Correction

(tiré de "Maths MP & MP1", J. Palacios, Ellipses 2024)

Préliminaires

1. Comme z est une racine de l'unité, il existe $d \in \mathbb{N}^*$ tel que $z^d = 1$. En passant au module, on a $|z|^d = 1$, en passant à la racine d-ième dans $\mathbb{R}_+^*$, on obtient $|z| = 1$.

2. Comme g est d'ordre d, on a $g^d = I_n$. Ainsi le polynôme $P(X) = X^d - 1$ est un polynôme annulateur de g. Ce polynôme est scindé à racine simple dans $\mathbb{C}$, donc g est diagonalisable. De plus les valeurs propres de g sont des racines du polynôme annulateur, ainsi toute valeur propre λ de g vérifie $\lambda^d = 1$, c'est-à-dire que ce sont des racines d-ièmes de l'unité.

3. (a) On a les égalités d'ensemble suivantes :

$$\{1 \leq k \leq m \text{ tels que } q|k\} = \left\{\alpha q, 1 \leq \alpha \leq \frac{m}{q}\right\} = \left\{\alpha q, 1 \leq \alpha \leq \lfloor \frac{m}{q} \rfloor\right\}.$$

Donc $\text{card}(\{1 \leq k \leq m \text{ tels que } q|k\}) = \lfloor \frac{m}{q} \rfloor$.

(b) Pour $i \in \mathbb{N}^*$, on note $A_i = \{1 \leq k \leq m \text{ tels que } q^i|k \text{ et } q^{i+1} \nmid k\}$. Comme m est fixé et que $q \geq 2$, il existe i_0 tel que pour tout $i \geq i_0$, on ait $A_i = \emptyset$. On a

$$v_q(m!) = \sum_{i=1}^{+\infty} i \,\text{card}(A_i).$$

Cette somme est finie car à partir de i_0 tous les termes sont nuls, par conséquent il n'y a pas de problème de convergence. De plus d'après la question précédente, on a

$$\begin{aligned}\text{card}(A_i) &= \text{card}(\{1 \leq k \leq m \text{ tels que } q^i|k\}) \\ &\quad - \text{card}(\{1 \leq k \leq m \text{ tels que } q^{i+1}|k\}) \\ &= \lfloor \frac{m}{q^i} \rfloor - \lfloor \frac{m}{q^{i+1}} \rfloor.\end{aligned}$$

Ainsi

$$\begin{aligned}v_q(m!) &= \sum_{i=1}^{+\infty} i \left(\lfloor \frac{m}{q^i} \rfloor - \lfloor \frac{m}{q^{i+1}} \rfloor \right) \\ &= \sum_{i=1}^{+\infty} i \lfloor \frac{m}{q^i} \rfloor - \sum_{i=2}^{+\infty} (i-1) \lfloor \frac{m}{q^i} \rfloor \\ &= \sum_{i=1}^{+\infty} \lfloor \frac{m}{q^i} \rfloor.\end{aligned}$$

Pour la suite du corrigé, on notera P1, P2 ou P3 la référence aux questions du préliminaire.

1 Éléments d'ordre fini de $GL_n(\mathbb{Z})$

1. D'après P2, g est diagonalisable dans $\mathbb{C}$, il existe $P \in GL_2(\mathbb{C}), \lambda$ et $\mu \in \mathbb{C}$ tels que
$$P^{-1}gP = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$$
λ et μ sont les valeurs propres de g, d'après la P2, λ et μ sont des racines d-ièmes de l'unité, et d'après P1, elles sont de module un. Alors
$$|\mathrm{Tr}(g)| = |\lambda + \mu| \leq |\lambda| + |\mu| = 2.$$

2. On a deux valeurs propres réelles et de module un, donc elles valent un ou moins un. Ainsi :
   - $P^{-1}gP = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, et $d = 1$.
   - $P^{-1}gP = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ et $d = 2$.
   - $P^{-1}gP = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ et $d = 2$.

   On peut conclure que $d = 1$ ou 2.

3. Le polynôme caractéristique de g s'écrit sous la forme $\chi_g(X) = X^2 - \mathrm{Tr}(g)X + \det(g)$. Comme $g \in GL_2(\mathbb{Z})$, on sait que $\det(g) = \pm 1$. On a $\Delta = (\mathrm{Tr}(g))^2 + 4\det(g)$. Si $\det(g) = -1$, alors $\Delta > 0$ et g aurait des valeurs propres réelles. Ce n'est pas possible, donc $\det(g) = 1$. De plus d'après la première question, $|\mathrm{Tr}(g)| \leq 2$, donc $\mathrm{Tr}(g) \in \{-2, -1, 0, 1, 2\}$, ainsi les polynômes caractéristiques possibles sont :
   - $X^2 - 2X + 1$, ce n'est pas possible, sinon 1 serait une valeur propre de g qui n'a pas de valeur propre réelle.
   - $X^2 - X + 1$.
   - $X^2 + 1$.
   - $X^2 + X + 1$.
   - $X^2 + 2X + 1$, ce n'est pas possible, sinon -1 serait une valeur propre de g.

4. - Si $\chi_g(X) = X^2+1$, alors $\mathrm{Sp}(g) = \{i, -i\}$ et g est semblable à $\mathrm{diag}(i, -i)$. Donc $d = 4$.
   - Si $\chi_g(X) = X^2 + X + 1$, alors $\mathrm{Sp}(g) = \{j, j^2\}$, où $j = e^{\frac{2i\pi}{3}}$, et g est semblable à $\mathrm{diag}(j, j^2)$. Donc $d = 3$.
   - Si $\chi_g(X) = X^2 - X + 1$, alors $\mathrm{Sp}(g) = \{e^{i\frac{\pi}{3}}, e^{-i\frac{\pi}{3}}\}$, et g est semblable à $\mathrm{diag}(e^{i\frac{\pi}{3}}, e^{-i\frac{\pi}{3}})$. Donc $d = 6$.

