Mathématiques D MP 2023 (U)

Nguyên & Coudreuse

22 avril 2023

Remarques préliminaires : Ce corrigé est loin d'être complet et de la rédaction attendue. Il s'agit plutôt d'éléments de correction à adapter pour obtenir un format correct de solution attendu aux concours. Beaucoup de points méritent plus de rédaction notamment le prolongement de certains morphismes en applications linéaires, la définition du degré sur $K[X_1, ..., X_n]$, etc.
Je remercie aussi F. Coudreuse pour sa participation à l'élaboration de ce document.

1 Exemples et contre-exemples pour les propriétés (F) et (TF)

1. On suppose que A a la propriété (F). Soit $S = (s_i)_{i\in I}$ une partie génératrice finie de A, de sorte que tout élément x de A s'écrivent sous la forme $x = \sum_{i=1}^{n} p_i s_i$ avec $s_i \in S$ et $p_i \in \mathbb{Z}$, pour un certain entier $n \in \mathbb{N}$. On écrit $F = \sum_{i=1}^{n} p_i X_i$ de sorte que $x = F(s_1, ..., s_n)$. Ainsi, A a la propriété (TF).
2. Soit $x \in \mathcal{A}(S_1)$, on écrit $x = F(s_1^{(1)}, ..., s_r^{(1)})$ avec $s_i^{(1)} \in S_1$. On écrit chaque $s_i^{(1)}$ sous la forme $s_i^{(1)} = F_i(s_1^{(2)}, ..., s_n^{(2)})$, ainsi, on a
$$x = F\big(F_1(s_1^{(2)}, ..., s_n^{(2)}), ..., F_r(s_1^{(2)}, ..., s_n^{(2)})\big) \in \mathcal{A}(S_2)$$
3. Tout groupe abélien fini a clairement la propriété (F), il s'engendre lui-même. On note $(e_1, ..., e_r)$ la base canonique de $\mathbb{R}^r$, alors pas définition de $\mathbb{Z}^r$, il est engendré par $(e_1, ..., e_r)$, donc $\mathbb{Z}^r$ a la propriété (F).
4. On note $\mathcal{S} = \{X_1, ..., X_n\}$, de sorte que tout élément de $\mathbb{Z}[X_1, ..., X_n]$ est bien un polynôme en les $X_1, ..., X_n$ par définition, donc $\mathbb{Z}[X_1, ..., X_n]$ a la propriété (TF).

   Soit S une partie finie de $\mathbb{Z}[X_1, ..., X_n]$, alors tous les éléments du sous-groupe engendré par S ont un degré majoré. Ainsi, S n'engendre jamais $\mathbb{Z}[X_1, ..., X_n]$.
5. Soit S une partie finie de $\mathbb{Q}$ et d un entier tel que $dS \in \mathbb{Z}$, alors $S \subset \mathbb{Z}\left[\frac{1}{d}\right]$ qui est un sous-anneau de $\mathbb{Q}$, donc $\mathcal{A}(S) \subset \mathbb{Z}\left[\frac{1}{d}\right]$. Or si p est un nombre premier qui ne divise pas q, on a $\frac{1}{p} \notin \mathbb{Z}\left[\frac{1}{d}\right]$, ainsi $\mathcal{A}(S)$ n'est jamais égal à $\mathbb{Q}$.

2 Comportement des propriétés (F) et (TF) via à vis des morphismes

1. Si $\alpha \in \mathbb{N}^n$ s'écrit $(\alpha_1, ..., \alpha_n)$, on écrit $X^\alpha = X_1^{\alpha_1}...X_n^{\alpha_n}$ de sorte que $(X^\alpha)_{\alpha\in\mathbb{N}^n}$ engendre $\mathbb{Z}[X_1, ..., X_n]$. Il suffit donc de verifier la propriété pour $F = X^\alpha$, ce qui est immédiat par la propriété de morphisme d'anneaux.
2. (a) Si f est un tel morphisme, alors $f(X^\alpha) = b_1^{\alpha_1}...b_n^{\alpha_n}$ et ceci définit f de façon unique sur $\mathbb{Z}[X_1, ..., X_n]$. Réciproquement, si on pose $f(X^\alpha) = b_1^{\alpha_1}...b_n^{\alpha_n}$, on a bien $f(X_i) = b_i$ et un morphisme d'anneaux $\mathbb{Z}[X_1, ..., X_n] \longrightarrow B$.

