Preliminaires

1. Soit z une racine de l'unité. Il existe $n \in \mathbb{N}^*$ tel que $z^n = 1$.
Rappelons que le module réalise un homomorphisme de groupes de $\mathbb{C}^*$ dans $\mathbb{R}^*$, donc :

$$|z|^n = |z^n| = |1| = 1.$$

Or 1 est le seul réel de $\mathbb{R}^*$ qui, élevé à la puissance n, vaut 1. Donc $\boxed{|z| = 1}$.

2. Puisque g est d'ordre d, $g^d = I_n$, donc $X^d - 1$ est un polynôme annulateur de g.
Or le polynôme $X^d - 1 = \prod_{k=0}^{n-1} (X - e^{\frac{2ik\pi}{n}})$ est scindé à racines simples dans $\mathbb{C}[X]$,
donc $\boxed{g \text{ est diagonalisable dans } \mathcal{M}_n(\mathbb{C})}$.
De plus, ses valeurs propres sont les racines de son polynôme minimal, lequel divise $X^d - 1$,
donc $\boxed{\text{ses valeurs propres sont des racines } d\text{-èmes de l'unité}}$.

3.a) Soit $d = \left\lfloor \frac{m}{q} \right\rfloor$ de sorte que $dq \leqslant m$ et $q(d+1) > m$.
Alors q, $2q, \cdots$, dq sont les seuls entiers de $[\![1, m]\!] \cap q\mathbb{Z}$. Donc :

$$\boxed{\text{Card}(\{1 \leqslant k \leqslant m \text{ tels que } q \,|\, k\}) = d = \left\lfloor \frac{m}{q} \right\rfloor}$$

3.b) D'après les propriétés algébriques de la q-valuation, $v_q(m!) = \sum_{k=1}^{m} v_q(k)$.
Soit $\alpha \in \mathbb{N}^*$. Si $k \in [\![1, m]\!]$ est multiple q^α mais pas de $q^{\alpha+1}$, alors $v_q(k) = \alpha$.
D'après la question **3.a**, on compte $\left\lfloor \frac{m}{q^\alpha} \right\rfloor - \left\lfloor \frac{m}{q^{\alpha+1}} \right\rfloor$ tels entiers k dans $[\![1, m]\!]$.
Posons $\alpha_0 = \left\lfloor \frac{\ln(m)}{\ln(q)} \right\rfloor$. Remarquons que $\left\lfloor \frac{m}{q^\alpha} \right\rfloor = 0$ dès que $\alpha > \alpha_0$. Alors :

$$\begin{aligned}
v_q(m!) &= \sum_{\alpha=1}^{\alpha_0} \alpha \left(\left\lfloor \frac{m}{q^\alpha} \right\rfloor - \left\lfloor \frac{m}{q^{\alpha+1}} \right\rfloor \right) \\
&= \sum_{\alpha=1}^{\alpha_0} \sum_{i=1}^{\alpha} \left(\left\lfloor \frac{m}{q^\alpha} \right\rfloor - \left\lfloor \frac{m}{q^{\alpha+1}} \right\rfloor \right) \\
&= \sum_{i=1}^{\alpha_0} \sum_{\alpha=i}^{\alpha_0} \left(\left\lfloor \frac{m}{q^\alpha} \right\rfloor - \left\lfloor \frac{m}{q^{\alpha+1}} \right\rfloor \right) \\
&= \sum_{i=1}^{\alpha_0} \left(\left\lfloor \frac{m}{q^i} \right\rfloor - \left\lfloor \frac{m}{q^{\alpha_0+1}} \right\rfloor \right) \\
&= \sum_{i=1}^{\alpha_0} \left\lfloor \frac{m}{q^i} \right\rfloor \\
\boxed{v_q(m!) &= \sum_{i=1}^{\infty} \left\lfloor \frac{m}{q^i} \right\rfloor}.
\end{aligned}$$

I Eléments d'ordre fini de $\mathbf{GL}_n(\mathbb{Z})$

1. Notons $\mathbb{U} = \{z \in \mathbb{C}\ ;\ |z| = 1\}$.
D'après la question **2** des préliminaires, $\mathrm{Sp}(g) \subset \mathbb{U}$. Notons $\{\lambda,\, \mu\} = \mathrm{Sp}(g)$.
Alors $\mathrm{Tr}(g) = -\lambda - \mu$, donc $\boxed{|\mathrm{Tr}(g)| \leqslant |\lambda| + |\mu| = 2}$.

2. Dans les prochaines questions, nous aurons besoin du lemme suivant :

Pour tout $g \in \mathbf{GL}_n(\mathbb{Z})$, l'ordre de g est le PPCM des ordres de ses valeurs propres.

