DM 19 : théorème de Skolem-Noether pour $M_n(\mathbb{C})$ [corrigé]

- Dans tout le problème, on fixe E un espace vectoriel complexe de dimension $n \geqslant 1$ (et toutes les notions d'algèbre linéaire sont à entendre sur le corps des scalaires $\mathbb{C}$).
- On note $\zeta = \exp\left(i\dfrac{2\pi}{n}\right)$.

Le but du problème est de déterminer tous les endomorphismes de la $\mathbb{C}$-algèbre $M_n(\mathbb{C})$, ce qui est un cas (très) particulier d'un théorème dû (indépendamment) à Thoralf Skolem et Emmy Noether.

Partie I. Co-réduction de deux endomorphismes.

1. **Un calcul préliminaire.**

   (a) Déterminer les racines du polynôme $X^n - 1$, et en déduire une factorisation de ce polynôme en polynômes de degré 1.

   Les racines du polynôme $X^n - 1$ sont, par définition, les n racines n-ièmes de l'unité.

   On a $X^n - 1 = \prod_{\omega \in \mathbb{U}_n} (X - \omega) = \prod_{k=0}^{n-1} (X - \zeta^k)$.

   (b) Soit $u \in \mathcal{L}(E)$ tel que $u^n = \mathrm{id}_E$.
   En utilisant la relation précédente, montrer qu'il existe $\omega \in \mathbb{U}_n$ tel que $u - \omega\, \mathrm{id}_E \notin GL(E)$.

   En appliquant év_u à l'égalité précédente, on obtient

   $$0_{\mathcal{L}(E)} = u^n - \mathrm{id}_E = \left(u - \mathrm{id}_E\right) \circ \left(u - \zeta\, \mathrm{id}_E\right) \circ \cdots \circ \left(u - \zeta^{n-1}\, \mathrm{id}_E\right).$$

   Si tous les endomorphismes $u - \zeta^k\, \mathrm{id}_E$ étaient des automorphismes, leur composée en serait également un. Comme ce n'est pas le cas, on a donc montré $\exists k \in [\![0, n-1]\!] : u - \zeta^k \notin GL(E)$, ce qui conclut.

   (c) Montrer que $\mathrm{Sp}(u)$ est une partie non vide de $\mathbb{U}_n$.

   Comme E est un espace vectoriel de dimension finie, le fait que $u - \omega\, \mathrm{id}_E$ ne soit pas un automorphisme entraîne qu'il n'est pas injectif : on peut donc trouver $x \in \ker(u - \omega\, \mathrm{id}_E)$ non nul, c'est-à-dire un vecteur propre associé à la valeur propre ω.
   Cela montre $\omega \in \mathrm{Sp}(u)$, et donc $\mathrm{Sp}(u) \neq \varnothing$.

Dans toute la suite de cette partie, on considère deux endomorphismes $u, v \in \mathcal{L}(E)$ vérifiant les relations $u^n = v^n = \mathrm{id}_E$ et $u \circ v = \zeta\,(v \circ u)$. On définit les matrices

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

2. Soit $\lambda \in \mathrm{Sp}(u)$. Montrer $\zeta\lambda \in \mathrm{Sp}(u)$.

   Puisque $\lambda \in \mathrm{Sp}(u)$, on peut trouver $x \in E$ non nul tel que $u(x) = \lambda x$.

On a alors $u(v(x)) = \zeta v(u(x)) = \zeta v(\lambda x) = \zeta\lambda v(x)$, *ce qui montre* $v(x) \in E_{\zeta\lambda}(u)$.
Par ailleurs, $v^n = \mathrm{id}_E$, *donc* v *est un automorphisme (d'inverse* v^{n-1}*), ce qui montre que* $v(x) \neq 0_E$.
Il s'agit donc bien d'un vecteur propre associé à la valeur propre $\zeta\lambda$, *ce qui montre* $\zeta\lambda \in \mathrm{Sp}(u)$.

3. En déduire $1 \in \mathrm{Sp}(u)$.

   D'après la première question, on peut trouver $\omega \in \mathbb{U}_n$ *tel que* $\omega \in \mathrm{Sp}(u)$.
   On peut alors trouver $k \in [\![0, n-1]\!]$ *tel que* $\omega = \zeta^k$. *Ainsi,* $\zeta^k \in \mathrm{Sp}(u)$.
   En appliquant de façon répétée la question précédente, on obtient donc $1 = \zeta^{n-k}\zeta^k \in \mathrm{Sp}(u)$.

> On peut trouver $x_0 \in E$ non nul tel que $u(x_0) = x_0$.

4. Montrer que, pour tout $k \in [\![0, n-1]\!]$, le vecteur $v^k(x_0)$ est un vecteur propre pour u, associé à la valeur propre ζ^k.