   (b) On suppose que B a la propriété (TF), on note $\mathcal{S} = (b_1, ..., b_n)$ une partie finie de B telle que $\mathcal{A}(S) = B$. Il existe alors un unique morphisme d'anneaux $\mathbb{Z}[X_1, ..., X_n] \xrightarrow{f} B$ tel que $f(X_i) = b_i$.

Reste à voir que f est surjective. Si $b \in B$, on écrit $b = F(b_1, ..., b_n)$ avec $F \in \mathbb{Z}[X_1, ..., X_n]$ et donc on a $f(F) = b$.

Réciproquement, on suppose qu'on a un morphisme surjectif $\mathbb{Z}[X_1, ..., X_n] \xrightarrow{f} B$. On note $b_i = f(X_i)$ et $S = \{b_1, ..., b_n\}$. Si $x \in B$, il existe $F \in \mathbb{Z}[X_1, ..., X_n]$ tel que $f(F) = x$, ie $F(X_1, ..., X_n) = b$.

(c) Si M a la propriété (F), on note $S = (s_1, ..., s_r)$ une famille finie qui engendre M. On définit un morphisme de groupes f tel que $f(e_i) = s_i$ que l'on étend par $\mathbb{Z}$-linéarité (notion non au programme, mais se généralise sans difficulté). Alors, f est un morphisme surjectif $\mathbb{Z}^r \longrightarrow M$.

Réciproquement, si on a un morphisme surjectif $\mathbb{Z}^r \xrightarrow{f} M$. On note $(e_1, ..., e_r)$ la base canonique de $\mathbb{Z}^r$ et $s_i = f(e_i)$. Ainsi, $S = \{s_1, ..., s_r\}$ engendre M par surjectivité de f.

(d) Si $A \longrightarrow B$ est surjectif et A a la propriété (TF), alors on a une chaîne de morphismes surjectifs $\mathbb{Z}[X_1, ..., X_n] \longrightarrow A \longrightarrow B$, en particulier la composition $\mathbb{Z}[X_1, ..., X_n] \longrightarrow B$ est surjective, donc B a la propriété (TF).

Le résultat est exactement si on remplace (TF) par (F) et par exactement le même argument.

3. Les sous-groupes de $\mathbb{Z}$ sont de la forme $m\mathbb{Z}$ avec $m \in \mathbb{N}$: si $m = 0$, $m\mathbb{Z}$ est trivial. Si $m = 1$, on a un isomorphisme $\mathbb{Z} \longrightarrow m\mathbb{Z}$ en envoyant 1 sur m.

Supposons que $x + me_1 = 0$, alors $p(x + me_1) = ma = 0$ et comme $a \neq 0$, on a $m = 0$ et donc $x = 0$. Ainsi, ce morphisme est injectif.
Réciproquement, si $x \in M$, alors $p(x) = am$ pour un certain $m \in \mathbb{Z}$ et on a $x = (x - me_1) + me_1$ et $p(x - me_1) = p(x) - mp(e_1) = p(x) - am = 0$, donc $x - me_1 \in N_1$. Ainsi, ce morphisme est aussi surjectif.

4. Le noyau de p est isomorphe à $\mathbb{Z}^{n-1}$ et donc N_1 est isomorphe à un sous-groupe de $\mathbb{Z}^{n-1}$. Ainsi, par hypothèse de récurrence, il existe r tel que N_1 soit isomorphe à $\mathbb{Z}^r$. Et comme M est isomorphe à $N_1 \times \mathbb{Z}$, il est isomorphe à $\mathbb{Z}^{r+1}$ dans le cas où $a \neq 0$ d'après la question précédente.
Sinon, $p(M) = 0$ et donc M est un sous-groupe de $\mathbb{Z}^{n-1}$, donc dans ce cas aussi, par hypothèse de récurrence, il est isomorphe à un $\mathbb{Z}^r$.