   Finalement en utilisant aussi la question 2, on en déduit que $d \in \{1, 2, 3, 4, 6\}$.

5. On rappelle la relation entre coefficients et racines dans le cas d'un polynôme scindé. Si $P(X) = \sum_{k=0}^{n} a_k X^k = \prod_{k=0}^{n} (X - z_k)$, alors
$$\forall p \in [\![0, n]\!], \quad (-1)^p \frac{a_{n-p}}{a_n} = \sum_{1 \leqslant i_1 < \ldots < i_p \leqslant n} \prod_{k=1}^{p} z_{i_k}.$$

On applique cette formule avec $p = n - i$ et on sait que $a_n = 1$, cela donne

$$\begin{aligned}(-1)^{n-i}a_i &= \sum_{1\leq j_1<\ldots<j_{n-i}\leq n}\prod_{k=1}^{n-i} z_{j_k}\\ |a_i| &\leq \sum_{1\leq j_1<\ldots<j_{n-i}\leq n} \alpha^{n-i} \quad \text{par l'inégalité triangulaire}\\ &\leq \binom{n}{n-i}\alpha^{n-i}\\ &\leq \binom{n}{i}\alpha^{n-i}.\end{aligned}$$

6. On note $A = \{\chi_g,$ tel que $g \in GL_n(\mathbb{Z})$ est d'ordre fini $\}$. Tout élément de A est un polynôme unitaire, à coefficients entiers de la forme $P(X) = X^n + \sum_{i=0}^{n-1} a_i X^i$ et toutes les racines de P sont racines de l'unité, d'après P2, donc de module 1 d'après P1, ainsi $\alpha = 1$. Donc pour tout $i \in [\![1, n-1]\!]$, $|a_i| \leq \binom{n}{i}$. Finalement
$$\text{card}(A) \leq \prod_{i=0}^{n-1}\left(1 + 2\binom{n}{i}\right).$$
Ainsi A est un ensemble fini.

7. On note $B = \{\text{racines de } P, P \in A\}$. Tout polynôme P de A est de degré n, donc a au plus n racines. Ainsi $\text{card}(B) \leq n \times \text{card}(A)$. L'ensemble B est fini. Tous les éléments de B sont des racines de l'unité. Si λ est une racine de l'unité, on appelle ordre de λ le plus petit entier $k \in \mathbb{N}^*$ tel que $\lambda^k = 1$. On note $b = \text{ppcm}\{\text{ordre de } \lambda, \lambda \in B\}$. On pose $C = \{d \in \mathbb{N} | \exists g \in GL_n(\mathbb{Z}) \text{ d'ordre } d\}$. Soit $d \in C$, alors il existe $g \in GL_n(\mathbb{Z})$ d'ordre d. Pour tout $\lambda \in \text{Sp}(\chi_g)$, l'ordre de λ divise b. Donc $g^b = 1$. Par conséquent $d|b$. L'ensemble des diviseurs de b étant fini, on en déduit que C est fini.

2ème Sous-groupes finis de $GL_n(\mathbb{Z})$

1. (a) Comme g est diagonalisable d'après P2, il existe $P \in GL_n(\mathbb{C})$ et D une matrice diagonale telle que $P^{-1}gP = D$. Alors $P^{-1}AP = \frac{1}{m}(P^{-1}gP - I_n) = \frac{1}{m}(D - I_n)$, qui est une matrice diagonale, donc A est diagonalisable sur $\mathbb{C}$. Soit λ une valeur propre de A, et soit x un vecteur propre associé à cette valeurs propre. Alors $Ax = \lambda x$, donc $g(x) = (1 + m\lambda)x$. D'après P1 et P2, on a $|1 + \lambda m| = 1$. Par l'inégalité triangulaire, on a
$$\begin{aligned}1 = |1 + m\lambda| &\geq m|\lambda| - 1\\ m|\lambda| &\leq 2\\ |\lambda| &\leq \frac{2}{m} < 1 \quad \text{car } m \geq 3.\end{aligned}$$

(b) On diagonalise A, il existe $P \in GL_n(\mathbb{C})$ et $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$ tels que

$$A = P \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} P^{-1}.$$

Alors pour tout $\ell \in \mathbb{N}$, on a $A^\ell = P\text{diag}(\lambda_1^\ell, \ldots, \lambda_n^\ell)P^{-1}$. Ainsi $\lim_{\ell \to +\infty} A^\ell = 0$. Or pour tout $\ell \geq 1$, on a $A^\ell \in \mathcal{M}_n(\mathbb{Z})$. Et une suite d'entiers qui converge vers zéro vaut zéro à partir d'un certain rang. Par conséquent il existe $k \in \mathbb{N}$ tel que $A^k = 0$.

(c) A est nilpotente, elle a donc pour seule valeur propre zéro, et comme en plus elle est diagonalisable, la matrice A est la matrice nulle. On en déduit que $g = I_n$.

