1}^{n} M_{ik} M_{kj} = \sum_{k=1}^{n} \omega^{(i-1)(k-1)} \omega^{(k-1)(j-1)}$

$$= \sum_{k=1}^{n} \omega^{(k-1)(i+j-2)} = \sum_{k=1}^{n} (\omega^{i+j-2})^{k-1} = \sum_{k=0}^{n-1} (\omega^{i+j-2})^k$$

or $(\omega^{i+j-2})^n = (\omega^n)^{i+j-2} = 1$ car $\omega^n = 1$

donc $\underline{\text{si } \omega^{i+j-2} \neq 1}$, $\sum_{k=0}^{n-1} (\omega^{i+j-2})^k = 0$ (cours sur les racines de l'unité)

pour $i,j \in [\![1,n]\!]$, on a $0 \leq i+j-2 \leq 2n-2$, $\underline{\omega^{i+j-2} = 1} \iff i+j-2 \equiv 0 \, [n]$

donc $\omega^{i+j-2} = 1 \iff i+j-2 = 0$ ou $n \iff i=j=1$ ou $i+j = n+2$

on a alors $M_{ij} = \sum_{k=0}^{n-1} (\omega^{i+j-2})^k = n$

ainsi $\boxed{M^2 = \begin{vmatrix} n & 0 & \cdots & \cdots & 0 \\ 0 & 0 & \cdots & 0 & n \\ \vdots & \vdots & & n & 0 \\ \vdots & 0 & ⋰ & ⋰ & \vdots \\ 0 & n & 0 & \cdots & 0 \end{vmatrix}_{[n]}}$ ainsi $\det M^2 = n \begin{vmatrix} 0 & \cdots & 0 & n \\ \vdots & ⋰ & ⋰ & 0 \\ 0 & ⋰ & & \vdots \\ n & 0 & \cdots & 0 \end{vmatrix}_{[n-1]}$

$$= n (-1)^n n \begin{vmatrix} 0 & \cdots & 0 & n \\ \vdots & ⋰ & ⋰ & 0 \\ n & 0 & \cdots & 0 \end{vmatrix}_{[n-2]}$$

donc $\det M^2 = n (-1)^n n (-1)^{n-1} n \cdots (-1)^2 n$

Problème Endomorphismes cycliques

Partie I. Exemples.

1. Dans cette question, on prend $E = \mathbb{R}^3$. Considérons l'application suivante de $\mathbb{R}^3$ dans $\mathbb{R}^3$:

$$u(x, y, z) = (6z, x - 11z, y + 6z).$$

(a) Soient $v = (x_1, y_1, z_1), w = (x_2, y_2, z_2) \in \mathbb{R}^3$ et $\lambda, \mu \in \mathbb{R}$. On a :

$$\lambda v + \mu w = (\lambda x_1 + \mu x_2, \lambda y_1 + \mu y_2, \lambda z_1 + \mu z_2).$$

$$\begin{aligned} u(\lambda v + \mu w) &= (6(\lambda z_1 + \mu z_2), (\lambda x_1 + \mu x_2) - 11(\lambda z_1 + \mu z_2), (\lambda y_1 + \mu y_2) + 6(\lambda z_1 + \mu z_2)) \\ &= \lambda(6z_1, x_1 - 11z_1, y_1 + 6z_1) + \mu(6z_2, x_2 - 11z_2, y_2 + 6z_2) \\ &= \lambda u(v) + \mu u(w) \end{aligned}$$

Donc u est un endomorphisme de $\mathbb{R}^3$.

(b) On a :

$$u(1, 0, 0) = (0, 1, 0) \quad ; \quad u^2(1, 0, 0) = u(0, 1, 0) = (0, 0, 1).$$

Ainsi, $(1, 0, 0), (0, 1, 0), (0, 0, 1) \in Vect(u^k(1, 0, 0)/k \in \mathbb{N})$. Comme $((1, 0, 0), (0, 1, 0), (0, 0, 1))$ est une famille génératrice de $\mathbb{R}^3$ (c'est la base canonique !), on a donc :

$$Vect(u^k(1, 0, 0)/k \in \mathbb{N}) = \mathbb{R}^3.$$

Ainsi u est un endomorphisme cyclique.

2. Dans cette question, on prend $E = \mathbb{R}_n[X]$. On considère l'endomorphisme de dérivation u défini pour tout $P \in E$ par $u(P) = P'$.

