

DEVOIR SURVEILLÉ 1 (4H)

Les calculatrices sont autorisées pour la partie 2.4 .

Problème 1 : où l'on revisite le résultat du DM 3 plus simplement

Dans tout le problème, on fixe E un espace vectoriel complexe de dimension $n \geq 1$ (et toutes les notions d'algèbre linéaire sont à entendre sur le corps des scalaires $\mathbb{C}$). On note $D_n(\mathbb{C})$ le sous-espace vectoriel des matrices diagonales dans $M_n(\mathbb{C})$.

On note $\zeta = \exp\left(i\frac{2\pi}{n}\right)$.

On définit les matrices :

$$\Delta = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & \zeta & 0 & \cdots & 0 & 0 \\ 0 & 0 & \zeta^2 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \zeta^{n-2} & 0 \\ 0 & 0 & 0 & \cdots & 0 & \zeta^{n-1} \end{pmatrix} \quad \text{et} \quad \Sigma = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix} \in M_n(\mathbb{C}).$$

Q 0) Résultat à admettre ici, à démontrer en D.M. 4 : On considère deux endomorphismes $u, v \in \mathcal{L}(E)$ vérifiant les relations $u^n = v^n = \text{id}_E$ et $u \circ v = \zeta \cdot (v \circ u)$, alors on admet ici qu'il existe une base $\mathcal{B}$ de E telle que $\text{Mat}_{\mathcal{B}}(u) = \Delta$ et $\text{Mat}_{\mathcal{B}}(v) = \Sigma$.

Q 1) (a) Soit $\lambda_0, \dots, \lambda_{n-1} \in \mathbb{C}$ et $P = \sum_{k=0}^{n-1} \lambda_k X^k$. Montrer l'équivalence

$$\sum_{k=0}^{n-1} \lambda_k \Delta^k = 0_{M_n(\mathbb{C})} \Leftrightarrow P = 0_{\mathbb{C}[X]}.$$

(b) En déduire que $(I_n, \Delta, \Delta^2, \dots, \Delta^{n-1})$ est une base de $D_n(\mathbb{C})$.

(c) Déterminer le polynôme minimal de Δ .

Q 2) (a) Pour tout $p \in \llbracket 0, n-1 \rrbracket$, on considère $V_p = \text{Vect} \{E_{i,j} \mid (i,j) \in \llbracket 1, n \rrbracket^2, i \equiv j + p \pmod{n}\}$. Que vaut V_0 ?

(b) Montrer $M_n(\mathbb{C}) = \bigoplus_{p=0}^{n-1} V_p$.

(c) En déduire que la famille $\mathcal{F} = (\Sigma^p \Delta^k)_{0 \leq p, k \leq n-1}$ est une base de $M_n(\mathbb{C})$.

(d) On considère la all-ones matrix $H = (1)_{1 \leq i, j \leq n}$. Décomposer H dans la base $\mathcal{F}$.

Q 3) Soit $P \in GL_n(\mathbb{C})$. Montrer que $\Psi_P : \begin{cases} M_n(\mathbb{C}) & \rightarrow M_n(\mathbb{C}) \\ M & \mapsto PMP^{-1} \end{cases}$ est un endomorphisme de la $\mathbb{C}$ -algèbre $M_n(\mathbb{C})$.

On va maintenant montrer la réciproque de ce résultat.

Q 4) On fixe donc un endomorphisme φ de la $\mathbb{C}$ -algèbre $M_n(\mathbb{C})$.

(a) On considère u (resp. v) l'endomorphisme de $\mathbb{C}^n$ canoniquement associé à $\varphi(\Delta)$ (resp. $\varphi(\Sigma)$). Montrer qu'il existe $P \in GL_n(\mathbb{C})$ tel que $\varphi(\Delta) = P\Delta P^{-1}$ et $\varphi(\Sigma) = P\Sigma P^{-1}$.

(b) En déduire qu'il existe $P \in GL_n(\mathbb{C})$ tel que $\varphi = \Psi_P$.

