

**ECOLE POLYTECHNIQUE  
ECOLES NORMALES SUPERIEURES**

**CONCOURS D'ADMISSION 2021**

**LUNDI 12 AVRIL 2021**

**08h00 - 12h00**

**FILIÈRE MP - Epreuve n° 1**

**MATHEMATIQUES A (XLCR)**

*Durée : 4 heures*

*L'utilisation des calculatrices n'est pas  
autorisée pour cette épreuve*

# Sous-groupes finis de $\mathbf{GL}_n(\mathbb{Z})$

Ce sujet traite de l'étude des cardinaux possibles pour les sous-groupes finis de  $\mathbf{GL}_n(\mathbb{Z})$ . Le but est de démontrer que pour tout  $n \in \mathbb{N}^*$ , il existe une borne (ne dépendant que de  $n$ ) sur le cardinal des sous-groupes finis de  $\mathbf{GL}_n(\mathbb{Z})$ , d'en expliciter une, et d'en donner une majoration raffinée dans le cas des sous-groupes dont le cardinal est une puissance d'un nombre premier.

Les préliminaires contiennent des résultats pouvant être utiles dans toute la suite du sujet.

Les parties 1, 2 et 3 sont indépendantes. La partie 4 est largement indépendante des autres, mais utilise le résultat de la dernière question de la partie 3.

## Notations

- Les lettres  $\mathbb{N}$ ,  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$  désignent respectivement l'ensemble des entiers naturels, des entiers relatifs, des nombres rationnels, des nombres réels, des nombres complexes. La notation  $\mathbb{N}^*$  désigne l'ensemble des entiers naturels non nuls.
- Si  $x \in \mathbb{R}$ , on note  $\lfloor x \rfloor$  la partie entière de  $x$ , c'est-à-dire le plus grand entier  $k$  tel que  $k \leq x$ .
- Si  $E$  est un ensemble fini, on note  $\text{card}(E)$  son cardinal.
- Si  $a, b \in \mathbb{Z}$ , on note  $b \mid a$  si  $b$  divise  $a$ , et  $b \nmid a$  dans le cas contraire.
- Si  $a, a', b \in \mathbb{Z}$ , on note  $a \equiv a' \pmod{b}$  si  $b|(a' - a)$ .
- Si  $q \geq 2$  est un nombre premier et  $a \in \mathbb{Z}$ , on note  $v_q(a)$  le plus grand entier  $v$  tel que  $q^v \mid a$ .
- Pour  $n \in \mathbb{N}^*$ ,  $\mathfrak{S}_n$  désigne le groupe des permutations de l'ensemble  $\{1, \dots, n\}$ , et  $\varepsilon : \mathfrak{S}_n \rightarrow \{\pm 1\}$  désigne le morphisme signature.
- Pour  $k, n \in \mathbb{N}$ , on notera  $\binom{n}{k} = \frac{n!}{k!(n-k)!}$  le nombre de parties à  $k$  éléments dans un ensemble à  $n$  éléments.
- Tous les anneaux considérés dans ce sujet sont unitaires.
- Si  $R$  est un anneau commutatif et  $n \in \mathbb{N}^*$ , on définit  $\mathcal{M}_n(R)$  comme l'ensemble des matrices carrées de taille  $n$  à coefficients dans  $R$ . On pourra utiliser librement le fait que l'addition coefficient par coefficient et la multiplication matricielle munissent  $\mathcal{M}_n(R)$  d'une structure d'anneau.
- Si  $R$  est un anneau commutatif et  $A \in \mathcal{M}_n(R)$ , en notant  $(a_{ij})_{1 \leq i, j \leq n}$  les coefficients de  $A$ , on définit la trace de  $A$  par la formule  $\text{Tr}(A) = \sum_{i=1}^n a_{ii}$  et le déterminant de  $A$  par la formule  $\det A = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{1 \leq i \leq n} a_{i\sigma(i)}$ . On pourra utiliser librement le fait que pour  $A, B \in \mathcal{M}_n(R)$ ,  $\det(AB) = (\det A)(\det B)$ .
- Si  $n \in \mathbb{N}^*$  et  $R$  est un anneau commutatif, pour tout  $A \in \mathcal{M}_n(R)$  on note  $\chi_A = \det(XI_n - A)$  le polynôme caractéristique de  $A$ .