C'est immédiat en diagonalisant g, ce qui est possible d'après la question **2** des préliminaires.
Donc si $\mathrm{Sp}(g) \subset \mathbb{R}$, alors $\mathrm{Sp}(g) \subset \mathbb{U} \cap \mathbb{R} = \{\pm 1\}$.
Donc d'après notre lemme, $\boxed{\text{les ordres possibles de } g \text{ sont 1 et 2}}$.
Ces ordres sont effectivement possibles, puisque I_2 et $-I_2$ sont d'ordre 1 et 2.

3. Puisque $g \in \mathbf{GL}_n(\mathbb{Z}) \subset \mathcal{M}_n(\mathbb{R})$, le polynôme caractérique χ_g est réel.
Donc dès que l'une des valeurs propres λ de g n'est pas réelle, la seconde vaut $\overline{\lambda}$.
Ainsi, $\chi_g = X^2 - 2\mathrm{Re}(\lambda)X + |\lambda|^2$.
Or $\lambda \in \mathbb{U} \setminus \mathbb{R}$, donc $2\mathrm{Re}(\lambda) \in]-2,\, 2[$ et $|\lambda|^2 = 1$.
De plus, $g \in \mathcal{M}_n(\mathbb{Z})$, donc $\mathrm{Tr}(g) \in \mathbb{Z}$.
Or $\mathrm{Tr}(g) = 2\mathrm{Re}(z)$, donc d'après ce qui précède, $\mathrm{Tr}(g) \in]-2,\, 2[\cap \mathbb{Z} = \{-1,\, 0,\, 1\}$.
Ainsi, $\boxed{g \text{ est l'un des polynômes suivants : } X^2+1,\ X^2+X+1,\ X^2-X+1}$.

4. Rappelons que l'ordre de g est le PPCM des ordres de ses valeurs propres (cf. question **2**).
- Si $\chi_g = X^2 + 1 = (X - i)(X + i)$, l'ordre de g est 4 ;
- si $\chi_g = X^2 + X + 1 = (X - j)(X - j^2)$, l'ordre de g est 3 ;
- si $\chi_g = X^2 - X + 1 = (X - e^{\frac{i\pi}{3}})(X - e^{-\frac{i\pi}{3}})$, l'ordre de g est 6.

Donc, en tenant compte de la question **2**, $\boxed{d \in \{1,\, 2,\, 3,\, 4,\, 6\}}$.

Rem. Ce n'était pas demandé, mais si l'on veut donner des matrices de $\mathbf{GL}_2(\mathbb{Z})$ ayant ces ordres, il suffit de considérer les matrices compagnons associées à ces polynômes :

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ d'ordre 4, } \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \text{ d'ordre 3, } \begin{pmatrix} 0 & -1 \\ 1 & +1 \end{pmatrix} \text{ d'ordre 6.}$$

5. D'après les relations coefficients racines, et puisque P est unitaire :

$$\forall k \in [\![1,\, n-1]\!],\ \frac{a_{n-k}}{1} = (-1)^k \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} \prod_{\ell=1}^{k} z_{i_\ell}\,.$$

Le nombre de n-uplets en indice correspond aux parties à k éléments de $[\![1,\, n]\!]$.
Donc, en posant $i = n - k$, on obtient :

$$\boxed{\forall i \in [\![0,\, n-1]\!],\ |a_i| \leqslant \binom{n}{i} \alpha^{n-i}}.$$

6. Soit $\mathcal{P} = \{\chi_g \ \text{ tels que } g \in \mathbf{GL}_n(\mathbb{Z}) \text{ est d'ordre fini}\}$.
Tout polynôme $P \in \mathcal{P}$ est unitaire et de degré n, donc est déterminé par ses coefficients $a_0, \cdots, a_{n-1}$.
Ceux-ci étant entiers, car $g \in \mathcal{M}_n(\mathbb{Z})$, et bornés d'après la question précédente,
ils ne peuvent prendre qu'un nombre fini de valeurs.
Donc $\boxed{\mathcal{P} \text{ ne contient qu'un nombre fini de polynômes}}$.

7. Puisque $\mathcal{P}$ est un ensemble fini de polynômes de degré n, l'ensemble des racines $\mathcal{Z}$ des polynômes de $\mathcal{P}$ est un ensemble fini.
En outre, les éléments de $\mathcal{Z}$ sont des racines de l'unité, donc sont d'ordre fini.
Notons m le PPCM des ordres de ces racines. Alors, l'ordre de g divise m,
car nous avions établi que l'ordre de g est le PPCM des ordres de ses valeurs propres.
Donc, $\boxed{\text{l'ensemble des ordres possibles des éléments d'ordre fini de } \mathbf{GL}_n(\mathbb{Z}) \text{ est fini}}$.