(a) Soit $P_0 \in E$ un polynôme de degré $d \geq 0$. On a :

$$u^k(P_0) = P_0^{(k)} \text{ pour } 0 \leq k \leq d \quad \text{et} \quad u^k(P_0) = 0 \text{ pour } k > d.$$

Ainsi, pour tout $k \in \mathbb{N}$, $u^k(P_0) \in \mathbb{R}_d[X]$. Comme de plus, $\mathbb{R}_d[X]$ est un espace vectoriel, on obtient :

$$Vect(u^k(P_0)/k \in \mathbb{N}) \subset \mathbb{R}_d[X].$$

De plus, $Vect(u^k(P_0)/k \in \mathbb{N}) = Vect(u^k(P_0)/0 \leq k \leq d)$, et la famille de polynômes $(P_0, u(P_0), \ldots, u^d(P_0))$ est échelonnée en degré. C'est donc une famille libre, et $\dim(Vect(u^k(P_0)/k \in \mathbb{N})) = d + 1$. Comme on a $\dim \mathbb{R}_d[X] = d + 1$, on obtient finalement :

$$Vect(u^k(P_0)/k \in \mathbb{N}) = \mathbb{R}_d[X].$$

(b) Prenons P_0 de degré n (par exemple $P_0 = X^n$). Alors d'après ce qu'on a fait, on a :

$$Vect(u^k(P_0)/k \in \mathbb{N}) = \mathbb{R}_n[X] = E.$$

Donc u est bien cyclique également.

3. Dans cette question, E est un $\mathbb{K}$-espace vectoriel de dimension $n \geq 2$. Soit u un endomorphisme nilpotent d'indice $p \geq 2$ (i.e. $u^p = 0_{\mathcal{L}(E)}$ et $u^{p-1} \neq 0_{\mathcal{L}(E)}$).

(a) Prenons $x_0 \in E$ tel que $u^{p-1}(x_0) \neq 0_E$ (existe car $u^{p-1} \neq 0_{\mathcal{L}(E)}$). Montrons que $(x_0, u(x_0), \ldots, u^{p-1}(x_0))$ est libre : soient $\lambda_0, \lambda_1, \ldots, \lambda_{p-1} \in \mathbb{K}$ tels que :

$$\lambda_0 x_0 + \lambda_1 u(x_0) + \cdots + \lambda_{p-1} u^{p-1}(x_0) = 0_E.$$

On applique u^{p-1} à cette égalité :

$$\lambda_0 u^{p-1}(x_0) = 0_E \quad \Rightarrow \quad \lambda_0 = 0(\text{ car } u^{p-1}(x_0) \neq 0_E).$$

On obtient en remplaçant $\lambda_1 u(x_0) + \cdots + \lambda_{p-1} u^{p-1}(x_0) = 0_E$. En appliquant u^{p-2}, on obtient $\lambda_1 = 0$, et ainsi de suite, $\lambda_k = 0$ pour tout k.

Ainsi la famille $(x_0, u(x_0), \ldots, u^{p-1}(x_0))$ est libre. Son cardinal est donc inférieur ou égal à la dimension de E, soit $p \leq n$.

(b) $\Rightarrow$ Supposons que u est cyclique, alors il existe $x_0 \in E$ tel que :

$$E = Vect(u^k(x_0)/k \in \mathbb{N}) = Vect(x_0, u(x_0), u^2(x_0), \ldots, u^{p-1}(x_0)).$$

La famille $(x_0, u(x_0), u^2(x_0), \ldots, u^{p-1}(x_0))$ est donc génératrice, et son cardinal est supérieur à la dimension de E, soit $p \geq n$. Comme on a de plus $p \leq n$, on obtient ainsi que $p = n$.

$\Leftarrow$ Supposons que $p = n$. On sait qu'il existe x_0 tel que $(x_0, u(x_0), \ldots, u^{n-1}(x_0))$ soit une famille libre. Comme elle est de cardinal n, c'est donc une base de E. Ainsi,

$$Vect(u^k(x_0)/k \in \mathbb{N}) = Vect(x_0, u(x_0), u^2(x_0), \ldots, u^{n-1}(x_0)) = E$$

et u est bien un endomorphisme cyclique.

Partie II. Étude générale.

