

DEVOIR SURVEILLÉ 1 : UNE SOLUTION

Problème 1 : théorème de Skolem-Noether dans $M_n(\mathbb{C})$

D'après un sujet et un corrigé de Maxime Bourrigan.

- Q 1)** a) Le produit de deux matrices diagonales s'effectuant coefficient par coefficient, on a

$$P(\Delta) = \text{diag}(P(1), P(\zeta), \dots, P(\zeta^{n-1})).$$

Ainsi,

$$P(\Delta) = 0_{M_n(\mathbb{C})} \Leftrightarrow \forall k \in [0, n-1], P(\zeta^k) = 0 \Leftrightarrow P = 0_{\mathbb{C}[X]},$$

le sens direct de la dernière équivalence provenant du fait que $P \in \mathbb{C}_{n-1}[X]$ admet n racines distinctes.

- b) La question précédente montre la liberté de cette famille de matrices diagonales. Comme elle possède $n = \dim D_n(\mathbb{C})$ vecteurs, c'est également une base de $D_n(\mathbb{C})$.

N.B. On sait que $\dim D_n(\mathbb{C}) = n$ car $(E_{i,i})_{i=1,\dots,n}$ en est une base.

- c) On sait par le cours que $\dim \mathbb{C}[D] = \deg(\mu_D)$. Par la question a), on sait que $\dim \mathbb{C}[D] \geq n$ donc $\deg(\mu_D) \geq n$. D'autre part $D^n = I$ donc le polynôme minimal est un diviseur unitaire de $X^n - 1$ et de degré au moins n :

$$\mu_D = X^n - 1.$$

- Q 2)** a) On a $V_0 = \text{Vect}(E_{1,1}, \dots, E_{n,n}) = D_n(\mathbb{C})$.

- b) Pour tout $p \in [0, n-1]$, notons $\mathcal{A}_p$ la famille de n matrices $(E_{p+1,1}, \dots, E_{n,n-p}, E_{1,n-p+1}, \dots, E_{p,n})$, si bien que $V_p = \text{Vect}(\mathcal{A}_p)$. On voit que la concaténation $\bigvee_{p=0}^{n-1} \mathcal{A}_p$ de toutes ces familles forme une famille de n^2 matrices, qui n'est rien d'autre que la base canonique, dans un ordre différent. On en déduit que $M_n(\mathbb{C}) = \text{Vect}(\bigvee_{p=0}^{n-1} \mathcal{A}_p) = \bigoplus_{p=0}^{n-1} \text{Vect}(\mathcal{A}_p) = \bigoplus_{p=0}^{n-1} V_p$.

- c) Un calcul direct montre que $\sum E_{i,j} = \sum_{k=1}^n \underbrace{E_{k+1,k} E_{i,j}}_{=0 \text{ si } k \neq i} = E_{i+1,i} E_{i,k} = E_{i+1,j}$, où l'on utilise la

convention que si, dans une matrice de la forme $E_{k,\ell}$, l'indice de ligne k (resp. l'indice de colonne ℓ) n'appartient pas à $[1, n]$, on le remplace par l'unique élément dans $[1, n]$ qui est congru à k (resp. ℓ) modulo n . (De façon moins formelle mais plus claire, k et ℓ sont « à comprendre modulo n »).

- Par une récurrence immédiate, pour tout $p \in [0, n-1]$, $\Sigma^p E_{i,j} = E_{i+p,j}$ (avec la même convention, on ne le précisera plus).

- La matrice Σ est inversible (par exemple parce que l'on voit très facilement que son noyau est nul, ou parce que le fait que $\forall i \in [1, n], \Sigma e_i = e_{i+1}$ entraîne $\forall i \in [1, n], \Sigma^n e_i = e_i$ et donc

$\Sigma^n = I_n$). L'endomorphisme $L_\Sigma : \begin{cases} M_n(\mathbb{C}) & \rightarrow M_n(\mathbb{C}) \\ A & \mapsto \Sigma A \end{cases}$ est donc un automorphisme, d'inverse $L_{\Sigma^{-1}}$.