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

1.a) Puisque g est diagonalisable et que I_n est la seule matrice de sa classe de conjugaison, la matrice $A = (g - I_n)/m$ est diagonalisable.
De plus, pour tout $\lambda \in \mathbb{C}$,

$$\lambda \in \mathrm{Sp}(g) \iff \frac{\lambda - 1}{m} \in \mathrm{Sp}(A).$$

Or nous avons vu que $\mathrm{Sp}(g) \subset \mathbb{U}$. Avec $m \geqslant 3$, on en déduit que :

$$\boxed{\text{toute valeur propre de } A \text{ est en module inférieure à } \frac{2}{m} < 1}.$$

1.b) Soit $P \in \mathbf{GL}_n(\mathbb{C})$ telle que $P^{-1}AP$ soit diagonale.
D'après la question **1.a)**, ses coefficients diagonaux sont en module strictement inférieur à 1.
Donc chacun des coefficients de $(P^{-1}AP)^k$ est nul ou tend vers 0 lorsque k tend vers $+\infty$. Donc :

$$P^{-1}A^kP = (P^{-1}AP)^k \xrightarrow[k\to+\infty]{} 0,$$

Or $\varphi : M \mapsto PMP^{-1}$ est continue, car linéaire en dimension finie, donc :

$$\boxed{A^k = \varphi(P^{-1}A^kP) \xrightarrow[k\to+\infty]{} 0}.$$

2. D'après les questions **1.a)** et et **1.b)**, A est à la fois diagonalisable et nilpotente.
Donc son spectre est égal à $\{0\}$ et sa forme diagonalisée est 0_n, donc $A = 0_n$. Ainsi,

$$\boxed{g = I_n}.$$

3.a) L'application canonique $\varphi : \mathcal{M}_n(\mathbb{Z}) \to \mathcal{M}_n(\mathbb{Z}/m\mathbb{Z})$ est un morphisme d'anneaux.
Supposons que g_1, $g_2 \in G$ sont tels que $\varphi(g_1) = \varphi(g_2)$. Alors :

$$\varphi(g_1{g_2}^{-1}) = \varphi(g_1)\varphi({g_2}^{-1}) = \varphi(g_2)\varphi({g_2}^{-1}) = \varphi(I_n).$$

Notons $g = g_1{g_2}^{-1}$. Alors $\varphi(g - I_n) = 0_n$, donc g vérifie les hypothèses de la question **1**.
Donc $g = I_n$, puis $g_1 = g_2$. Ainsi, $\boxed{\text{la restriction de } \varphi \text{ à } G \text{ est injective}}$.

3.b) Prenons $m = 3$.
D'après la question précédente, G s'injecte dans $\mathcal{M}_n(\mathbb{Z}/3\mathbb{Z})$ de cardinal 3^{n^2}, donc :

$$\boxed{\mathrm{Card}(G) \leqslant 3^{n^2}}.$$

Remarque : D'après la RMS, il est tombé en 2020 à l'oral de l'X l'énoncé suivant :

Soient $n \in \mathbb{N}^*$ et G un sous-groupe fini de $\mathbf{GL}_n(\mathbb{Z})$. Montrer que $|G| \leqslant \prod_{i=0}^{n-1}(3^n - 3^i)$.

cf. `https://www.rms-math.com/images/stories/documents/exosetoiles-2020.pdf`, exercice 48.

III Traces des éléments d'un p-sous-groupes de $\mathbf{GL}_n(\mathbb{Z})$.

1.a) Si $k \in [\![1,\, \ell-1]\!]$, $v_\ell((\ell-k)!) = v_\ell(k!) = 0$ car ℓ étant premier, $\ell \wedge k! = \ell \wedge (\ell-k)! = 1$. Donc :

$$v_\ell\left(\binom{\ell}{k}\right) = v_\ell\left(\frac{\ell!}{(\ell-k)!k!}\right) = v_\ell(\ell!) - v_\ell((\ell-k)!) - v_\ell(k!) = 1.$$

Ainsi,

$$\boxed{\binom{\ell}{k} \text{ est multiple de } \ell}.$$

1.b) Comme x et y commutent, on peut utiliser le binôme de Newton dans R :

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

Or pour tout $k \in [\![1,\, \ell-1]\!]$, d'après la question **1.a)**, $\binom{\ell}{k} x^k y^{\ell-k} \in \ell R$, donc :

$$\boxed{(x+y)^\ell - (x^\ell + y^\ell) \in \ell R}.$$

2. Partons de : $\det(A+B) - \det(A) = \sum_{\sigma \in \Sigma_n} \varepsilon(\sigma) \left(\prod_{j=1}^{n} (a_{\sigma(j),j} + b_{\sigma(j),j}) - \prod_{j=1}^{n} a_{\sigma(j),j} \right)$.