2. (a) On note $\varphi : G \to \mathcal{M}_n(\mathbb{Z}/m\mathbb{Z}), g \mapsto [g]$ l'application de réduction modulo m des coefficients. φ réalise un morphisme du groupe $(G, \times)$ dans $(GL_n(\mathbb{Z}/m\mathbb{Z}), \times)$. Pour que φ soit injective, il suffit de montrer que $\ker(\varphi) = \{I_n\}$. Soit $g \in \ker(\varphi)$. Alors $\varphi(g) = [I_n]$, ou encore $[g - I_n] = 0$, c'est-à-dire que $g - I_n$ a tous ses coefficients divisibles par m. De plus $g \in G$ et G est un groupe fini, donc l'ordre de g divise le cardinal de G, en particulier g est d'ordre fini, d'après la question précédente, on en déduit que $g = I_n$, donc φ est injective.

(b) Comme φ est injective, on a

$$\text{card}(G) \leq \text{card}(\mathcal{M}_n(\mathbb{Z}/m\mathbb{Z})) = m^{n^2}.$$

Ceci est vrai pour tout $m \geq 3$, en particulier pour $m = 3$, cela donne

$$\text{card}(G) \leq 3^{n^2}.$$

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

1. (a) Pour tout $1 \leq k \leq \ell - 1$, on a l'égalité suivante : $\binom{\ell}{k} = \frac{\ell}{\ell - k}\binom{\ell - 1}{k}$. Donc

$$(\ell - k)\binom{\ell}{k} = \ell\binom{\ell - 1}{k}.$$

ℓ est nombre premier et $\ell \nmid \ell - k$, donc par Gauss, $\ell | \binom{\ell}{k}$.

(b) Comme x et y commutent, on peut appliquer la formule du binôme.

$$(x+y)^\ell - x^\ell - y^\ell = \sum_{k=0}^{\ell} \binom{\ell}{k} x^k y^{\ell-k} - x^\ell - y^\ell = \sum_{k=1}^{\ell-1} \binom{\ell}{k} x^k y^{\ell-k}.$$

D'après la question précédente, pour tout $1 \leq k \leq \ell - 1$, $\binom{\ell}{k}$ est un multiple de ℓ, donc pour tout $1 \leq k \leq \ell - 1$, on a $\binom{\ell}{k} x^k y^{\ell-k} \in \ell R$.

Comme $(R,+)$ est un groupe, on en déduit que la somme est encore dans ℓR. Finalement $(x+y)^\ell - (x^\ell + y^\ell) \in \ell R$.

2. On a

$$\begin{aligned}&\det(A+B) - \det(A)\\ &= \sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma)\left(\prod_{k=1}^{n}(a_{k,\sigma(k)} + b_{k,\sigma(k)}) - (a_{1,\sigma(1)}\dots a_{n,\sigma(n)})\right).\end{aligned}$$

Pour tout $\sigma \in \mathfrak{S}_n$, on a

$$\prod_{k=1}^{n}(a_{k,\sigma(k)} + b_{k,\sigma(k)}) = \sum_{k=0}^{n} \sum_{\substack{1\le i_1<\dots<i_k\le n\\ 1\le j_1<\dots<j_{n-k}\le n\\ \{(i_1,\dots,i_k,j_1,\dots,j_{n-k})\}=\{1,\dots,n\}}} a_{i_1,\sigma(i_1)}\dots a_{i_k,\sigma(i_k)} b_{j_1,\sigma(j_1)}\dots b_{j_{n-k},\sigma(j_{n-k})}.$$

Par conséquent

$$\prod_{k=1}^{n}(a_{k,\sigma(k)} + b_{k,\sigma(k)}) - (a_{1,\sigma(1)}\dots a_{n,\sigma(n)}) = \sum_{k=0}^{n-1} \sum_{\substack{1\le i_1<\dots<i_k\le n\\ 1\le j_1<\dots<j_{n-k}\le n\\ \{(i_1,\dots,i_k,j_1,\dots,j_{n-k})\}=\{1,\dots,n\}}} a_{i_1,\sigma(i_1)}\dots a_{i_k,\sigma(i_k)} b_{j_1,\sigma(j_1)}\dots b_{j_{n-k},\sigma(j_{n-k})}.$$

Comme tous les coefficients de B sont dans I est que I est un idéal, on en déduit que chaque terme de la somme est dans I, et $(I,+)$ est un groupe, donc la somme est dans I. Finalement $\det(A+B) - \det(A) \in I$.

3. Soit $P(X) = \sum_{k=0}^{n} a_k X^k$. On a en utilisant à chaque fois 1. (b) avec $R = \mathbb{Z}[X]$ chaque ligne suivante est dans $\ell\mathbb{Z}[X]$,

$$\begin{aligned}&(a_0 + \dots + a_n X^n)^\ell - (a_0 + \dots + a_{n-1}X^{n-1})^\ell - (a_n X^n)^\ell\\ &(a_0 + \dots + a_{n-1}X^{n-1})^\ell - (a_0 + \dots + a_{n-2}X^{n-2})^\ell - (a_{n-1}X^{n-1})^\ell\\ &\dots\\ &(a_0 + a_1 X)^\ell - a_0^\ell - (a_1 X)^\ell.\end{aligned}$$

On additionne les lignes une à une et cela donne

$$P(X)^\ell - \sum_{k=0}^{n} a_k^\ell (X^k)^\ell \in \ell\mathbb{Z}[X].$$

Par le petit théorème de Fermat, comme ℓ est premier, on obtient $a_k^\ell \equiv a_k \pmod{\ell}$. Finalement

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

4. (a) On applique la question 1 (b) avec $R = \mathcal{M}_n(\mathbb{Z}[X])$. On a $XI_n \in \mathcal{M}_n(\mathbb{Z}[X])$ et $M \in \mathcal{M}_n(\mathbb{Z}) \subset \mathcal{M}_n(\mathbb{Z}[X])$. De plus XI_n et M commutent. Les hypothèses sont réunies, on a

$$(XI_n - M)^\ell - (XI_n)^\ell - (-M)^\ell \in \ell\mathcal{M}_n(\mathbb{Z}[X]).$$

