# X/ENS Maths A MP 2021 — Corrigé

Ce corrigé est proposé par Florian Metzger (professeur en CPGE) ; il a été relu par Pierre Bosch (professeur en CPGE) et Céline Chevalier (enseignant-chercheur à l'université).

---

L'objet de ce sujet est l'étude des sous-groupes finis de $\mathrm{GL}_n(\mathbb{Z})$, l'ensemble des matrices inversibles à coefficients entiers dont l'inverse est encore à coefficients entiers. Il traite plus particulièrement de l'étude des cardinaux possibles pour les sous-groupes finis de $\mathrm{GL}_n(\mathbb{Z})$.

Comme le présente l'énoncé lui-même, le but est de démontrer, pour tout entier $n \in \mathbb{N}^*$, l'existence d'une borne (ne dépendant que de $n$) pour le cardinal des sous-groupes finis de $\mathrm{GL}_n(\mathbb{Z})$, d'en expliciter une, et d'en donner une majoration raffinée dans le cas d'un $p$-sous-groupe, c'est-à-dire d'un sous-groupe dont le cardinal est une puissance d'un nombre premier $p$.

Les trois premières parties sont indépendantes. La quatrième est largement indépendante des autres, mais utilise le résultat de la dernière question de la troisième partie.

- Quelques questions préliminaires de réduction et d'arithmétique utiles tout au long du sujet permettent un début d'épreuve facile.
- Dans la partie I, on s'intéresse aux éléments d'ordre fini de $\mathrm{GL}_n(\mathbb{Z})$. Si $n = 2$, on montre qu'il n'y a que 5 ordres possibles, les entiers $1, 2, 3, 4$ et $6$. On établit plus généralement que l'ensemble des ordres possibles dans $\mathrm{GL}_n(\mathbb{Z})$ est fini.
- Dans la partie II, on prouve que tout sous-groupe fini de $\mathrm{GL}_n(\mathbb{Z})$ est de cardinal inférieur à $3^{n^2}$.
- La troisième partie s'attache à démontrer que la trace de toute matrice d'un $p$-sous-groupe quelconque de $\mathrm{GL}_n(\mathbb{Z})$ ne peut prendre qu'un nombre fini de valeurs parmi un ensemble décrit en fonction de $n$ et $p$ uniquement :

$$\{n - pj \mid 0 \leqslant j \leqslant \lfloor n/(p-1) \rfloor\}$$

- Dans la quatrième et dernière partie, on se sert d'une loi appelée *produit de Kronecker* sur les matrices pour raffiner la majoration de la partie II. On établit notamment, pour tout sous-groupe G de $\mathrm{GL}_n(\mathbb{Z})$ de cardinal $p^r$ avec $p$ premier, et pour tout entier $s \in \mathbb{N}^*$,

$$\sum_{g \in \mathrm{G}} (\mathrm{Tr}\ g)^s \text{ est un entier divisible par } p^r$$

  On en déduit que le cardinal de tout $p$-sous-groupe de $\mathrm{GL}_n(\mathbb{Z})$ est majoré par $4^n$.

Ce sujet aborde principalement les thématiques d'algèbre linéaire générale, polynômes, groupes, réduction, et arithmétique. Nombre de questions sont très classiques et aucune ne comporte de difficulté insurmontable pour tout candidat solidement préparé sur les thèmes évoqués. Il fallait cependant une grande aisance et du recul sur ces notions d'algèbre pour traiter tout le problème dans le temps imparti.

# Indications

## Préliminaires

P.3.a Expliciter l'ensemble en question pour le mettre en bijection avec un sous-ensemble de $\mathbb{N}$.

P.3.b Commencer par dénombrer les entiers de $[\![ 1\,;m ]\!]$ qui sont multiples de $q^i$, mais non multiples de $q^{i+1}$.

## Partie 1

1.1 La trace d'une matrice est la somme de ses valeurs propres complexes.

1.2 Quels nombres complexes de module 1 sont réels ?

1.3 Considérer l'expression du polynôme caractéristique pour une matrice carrée de taille 2. On pourra d'abord justifier que $\det g = 1$.

1.4 Quelles sont les valeurs propres possibles pour une matrice ayant un polynôme caractéristique parmi ceux de la question 1.3 ?

1.5 Utiliser les relations coefficients-racines pour les polynômes scindés.

1.6 Se servir du résultat de la question 1.5 en remarquant que toutes les valeurs propres d'une matrice d'ordre fini sont de module 1.

1.7 Montrer que l'ordre de tout élément $g$ de $\mathrm{GL}_n(\mathbb{Z})$ d'ordre fini est un diviseur d'un entier $\omega$ indépendant de $g$, construit en utilisant les racines des polynômes de la question 1.6.