Dans cette partie, on note u un endomorphisme cyclique de l'espace vectoriel E, avec E de dimension $n \geq 1$. On fixe $x_0 \in E$ tel que $E = Vect(u^k(x_0)/k \in \mathbb{N})$.

1. (a) La famille $(x_0, u(x_0), \ldots, u^n(x_0))$ est de cardinal $n+1$ dans un espace vectoriel E de dimension n, elle est donc liée.

(b) Tout d'abord, notons que comme $E \neq \{0_E\}$ et que $E = Vect(u^k(x_0)/k \in \mathbb{N})$, alors $x_0 \neq 0_E$. Considérons l'ensemble $A = \{k \in \mathbb{K}/(x_0, u(x_0), \ldots, u^k(x_0)) \text{ libre}\}$. C'est un ensemble non vide de $\mathbb{N}$ (car $0 \in A$, la famille (x_0) étant libre), et majorée par n ($(x_0, u(x_0), \ldots, u^n(x_0))$ est liée, et toute surfamille de cette famille est donc liée). On en déduit qu'il existe un entier p, maximal, pour lequel la famille $(x_0, u(x_0), \ldots, u^p(x_0))$ soit libre.

(c) Par définition de p, la famille $(x_0, u(x_0), \ldots, u^p(x_0))$ est libre et $(x_0, u(x_0), \ldots, u^p(x_0), u^{p+1}(x_0))$ est liée. Par le cours, on sait alors que $u^{p+1}(x_0) \in Vect(x_0, u(x_0), \ldots, u^p(x_0))$

(d) On procède par récurrence.

- **Initialisation.** Pour tout $0 \leq k \leq p$, on a bien $u^k(x_0) \in Vect(x_0, u(x_0), \ldots, u^p(x_0))$ donc la propriété est vraie aux rang $0 \leq k \leq p$. Elle est vraie également au rang $p+1$ par la question précédente.
- **Hérédité.** Soit $k \geq p$ et supposons la propriété vraie au rang k. Montrons la propriété au rang $k+1$.

  Par hypothèse de récurrence, on a $u^k(x_0) \in Vect(x_0, u(x_0), \ldots, u^p(x_0))$. Il existe donc $(\lambda_0, \ldots, \lambda_{p-1}, \lambda_p) \in \mathbb{K}^{p+1}$ tels que :

  $$u^k(x_0) = \lambda_0 x_0 + \cdots + \lambda_{p-1} u^{p-1}(x_0) + \lambda_p u^p(x_0)).$$

  On compose par u :

  $$u^{k+1}(x_0) = \lambda_0 u(x_0) + \cdots + \lambda_{p-1} u^p(x_0) + \lambda_p u^{p+1}(x_0)).$$

  Or on a $u(x_0), \ldots, u^p(x_0), u^{p+1}(x_0)) \in Vect(x_0, u(x_0), \ldots, u^p(x_0))$, donc $u^{k+1}(x_0) \in Vect(x_0, u(x_0), \ldots, u^p(x_0))$. D'où la propriété au rang $k+1$.

On conclut par principe de récurrence.

(e) On a montré que pour tout $k \in \mathbb{N}$, $u^k(x_0) \in Vect(x_0, u(x_0), \ldots, u^p(x_0))$. Ainsi, on a :

$$E = Vect(u^k(x_0)/k \in \mathbb{N}) = Vect(x_0, u(x_0), \ldots, u^p(x_0)).$$

La famille $(x_0, u(x_0), \ldots, u^p(x_0))$ est donc génératrice de E. Comme c'est une famille libre par définition de p, c'est donc une base de E. Son cardinal est donc égal à la dimension de E, soit $p + 1 = n$.

2. (a) On a montré précédemment que $u^n(x_0) \in Vect(x_0, u(x_0), \ldots, u^{n-1}(x_0))$, donc il existe $(p_0, \ldots, p_{n-1}) \in \mathbb{K}^n$ tels que :

$$u^n(x_0) = p_0 x_0 + p_1 u(x_0) + \cdots + p_{n-1} u^{n-1}(x_0).$$

Dans la suite, on posera $P(X) = X^n - p_{n-1}X^{n-1} - \cdots - p_1 X - p_0 \in \mathbb{K}[X]$.