Or ℓ est un nombre premier, si $\ell > 2$, il est impair et $(-1)^\ell = -1$. Si $\ell = 2$, alors $(-1)^\ell = 1 \equiv -1 \pmod 2$. Dans tous les cas

$$(XI_n - M)^\ell - X^\ell I_n + M^\ell \in \ell\mathcal{M}_n(\mathbb{Z}[X]).$$

Ou encore, il existe $A \in \mathcal{M}_n(\mathbb{Z}[X])$ tel que

$$(XI_n - M)^\ell - (X^\ell I_n - M^\ell) = \ell A.$$

(b) On a

$$\begin{aligned}(\chi_M(X))^\ell &= (\det(XI_n - M))^\ell \\ &= \det((XI_n - M)^\ell) \\ &= \det((XI_n - M)^\ell - (X^\ell I_n - M^\ell) + X^\ell I_n - M^\ell) \\ &= \det(X^\ell I_n - M^\ell + \ell A).\end{aligned}$$

On applique la question 2 avec $I = \ell\mathbb{Z}[X]$, cela donne $(\chi_M(X))^\ell - \det(X^\ell I_n - M^\ell) \in \ell\mathbb{Z}[X]$, ou encore

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

(c) On sait que $\chi_{M^\ell}(X^\ell) - \chi_M(X)^\ell \in \ell\mathbb{Z}[X]$, autrement dit

$$(X^{\ell n} - \mathrm{Tr}(M^\ell)X^{\ell(n-1)} + \ldots) - (X^n - \mathrm{Tr}(M)X^{n-1} + \ldots)^\ell \in \ell\mathbb{Z}[X].$$

On utilise la question 3 pour obtenir

$$(X^{\ell n} - \mathrm{Tr}(M^\ell)X^{\ell(n-1)} + \ldots) - (X^{\ell n} - \mathrm{Tr}(M)X^{\ell(n-1)} + \ldots) \in \ell\mathbb{Z}[X].$$

En particulier, le coefficient du terme en degré $X^{\ell(n-1)}$ est dans $\ell\mathbb{Z}$, c'est-à-dire

$$-(\mathrm{Tr}(M^\ell) + \mathrm{Tr}(M) \in \ell\mathbb{Z} \Leftrightarrow \mathrm{Tr}(M^\ell) \equiv \mathrm{Tr}(M) \pmod \ell.$$

5. On démontre par récurrence sur $m \in \mathbb{N}^*$, que

$$\forall m \geq 1, \quad \mathrm{Tr}(g^{p^m}) \equiv \mathrm{Tr}(g) \pmod p.$$

Initialisation, pour $m = 1$, le résultat est vrai.
Hérédité. Soit $m \geq 1$, on suppose le résultat vrai au rang m. On applique la question 4 (c) avec $\ell = p$ et $M = g^{p^m}$, cela donne

$$\begin{aligned}\mathrm{Tr}((g^{p^m})^p) &= \mathrm{Tr}(g^{p^m}) \pmod p \\ \mathrm{Tr}(g^{p^{m+1}}) &= \mathrm{Tr}(g) \pmod p \quad \text{par hypothèse de récurrence.}\end{aligned}$$

D'où le résultat au rang $m+1$. Conclusion, par le principe de récurrence, le résultat est vrai pour tout $m \in \mathbb{N}^*$. En particulier pour $m = r$, on a $\mathrm{Tr}(g^{p^r}) \equiv \mathrm{Tr}(g) \pmod{p}$. L'ordre d'un élément divise l'ordre du groupe, donc $g^{p^r} = I_n$. Finalement, $\mathrm{Tr}(g) \equiv \mathrm{Tr}(I_n) \pmod{p}$, ou encore

$$\mathrm{Tr}(g) \equiv n \pmod{p}.$$

6. On note $\{\lambda_1, \ldots, \lambda_n\}$ le spectre de g, comptées avec leur multiplicité. On sait d'après P1 et P2 que pour tout $i \in [\![1, n]\!]$, $|\lambda_i| = 1$. Comme $\mathrm{Tr}(g) = \sum_{i=1}^{n} \lambda_i$, on en déduit que $-n \leq \mathrm{Tr}(g) \leq n$. Le spectre de g^ℓ est $\{(\lambda_1)^\ell, \ldots, (\lambda_n)^\ell\}$. Ces valeurs propres sont toutes également de module 1, donc on a aussi $-n \leq \mathrm{Tr}(g^\ell) \leq n$. De plus d'après la question 4 (c) avec $M = g$, on a $\mathrm{Tr}(g^\ell) \equiv \mathrm{Tr}(g) \pmod{\ell}$, ou encore $\ell | (\mathrm{Tr}(g^\ell) - \mathrm{Tr}(g))$. On résume

$$\begin{aligned}
-n &\leq \mathrm{Tr}(g) \leq n \\
-n &\leq \mathrm{Tr}(g^\ell) \leq n \\
-2n &\leq \mathrm{Tr}(g^\ell) - \mathrm{Tr}(g) \leq 2n \\
-\ell &< \mathrm{Tr}(g^\ell) - \mathrm{Tr}(g) < \ell \quad \text{et} \quad \ell | (\mathrm{Tr}(g^\ell) - \mathrm{Tr}(g)).
\end{aligned}$$

Donc $\mathrm{Tr}(g^\ell) = \mathrm{Tr}(g)$.