N.B. Les personnes ayant travaillé la partie 3 du DM3 se diront à juste titre que cette preuve est plus simple. Mais on utilise ici l'hypothèse que le corps de base est $\mathbb{C}$.

Problème 2 : Résultant de deux polynômes

Soit p et q deux entiers naturels non nuls, soit

$$P = \sum_{k=0}^p a_k X^k \quad \text{et} \quad Q = \sum_{k=0}^q b_k X^k$$

deux polynômes de $\mathbb{C}[X]$ avec $a_p \neq 0, b_q \neq 0$. Le résultant des polynômes P et Q est le nombre complexe noté $\text{Res}(P, Q)$:

$$\text{Res}(P, Q) = \begin{vmatrix} a_0 & & & b_0 & & \\ a_1 & \ddots & & b_1 & \ddots & \\ \vdots & & a_0 & \vdots & & b_0 \\ a_p & & a_1 & a_0 & \vdots & b_1 \\ & \ddots & \vdots & a_1 & b_q & \vdots \\ & & a_p & \vdots & & \ddots \\ & & & a_p & & b_q \end{vmatrix}.$$

C'est un déterminant $q + p$ colonnes, dont les q premières colonnes représentent les coefficients du polynôme P et les p suivantes représentent les coefficients du polynôme Q ; les positions non remplies étant des zéros. Par exemple, si $P = 1 + 2X + 3X^2$ et $Q = 4 + 5X + 6X^2 + 7X^3$,

$$\text{Res}(P, Q) = \begin{vmatrix} 1 & 0 & 0 & 4 & 0 \\ 2 & 1 & 0 & 5 & 4 \\ 3 & 2 & 1 & 6 & 5 \\ 0 & 3 & 2 & 7 & 6 \\ 0 & 0 & 3 & 0 & 7 \end{vmatrix}.$$

La matrice servant à définir $\text{Res}(P, Q)$ pourra être notée $M_{P,Q}$:

$$\text{Res}(P, Q) = \det M_{P,Q}.$$

On note $E = \mathbb{C}_{q-1}[X] \times \mathbb{C}_{p-1}[X]$ et $F = \mathbb{C}_{p+q-1}[X]$.

Soit u l'application de E vers F définie pour $(A, B) \in E$ par : $u(A, B) = PA + QB$.

2.1. Cas où u est bijective

- (a) Démontrer que u est une application linéaire.
- (b) Si on suppose que u est bijective, démontrer que P et Q sont premiers entre eux.
- (c) Si on suppose que P et Q sont premiers entre eux, déterminer $\text{Ker } u$ et en déduire que u est bijective.

2.2. Matrice de u

On note $\mathcal{B} = ((1, 0), (X, 0), \dots, (X^{q-1}, 0), (0, 1), (0, X), \dots, (0, X^{p-1}))$ une base de E et $\mathcal{B}' = (1, X, \dots, X^{p+q-1})$ la base canonique de F .

- (a) Déterminer la matrice de u par rapport aux bases $\mathcal{B}$ et $\mathcal{B}'$.
- (b) Démontrer que $\text{Res}(P, Q) \neq 0$ si et seulement si, P et Q sont premiers entre eux (donc $\text{Res}(P, Q) = 0$ si et seulement si, P et Q ont au moins une racine commune complexe).
- (c) Calculer $\text{Res}(P, Q)$ si $P = \sum_{k=0}^n a_k X^k$ et $Q = b_1 X + b_0$ et vérifier le résultat du b) sur cet exemple.

2.3. Racine multiple

- (a) Démontrer qu'un polynôme P de $\mathbb{C}[X]$ admet une racine multiple dans $\mathbb{C}$ si et seulement si, $\text{Res}(P, P') = 0$.
- (b) On appelle *discriminant* de P le nombre $\Delta(P) = \text{Res}(P, P')$. Soit $P = aX^2 + bX + c$. Calculer $\Delta(P)$ et commentez.
- (c) Déterminer une condition nécessaire et suffisante sur les nombres complexes a et b pour que $P = X^3 + aX + b$ ait une racine multiple dans $\mathbb{C}$.