(b) On a $P(u) = u^n - p_{n-1}u^{n-1} - \cdots - p_1 u - p_0 Id_E \in \mathbb{K}[X]$, d'où en évaluant :

$$P(u)(x_0) = u^n(x_0) - p_{n-1}u^{n-1}(x_0) - \cdots - p_1 u(x_0) - p_0 x_0 = 0_E.$$

$$\begin{aligned} P(u)(u(x_0)) &= u^n(u(x_0)) - p_{n-1}u^{n-1}(u(x_0)) - \cdots - p_1 u(u(x_0)) - p_0 u(x_0) \\ &= u(u^n(x_0) - p_{n-1}u^{n-1}(x_0) - \cdots - p_1 u(x_0) - p_0 x_0) = u(0_E) = 0_E. \end{aligned}$$

De même, on a $P(u)(u^k(x_0)) = 0_E$ pour tout $0 \leq k \leq n-1$.
Ainsi $P(u)$ est un endomorphisme de E qui s'annule sur la base $(x_0, u(x_0), \ldots, u^{n-1}(x_0))$, c'est donc l'endomorphisme nul : $P(u) = 0_{\mathcal{L}(E)}$.
On dit que P est un polynôme annulateur de u.

(c) Montrons que $(Id_E, u, \ldots, u^{n-1})$ est une famille libre de $\mathcal{L}(E)$: soient $(\lambda_0, \ldots, \lambda_{n-1}) \in \mathbb{K}^n$ tels que :

$$\lambda_0 Id_E + \lambda_1 u + \cdots + \lambda_{n-1}u^{n-1} = 0_{\mathcal{L}(E)}.$$

On évalue en x_0 :

$$\lambda_0 x_0 + \lambda_1 u(x_0) + \cdots + \lambda_{p-1}u^{n-1}(x_0) = 0_E.$$

Or la famille de vecteurs $(x_0, u(x_0), \ldots, u^{n-1}(x_0))$ est libre dans E. Donc $\lambda_0 = \lambda_1 = \cdots = \lambda_{n-1} = 0$. Ainsi $(Id_E, u, \ldots, u^{n-1})$ est une famille libre de $\mathcal{L}(E)$.

(d)
- Supposons qu'un tel polynôme $Q = a_0 + a_1 X + \cdots + a_q X^q$ existe : $q < n$ et $Q(u) = 0_{\mathcal{L}(E)}$. Alors on aurait :

$$a_0 Id_E + a_1 u + \cdots + a_q u^q = 0_{\mathcal{L}(E)}$$

Comme $Q \neq 0$, il existe $a_i \neq 0$, et la famille $(Id_E, u, \ldots, u^q)$ serait liée. Mais alors la surfamille $(Id_E, u, \ldots, u^{n-1})$ serait liée également, ce qui est faux car $(Id_E, u, \ldots, u^{n-1})$ est libre.

- Soit $Q = X^n - a_{n-1}X^{n-1} - \cdots - a_1 X - a_0$ un polynôme unitaire de degré n tel que $Q(u) = 0_{\mathcal{L}(E)}$. Alors :

$$u^n - p_{n-1}u^{n-1} - \cdots - p_1 u - p_0 Id_E = u^n - a_{n-1}u^{n-1} - \cdots - a_1 u - a_0 Id_E.$$

D'où :

$$p_{n-1}u^{n-1} + \cdots + p_1 u + p_0 Id_E = a_{n-1}u^{n-1} + \cdots + a_1 u + a_0 Id_E.$$

Par unicité de la décomposition d'un vecteur dans la famille libre $(Id_E, u, \ldots, u^{n-1})$, on en déduit :

$$p_k = a_k \quad \text{pour tout } 0 \leq k \leq n-1.$$

Ainsi $P = Q$, et P est bien l'unique polynôme unitaire de degré n tel que $P(u) = 0_{\mathcal{L}(E)}$.

Le polynôme P est appelé le polynôme minimal de u.

(e) On procède comme précédemment pour trouver ce polynôme : on écrit $u^3(1,0,0)$ en fonction de $(1,0,0), u(1,0,0), u^2(1,0,0)$. Or on a :

$$u(1,0,0) = (0,1,0) \quad ; \quad u^2(1,0,0) = (0,0,1) \quad ; \quad u^3(1,0,0) = (6,-11,6).$$

Ainsi, $u^3(1,0,0) = 6(1,0,0) - 11u(1,0,0) + 6u^2(1,0,0)$ et le polynôme minimal de u est donc :

$$P(X) = X^3 - 6X^2 + 11X - 6.$$

Partie III. Étude du commutant.