7. (a) Pour alléger les notations, on pose

$$\alpha = \prod_{\substack{\ell \text{ premier} \\ \ell \leq 2n \\ \ell \text{ ne divise pas } k}} \ell.$$

Soit q un facteur premier de m. Raisonnons par l'absurde en supposant que q est inférieur ou égal à $2n$.
Premier cas : q divise k. Alors q divise $m - k = p^r \alpha$. Or q divise k qui n'est pas divisible par p, donc $q \neq p$, par Gauss, q ne divise pas α, ainsi, encore par Gauss q ne divise pas $p^r \alpha$, c'est absurde.
Deuxième cas : q ne divise pas k, alors q divise α, donc q divise $p^r \alpha$, par conséquent q divise $m - p^r \alpha = k$, c'est encore absurde.
Finalement, tous les facteurs premiers de m sont strictement supérieurs à $2n$.

(b) On décompose m en facteurs premiers, $m = q_1 \ldots q_s$. D'après la question précédente, tous les facteurs sont strictement supérieurs à $2n$. On applique la question 6 et on obtient

$$\mathrm{Tr}(g^m) = \mathrm{Tr}((g^{q_1 \cdots q_{s-1}})^{q_s}) = \mathrm{Tr}(g^{q_1 \cdots q_{s-1}}) = \ldots = \mathrm{Tr}(g).$$

Alors

$$\begin{aligned}
\mathrm{Tr}(g^m) &= \mathrm{Tr}(g) \\
\mathrm{Tr}(g^{k+p^r\alpha}) &= \mathrm{Tr}(g) \\
\mathrm{Tr}(g^k (g^{p^r})^\alpha) &= \mathrm{Tr}(g) \\
\mathrm{Tr}(g^k I_n) &= \mathrm{Tr}(g) \\
\mathrm{Tr}(g^k) &= \mathrm{Tr}(g).
\end{aligned}$$

8. (a) On procède par double inclusion. Soit $k \in J_r$. On effectue la division euclidienne de k par p. Il existe $s \in \mathbb{N}$ et $0 \leq t \leq p-1$ tels que $k = ps+t$. Si $t = 0$, alors p divise k et ce n'est pas possible, donc $1 \leq t \leq p-1$. De plus

$$\begin{aligned} ps + t &\leq p^r - 1 \\ ps &\leq p^r - 1 - t \\ ps &< p^r \\ s &< p^{r-1} \\ s &\leq p^{r-1} - 1. \end{aligned}$$

Ainsi $k \in \cup_{0 \leq s \leq p^{r-1}-1}\{ps + t \text{ tels que } 1 \leq t \leq p-1\}$.
Inversement, soit $k \in \cup_{0 \leq s \leq p^{r-1}-1}\{ps + t \text{ tels que } 1 \leq t \leq p-1\}$. Il existe $s \in [\![0, p^{r-1} - 1]\!]$ et $1 \leq t \leq p-1$ tels que $k = ps + t$. Si p divise k, alors p divise $k - ps = t$, c'est impossible, donc $p \nmid k$. De plus

$$\begin{aligned} 0 &\leq s \leq p^{r-1} - 1 \\ 0 &\leq sp \leq p^r - p \\ 1 &\leq sp + t \leq p^r - p + p - 1 \\ 1 &\leq k \leq p^r - 1. \end{aligned}$$

Donc $k \in J_r$.

(b) En utilisant la question précédente, on a

$$\sum_{j \in J_r} \zeta^j = \sum_{s=0}^{p^{r-1}-1} \sum_{t=1}^{p-1} \zeta^{ps+t}.$$

Premier cas, $\zeta = 1$, alors

$$\sum_{j \in J_r} \zeta^j = \sum_{s=0}^{p^{r-1}-1} \sum_{t=1}^{p-1} 1 = p^{r-1}(p-1).$$

Deuxième cas, ζ est d'ordre p, alors

$$\begin{aligned} \sum_{j \in J_r} \zeta^j &= \sum_{s=0}^{p^{r-1}-1} \sum_{t=1}^{p-1} \zeta^t \\ &= p^{r-1} \left(\sum_{t=0}^{p-1} \zeta^t - 1 \right) \\ &= p^{r-1} \left(\frac{1 - \zeta^p}{1 - \zeta} - 1 \right) \\ &= -p^{r-1}. \end{aligned}$$

Troisième cas, $\zeta \neq 1$ et ζ n'est pas d'ordre p, alors

$$\begin{aligned}
\sum_{j\in J_r}\zeta^j &= \sum_{s=0}^{p^{r-1}-1}\sum_{t=1}^{p-1}\zeta^{ps+t} \\
&= \sum_{s=0}^{p^{r-1}-1}\zeta^{ps}\left(\sum_{t=1}^{p-1}\zeta^t\right) \\
&= \left(\sum_{t=1}^{p-1}\zeta^t\right)\left(\sum_{s=0}^{p^{r-1}-1}(\zeta^p)^s\right) \\
&= \left(\sum_{t=1}^{p-1}\zeta^t\right)\left(\frac{1-(\zeta^p)^{p^{r-1}}}{1-\zeta^p}\right) \\
&= \left(\sum_{t=1}^{p-1}\zeta^t\right)\left(\frac{1-\zeta^{p^r}}{1-\zeta^p}\right) = 0.
\end{aligned}$$