5. Soit r, r' deux entiers tel que M soit isomorphe à $\mathbb{Z}^r$ et $\mathbb{Z}^{r'}$. Alors, on a un isomorphisme de groupes entre $\mathbb{Z}^r$ et $\mathbb{Z}^{r'}$.
Soit $(e_1, ..., e_r)$ la base canonique de $\mathbb{Z}^r$, alors on peut étendre l'isomorphisme précédent en une application $\mathbb{Q}$-linéaire entre $\mathbb{Q}^r$ et $\mathbb{Q}^{r'}$, celle-ci reste injective. Son inverse s'étend aussi en une application $\mathbb{Q}$-linéaire entre $\mathbb{Q}^{r'}$ et $\mathbb{Q}^r$, ainsi, on a un isomorphisme de $\mathbb{Q}$-espaces vectoriels entre $\mathbb{Q}^r$ et $\mathbb{Q}^{r'}$, d'où $r = r'$.

6. (a) Quitte à remplacer S par l'ensemble des monômes (ie de la forme $X^m Y^n$ pour $m, n \in \mathbb{N}$) constituant les éléments de S, on suppose que S ne contient que des monômes de la forme $\alpha X^a Y^b$.
On écrit la division euclidienne de b par $a-1$: $b = (a-1)q + r$ avec $r \leqslant a-2$ de sorte que $\alpha X^a X^{pa+r} = \alpha (XY^p)^{a-1} XY^r$. On note alors $m = \left(\left\{ p, r, X^a Y^{pa+r} \in S \right\}, 1 \right)$ qui est fini car S est fini. On a alors $S \subset \mathcal{A}(\{X, XY, ..., XY^m\})$ et donc,

$$\mathcal{A}(S) \subset \mathcal{A}\big(\{X, XY, ..., XY^m\} \big)$$

(b) Soit R_m l'ensemble des éléments de B qui s'écrivent comme somme de monômes de la forme $X^i Y^j$ avec $j \leqslant mi$. Alors, B contient $\{X, XY, ..., XY^m\}$ et B est stable par addition.
Si $j \leqslant mi$ et $j' \leqslant mi'$, alors $(X^i Y^j)(X^{i'} Y^{j'}) = X^{i+i'} Y^{j+j'}$ avec $j + j' \leqslant m(i + i')$, d'où la stabilité par produit.
Ainsi, R_m est un sous-anneau de B et donc $\mathcal{A}(S) \subset \mathcal{A}\big(\{X, XY, ..., XY^m\} \big) \subset R_m$ et donc $N = m$ convient.

(c) Si S est fini, il existe $m > 0$ tel que $\mathcal{A}(S) \subset R_m$, mais si $k > m$, alors XY^k n'est pas dans R_m. Ainsi, $R_m \neq B$, d'où $\mathcal{A}(S) \neq B$. Ainsi, B n'a pas la propriété (TF).

3 Déterminants sur un anneau commutatif

1. Soit S l'ensemble des coefficients des matrices de E qui est fini car E est fini, et $B = \mathcal{A}(S)$ convient.

2. (a) Comme A est intègre, on peut construire son corps des fractions K de la façon suivante : $K = A \times (A \setminus \{0\})/\sim$ où $\sim$ est la relation d'équivalence $(a,b) \sim (c,d)$ ssi $ad = bc$. On laisse la vérificaton que K est bien un corps et que A s'identifie au sous-anneau de K engendré par $(1,1)$.
Alors, $M_n(A)$ est un sous-anneau de $M_n(K)$. La formule étant vraie dans $M_n(K)$, elle reste vraie par restriction à $M_n(A)$ car si $M \in M_n(A)$, alors $\det(M) \in A$ et $\widetilde{M} \in M_n(A)$.

