151. Dimension d'un espace vectoriel : indications de solutions

1. Soit E_r l'ensemble des matrices de $M_n(\mathbf{R})$ de rang au moins r. Supposons $0 < r \leq n$; on observe que pour tout $n \in \mathbf{N}^*$, la matrice-bloc

$$\begin{pmatrix} I_{r-1} & 0 \\ 0 & 1/n \end{pmatrix}$$

est de rang r, alors que quand on fait tendre n vers $+\infty$, la matrice limite est de rang $r-1$. Ainsi, E_r n'est pas un fermé de $M_n(\mathbf{R})$. (pour $r = 0$, on a $E_r = M_n(\mathbf{R})$ donc E_r est bien sûr fermé dans $M_n(\mathbf{R})$).

Soit maintenant $A \in E_r$, alors il existe une matrice (r, r) extraite de A dont le déterminant est non nul, par exemple > 0. Par continuité du déterminant, le mineur (r, r) correspondant reste > 0 dans un voisinage de A, ce qui montre que E_r est ouvert dans $M_n(\mathbf{R})$. Bien entendu, les conclusions de cet exercice restent valables en remplaçant $M_n(\mathbf{R})$ par $M_n(\mathbf{C})$.

2. Soit $E = K^3$ et E^* le dual de E. Le transposé $u^* : E^* \to E^*$ stabilise exactement trois droites, à savoir les orthogonaux dans E^* des trois plans laissés stables par u, via la formule

$$u^*(\varphi)(x) = \varphi(u(x))$$

pour tous $\varphi \in u^*, x \in E$. Ainsi, u^* est diagonalisable avec trois valeurs propres distinctes (s'il y avait une valeur propre multiple, il y aurait un plan contenant une infinité de droites stables); on en déduit que u est diagonalisable à valeurs propres distinctes (diagonaliser u^* dans une base, alors la matrice de u dans la base antéduale est diagonale).

3. a) Supposons x algébrique sur K. Alors il existe une famille finie $(a_0, ..., a_{k-1})$ d'éléments de K tellle que

$$x^k + a_{k-1}x^{k-1} + ... + a_0 = 0.$$

On vérifie alors immédiatement par récurrence sur n que pour tout $n \geq k$, x^n est dans le K-espace vectoriel engendré par $1, x, ...x^{k-1}$, ce qui prouve que le K-espace vectoriel $K[x]$ engendré par tous les x^n est de dimension au plus k. En sens inverse, si $K[x]$ est de dimension finie, alors la famille infinie des x^n est liée, ce qui donne immédiatement qu'il existe un polynôme non nul P (qu'on peut supposer unitaire, quitte à diviser par le coefficient dominant) P de $K[X]$ tel que $P(x) = 0$.

b) Il est immédiat que $K[x]$ est un sous-anneau de L. Si $x \neq 0$ est algébrique, alors $K[x]$ est un corps car c'est une K-algèbre intègre de dimension finie (et donc l'endomorphisme $z \mapsto yz$, qui est injectif si $z \neq 0$, est bijectif de $K[x]$ dans lui-même). Autre méthode : on a $K[x] \simeq K[X]/(P)$, où P est le polynôme minimal de x qui est irréductible, ce qui implique que l'idéal (P) est maximal vu que l'anneau $K[X]$ est principal.

En sens inverse, si x n'est pas algébrique, alors on voit tout de suite que $P \mapsto P(x)$ est un isomorphisme de K-algèbres de $K[X]$ sur $K[x]$, donc $K[x]$ ne peut pas être un corps.