9. D'après la question 7, on a pour tout $k \in J_r, \mathrm{Tr}(g^k) = \mathrm{Tr}(g)$. De plus $\mathrm{card}(J_r) = p^{r-1}(p-1)$. On note $\{\lambda_1, \ldots, \lambda_n\}$ les valeurs propres de g, comptées avec multiplicité. On rappelle que pour tout $i \in [\![1, n]\!], \lambda_i^{p^r} = 1$. En appliquant la question 8, on obtient

$$\begin{aligned}
\sum_{k\in J_r}\mathrm{Tr}(g^k) &= \mathrm{card}(J_r)\mathrm{Tr}(g) \\
\mathrm{card}(J_r)\mathrm{Tr}(g) &= \sum_{i=1}^{n}\sum_{j\in J_r}\lambda_i^j \\
p^{r-1}(p-1)\mathrm{Tr}(g) &= n_0 p^{r-1}(p-1) + n_1(-p^{r-1}) \\
\mathrm{Tr}(g) &= n_0 - \frac{n_1}{p-1}.
\end{aligned}$$

10. D'après la question 5, on sait que $\mathrm{Tr}(g) \equiv n \pmod p$, donc il existe $v \in \mathbb{Z}$ tel que $\mathrm{Tr}(g) = n - pv$. On a $-n \leq \mathrm{Tr}(g) \leq n$ comme on l'a vu dans la question 6, ainsi $n - pv \leq n$, donc $v \geq 0$. D'autre part, en utilisant la question 9, on a $\mathrm{Tr}(g) = n_0 - \frac{n_1}{p-1}$, donc $\mathrm{Tr}(g) \geq -\frac{n}{p-1}$. Ainsi

$$\begin{aligned}
n - pv &\geq -\frac{n}{p-1} \\
pv &\leq n\left(1 + \frac{1}{p-1}\right) \\
v &\leq \frac{n}{p-1} \\
v &\leq \left\lfloor \frac{n}{p-1} \right\rfloor \quad \text{car } v \text{ est un entier.}
\end{aligned}$$

4 Cardinaux des p-sous-groupes de $GL_n(\mathbb{Z})$

1. (a) On commence par montrer que f est un projecteur. On calcule

$$f^2 = \frac{1}{(\mathrm{card}(G))^2} \sum_{g\in G} \sum_{h\in G} gh.$$

Pour $g \in G$ fixé, l'application $G \to G, h \mapsto gh$ est bijective, par conséquent $\sum_{h\in G} gh = \sum_{h\in G} h \quad (*)$. Donc

$$f^2 = \frac{1}{(\mathrm{card}(G))^2} \sum_{g\in G} \sum_{h\in G} h$$

$$f^2 = \frac{1}{(\mathrm{card}(G))^2} \times \mathrm{card}(G) \sum_{h\in G} h$$

$$f^2 = f.$$

Donc f est un projecteur.
Montrons maintenant que $\mathrm{Im}(f) = \{x \in \mathbb{C}^n | \forall g \in G, g(x) = x\}$. On procède par double inclusion. Soit $x \in \{x \in \mathbb{C}^n | \forall g \in G, g(x) = x\}$, alors

$$f(x) = \frac{1}{\mathrm{card}(G)} \sum_{g\in G} gx = \frac{1}{\mathrm{card}(G)} \sum_{g\in G} x = \frac{1}{\mathrm{card}(G)} \times \mathrm{card}(G)x = x.$$

Soit $x \in \mathrm{Im}(f)$, alors $f(x) = x$, soit $g \in G$, on a

$$g(x) = g(f(x)) = g\left(\frac{1}{\mathrm{card}(G)} \sum_{h\in G} hx\right)$$

$$= \frac{1}{\mathrm{card}(G)} \left(\sum_{h\in G} gh\right)(x)$$

$$= \frac{1}{\mathrm{card}(G)} \left(\sum_{h\in G} h\right)(x) \quad \text{d'après } (*)$$

$$= f(x) = x.$$

f est bien un projecteur sur $\{x \in \mathbb{C}^n | \forall g \in G, g(x) = x\}$.

(b) Comme f est un projecteur, on a $\mathrm{rg}(f) = \mathrm{Tr}(f)$. Alors $\mathrm{rg}(f) = \frac{1}{\mathrm{card}(G)} \sum_{g\in G} \mathrm{Tr}(g)$, donc

$$\sum_{g\in G} \mathrm{Tr}(g) = \mathrm{card}(G) \times \mathrm{rg}(f).$$

Donc $\sum_{g\in G} \mathrm{Tr}(g)$ est un entier divisible par $\mathrm{card}(G)$.

2. (i) En calculant la trace par blocs, on obtient

$$\mathrm{Tr}(g \otimes h) = \sum_{k=1}^{n} \mathrm{Tr}(g_{kk}h) = \sum_{k=1}^{n} g_{kk}\mathrm{Tr}(h) = \mathrm{Tr}(h) \sum_{k=1}^{n} g_{kk} = \mathrm{Tr}(h)\mathrm{Tr}(g).$$

(ii) Pour tout $i, j \in [\![1, n]\!]$, on a, en tant que bloc :

$$[(g \otimes h)(g' \otimes h')]_{i,j} = \sum_{\ell=1}^{n} g_{i,\ell} h g'_{\ell,j} h' = \left(\sum_{\ell=1}^{n} g_{i,\ell} g'_{\ell,j} \right) hh' = [gg']_{i,j} hh'$$
$$= [gg' \otimes hh']_{i,j}.$$

Donc $(g \otimes h)(g' \otimes h') = gg' \otimes hh'$.

(iii) D'après la question précédente, on a $(g \otimes h)(g^{-1} \otimes h^{-1}) = (gg^{-1}) \otimes (hh^{-1}) = I_n \otimes I_k$. Or

$$I_n \otimes I_k = \begin{pmatrix} I_k & & 0 \\ & \ddots & \\ 0 & & I_k \end{pmatrix} = I_{nk}.$$

Par conséquent $g \otimes h$ est inversible et son inverse est $g^{-1} \otimes h^{-1}$.