- Pour  $n \in \mathbb{N}^*$ ,  $\mathcal{M}_n(\mathbb{C})$  désigne l'ensemble des matrices carrées de taille  $n$  à coefficients dans  $\mathbb{C}$ , et  $\mathbf{GL}_n(\mathbb{C})$  désigne le groupe multiplicatif des matrices inversibles de taille  $n$  à coefficients dans  $\mathbb{C}$ .
- Pour  $n \in \mathbb{N}^*$ ,  $\mathcal{M}_n(\mathbb{Z})$  désigne l'ensemble des matrices carrées de taille  $n$  à coefficients dans  $\mathbb{Z}$ , et  $\mathbf{GL}_n(\mathbb{Z})$  désigne le sous-groupe de  $\mathbf{GL}_n(\mathbb{C})$  constitué des matrices  $A \in \mathcal{M}_n(\mathbb{Z})$  inversibles dont l'inverse est dans  $\mathcal{M}_n(\mathbb{Z})$  (on ne demande pas de démontrer que cet ensemble est bien un sous-groupe de  $\mathbf{GL}_n(\mathbb{C})$ ).
- Si  $G$  est un groupe d'élément neutre  $e$ , on rappelle qu'un élément  $g$  de  $G$  est dit d'ordre fini s'il existe un entier  $d > 0$  tel que  $g^d = e$ . Dans ce cas, l'ordre de  $g$  est le plus petit entier  $d > 0$  tel que  $g^d = e$ .
- Si  $z \in \mathbb{C}$  et  $d \in \mathbb{N}^*$ , on dit que  $z$  est une racine  $d$ -ième de l'unité si  $z^d = 1$ . S'il existe  $d \in \mathbb{N}^*$  tel que  $z \in \mathbb{C}$  soit une racine  $d$ -ième de l'unité, on dira simplement que  $z$  est une racine de l'unité.

## Préliminaires

1. Soit  $z \in \mathbb{C}$  une racine de l'unité. Justifier que  $|z| = 1$ .
2. Soit  $g \in \mathbf{GL}_n(\mathbb{C})$ , et soit  $d \in \mathbb{N}^*$ . On suppose que  $g$  est d'ordre  $d$ . Démontrer que  $g$  est diagonalisable, et que toutes ses valeurs propres sont des racines  $d$ -ièmes de l'unité.
3. Soit  $m \in \mathbb{N}$ , et soit  $q \in \mathbb{N}^*$ .
  - (a) Démontrer que  $\text{card}(\{1 \leq k \leq m \text{ tels que } q \mid k\}) = \lfloor \frac{m}{q} \rfloor$ .
  - (b) En déduire que si  $q$  est premier,  $v_q(m!) = \sum_{i=1}^{+\infty} \lfloor \frac{m}{q^i} \rfloor$ .

## 1 Éléments d'ordre fini de $\mathbf{GL}_n(\mathbb{Z})$

Le but de cette partie est de démontrer que l'ensemble des ordres possibles pour les éléments d'ordre fini de  $\mathbf{GL}_n(\mathbb{Z})$  est fini.

On commence par détailler le cas  $n = 2$ . Soit  $g \in \mathbf{GL}_2(\mathbb{Z})$ . On suppose que  $g$  est d'ordre fini  $d \in \mathbb{N}^*$ .

1. Démontrer que  $|\text{Tr}(g)| \leq 2$ .
2. On suppose que les valeurs propres de  $g$  sont réelles, déterminer les valeurs possibles pour  $d$ .
3. On suppose maintenant que  $g$  n'a pas de valeurs propres réelles. Démontrer que le polynôme caractéristique de  $g$  est l'un des polynômes suivants :  $X^2 + 1, X^2 + X + 1, X^2 - X + 1$ .
4. En déduire que  $d \in \{1, 2, 3, 4, 6\}$ .