c) Il est clair que 0 et 1 sont dans E. Si x est dans E, le K-ev engendré par les x^n est clairement le même que celui engendré par les $(-x)^n$, donc $(-x)$ est dans E d'après a). De même, si $x \neq 0$ est dans E, il vérifie une équation du type

$$x^k + a_{k-1}x^{k-1} + ... + a_0 = 0,$$

donc $1 + a_{k-1}x + ... + a_0/x^k = 0$, ce qui montre que $1/x$ est encore dans E, vu qu'il annule un polynôme non nul à coefficients dans K. Il reste à montrer que si $x, y \in E$, alors $(x + y)$ et xy sont dans E. Or, le K-espace vectoriel $K[x + y]$ engendré par $x + y$ est un sous-ev du K-espace vectoriel $K[x, y] = (K[x])[y]$ (constitué des polynômes en y à coefficients dans $K[x]$). On a vu en b) que $K[x]$ est un corps; comme y est algébrique sur K, il l'est a fortiori sur $K[x]$, donc $K[x, y]$ est de dimension finie sur $K[x]$. Comme $K[x]$ est de dimension finie sur K puisque x est algébrique sur K, le théorème de la base télescopique donne que $K[x, y]$ est de dimension finie sur K, donc aussi $K[x + y]$ qui en est un sous-espace. De même pour $K[xy]$. On conclut avec a).

4. a) Pour tout $n \in \mathbf{N}$, l'ensemble $\mathbf{Q}_n[X]$ des polynômes de degré au plus n est dénombrable, car en bijection avec $\mathbf{Q}^{n+1}$. L'ensemble Z_n des éléments de $\overline{\mathbf{Q}}$ qui annulent un polynôme non nul de $\mathbf{Q}_n[X]$ est donc dénombrable, puisque chaque polynôme non nul de $\mathbf{Q}_n[X]$ n'a qu'un nombre fini de racines. On en déduit que $\overline{\mathbf{Q}}$, qui est réunion dénombrable des Z_n pour $n \in \mathbf{N}$, est dénombrable.

b) Soit $P = X^n + a_{n-1}X^{n-1} + ... + a_0$ un polynôme unitaire à coefficients dans $\overline{\mathbf{Q}}$. Alors $\mathbf{Q}(a_0)$ est un $\mathbf{Q}$-ev de dimension finie car a_0 est algébrique sur $\mathbf{Q}$. Par récurrence, on voit que $K := \mathbf{Q}(a_0, ..., a_{n-1})$ est de dimension finie sur $\mathbf{Q}$ (car chaque a_i est algébrique sur $\mathbf{Q}$, donc a fortiori sur $\mathbf{Q}(a_0, ..., a_{i-1})$). Soit x une racine de P, alors x est algébrique sur K par définition, donc $K(x)$ est de dimension finie sur K, donc finalement aussi sur $\mathbf{Q}$ puisque K est de dimension finie sur $\mathbf{Q}$. Comme $\mathbf{Q}(x)$ est un sous-espace de $K(x)$, il est également de dimension finie sur $\mathbf{Q}$, ce qui signifie que x est algébrique sur $\mathbf{Q}$, i.e. $x \in \overline{\mathbf{Q}}$ comme on voulait.

c) On vient de voir que $\overline{\mathbf{Q}}$ est un sous-corps algébriquement clos de $\mathbf{C}$ qui contient $\mathbf{Q}$. C'est le plus petit car si L est un tel corps, il contient les racines de tous les polynômes non nuls à coefficients dans $\mathbf{Q}$, donc il contient $\overline{\mathbf{Q}}$. Plus généralement, si F est un corps inclus dans un corps algébriquement clos F', on obtient la clôture algébrique de F en prenant l'ensemble des éléments de F' algébriques sur F; la difficulté pour montrer l'existence de la clôture algébrique est qu'il faut d'abord montrer l'existence d'un tel F', ce qui nécessite entre autres le lemme de Zorn.

d) Non : il suffit pour voir cela de trouver des polynômes irréductibles de $\mathbf{Q}[X]$ de degré d arbitrairement grand car alors une racine x d'un tel polynôme vérifiera $[\mathbf{Q}[x] : \mathbf{Q}] = d$ arbitrairement grand (alors que ce nombre serait majoré par la dimension $[\overline{\mathbf{Q}} : \mathbf{Q}]$ si celle-ci était finie). Or le polynôme $X^d - p$ pour p premier est irréductible sur $\mathbf{Q}$ via le critère d'Eisenstein.