3. (a) Supposons que $\varphi^{-1}(\{\gamma'\})$ ne soit pas vide. Alors il existe $\gamma \in \Gamma$ tel que $\varphi(\gamma) = \gamma'$. Montrons que $\varphi^{-1}(\{\gamma'\}) = \gamma H$. On procède par double inclusion. Soit $x \in \gamma H$, il existe $h \in H$ tel que $x = \gamma h$, alors

$$\varphi(x) = \varphi(\gamma h) = \varphi(\gamma)\varphi(h) = \gamma' e' = \gamma'.$$

Donc $x \in \varphi^{-1}(\{\gamma'\})$. On a démontré que $\gamma H \subset \varphi^{-1}(\{\gamma'\})$. Inversement, soit $x \in \varphi^{-1}(\{\gamma'\})$, alors $\varphi(x) = \gamma' = \varphi(\gamma)$, ainsi $\varphi(\gamma^{-1}x) = (\varphi(\gamma))^{-1}\varphi(x) = e'$, donc $\gamma^{-1}x \in H$, ou encore $x \in \gamma H$. Finalement, si $\varphi^{-1}(\{\gamma'\})$ est non vide il est de la forme γH.

(b) Les groupes étant finis, il existe $\gamma'_1, \ldots, \gamma'_s \in \Gamma'$ deux à deux distincts, tels que $\varphi(\Gamma) = \{\gamma'_1, \ldots, \gamma'_s\}$. On a l'union disjointe $\Gamma = \bigcup_{i=1}^{s} \varphi^{-1}(\{\gamma'_i\})$. D'après la question précédente, pour tout i, il existe $\gamma_i \in \Gamma$ tel que $\varphi^{-1}(\{\gamma'_i\}) = \gamma_i H$. De plus pour tout i, l'application $t_i : H \to \gamma_i H, h \mapsto \gamma_i h$ est bijective. Donc

$$\text{card}(\varphi^{-1}(\{\gamma'_i\})) = \text{card}(\gamma_i H) = \text{card}(H).$$

Finalement

$$\text{card}(\Gamma) = \sum_{i=1}^{s} \text{card}(\varphi^{-1}(\{\gamma'_i\}) = s \times \text{card}(H) = \text{card}(\varphi(\Gamma))\text{card}(H).$$

4. (a) Montrons par récurrence sur s que φ_s est un morphisme de groupes.
Initialisation, pour $s = 1, \varphi_s$ est l'identité, donc un morphisme de groupe.
Hérédité. Soit $s \geq 1$. On suppose le résultat vrai au rang s. Soient g et $h \in GL_n(\mathbb{C})$, on a

$$\begin{aligned}
\varphi_{s+1}(gh) &= (gh)^{(s+1)} = (gh)^{(s)} \otimes (gh) = \varphi_s(gh) \otimes (gh) \\
&= \varphi_s(g)\varphi_s(h) \otimes (gh) \quad \text{par hypothèse de récurrence} \\
&= (\varphi_s(g) \otimes g)(\varphi_s(h) \otimes h) \quad \text{d'après la question 2) (ii)} \\
&= (g^{(s)} \otimes g)(h^{(s)} \otimes h) = g^{(s+1)} h^{(s+1)} \\
&= \varphi_{s+1}(g)\varphi_{s+1}(h).
\end{aligned}$$

Donc φ_{s+1} est un morphisme de groupes, le résultat est vrai au rang $s+1$. Conclusion, par le principe de récurrence, pour tout $s \geq 1, \varphi_s$ est un morphisme de groupes.
On considère l'application $\varphi_{s|G} : G \mapsto GL_{n^s}(\mathbb{C})$. Comme G est un groupe fini, $\varphi_s(G)$ est un sous-groupe fini de $GL_{n^s}(\mathbb{C})$. Il existe $g'_1, \ldots, g'_t$ des éléments de $\varphi_s(G)$ tels que $\varphi_s(G) = \{g'_1, \ldots, g'_t\}$. D'après 3.a) pour tout $i \in [\![1, t]\!]$, il existe $g_i \in G$ tel que $\varphi^{-1}(\{g'_i\}) = g_i \ker(\varphi_s \cap G)$. On pose $G_i = g_i \ker(\varphi_s \cap G)$, on a démontré en 3.b) que $\text{card}(G_i) = \text{card}(\ker(\varphi_s \cap G))$. Avec ces notations, on a l'union disjointe suivante, $G = \overset{t}{\underset{i=1}{\cup}} G_i$. De plus d'après 2. (i) et une récurrence immédiate, on a $\text{Tr}(g)^s = \text{Tr}(g^{(s)})$. Ainsi

$$\begin{aligned}
\sum_{g\in G} \text{Tr}(g)^s &= \sum_{g\in G} \text{Tr}(g^{(s)}) \\
&= \sum_{i=1}^{t} \sum_{g\in G_i} \text{Tr}(\varphi_s(g)) \\
&= \sum_{i=1}^{t} \sum_{g\in G_i} \text{Tr}(g'_i) = \sum_{i=1}^{t} \text{card}(G_i)\text{Tr}(g'_i) \\
&= \text{card}(G \cap \varphi_s) \sum_{i=1}^{t} \text{Tr}(g'_i) \\
&= \text{card}(G \cap \varphi_s) \sum_{g'\in\varphi_s(G)} \text{Tr}(g').
\end{aligned}$$

(b) D'après 1.b), $\sum_{g'\in\varphi_s(G)} \text{Tr}(g')$ est divisible par $\text{card}(\varphi_s(G))$, donc il existe $\lambda \in \mathbb{Z}$, tel que $\sum_{g'\in\varphi_s(G)} \text{Tr}(g') = \text{card}(\varphi_s(G)) \times \lambda$, alors

$$\begin{aligned}
\sum_{g\in G} \text{Tr}(g)^s &= \text{card}(G \cap \ker \varphi_s) \times \text{card}(\varphi_s(G)) \times \lambda \\
&= \text{card}(\ker(\varphi_{s|G})) \times \text{card}(\varphi_s(G)) \times \lambda \\
&= \text{card}(G) \times \lambda \quad \text{d'après 3.b)}
\end{aligned}$$

Donc $\sum_{g\in G} \text{Tr}(g)^s$ est divisible par $\text{card}(G)$.