On traite maintenant le cas de  $\mathbf{GL}_n(\mathbb{Z})$  où  $n \geq 1$  est un entier quelconque.

5. Soit  $P = X^n + \sum_{i=0}^{n-1} a_i X^i \in \mathbb{C}[X]$  unitaire de degré  $n$ . On note  $z_1, \dots, z_n$  les racines de  $P$  (comptées avec multiplicité) et  $\alpha = \max_{1 \leq i \leq n} |z_i|$ . Démontrer que pour tout  $0 \leq i \leq n-1$ ,  $|a_i| \leq \binom{n}{i} \alpha^{n-i}$ .
6. Montrer que  $\{\chi_g \text{ tels que } g \in \mathbf{GL}_n(\mathbb{Z}) \text{ est d'ordre fini}\}$  est fini.
7. En déduire que  $\{d \in \mathbb{N} \mid \exists g \in \mathbf{GL}_n(\mathbb{Z}) \text{ d'ordre } d\}$  est fini.

## 2 Sous-groupes finis de $\mathbf{GL}_n(\mathbb{Z})$

Soit  $n \in \mathbb{N}^*$ . Le but de cette partie est de majorer le cardinal des sous-groupes finis de  $\mathbf{GL}_n(\mathbb{Z})$  par une quantité ne dépendant que de  $n$ .

1. Soit  $m \geq 3$  un entier. Soit  $g \in \mathbf{GL}_n(\mathbb{Z})$ . On suppose que  $g$  est d'ordre fini et que  $g - I_n$  a tous ses coefficients divisibles par  $m$ . Soit  $A = (g - I_n)/m$ .
  - (a) Montrer que  $A$  est diagonalisable sur  $\mathbb{C}$ , et que pour toute valeur propre  $\lambda$  de  $A$ , on a  $|\lambda| < 1$ .
  - (b) En déduire qu'il existe  $k \in \mathbb{N}$  tel que  $A^k = 0$ .
  - (c) Conclure que  $g = I_n$ .
2. Soit  $G$  est un sous-groupe fini de  $\mathbf{GL}_n(\mathbb{Z})$ , et soit  $m \geq 3$  un entier.

- (a) Démontrer que l'application  $\mathcal{M}_n(\mathbb{Z}) \rightarrow \mathcal{M}_n(\mathbb{Z}/m\mathbb{Z})$  de réduction modulo  $m$  des coefficients induit une application injective  $G \rightarrow \mathcal{M}_n(\mathbb{Z}/m\mathbb{Z})$ .
- (b) En déduire que  $\text{card}(G) \leq 3^{n^2}$ .

### 3 Traces des éléments d'un $p$ -sous-groupe de $\mathbf{GL}_n(\mathbb{Z})$

Soit  $p$  un nombre premier et  $r \geq 1$  un entier. Dans cette partie, on suppose que  $G$  est un sous-groupe de cardinal  $p^r$  de  $\mathbf{GL}_n(\mathbb{Z})$ . Le but de cette partie est de déterminer l'ensemble des valeurs possibles pour les traces des éléments de  $G$ .

1. Soit  $\ell$  un nombre premier.
  - (a) Démontrer que pour tout  $1 \leq k \leq \ell - 1$ , l'entier  $\binom{\ell}{k}$  est multiple de  $\ell$ .
  - (b) Soit  $R$  un anneau. On note  $\ell R = \{\ell x, x \in R\}$ . Démontrer que pour tous  $x, y \in R$  tels que  $xy = yx$ , on a  $(x + y)^\ell - (x^\ell + y^\ell) \in \ell R$ .
2. Soit  $R$  un anneau commutatif, et soit  $I$  un idéal de  $R$ . Soient  $n \in \mathbb{N}^*$  et  $A, B \in \mathcal{M}_n(R)$ . On suppose que tous les coefficients de  $B$  sont dans l'idéal  $I$ . Démontrer que  $\det(A + B) - \det A \in I$ .
3. Soit  $\ell \in \mathbb{N}$  un nombre premier. Démontrer que pour tout polynôme  $P \in \mathbb{Z}[X]$ , on a :