- Soit $p \in [0, n-1]$ En particulier, l'automorphisme $L_\Sigma^p = L_{\Sigma^p}$ induit un isomorphisme

$$\varphi_p : D_n(\mathbb{C}) = \text{Vect}(E_{1,1}, \dots, E_{n,n}) \rightarrow \text{Vect}(E_{1+p,n}, \dots, E_{p,n+p}) = \text{Vect}(\mathcal{A}_p) = V_p.$$

- En particulier, la famille $(\Sigma^p \Delta^k)_{0 \leq k \leq n-1}$, image de la base $(\Delta^k)_{0 \leq k \leq n-1}$ de $D_n(\mathbb{C})$ par l'isomorphisme φ_p , est une base de V_p .

- Par concaténation, $(\Sigma^p \Delta^k)_{0 \leq p, k \leq n-1}$ est une base de $\bigoplus_{p=0}^{n-1} V_p = M_n(\mathbb{C})$.

- d) On a

$$H = \sum_{1 \leq i, j \leq n} E_{i,j}$$

$$\begin{aligned}
&= \sum_{p=1}^n \sum_{k=1}^n \underbrace{E_{p+k,k}}_{\Sigma^p E_{k,k}} \\
&= \sum_{p=1}^n \Sigma^p \underbrace{\sum_{k=1}^n E_{k,k}}_{=I_n=\Delta^0} \\
&= \sum_{p=1}^n \Sigma^p.
\end{aligned}$$

Q 3) Toutes les vérifications, à savoir :

- $\forall M_1, M_2 \in M_n(\mathbb{C}), \forall \lambda \in \mathbb{C}, \Psi_P(\lambda M_1 + M_2) = \lambda \Psi_P(M_1) + \Psi_P(M_2)$;
- $\Psi_P(I_n) = I_n$;
- $\forall M_1, M_2 \in M_n(\mathbb{C}), \Psi_P(M_1 M_2) = \Psi_P(M_1) \Psi_P(M_2)$,

sont immédiates.

Q 4) a) Notons $\mathcal{C}$ la base canonique de $\mathbb{C}^n$.

- On a déjà vu que $\Delta^n = \Sigma^n = I_n$. Un calcul direct montre également que $\Delta \Sigma = \zeta \Sigma \Delta$. Comme φ est un morphisme d'algèbres, on en déduit
 - $\varphi(\Delta)^n = \varphi(\Delta^n) = I_n^n = I_n$;
 - de même, $\varphi(\Sigma)^n = I_n$;
 - $\varphi(\Delta)\varphi(\Sigma) = \varphi(\Delta \Sigma) = \varphi(\zeta \Sigma \Delta) = \zeta \varphi(\Sigma)\varphi(\Delta)$.

On en déduit que les endomorphismes u et v canoniquement associés à $\varphi(\Sigma)$ et $\varphi(\Delta)$ vérifient $u^n = v^n = \text{id}_E$ et $u \circ v = \zeta(v \circ u)$.

D'après la Q0, on peut donc trouver une base $\mathcal{B}$ telle que $\text{Mat}_{\mathcal{B}}(u) = \Delta$ et $\text{Mat}_{\mathcal{B}}(v) = \Sigma$. Notons $P = P_{\mathcal{C}, \mathcal{B}} \in \text{GL}_n(\mathbb{C})$. On a alors

$$\varphi(\Delta) = \text{Mat}_{\mathcal{C}}(u) = P \text{Mat}_{\mathcal{B}}(u) P^{-1} = P \Delta P^{-1} \quad \text{et, de même,} \quad \varphi(\Sigma) = P \Sigma P^{-1}.$$

- b) - La question précédente montre que φ et Ψ_P coïncident sur la famille (Σ, Δ) .
 - Comme il s'agit de deux morphismes d'algèbres, on en déduit que, pour tous $k, p \in \llbracket 0, n-1 \rrbracket$,

$$\varphi(\Sigma^p \Delta^k) = \varphi(\Sigma)^p \varphi(\Delta)^k = \Psi_P(\Sigma)^p \Psi_P(\Delta)^k = \Psi_P(\Sigma^p \Delta^k).$$