   (b) Soit $B \xrightarrow{f} A$ un morphisme surjectif avec B intègre qu'on étend en un morphisme surjectif $\widetilde{f} : M_n(B) \longrightarrow M_n(A)$. On a la propriété

$$f(\det N) = f\left(\sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma)\prod_{i=1}^{n} N_{i,\sigma(i)}\right) = \sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma)\prod_{i=1}^{n} f(N_{i,\sigma(i)}) = \det f(N)$$

   Ainsi, on a $\widetilde{f(\widetilde{N})} = f(\widetilde{N})$. Donc, si $M \in A$, on écrit $M = f(N)$ avec $N \in M_n(B)$ et alors

$$\widetilde{M}M = f(\widetilde{N}N) = f(\det(N)I_n) = f(\det N)I_n = \det(M)I_n$$

   (c) On reprend S de la question 1 et $B = \mathcal{A}(S)$ assoié. Alors, $M \in M_n(B)$ et $\widetilde{M} \in M_n(B)$ et B vérifie (TF), donc on a un morphisme surjectif $\mathbb{Z}[X_1,...,X_n] \longrightarrow B$ pour un certain n et comme $\mathbb{Z}[X_1,...,X_n]$ est intègre, on a le résultat via la question précédente.

   (d) Le raisonnement est exactement le même : si A est intègre, on a le résultat en plongeant A dans son corps des fractions. Si on a un morphisme surjectif $B \longrightarrow A$ avec B intègre, le résultat tient toujours.
Pour le dernier point, il s'agit de prendre S associé à $E = \{M, N\}$ et le résultat s'applique de même.

3. (a) Soit $(e_1,...,e_s)$ la base canonique de A^s, ie $e_i = (0,...,1,...,0)$ avec 1 en i-ème position. Par surjectivité de u, il existe $X_1,...,X_s \in A_r$ tel que $u(X_i) = MX_i = e_i$ et on pose $N = (X_1|...|X_s) \in M_{r,s}(A)$ de sorte que $MN = I_s$.

   (b) On a $M_1N_1 = MN = I_s$.

   (c) Mais comme $r < s$, M_1 contient une ligne complète de 0 et donc $\det(M_1) = 0$ et donc par produit $\det(I_s) = 0$, ce qui n'est pas. Donc, $r \geqslant s$.

   (d) $i) \Longrightarrow ii)$. Si u est surjective, on trouve N tel que $MN = I_n$ et donc $\det(M)\det(N) = 1$ et donc $\det(M) \in A^*$.

   $ii) \Longrightarrow iii)$ On pose $N = \det(M)^{-1}\widetilde{M}$ qui convient par la formule de 2..

   $iii) \Longrightarrow iv)$ Soit $v : A^r \longrightarrow A^r$ définie par $v(Y) = NY$, alors $v \circ u = \mathrm{Id}$ et $u \circ v = \mathrm{Id}$, donc u est bijective.

   $iv) \Longrightarrow i)$ est trivial.

4 Équivalences de matrices de $M_n(\mathbb{Z})$ et $M_n(\mathbb{C})$

1. (a) Si $M, N \in GL_r(A)$, $\det(MN) = \det(M)\det(N) \in A^*$ car A^* est un groupe. Enfin, si $A \in GL_r(A)$, alors on définit son inverse par $\det(A)^{-1}\widetilde{A} \in GL_r(A)$, donc $GL_r(A)$ est bien muni d'une structure de groupes.

   (b) Sans difficulté.
   - $M \sim M$ avec $U = I_s$ et $V = I_r$.
   - Si $L \sim M$ et $M \sim N$, on écrit $L = UMV$ et $M = U'NV'$, alors $L = (UU')N(VV')$ et $L \sim N$.
   - Si $M \sim N$, on écrit $M = UNV$ et alors $N = U^{-1}MV^{-1}$ et $N \sim M$.