5. Non, E est isomorphe à $K^{(I)}$ (familles *presque nulles* à coefficients dans K), par contre E^* est bien isomorphe à K^I (se donner une forme linéaire revient à se donner ses valeurs sur une base). Noter qu'on n'a pas de "base duale" en dimension infinie, la famille correspondante n'engendrant pas tout E^* mais seulement les formes linéaires qui s'annulent sur presque tous les vecteurs de la base de départ. Bien que ce ne soit pas évident, K^I n'est jamais isomorphe à $K^{(I)}$ si I est infini (penser au cas $K = \mathbf{Z}/2\mathbf{Z}$, où le premier a le cardinal de l'ensemble des parties de I et le deuxième celui de l'ensemble des parties finies de I, qui est le même que celui de I si I est infini). Le théorème de Zorn dit que K^I admet une base, donc est isomorphe à $K^{(J)}$ pour un certain ensemble J, mais on ne peut pas déterminer explicitement J en général !

6. On voit tout de suite que l'hypothèse $px = 0$ permet de voir A comme un $\mathbf{Z}/p\mathbf{Z}$-espace vectoriel. Il est fini, donc de dimension finie $d \in \mathbf{N}$, donc isomorphe à $(\mathbf{Z}/p\mathbf{Z})^d$ (comme groupe abélien ou comme espace vectoriel sur $\mathbf{Z}/p\mathbf{Z}$). Si A est infini, en admettant l'existence d'une base dans tout espace vectoriel, on peut juste dire que A est isomorphe à $(\mathbf{Z}/p\mathbf{Z})^{(I)}$ pour un certain cardinal I (qui est le cardinal de la base).

7. On voit tout de suite que E est un espace vectoriel réel, mais pas complexe à cause de la formule $(\lambda A)^* = \bar{\lambda} A^*$. L'espace E est l'ensemble des matrices de la forme

$$\begin{pmatrix} a & z \\ \bar{z} & -a \end{pmatrix}$$

avec $a \in \mathbf{R}$ et $z \in \mathbf{C}$, donc en écrivant $z = b + ic$ avec a, b réels, on voit que E est de dimension 3.

8. a) On note $e_1 = (1, 0, ...0)$, $e_2 = (0, 1, 0, ...)$ etc. Si $a = (a_1, ..., a_r)$ est dans $(A/I)^r$, posons $\bar{a} = (\bar{a_1}, ..., \bar{a_r})$, où $\bar{x}$ désigne la classe dans A/I d'un élément x de A. Définissons $\bar{f} : (A/I)^r \to (A/I)^s$ par $f(\bar{a}) = \overline{f(a)}$. Cette application est bien définie via le fait que si $x = (x_1, ..., x_r)$ avec tous les x_i dans I, alors

$$f(x) = f(x_1 e_1 + ... + x_r e_r) = x_1 f(e_1) + ... + x_r f(e_r)$$

est dans I^r, ce qui montre que $\overline{f(x)} = 0$. Il est immédiat que f est A/I-linéaire et qu'elle reste surjective car f l'est.

Comme A est non nul, on peut choisir pour I un idéal maximal, ce qui dit que A/I est un corps. Le théorème du rang appliqué à $\overline{f}$ (qui est un morphisme de A/I-espaces vectoriels) donne alors $r \geq s$.

b) Si M admet des bases de cardinal respectifs r et s, alors il est isomorphe à A^r et à A^s, qui sont donc isomorphes comme A-modules. Ainsi $r \geq s$ et $s \geq r$ d'après a), donc $r = s$.

Par contre, le $\mathbf{Z}$-module $\mathbf{Z}/2\mathbf{Z}$ n'a pas de base (sinon il serait infini vu que $\mathbf{Z}$ est infini). Le $\mathbf{Z}$-module $\mathbf{Z}$ est libre de rang 1 (une base en est (1)), tout comme son sous-module strict $2\mathbf{Z}$ (dont une base est (2)). La théorie des modules sur un anneau principal dit quand même que tout sous-module de $\mathbf{Z}^r$ est libre de rang au plus r, mais c'est un résultat plus difficile.