5. (a) Si $\text{Tr}(g) \neq n$, d'après III.10 on sait qu'il existe $v \in [\![1, a]\!]$ tel que $\text{Tr}(g) = n - pv = \tau_v$. Donc $\text{Tr}(g)$ est une racine de P. Si $\text{Tr}(g) = n$, montrons que $g = I_n$. En effet, si l'on note $\{\lambda_1, \ldots, \lambda_n\}$ les valeurs propres de g, alors on a

$$\lambda_1 + \ldots + \lambda_n = \text{Tr}(g) = n = |\lambda_1| + \ldots + |\lambda_n|.$$

On a une égalité dans l'inégalité triangulaire, les coefficients sont donc tous positivement liés. Il existe $t_2, \ldots, t_n$ strictement positifs tels que

pour tout $i \in [\![2,n]\!], \lambda_i = t_i\lambda_1$, donc $|\lambda_i| = t_i|\lambda_1|$, ou encore $t_i = 1$. Finalement $\mathrm{Tr}(g) = n\lambda_1 = n$, donc $\mathrm{Sp}(g) = \{1\}, g$ est diagonalisable avec pour seule valeur propre 1, donc $g = I_n$. Alors

$$\sum_{g\in G} P(\mathrm{Tr}(g)) = P(\mathrm{Tr}(I_n)) = P(n).$$

D'autre part si on écrit $P(X) = \sum_{k=0}^{d} a_k X^k$, alors

$$P(\mathrm{Tr}(g)) = \sum_{k=0}^{d} a_k (\mathrm{Tr}(g))^k$$

$$\sum_{g\in G} P(\mathrm{Tr}(g)) = a_0 \sum_{g\in G} 1 + \sum_{k=1}^{d} a_k \sum_{g\in G} (\mathrm{Tr}(g))^k.$$

$P(X) \in \mathbb{Z}[X]$, donc $a_0 \in \mathbb{Z}$ et $a_0 \sum_{g\in G} 1 = a_0 \mathrm{card}(G)$ est donc divisible par $\mathrm{card}(G)$. D'après la question 4.b), on sait aussi que pour tout $k \in [\![1,d]\!], \mathrm{card}(G)$ divise $\sum_{g\in G} (\mathrm{Tr}(g))^k$, les a_k étant tous des entiers, on en déduit que $\mathrm{card}(G)$ divise $\sum_{g\in G} P(\mathrm{Tr}(g)) = P(n)$.

(b) Comme $\mathrm{card}(G) = p^r$, on en déduit que $v_p(p^r) \leq v_p(P(n))$. Or $P(n) = \prod_{1\leq j\leq a}(n - (n - pj)) = p^a a!$. Donc

$$r = v_p(p^r) \leq v_p(P(n)) = v_p(p^a a!) = a + v_p(a!).$$

6. (a) D'après la question P3 (b), on a

$$r \leq \lfloor \frac{n}{p-1} \rfloor + \sum_{i=1}^{+\infty} \lfloor \frac{\lfloor \frac{n}{p-1} \rfloor}{p^i} \rfloor$$

$$r \leq \frac{n}{p-1} \sum_{i=0}^{+\infty} \frac{1}{p^i}$$

$$r \leq \frac{n}{p-1} \times \frac{1}{1-\frac{1}{p}}$$

$$r \leq \frac{np}{(p-1)^2}.$$

(b) Par conséquent

$$\mathrm{card}(G) = p^r \leq p^{\frac{pn}{(p-1)^2}} = \left(p^{\frac{p}{(p-1)^2}}\right)^n.$$

Il ne reste plus qu'à démontrer que $p^{\frac{p}{(p-1)^2}} \leq 4$. Ou encore que $\frac{p}{(p-1)^2} \ln(p) \leq \ln(4)$. On pose pour tout $x \geq 2, f(x) = \frac{x}{(x-1)^2} \ln(x)$. On a

$$f'(x) = \frac{-x-1}{(x-1)^3} \ln(x) + \frac{1}{(x-1)^2} = \frac{1}{(x-1)^3}(x - 1 - (x+1)\ln(x))$$

On pose $g(x) = x - 1 - (x+1)\ln(x)$, on a $g'(x) = -\ln(x) - \frac{1}{x}$. La fonction g est décroissante, et $g(2) = 1 - 3\ln(2) < 0$, donc g est négative sur $[2, +\infty[$, par conséquent $f'(x)$ est négative également, donc f est décroissante sur $[2, +\infty[$. On a $f(2) = 2\ln(2) = \ln(4)$, ainsi

$$\forall x \geq 2, \quad \frac{x}{(x-1)^2}\ln(x) \leq \ln(4).$$

Donc pour tout nombre premier p on a $p^{\frac{p}{(p-1)^2}} \leq 4$, finalement

$$\mathrm{card}(G) \leq 4^n.$$