   Soit $k \in [\![0, n-1]\!]$. *La relation* $u \circ v = \zeta(v \circ u)$ *et une petite récurrence montrent* $u \circ v^k = \zeta^k(v^k \circ u)$.
   On en déduit que $u(v^k(x_0)) = \zeta^k v^k(u(x_0)) = \zeta^k v^k(x_0)$. *Comme* v *est un automorphisme,* $v^k(x_0) \neq 0_E$, *et c'est donc bien un vecteur propre pour* u, *associé à la valeur propre* ζ^k.

5. Montrer que la famille $\mathcal{B} = (x_0, v(x_0), \dots, v^{n-1}(x_0))$ est une base de E.

   Les $v^k(x_0)$, $k \in [\![0, n-1]\!]$ *sont des vecteurs propres pour* u, *associés à des valeurs propres différentes, donc la famille* $\mathcal{B}$ *par eux formée est libre.*
   Comme cette famille possède $n = \dim E$ *vecteurs, c'est une base de* E.

6. Montrer $\mathrm{Mat}_{\mathcal{B}}(u) = \Delta$ et $\mathrm{Mat}_{\mathcal{B}}(v) = \Sigma$.

   - *Pour tout* $k \in [\![0, n-1]\!]$, *on a* $u(v^k(x_0)) = \zeta^k v^k(x_0)$, *donc la* $(k+1)$*-ième colonne (les colonnes sont numérotées à partir de 1...) de* $\mathrm{Mat}_{\mathcal{B}}(u)$ *est* $\zeta^k\, e_{k+1}$.
     Cela montre $\mathrm{Mat}_{\mathcal{B}}(u) = \mathrm{diag}(1, \zeta, \dots, \zeta^{n-1}) = \Delta$.
   - *On a :*
     - *pour tout* $k \in [\![0, n-1]\!]$, $v(v^k(x_0)) = v^{k+1}(x_0)$, *donc la* $(k+1)$*-ième colonne de* $\mathrm{Mat}_{\mathcal{B}}(v)$ *est* e_{k+2} *;*
     - $v(v^{n-1}(x_0)) = v^n(x_0) = x_0$, *donc la* n*-ième colonne de* $\mathrm{Mat}_{\mathcal{B}}(v)$ *est* e_1.

     Cela montre $\mathrm{Mat}_{\mathcal{B}}(v) = \Sigma$.

Partie II. Une base de $M_n(\mathbb{C})$.

7. **Une base de** $D_n(\mathbb{C})$.

   (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

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

   Le produit de deux matrices diagonales s'effectuant coefficient par coefficient, on a

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

   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 critère radical de nullité, car $P \in \mathbb{C}_{n-1}[X]$.

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

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* $D_n(\mathbb{C})$.

8. (a) Pour tout $p \in [\![0, n-1]\!]$, on considère $V_p = \mathrm{Vect}\left\{E_{i,j} \,\middle|\, (i,j) \in [\![1,n]\!]^2, i \equiv j + p \pmod n\right\}$.
Que vaut V_0 ?

On a $V_0 = \mathrm{Vect}\left(E_{1,1}, \dots, E_{n,n}\right) = D_n(\mathbb{C})$.

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

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* $V_p = \mathrm{Vect}(\mathcal{A}_p)$.

On voit que la concaténation $\displaystyle\bigvee_{p=0}^{n-1} \mathcal{A}_p$ *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 $M_n(\mathbb{C}) = \mathrm{Vect}\left(\displaystyle\bigvee_{p=0}^{n-1} \mathcal{A}_p\right) = \displaystyle\bigoplus_{p=0}^{n-1} \mathrm{Vect}(\mathcal{A}_p) = \bigoplus_{p=0}^{n-1} V_p$.

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

- *Un calcul direct montre que* $\Sigma E_{i,j} = \displaystyle\sum_{k=1}^{n} \underbrace{E_{k+1,k} E_{i,j}}_{=0 \text{ si } k \neq i} = E_{i+1,i} E_{i,k} = E_{i+1,j}$, *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 $L_\Sigma : \begin{cases} M_n(\mathbb{C}) \to M_n(\mathbb{C}) \\ \quad A \quad \mapsto \quad \Sigma A \end{cases}$ *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*
$$\varphi_p : D_n(\mathbb{C}) = \mathrm{Vect}(E_{1,1}, \dots, E_{n,n}) \to \mathrm{Vect}(E_{1+p,n}, \dots, E_{p,n+p}) = \mathrm{Vect}(\mathcal{A}_p) = V_p.$$
- *En particulier, la famille* $\left(\Sigma^p \,\Delta^k\right)_{0 \leqslant k \leqslant n-1}$, *image de la base* $\left(\Delta^k\right)_{0 \leqslant k \leqslant n-1}$ *de* $D_n(\mathbb{C})$ *par l'isomorphisme* φ_p, *est une base de* V_p.
- *Par concaténation,* $\left(\Sigma^p \,\Delta^k\right)_{0 \leqslant p,k \leqslant n-1}$ *est une base de* $\displaystyle\bigoplus_{p=0}^{n-1} V_p = M_n(\mathbb{C})$.