1. Tout d'abord $\mathcal{C}(u) \subset \mathcal{L}(E)$ est non vide car l'endomorphisme nul commute bien avec u.

   Soient $f, g \in \mathcal{C}(u)$ et $(\lambda, \mu) \in \mathbb{K}^2$. Montrons que $\lambda f + \mu g \in \mathcal{C}(u)$:

   $$u \circ (\lambda f + \mu g) = \lambda u \circ f + \mu u \circ g = \lambda f \circ u + \mu g \circ = (\lambda f + \mu g) \circ u.$$

   Donc le commutant $\mathcal{C}(u) = \{v \in \mathcal{L}(E)/u \circ v = v \circ u\}$ est un sous-espace vectoriel de $\mathcal{L}(E)$.

2. On a déjà de manière évidente que pour tout $k \in \mathbb{N}$, $u^k \in \mathcal{C}(u)$. Comme de plus $\mathcal{C}(u)$ est un sous-espace vectoriel de $\mathcal{L}(E)$, les combinaisons linéaires de tels vecteurs sont aussi dans $\mathcal{C}(u)$. Ainsi pour tout $P \in \mathbb{K}[X]$, on a bien $P(u) \in \mathcal{C}(u)$. D'où l'inclusion $\mathbb{K}[u] \subset \mathcal{C}(u)$

3. (a) Soient deux endomorphismes v et w de $\mathcal{C}(u)$. Supposons que $v(x_0) = w(x_0)$, et montrons que $v = w$. On a pour tout $k \in \mathbb{N}^*$,

   $$v(u^k(x_0)) = v \circ u^k(x_0) = u^k \circ v(x_0) = u^k \circ w(x_0) = w(u^k(x_0)).$$

   Ainsi v et w coïncident sur la base $(x_0, \ldots, u^{n-1}(x_0))$. Elles sont donc égales.

   (b) Soit $v \in \mathcal{C}(u)$.

   i. Comme $(x_0, \ldots, u^{n-1}(x_0))$ est une base de E, donc une famille génératrice de E, il existe bien $(a_0, \ldots, a_{n-1}) \in \mathbb{K}^n$ tel que $v(x_0) = a_{n-1}u^{n-1}(x_0) + \cdots + a_1 u(x_0) + a_0 x_0$.

   ii. Posons $w = a_{n-1}u^{n-1} + \cdots + a_1 u + a_0 Id_E$. On a clairement que w commute avec u (c'est un polynôme en u !). De plus on a $v(x_0) = w(x_0)$. Par la question précédente, on en déduit immédiatement que $v = w$.

4. On a déjà que $\mathbb{K}[u] \subset \mathcal{C}(u)$. Réciproquement, on vient de montrer que si $v \in \mathcal{C}(u)$, alors $v \in \mathbb{K}[u]$. On en déduit donc que $\mathcal{C}(u) = \mathbb{K}[u]$.

5. On sait déjà que la famille $(Id_E, u, \ldots, u^{n-1})$ est libre, et qu'il existe un unique polynôme P de degré n et unitaire tel que $P(u) = 0_{\mathcal{L}(E)}$ (c'est le polynôme minimal). On va montrer que :

   $$K[u] = Vect(Id_E, u, \ldots, u^{n-1}).$$

   Prenons un élément de $K[u]$, il est de la forme $A(u)$ avec $A \in \mathbb{K}[X]$. On fait la division euclidienne de A par P : il existe un couple $(Q, R) \in \mathbb{K}[X]^2$ tels que :

   $$\begin{cases} A = QP + R \\ \deg(R) < n \end{cases}$$

   On évalue en u :

   $$A(u) = Q(u) \circ P(u) + R(u).$$

   Or $P(u) = 0_{\mathcal{L}(E)}$, donc $A(u) = R(u)$. Comme enfin $\deg(R) < n$, on en déduit que $R(u) \in Vect(Id_E, u, \ldots, u^{n-1})$. Finalement, on a bien que :

   $$\mathcal{C}(u) = K[u] = Vect(Id_E, u, \ldots, u^{n-1}).$$

   La famille $(Id_E, u, \ldots, u^{n-1})$ étant libre et génératrice de $\mathcal{C}(u)$, c'est donc une base de cet espace, et $\dim(\mathcal{C}(u)) = n$.