$$P(X^\ell) - P(X)^\ell \in \ell \mathbb{Z}[X].$$

4. Soit  $M \in \mathcal{M}_n(\mathbb{Z})$ , et soit  $\ell \in \mathbb{N}$  un nombre premier.
  - (a) Justifier qu'il existe  $A \in \mathcal{M}_n(\mathbb{Z}[X])$  telle que  $(XI_n - M)^\ell - (X^\ell I - M^\ell) = \ell A$ .
  - (b) Démontrer que  $\chi_{M^\ell}(X^\ell) - \chi_M(X)^\ell \in \ell \mathbb{Z}[X]$
  - (c) En déduire que  $\text{Tr}(M^\ell) \equiv \text{Tr}(M) \pmod{\ell}$ .
5. Soit  $g \in G$ . Démontrer que  $\text{Tr}(g) \equiv n \pmod{p}$ .
6. Soit  $g \in G$  et soit  $\ell$  un nombre premier. On suppose que  $\ell > 2n$ . Démontrer que  $\text{Tr}(g^\ell) = \text{Tr}(g)$ .
7. Soit  $k \in \mathbb{N}$  non divisible par  $p$ . On note

$$m = k + p^r \prod_{\substack{\ell \text{ premier} \\ \ell \leq 2n \\ \ell \text{ ne divise pas } k}} \ell.$$

8. On note  $J_r = \{1 \leq k \leq p^r - 1 \text{ tels que } p \nmid k\}$ .
  - (a) Démontrer que  $J_r = \bigcup_{0 \leq s \leq p^{r-1}-1} \{ps + t \text{ tels que } 1 \leq t \leq p-1\}$ .
  - (b) Soit  $\zeta \in \mathbb{C}$  tel que  $\zeta^{p^r} = 1$ . Montrer que :

$$\sum_{j \in J_r} \zeta^j = \begin{cases} p^{r-1}(p-1) & \text{si } \zeta = 1 \\ -p^{r-1} & \text{si } \zeta \text{ est d'ordre } p \\ 0 & \text{sinon} \end{cases}.$$

9. Soit  $g \in G$ . On note  $n_0$  la multiplicité de 1 comme racine de  $\chi_g$ , et  $n_1$  le nombre de racines  $\zeta$  de  $\chi_g$  d'ordre  $p$  (comptées avec multiplicité). Démontrer que  $\text{Tr}(g) = n_0 - \frac{n_1}{p-1}$ .
10. On note  $a = \lfloor \frac{n}{p-1} \rfloor$ . Soit  $g \in G$ , démontrer que  $\text{Tr}(g) \in \{n - pv \mid 0 \leq v \leq a\}$ .

## 4 Cardinaux des $p$ -sous-groupes de $\mathbf{GL}_n(\mathbb{Z})$

Soit  $G \subset \mathbf{GL}_n(\mathbb{C})$  un sous-groupe fini. Dans cette partie, on démontre que pour tout  $s \in \mathbb{N}$ ,  $\sum_{g \in G} \text{Tr}(g)^s$  est un entier divisible par  $\text{card}(G)$ . On en déduit une borne uniforme sur le cardinal des sous-groupes finis de  $\mathbf{GL}_n(\mathbb{Z})$  dont le cardinal est une puissance d'un nombre premier.

1. Soit  $G \subset \mathbf{GL}_n(\mathbb{C})$  un sous-groupe fini. Soit  $f = \frac{1}{\text{card}(G)} \sum_{g \in G} g \in \mathcal{M}_n(\mathbb{C})$ .
  - (a) Démontrer que  $f$  est un projecteur sur  $\{x \in \mathbb{C}^n \mid \forall g \in G, g(x) = x\}$ .
  - (b) En déduire que  $\sum_{g \in G} \text{Tr}(g)$  est un entier divisible par  $\text{card}(G)$ .
2. Soient  $k, n \in \mathbb{N}^*$ . Pour  $g \in \mathbf{GL}_n(\mathbb{C})$  et  $h \in \mathbf{GL}_k(\mathbb{C})$ , on note  $g \otimes h$  la matrice par blocs, de taille  $nk \times nk$ , définie par :

$$g \otimes h = \begin{pmatrix} g_{11}h & g_{12}h & \cdots & g_{1n}h \\ g_{21}h & \cdots & \cdots & g_{2n}h \\ \vdots & & & \vdots \\ g_{n1}h & \cdots & \cdots & g_{nn}h \end{pmatrix}.$$