2.4. Application à l'équation de Bézout

Dans cette question, on note $P = X^4 + X^3 + 1$ et $Q = X^3 - X + 1$.

- (a) (i) En utilisant ce qui précède, comment pourrait-on démontrer que les polynômes P et Q sont premiers entre eux ? On ne demande PAS de faire le calcul correspondant. (ii) Donner une autre démonstration, avec moins de calcul, du fait que P et Q sont premiers entre eux.
- (b) On cherche un couple (A_0, B_0) de polynômes de $\mathbb{C}[X]$ tel que

$$PA_0 + QB_0 = 1.$$

Expliquer comment on pourrait trouver un tel couple en utilisant la matrice de u puis donner un couple solution à l'aide d'une autre méthode.

- (c) Déterminer tous les couples (A, B) de polynômes de $\mathbb{C}[X]$ vérifiant

$$PA + QB = 1.$$

2.5. Application à l'obtention d'un polynôme annulateur d'une somme de deux nombres algébriques

Un nombre $\alpha \in \mathbb{C}$ est dit *algébrique* (sur $\mathbb{Q}$) si et seulement si il existe $P \in \mathbb{Q}[X] \setminus \{0\}$ tel que $P(\alpha) = 0$.

Le polynôme annulateur unitaire de plus petit degré de α s'appelle *polynôme minimal* de α .

Par exemple $\sqrt{2}$ est algébrique de polynôme minimal $P = X^2 - 2 \in \mathbb{Q}[X]$.

- (a) Montrer que si α est un nombre algébrique, son polynôme minimal P est toujours *irréductible* dans $\mathbb{Q}[X]$.
- (b) Montrer que si α et β sont deux nombres algébriques de polynômes annulateurs respectifs P, Q alors le résultant pour l'indéterminée Y , noté $R_Y(P(Y), Q(X - Y))$ est un polynôme en X , annulateur de $\alpha + \beta$.
- (c) En déduire un polynôme annulateur de $\sqrt{3} + \sqrt{7}$ de degré 4 à coefficients entiers.

Appendice hors D.S. à faire en D.M. 4

2.6. En arithmétique dans $\mathbb{Z}$:

Il s'agit d'expliquer le phénomène suivant que Jean-Paul Delahaye évoque dans son livre *Merveilleux nombres premiers*, Belin, 2000.

Soit n un entier. Les nombres $n^{17} + 9$ et $(n + 1)^{17} + 9$ sont-ils toujours premiers entre eux ?

On montre que c'est vrai pour tout n jusqu'à des milliards de milliards, mais il y a un contre-exemple pour :

$$n = 8424432925592889329288197322308900672459420460792433$$

le facteur commun étant :

$$p = 8936582237915716659950962253358945635793453256935559$$

L'explication est simple :

- on calcule le résultant des polynômes $P(X) = X^{17} + 9$ et $Q(X) = (X + 1)^{17} + 9$ dans $\mathbf{Z}$. On trouve le nombre p . Cela montre que les deux polynômes ont un facteur commun dans $\mathbf{Z}/p\mathbf{Z}$.
- On cherche donc le *pgcd* de ces polynômes dans $\mathbf{Z}/p\mathbf{Z}[X]$. On trouve le polynôme $X - n$. On a donc une racine commune n entre ces deux polynômes modulo p , ce qui signifie que p divise $n^{17} + 9$ et $(n + 1)^{17} + 9$.

Travail à faire : faire tout ceci en Python à l'aide du module `numpy.polynomial` et de la documentation Centrale sur ce module.

2.7. En topologie matricielle (5/2 seulement)

A l'aide du discriminant Δ montrer que l'ensemble $\mathcal{R}$ des matrices ayant n valeurs propres distinctes dans $\mathbb{C}$ est un ouvert de $M_n(\mathbb{C})$, puis que $\mathcal{R}$ est l'intérieur de l'ensemble des matrices diagonalisables dans $M_n(\mathbb{C})$.