Problème 2 : Résultant de deux polynômes d'après CCINP MP 2009

2.1)

- (a) Commençons par remarquer, par considération des degrés, que u est bien une application de E dans F . Soient $(\lambda, \mu) \in \mathbb{C}^2$ et $((A, B), (C, D)) \in E^2$. On a :

$$\begin{aligned}
u(\lambda(A, B) + \mu(C, D)) &= u(\lambda A + \mu C, \lambda B + \mu D) \\
&= P \cdot (\lambda A + \mu C) + Q \cdot (\lambda B + \mu D) \\
&= \lambda(PA + QB) + \mu(PC + QD) \\
&= \lambda u(A, B) + \mu u(C, D)
\end{aligned}$$

- (b) Si u est bijective il existe en particulier $(A, B) \in E$ tel que $u(A, B) = 1$ ce qui prouve que P et Q sont premiers entre eux par le théorème de Bézout.
 (c) Supposons P et Q premiers entre eux et soit $(A, B) \in \text{Ker } u$. On a $PA = -QB$ donc Q divise A par le théorème de Gauss (car Q divise PA et est premier avec P).

Or Q est de degré q et A de degré au plus $q-1$ (avec la convention usuelle que le degré du polynôme nul est égal à $-\infty$). Il en résulte que A est le polynôme nul.

Il reste alors $QB = 0$ donc $B = 0$ car P est non nul. Ainsi $\text{Ker } u$ est réduit au polynôme nul et u est bijective en tant qu'application linéaire injective entre deux espaces de même dimension finie $p+q$.

2.2)

- (a) L'image de la base $\mathcal{B}$ par u est la famille $(P, XP, \dots, X^{q-1}P, Q, XQ, \dots, X^{p-1}Q)$ dont la matrice dans la base canonique $\mathcal{B}'$ de F est la matrice $M_{P,Q}$ associée à $\text{Res}(P, Q)$.
- (b) Ainsi $\det u = \text{Res}(P, Q)$ et compte tenu de la question 1) : $\text{Res}(P, Q) \neq 0$ si et seulement si P et Q sont premiers entre eux.
- (c) si $P = \sum_{k=0}^n a_k X^k$ et $Q = b_1 X + b_0$ avec $b_1 \neq 0$ alors par définition :

$$\text{Res}(P, Q) = \begin{vmatrix} a_0 & b_0 & 0 & \dots & 0 \\ a_1 & b_1 & b_0 & & \\ \vdots & 0 & b_1 & \ddots & \\ . & & & \ddots & 0 \\ a_n & 0 & \dots & b_1 & b_0 \\ & & & 0 & b_1 \end{vmatrix}$$

En développant ce déterminant $(n+1) \times (n+1)$ par rapport à sa première colonne, on a :

$$\text{Res}(P, Q) = a_0 b_1^n - a_1 b_0 b_1^{n-1} + \dots + (-1)^k a_k b_0^k b_1^{n-k} + \dots + (-1)^n a_n b_0^n$$

Comme $b_1 \neq 0$, on peut factoriser par b_1^n dans cette expression et

$$\text{Res}(P, Q) = 0 \Leftrightarrow a_0 + a_1(-b_0/b_1) + \dots + a_k(-b_0/b_1)^k + \dots + a_n(-b_0/b_1)^n = 0$$

Donc

$$\text{Res}(P, Q) = 0 \Leftrightarrow P(-b_0/b_1) = 0$$

Or $-b_0/b_1$ est l'unique racine de Q , ce qui redonne le résultat annoncé dans ce cas particulier.

2.3) Racines multiples.

- (a) P admet une racine multiple dans $\mathbb{C}$ si et seulement si P et P' admettent une racine commune dans $\mathbb{C}$ donc si et seulement si P et P' ne sont pas premiers entre eux donc si et seulement si $\text{Res}(P, P') = 0$.

(b) Par définition $\Delta(P) = R(P, P') = \begin{vmatrix} c & b & 0 \\ b & 2a & b \\ a & 0 & 2a \end{vmatrix} = 4a^2c - b^2a$.