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

On a
$$H = \sum_{1 \leqslant i,j \leqslant n} E_{i,j}$$

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

Partie III. Théorème de Skolem-Noether pour $M_n(\mathbb{C})$.

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

   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.

> On va maintenant montrer la réciproque de ce résultat.
> On fixe donc un endomorphisme φ de la $\mathbb{C}$-algèbre $M_n(\mathbb{C})$.

10. (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 $\varphi(\Sigma) = P\Sigma P^{-1}$.

    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,* $\varphi(\Sigma)^n = I_n$ *;*
      - $\varphi(\Delta)\varphi(\Sigma) = \varphi(\Delta\Sigma) = \varphi(\zeta\Sigma\Delta) = \zeta\varphi(\Sigma)\varphi(\Delta)$.

      Comme « composer, c'est multiplier » [1]*, on en déduit que les endomorphismes u et v canoniquement associés à $\varphi(\Sigma)$ et $\varphi(\Delta)$ vérifient $u^n = v^n = \mathrm{id}_E$ et $u \circ v = \zeta(v \circ u)$.*
    - *D'après la partie I, on peut donc trouver une base $\mathcal{B}$ telle que $\mathrm{Mat}_{\mathcal{B}}(u) = \Delta$ et $\mathrm{Mat}_{\mathcal{B}}(u) = \Sigma$.*
      Notons $P = P_{\mathcal{C}\to\mathcal{B}} \in GL_n(\mathbb{C})$. On a alors

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

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

    - *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 $k, p \in [\![0, n-1]\!]$,*

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

1. Ou, de manière plus chic, comme $\mathrm{Mat}_{\mathcal{C}} : \mathcal{L}(E) \to M_n(\mathbb{C})$ est un isomorphisme d'algèbres...

- *Autrement dit, φ et Ψ_P coïncident sur la base $\mathcal{F}$. Comme il s'agit notamment de deux applications linéaires, on en déduit que $\varphi = \Psi_P$ par prolongement des identités.*

Remarque. *On a en fait utilisé, sans le dire, un « prolongement des identités » pour passer de Σ et Δ à la sous-algèbre que ces deux matrices engendrent, c'est-à-dire $M_n(\mathbb{C})$ tout entière.*

11. En déduire que tout endomorphisme de la $\mathbb{C}$-algèbre $M_n(\mathbb{C})$ est un automorphisme.

    Il suffit de remarquer que Ψ_P est un automorphisme, d'inverse $\Psi_P^{-1} = \Psi_{P^{-1}}$...

12. Déterminer les endomorphismes de la $\mathbb{C}$-algèbre $\mathcal{L}(E)$.

    On va raisonner par « transfert de structure ».
    Soit $\mathcal{B}$ une base de E, qui fournit un isomorphisme $\theta = \mathrm{Mat}_{\mathcal{B}} : \mathcal{L}(E) \to M_n(\mathbb{C})$.
    Soit φ un endomorphisme de $\mathcal{L}(E)$. Par composition, $\varphi' = \theta \circ \varphi \circ \theta^{-1}$ est un endomorphisme de $M_n(\mathbb{C})$, donc il existe $P \in GL_n(\mathbb{C})$ telle que $\varphi' = \Psi_P$.

$$\begin{tikzcd}
\mathcal{L}(E) \arrow[r, "\varphi"] \arrow[d, "\theta"'] & \mathcal{L}(E) \arrow[d, "\theta"] \\
M_n(\mathbb{C}) \arrow[r, "\varphi'"] & M_n(\mathbb{C})
\end{tikzcd}$$

    Si l'on note $u = \theta^{-1}(P)$, c'est-à-dire l'endomorphisme associé à P dans la base $\mathcal{B}$ (qui est un automorphisme, par inversibilité) de P, on a, pour tout endomorphisme $w \in \mathcal{L}(E)$,

$$\theta(\varphi(w)) = \varphi'(\theta(w)) = P\theta(w)P^{-1} = \theta(u)\theta(w)\theta(u)^{-1} = \theta(u \circ w \circ u^{-1}),$$

    ce qui montre $\forall w \in \mathcal{L}(E), \varphi(w) = u \circ w \circ u^{-1}$: l'endomorphisme φ est l'automorphisme de conjugaison par $u \in GL(E)$, ce qui est l'analogue pour les applications linéaires du théorème de Skolem-Noether pour $M_n(\mathbb{C})$.

Remarque. *Le même théorème est en fait vrai pour $M_n(K)$, pour un corps K quelconque, alors que notre démonstration ne s'adapte qu'aux corps K possédant n racines de l'unité distinctes.*

Le « vrai » théorème de Skolem-Noether est encore plus général, puisqu'il s'adapte à une généralisation des algèbres de matrices que l'on appelle les algèbres centrales simples.