## Partie 2

2.1.a Pour l'inégalité, exprimer les valeurs propres de A en fonction de celles de $g$, puis appliquer l'inégalité triangulaire gauche.

2.1.b Montrer d'abord que $\mathrm{A}^k \xrightarrow[k\to+\infty]{} 0$ pour la norme infinie.

2.1.c La matrice $g$ est diagonalisable ; quel est son spectre ?

2.2.a Si $a$ et $b$ dans G ont la même réduction modulo $m$, montrer que $ab^{-1} = \mathrm{I}_n$ en utilisant la question 2.1.

## Partie 3

3.1.a Remarquer en premier lieu que $\ell$ divise $k!\binom{\ell}{k}$.

3.1.b Comment développer une somme de termes qui commutent mise à une puissance entière ?

3.2 Utiliser la formule sommatoire du déterminant, et développer un produit du type $\displaystyle\prod_{i=1}^{n}(a_i + b_i)$.

3.3 Commencer par appliquer le résultat de 3.2 avec $\mathrm{R} = \mathbb{Z}[\mathrm{X}]$ et $\mathrm{P} = \displaystyle\sum_{i=0}^{n} a_i\,\mathrm{X}^i$, puis utiliser le petit théorème de Fermat pour conclure.

3.4.a Pour $\ell \geqslant 3$ premier, alors $\ell$ est impair : considérer le résultat de la question 3.1.b.

3.4.b Se servir du résultat de la question 3.2.

3.4.c Relier la trace au polynôme caractéristique et décomposer $\chi_{\mathrm{M}^\ell}(\mathrm{X}^\ell) - \chi_{\mathrm{M}}(\mathrm{X}^\ell)$ en accord avec les résultats des questions 3.3 et 3.4.b.

3.5 Utiliser le résultat de la question 3.4.c avec $\ell = p$.

3.6 Prouver que $\mathrm{Tr}\, g \in [\![ -n\,;n ]\!]$ pour tout $g \in \mathrm{G}$.

3.7.a Raisonner par l'absurde et distinguer les cas suivant qu'un diviseur $\ell$ de $m$ vérifiant $\ell \leqslant 2n$ divise $k$ ou non.

3.7.b Noter que $g^m = g^k$ pour tout $g \in \mathrm{G}$, puis considérer un diviseur premier de $m$ avec le résultat de la question 3.7.a.

3.8.a Remarquer que $\mathrm{J}_r$ est un simple intervalle d'entiers privé des multiples de $p$.

3.8.b Écrire la somme à calculer en utilisant le résultat de la question 3.8.a.

3.9 Les valeurs propres de $g$ sont des racines $p^r$-ièmes de l'unité. Utiliser le résultat de la question 3.7.b pour tout $j \in \mathrm{J}_r$, et sommer les traces de $g^j$ en se souvenant de la question 3.8.b.

3.10 Utiliser le résultat de la question 3.5, puis celui de la question 3.9, en notant que $n_0$ et $n_1$ sont inférieurs à $n$.

**Partie 4**

4.1.a Commencer par calculer $\gamma f$ pour tout $\gamma \in \mathrm{G}$.

4.1.b Que vaut la trace d'un projecteur ?

4.2.i Expliciter la diagonale de $g \otimes h$.

4.2.ii Faire le produit par blocs de taille $(k, k)$ pour $(g \otimes h)(g' \otimes h')$.

4.2.iii Utiliser le résultat donné par la question 2.ii.

4.3.a Distinguer les cas suivant que $\gamma' \in \mathrm{Im}\, \varphi$ ou non.

4.3.b Utiliser la question 3.a en considérant des éléments deux à deux distincts composant $\mathrm{Im}\, \varphi$. Quel est le cardinal de $\gamma\mathrm{H}$ pour tout $\gamma \in \mathrm{G}$ ?

4.4.a Raisonner par récurrence en utilisant la question 2.ii. Regrouper ensuite les images égales par $\varphi_s$, pour calculer $\displaystyle\sum_{g\in\mathrm{G}} \varphi_s(g)$.

4.4.b Se servir du résultat démontré à la question 4.3.b.

4.5.a Utiliser la question 3.10 et déterminer l'ensemble des $g \in \mathrm{G}$ dont la trace est $n$ pour exprimer la somme en fonction de $\mathrm{P}(n)$. Ensuite, appliquer le résultat de la question 4.4.b, en examinant à part le cas $s = 0$.

4.5.b Calculer $\mathrm{P}(n)$ en fonction de $a$.

4.6.a Faire appel à la question préliminaire P.3.b.