2. On note $c_k(M)$ l'idéal de $\mathbb{Z}$ engendré par les mineurs de taille k de M. Il s'agit de montrer que $c_k(M) = c_k(N)$.
On montre que $c_k(MQ) \subset c_k(M)$. En effet, on a $\mathrm{colonne}_j(MQ) = \sum_{k=1}^{r} q_{k,j}\mathrm{colonne}_k(M)$. Et donc, par multilinéarité alternéede det, on a pour tout $I \subset [\![1,s]\!]$ et $J \subset [\![1,r]\!]$ de taille k, on a, en notant $\det(MN)_{I,J}$ le déterminant de la matrice extraite $(MN)_{(i,j)\in I\times J}$:

$$\det(MN)_{I,J} \in \sum_{K\subset[\![1,q]\!],\mathrm{Card}(K)=k} A\det(M_{I,K})$$

Ainsi, $c_k(MQ) \subset c_k(M)$. Et comme Q est inversible, on a $c_k(M) = c_k(MQQ^{-1}) \subset c_k(MQ) \subset c_k(M)$.
En développant de même selon les lignes, on trouve $c_k(PM) = c_k(M)$ pour $P \in GL_p(A)$.

Ainsi, si $M \sim N$, on a $c_k(M) = c_k(N)$ et donc $m_k(M) = m_k(N)$.

3. Non, $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}$ ont même rang, donc sont $\mathbb{C}$-équivalentes, mais $m_1(A) = 1$ et $m_1(B) = 2$.

5 Sous-espaces de $M_n(\mathbb{C})$ constitués de matrices de petit rang

1. Quitte à réduire r, on suppose que V contient une matrice de rang exactement r. Pour tout $P, Q \in GL_m(\mathbb{C})$, $M \in V \longmapsto PMQ$ est un isomorphisme linéaire qui laisse le rang invariant, donc quitte à prendre PVQ pour P, Q tels que $M = PAQ$, on suppose que $A \in V$.

2. (a) On considère la matrice $B - \lambda A$ qui doit avoir un rang $\leqslant r$. On a $B - \lambda A = \begin{pmatrix} B_{1,1} - \lambda I_r & B_{1,2} \\ B_{2,1} & B_{2,2} \end{pmatrix}$. On considère une matrice extraite d'ordre $r+1$ qui borde $B_{1,1} - \lambda I_r$ qui est donc de la forme $\begin{pmatrix} B_{1,1} - \lambda I_r & Y_j \\ X_i & b_{i,j} \end{pmatrix}$ où X_i est la i-ième ligne de $B_{2,1}$ et Y_j la j-ième colonne de $B_{1,2}$ et $b_{i,j}$ le (i,j)-ième coefficient de $B_{2,2}$. Alors, son déterminant est identiquement nul car $B - \lambda A$ est de rang r. Mais cette application étant polynomiale, tous ses coefficients sont nuls. On va alors développer et identifier les deux premiers coefficients. On note $(e_1, ..., e_n)$ la base canonique de $\mathbb{R}^n$, $(C_1|...|C_p) = \begin{pmatrix} A \\ X_i \end{pmatrix}$ de sorte que

$$f(\lambda) = \det\left(C_1 - \lambda e_1, ..., C_p - \lambda e_p, \begin{pmatrix} Y_j \\ 0 \end{pmatrix}\right)$$

- Le coefficient en λ^p est $(-1)^p b_{i,j} = 0$ et donc on a déjà $B_{2,2} = 0$.
- Le coefficient en λ^{p-1} se calcule comme suit. On écrit $X = (x_1, ..., x_p)$ et $Y = \begin{pmatrix} y_1 \\ \vdots \\ y_p \end{pmatrix}$. Alors, le coefficient en λ^{p-1} est

$$\sum_{k=1}^{p} \begin{vmatrix} -\lambda & & c_{1,k} & & y_1 & \\ & \ddots & \vdots & & \vdots & \\ & & c_{k,k} & & y_k & \\ & & \vdots & \ddots & & \vdots \\ & & c_{p,k} & & -\lambda & y_p \\ 0 & \dots & x_k & \dots & 0 & 0 \end{vmatrix} = (-\lambda)^{p-1} \sum_{k=1}^{p} \begin{vmatrix} c_{k,k} & y_k \\ x_k & 0 \end{vmatrix}$$

Ce qui s'écrit finalement $(-1)^{p-1} X_i Y_j = 0$, mais comme X_i est la i-ème ligne de $B_{2,1}$ et Y_j la j-ième colonne de $B_{1,2}$, on a $B_{2,1} B_{1,2} = 0$.