En factorisant par $-a$, on remarque que $\Delta(P) = -a(b^2 - 4ac)$ où la parenthèse est le discriminant usuel.

- (c) Pour $P = X^3 + aX + b$, alors par définition :

$$\Delta(P) = \begin{vmatrix} b & 0 & a & 0 & 0 \\ a & b & 0 & a & 0 \\ 0 & a & 3 & 0 & a \\ 1 & 0 & 0 & 3 & 0 \\ 0 & 1 & 0 & 0 & 3 \end{vmatrix}$$

En faisant $L_2 \leftarrow L_2 - a/3L_4$ et $L_3 \leftarrow L_3 - a/3L_5$, on obtient :

$$\Delta(P) = \begin{vmatrix} b & 0 & a & 0 & 0 \\ \frac{2a}{3} & b & 0 & 0 & 0 \\ 0 & \frac{2a}{3} & 3 & 0 & 0 \\ 1 & 0 & 0 & 3 & 0 \\ 0 & 1 & 0 & 0 & 3 \end{vmatrix}$$

La matrice obtenue est triangulaire-inférieure par bloc avec un bloc 2×2 de zéro en haut à droite ; donc

$$\Delta(P) = \begin{vmatrix} b & 0 & a \\ \frac{2a}{3} & b & 0 \\ 0 & \frac{2a}{3} & 3 \end{vmatrix} \cdot \begin{vmatrix} 3 & 0 \\ 0 & 3 \end{vmatrix} = 9 \cdot (3b^2 + 4a^3/9) = 27b^2 + 4a^3$$

Donc un tel polynôme P admet une racine multiple dans $\mathbb{C}$ si et seulement $27b^2 + 4a^3 = 0$.

N.B On peut retrouver ce résultat avec l'algorithme d'Euclide appliqué à P et P' .

2.4.)

(a) L'énoncé suggère (impose?) de vérifier que $\text{Res}(P, Q) \neq 0$.

$$\text{Res}(P, Q) = \begin{vmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & -1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & -1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{vmatrix}.$$

Or il s'agit là d'un déterminant 7×7 sans rien de particulier! Un calcul stupide qui consiste à tout rentrer dans la calculatrice ou à la main montre que ce déterminant vaut 1. Il est beaucoup plus rapide de noter que $P = (X+1)Q + X^2$ ce qui prouve que la seule racine commune possible de P et Q est 0 qui ne convient pas!

(b) Comme u est bijective, un tel couple existe et est unique : il s'agit de $u^{-1}(1)$. Donc $A_0 = a_0 + a_1X + a_2X^2$ et $B_0 = b_0 + b_1X + b_2X^2 + b_3X^3$ convient (Cf question 2.a) si et seulement si, en notant $C = (a_0, a_1, a_2, b_0, b_1, b_2, b_3)^T$ et $D = (1, 0, 0, 0, 0, 0, 0)^T$, on a $M_{P,Q}C = D$. Cela conduit à résoudre un système linéaire de 7 équations à 7 inconnues. La méthode du pivot de Gauss conduit à la solution $A_0 = 1 - X - X^2$ et $B_0 = X + 2X^2 + X^3$, à la calculatrice, on peut calculer l'inverse de $M_{P,Q}$ et obtenir $C = M_{P,Q}^{-1}D$.

Là encore il est plus rapide d'appliquer l'algorithme d'Euclide : En notant $R_0 = X^2$, $R_1 = -X + 1$, $Q_0 = X + 1$, $Q_1 = X$ et $Q_2 = -X - 1$ on obtient (algorithme d'Euclide) :

$$\begin{cases} P = QQ_0 + R_0 \\ Q = R_0Q_1 + R_1 \\ R_0 = R_1Q_2 + 1 \end{cases}$$