4.6.b Optimiser la majoration en $p \geqslant 2$ donnée par la question 4.6.a en étudiant la fonction argument du cardinal $p^r$ mis sous forme exponentielle.

## Préliminaires

**P.1** Soient $z \in \mathbb{C}$ une racine de l'unité et $d \in \mathbb{N}^*$ tel que $z^d = 1$. Alors d'après la description des racines $d$-ièmes de l'unité, il existe $k \in [\![ 0\,;d-1 ]\!]$ tel que $z = \mathrm{e}^{\,\mathrm{i}\,2k\pi/d}$ et donc immédiatement

$$\boxed{\forall z \in \mathbb{C} \quad \forall d \in \mathbb{N}^* \qquad (z^d = 1 \Longrightarrow |z| = 1)}$$

**P.2** Soit $g \in \mathrm{GL}_n(\mathbb{C})$ d'ordre $d \in \mathbb{N}^*$. L'élément neutre du groupe $\mathrm{GL}_n(\mathbb{C})$ étant $\mathrm{I}_n$, il vient donc $g^d = \mathrm{I}_n$, de sorte que $\mathrm{P} = \mathrm{X}^d - 1$ est un polynôme scindé à racines simples qui annule $g$. D'après le cours, on en déduit que

$$\boxed{\begin{array}{l}\text{Si } g \in \mathrm{GL}_n(\mathbb{C}) \text{ est d'ordre fini } d \in \mathbb{N}^*, \text{ alors } g \\ \text{est diagonalisable et } \mathrm{sp}\,(g) \subset \mathrm{P}^{-1}(\{0\}) = \mathbb{U}_d.\end{array}}$$

**P.3.a** Soient $m \in \mathbb{N}$ et $q \in \mathbb{N}^*$. Alors

$$\begin{aligned}\{k \in [\![ 1\,;m ]\!] \mid q \text{ divise } k\} &= \{pq \mid p \in \mathbb{N} \quad \text{et} \quad 1 \leqslant pq \leqslant m\} \\ &= \{pq \mid p \in \mathbb{N} \cap [\,1\,;m/q\,]\} \\ \{k \in [\![ 1\,;m ]\!] \mid q \text{ divise } k\} &= \{pq \mid p \in [\![ 1\,;\lfloor m/q \rfloor ]\!]\}\end{aligned}$$

L'application $p \mapsto pq$ induit donc une surjection de $[\![ 1\,;\lfloor m/q \rfloor ]\!]$ sur l'ensemble

$$\{k \in [\![ 1\,;m ]\!] \mid q \text{ divise } k\}$$

Étant trivialement injective, il vient

$$\boxed{\forall m \in \mathbb{N} \quad \forall q \in \mathbb{N}^* \quad \mathrm{Card}\,\{k \in [\![ 1\,;m ]\!] \mid q \text{ divise } k\} = \lfloor m/q \rfloor}$$

**P.3.b** Soit $q$ un nombre premier. Remarquons déjà que $\sum_i \lfloor m/q^i \rfloor$ converge : en effet c'est une somme finie puisque le terme général de cette série est nul pour $q^i > m$, c'est-à-dire $i > \ln m / \ln q$. Soit $i \in \mathbb{N}^*$. D'après le résultat de la question P.3.a, le nombre de multiples de $q^i$ mais non multiples de $q^{i+1}$ dans $[\![ 1\,;m ]\!]$ est

$$n_i = f_i - f_{i+1} \qquad \text{avec} \qquad f_i = \left\lfloor \frac{m}{q^i} \right\rfloor$$

En effet, en notant
$$\begin{aligned}\mathrm{E}_i &= \{k \in [\![ 1\,;m ]\!] \mid v_q(k) = i\} \\ \mathrm{F}_i &= \{k \in [\![ 1\,;m ]\!] \mid v_q(k) \geqslant i\}\end{aligned} \qquad \text{pour tout } i \in \mathbb{N}$$

alors
$$[\![ 1\,;m ]\!] = \bigsqcup_{i=0}^{+\infty} \mathrm{E}_i = \bigsqcup_{i=0}^{+\infty} (\mathrm{F}_i \smallsetminus \mathrm{F}_{i+1}) \qquad \text{(union disjointe)}$$

Comme pour tout $i$ on a $\mathrm{F}_{i+1} \subset \mathrm{F}_i$, cela prouve le cardinal annoncé.

Ces entiers multiples de $q^i$ mais pas de $q^{i+1}$ contribuent chacun pour $i$ dans la valuation $q$-adique de $m!$. Il reste à sommer pour obtenir toutes les contributions $q$-adiques des entiers entre 1 et $m$ dans la valuation de $m!$ : par linéarité pour les sommes suivantes qui sont toutes finies, et changement d'indice, on trouve