(b) Comme $B + C \in V$, on a par la question précédente, $(B_{2,1} + C_{2,1})(B_{1,2} + C_{1,2}) = 0$, ce qu'on développe en utilisant $B_{2,1}B_{1,2} = C_{2,1}C_{1,2} = 0$ en l'égalité recherchée.

3. (a) Montrons que $\mathrm{Im}(\psi) \subset \varphi(V)^\perp$. Soit $B \in W$ et $C \in V$, on a $\varphi(C) = (C_{1,1}, C_{1,2})$. Alors,

$$\psi(B) \cdot \varphi(C) = \mathrm{Tr}(B_{2,1} C_{1,2})$$

Or, on a $B_{2,1}C_{1,2} + C_{2,1}B_{1,2} = 0$ et comme $B_{1,2} = 0$ car $B \in W$, on en déduit que $B_{2,1}C_{1,2} = 0$ et donc $\psi(B) \cdot \varphi(C) = 0$ pour tout $C \in V$ et donc $\mathrm{Im}(\psi) \subset \varphi(V)^\perp$.

On a $\dim\left(\varphi(V)^\perp\right) = \dim\left(M_{r,m}(\mathbb{C})\right) - \dim(\varphi(V)) = rm - \dim\left(\varphi(V)\right)$ et que $\mathrm{rg}(\psi) \leqslant \dim(\varphi(V))$ par inclusion, on en déduit que

$$\dim\left(\varphi(V)\right) \leqslant rm - \mathrm{rg}(\psi)$$

Or ψ est injective. En effet, si $\mathrm{Tr}(B_{2,1}C_{1,2}) = 0$ pour tout $C = (C_{1,1}, C_{1,2}) \in M_{r,m}(\mathbb{C})$, alors $\mathrm{Tr}(B_{2,1}D) = 0$ pour tout $D \in M_{r,m-r}(\mathbb{C})$ en prenant $C = (0, D)$. Et en prenant pour D les matrices élémentaires, on trouve $B_{2,1} = 0$. Ainsi, $\mathrm{rg}(\psi) = s$ et donc

$$\dim\left(\varphi(V)\right) \leqslant rm - s$$

(b) Soit K l'ensemble des matrices de V de la forme $\begin{pmatrix} B_{1,1} & B_{1,2} \end{pmatrix}$ de sorte que $V = K \oplus W$. Alors, φ est bijective de K sur $\varphi(V)$, d'inverse $(B_{1,1}, B_{1,2}) \longmapsto \begin{pmatrix} B_{1,1} & B_{1,2} \\ 0 & 0 \end{pmatrix}$. Ainsi,

$$\dim(V) = \dim(K) + \dim(W) = \dim\big(\varphi(V)\big) + s \leqslant mr$$

4. (a) Soit $\psi : A \in M_{m,n}(\mathbb{C}) \longmapsto \begin{pmatrix} A & 0 \end{pmatrix} \in M_m(\mathbb{C})$, alors ψ est injective et préserve le rang. En particulier, si E est un sous-espace de $M_{m,n}(\mathbb{C})$ ne contenant que des matrices de rang $\leqslant r$, alors $\psi(E)$ est un sous-espace de $M_m(\mathbb{C})$ ne contenant que des matrices de rang $\leqslant r$. Ainsi, par injectivité de ψ, on a

$$\dim(E) = \dim\big(\psi(E)\big) \leqslant mr$$

(b) On considère le sous-espace de $M_{m,n}(\mathbb{C})$ dont les matrices ont les $n - r$ dernières colonnes nulles qui est un sous-espace de $M_{m,n}(\mathbb{C})$ de dimension mr où toute matrice est de rang au plus r.