c) Supposons $\det P \in A^*$. Alors l'identité de la comatrice $P\widetilde{P} = \widetilde{P}P = (\det P) I_r$ (où $\widetilde{P}$ est la transposée de la comatrice) donne que P est inversible, d'inverse $(\det P)^{-1}\widetilde{P}$. Noter que l'identité de la comatrice est bien valable sur un anneau commutatif quelconque, elle résulte de la formule du développement par rapport à une ligne ou une colonne (on peut aussi observer que comme on la connaît sur $\mathbf{Q}$ qui est un corps, on la connaît sur $\mathbf{Z}$, et qu'elle correspond à des identités entre polynômes à coefficients dans $\mathbf{Z}$, donc ces identités sont valables sur tout anneau commutatif A via le morphisme canonique de $\mathbf{Z}$ dans A). Si maintenant P est inversible, l'application

f est bijective, donc en particulier surjective. Supposons enfin f surjective. Alors on construit une matrice Q telle que $PQ = I_r$ en prenant pour vecteurs colonnes de Q des vecteurs envoyés sur les vecteurs $e_1, ..., e_2, ..., e_r$ de la base canonique. Alors $(\det P).(\det Q) = 1$, donc $\det P$ est inversible. Noter qu'on peut retrouver a) et b) via ce résultat.

d) Supposons $\det P$ non diviseur de zéro. Soit X un vecteur colonne tel que $P.X = 0$. Alors $(\widetilde{P}P)X = 0$, d'où $(\det P).X = 0$, ce qui implique que toutes les coordonnées de X sont nulles puisque $\det P$ n'est pas diviseur de zéro. Ainsi f est injective. Supposons réciproquement que $\det P = a$ vérifie $ab = 0$ avec b non nul dans A, et montrons que f n'est pas injectif. Si tous les coefficients p_{ij} de P vérifient $p_{ij}.b = 0$, il est clair que f n'est pas injective, puisque P annule par exemple le vecteur $(b, b, ..., b)$. Sinon, on peut choisir un mineur m de taille maximale tel que $mb \neq 0$, et ce mineur est de taille $s < r$ vu que $\det P.b = 0$. Supposons (pour simplifier les notations) que ce soit le mineur correspondant aux s premières lignes et aux s premières colonnes de P. Soit X le vecteur $(x_1, ..., x_s, x_{s+1}, 0, ..., 0$ avec $x_i = b(-1)^i m_i$, où $m_{s+1} = m$ et pour $1 \leq i \leq s$, m_i est le mineur (s, s) obtenu en gardant les s premières lignes et les $s+1$ premières colonnes à l'exception de la i-ième. Alors $X \neq 0$ car $x_{s+1} \neq 0$ vu que $bm \neq 0$; mais les coordonnées y_i de PX sont toutes nulles : en effet, la formule de développement du déterminant par rapport à une ligne donne qu'elles sont obtenues soit (pour les s premières) comme le produit de b par un déterminant de taille $s+1$ ayant deux lignes égales, soit (pour les suivantes) comme le produit de b par un mineur de taille $s+1$ de P, produit qui est nul par hypothèse. Donc f n'est pas injective.

e) Soit j l'injection linéaire de A^r dans A^s qui envoie $(x_1, ..., x_r)$ sur $(x_1, ..., x_r, 0, ...0)$. Si $g : A^s \to A^r$ était linéaire injective, il en irait de même de $f := j \circ g : A^s \to A^s$. Mais la matrice de f dans la base canonique a ses $(s-r)$ dernières lignes nulles, donc son déterminant est nul, donc d'après d) l'application linéaire g ne peut pas être injective.

f) Un A-module M engendré par r éléments est un quotient de A^r, et il suffit donc de montrer qu'une famille $(x_1, ...x_s)$ de s éléments avec $s > r$ est liée dans A^r. Ceci résulte de e), vu que l'application linéaire de A^s dans A^r qui envoie $(\alpha_1, ...\alpha_s)$ sur $\sum_{i=1}^{s} \alpha_i x_i$ ne peut pas être injective.

Il en résulte que si M est un A-module libre de type fini r, un sous-module libre de M est forcément de rang au plus r. Par exemple, un idéal non principal d'un anneau commutatif non nul A ne peut pas être un A-module libre.