Justifier les affirmations suivantes :

- (i) si  $g \in \mathbf{GL}_n(\mathbb{C})$  et  $h \in \mathbf{GL}_k(\mathbb{C})$ ,  $\text{Tr}(g \otimes h) = \text{Tr}(g)\text{Tr}(h)$ .
- (ii) si  $g, g' \in \mathbf{GL}_n(\mathbb{C})$  et  $h, h' \in \mathbf{GL}_k(\mathbb{C})$ ,  $(g \otimes h)(g' \otimes h') = gg' \otimes hh'$ .
- (iii) si  $g \in \mathbf{GL}_n(\mathbb{C})$  et  $h \in \mathbf{GL}_k(\mathbb{C})$ ,  $g \otimes h \in \mathbf{GL}_{nk}(\mathbb{C})$  et  $(g \otimes h)^{-1} = g^{-1} \otimes h^{-1}$ .
3. Soient  $\Gamma, \Gamma'$  des groupes finis et  $\varphi : \Gamma \rightarrow \Gamma'$  un morphisme de groupes. Soit  $H = \ker \varphi$ .
  - (a) Soit  $\gamma' \in \Gamma'$ . Démontrer que  $\varphi^{-1}(\{\gamma'\})$  est vide ou de la forme  $\gamma H = \{\gamma h \mid h \in H\}$  pour un certain  $\gamma \in \Gamma$ .
  - (b) Démontrer que  $\text{card}(\Gamma) = \text{card}(\varphi(\Gamma))\text{card}(H)$ .
4. Pour  $g \in \mathbf{GL}_n(\mathbb{C})$ , on définit par récurrence sur  $s$  :  $g^{(1)} = g$  et  $g^{(s+1)} = g^{(s)} \otimes g$ . Soit  $s \geq 1$ , on définit l'application :

$$\begin{aligned} \varphi_s : \mathbf{GL}_n(\mathbb{C}) &\rightarrow \mathbf{GL}_{n^s}(\mathbb{C}) \\ g &\mapsto g^{(s)}. \end{aligned}$$

Soit  $G$  un sous-groupe fini de  $\mathbf{GL}_n(\mathbb{C})$ .

- (a) Justifier que  $\varphi_s$  est un morphisme de groupes et démontrer que :

$$\sum_{g \in G} \text{Tr}(g)^s = \text{card}(G \cap \ker \varphi_s) \sum_{g' \in \varphi_s(G)} \text{Tr}(g').$$

- (b) En déduire que  $\sum_{g \in G} \text{Tr}(g)^s$  est un entier divisible par  $\text{card}(G)$ .

Soit  $p$  un nombre premier et soit  $r \in \mathbb{N}^*$ . Soit  $G$  un sous-groupe de  $\mathbf{GL}_n(\mathbb{Z})$  de cardinal  $p^r$ .

5. On rappelle qu'on a noté  $a = \left\lfloor \frac{n}{p-1} \right\rfloor$ . Pour  $1 \leq j \leq a$ , on note  $\tau_j = n - pj$ , et  $P(X) = \prod_{1 \leq j \leq a} (X - \tau_j)$ .
  - (a) En considérant  $\sum_{g \in G} P(\text{Tr}(g))$ , démontrer que  $\text{card}(G)$  divise  $P(n)$ .
  - (b) En déduire que  $r \leq a + v_p(a!)$ .
6. (a) Démontrer que  $r \leq \frac{pn}{(p-1)^2}$ .
  - (b) En déduire que  $\text{card}(G) \leq 4^n$ .