Puis on remonte l'algorithme :

$$1 = -R_1Q_2 + R_0 = -(Q - R_0Q_1)Q_2 + R_0 = -(Q + (QQ_0 - P)Q_1)Q_2 - QQ_0 + P$$

donc $(Q_1Q_2 + 1)P - (Q_0 + Q_2 + Q_0Q_1Q_2)Q = 1$ et finalement

$$(1 - X - X^2)P + (X + 2X^2 + X^3)Q = 1.$$

(c) • Si (A, B) vérifie $PA + QB = 1$ alors $PA + QB = PA_0 + QB_0$ donc $P(A - A_0) = -Q(B - B_0)$. Ainsi Q divise $(A - A_0)P$ donc $A - A_0$ d'après le théorème de Gauss puisque P et Q sont premiers entre eux. Donc il existe $R \in \mathbb{C}[X]$ tel que $A = A_0 + QR$. (1) s'écrit alors $PR = -(B - B_0)$ donc $B = B_0 - PR$. ainsi si (A, B) est solution, il existe $R \in \mathbb{C}[X]$ tel que $A = A_0 + QR$ et $B = B_0 - PR$.

- Réciproquement tout couple de cette forme convient clairement.

- En conclusion les couples solution sont tous les couples de la forme $(A_0 + QR, B_0 - PR)$ avec $R \in \mathbb{C}[X]$.

2.5

a) C'est une grande différence avec le cas des matrices ou des endomorphismes, cela vient de l'intégrité de $\mathbb{C}$.

Soit $P \in \mathbb{Q}[X]$ le polynôme minimal d'un nombre complexe algébrique α .

Par l'absurde supposons que $P = U.V$ avec U et V non constant dans $\mathbb{Q}[X]$ donc aussi $\deg(U) < \deg(P)$ et $\deg(V) < \deg(P)$.

Comme $P(\alpha) = 0$ on a $U(\alpha) = 0$ ou $V(\alpha) = 0$. Et dans ce cas U (resp. V) est un polynôme annulateur non nul de α de degré strictement inférieur à celui de P , *contradiction*.

b) Notons $R(X) = R_Y(P(Y), Q(X - Y))$.

On a $R(\alpha + \beta) = \text{Res}_Y(P(Y), Q(\alpha + \beta - Y))$. Or les polynômes $P(Y)$ et $Q(\alpha + \beta - Y)$ admettent α comme racine commune, si bien que $R(\alpha + \beta) = 0$.

c) Ici $P(X) = X^2 - 3$ et $Q(X) = X^2 - 7$. Donc $Q(X - Y) = (X - Y)^2 - 7 = Y^2 - 2XY + X^2 - 7$.

$$\text{On explicite } R_Y(P(Y), Q(X - Y)) = \begin{vmatrix} -3 & 0 & X^2 - 7 & 0 \\ 0 & -3 & -2X & X^2 - 7 \\ 1 & 0 & 1 & -2X \\ 0 & 1 & 0 & 1 \end{vmatrix}.$$

On note $\Pi(X)$ ce polynôme, qui par a) annule $\sqrt{3} + \sqrt{7}$.

Via $C_4 \leftarrow C_4 - C_2$ et $C_3 \leftarrow C_3 - C_1$, on a :

$$\Pi(X) = \begin{vmatrix} -3 & 0 & X^2 - 4 & 0 \\ 0 & -3 & -2X & X^2 - 4 \\ 1 & 0 & 0 & -2X \\ 0 & 1 & 0 & 0 \end{vmatrix}.$$

En développant par rapport à la quatrième ligne :

$$\Pi(X) = \begin{vmatrix} -3 & X^2 - 4 & 0 \\ 0 & -2X & X^2 - 4 \\ 1 & 0 & -2X \end{vmatrix}.$$

Via $C_3 \leftarrow C_3 + 2XC_1$:

$$\Pi(X) = \begin{vmatrix} -3 & X^2 - 4 & -6X \\ 0 & -2X & X^2 - 4 \\ 1 & 0 & 0 \end{vmatrix}.$$

Par développement par rapport à la troisième ligne :

$$\Pi(X) = \begin{vmatrix} X^2 - 4 & -6X \\ 2X & X^2 - 4 \end{vmatrix}.$$

On conclut que $\Pi(X) = (X^2 - 4)^2 - 12X^2$ convient.