Développons le produit $\prod_{j=1}^{n} (a_{\sigma(j),j} + b_{\sigma(j),j})$; tous les termes contiennent au moins un facteur $b_{\sigma(j),j}$ à l'exception d'un seul : le terme $\prod_{j=1}^{n} a_{\sigma(j),j}$, donc tous sauf celui-là sont dans I.

Donc pour tout $\sigma \in \mathfrak{S}_n$, la différence $\prod_{j=1}^{n} (a_{\sigma(j),j} + b_{\sigma(j),j}) - \prod_{j=1}^{n} a_{\sigma(j),j}$ est dans I. Par conséquent,

$$\boxed{\det(A+B) - \det(A) \in I}.$$

3. Notons $\equiv$ la relation d'équivalence dans $\mathbb{Z}[X]$ selon l'idéal $\ell\,\mathbb{Z}[X]$.
Soient $P \in \mathbb{Z}[X] \smallsetminus 0$, $d = \deg(P)$, $a \in \mathbb{Z}^*$, $A = aX^d$, et $B = P - A$, donc $\deg(B) < \deg(A)$. Alors :

$$\begin{aligned} P(X^\ell) - P(X)^\ell &\equiv A(X^\ell) + B(X^\ell) - (A+B)^\ell \\ &\underset{(1)}{\equiv} A(X^\ell) + B(X^\ell) - A^\ell - B^\ell \\ &\equiv (a - a^\ell)X^{d\ell} + B(X^\ell) - B^\ell \\ &\underset{(2)}{\equiv} B(X^\ell) - B^\ell \end{aligned}$$

(1) car d'après la question **1.b)**, dans l'anneau commutatif $\mathbb{Z}[X]$, $(A+B)^\ell - A^\ell - B^\ell \equiv 0$;
(2) car d'après le petit théorème de Fermat, ℓ étant premier, $\ell \mid a^\ell - a$.

Notons $\mathcal{P}_d$: « Tout polynôme P de degré d vérifie $P(X^\ell) - P(X)^\ell \equiv 0$. ».
Nous venons de montrer à la fois $\mathcal{P}_0$ et $\forall d \geqslant 1,\ \mathcal{P}_{d-1} \Rightarrow \mathcal{P}_d$. Donc par récurrence,

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

4.a) • Prenons $\ell = 2$. Alors :

$$(XI_n - M)^2 - (X^2 I_n - M^2) = -2XM + 2M^2 = 2A \text{ avec } A = -XM + M^2 \in \mathcal{M}_n(\mathbb{Z}[X]).$$

• Considérons maintenant le cas ℓ premier impair.

Dans l'anneau $\mathcal{M}_n(\mathbb{Z}[X])$, XI_n et M commutent, donc d'après la question **1.b)** :

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

Ainsi, dans tous les cas, $\boxed{\big(XI_n - M\big)^\ell - (X^\ell I_n - M^\ell) \in \ell\mathcal{M}_n(\mathbb{Z}[X])}$.

4.b) Appliquons la question **2** à $A = (X^\ell I_n - M^\ell)$ et $B = \big(XI_n - M\big)^\ell - (X^\ell I_n - M^\ell)$ dans l'anneau commutatif $\mathcal{M}_n(\mathbb{Z}[X])$ avec l'idéal $\ell\mathcal{M}_n(\mathbb{Z}[X])$ contenant B.

En notant $\equiv$ la relation d'équivalence selon l'idéal $\ell\mathbb{Z}[X]$ dans l'anneau $\mathbb{Z}[X]$, on a :

$$\chi_M(X)^\ell = \det\big(\big(XI_n - M\big)^\ell\big) = \det(A + B) \underset{\substack{\uparrow \\ \text{question } \mathbf{2}}}{\equiv} \det(A) = \det(X^\ell I_n - M^\ell) = \chi_{M^\ell}(X^\ell),$$

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

4.c) En notant $\equiv$ la relation d'équivalence selon l'idéal $\ell\mathbb{Z}[X]$ dans l'anneau $\mathbb{Z}[X]$, on a :

$$\chi_{M^\ell}(X^\ell) \underset{\substack{\uparrow \\ \text{question } \mathbf{4.b)}}}{\equiv} \chi_M(X)^\ell \underset{\substack{\uparrow \\ \text{question } \mathbf{3}}}{\equiv} \chi_M(X^\ell).$$

Alors, les coefficient en $X^{(n-1)\ell}$ de $\chi_{M^\ell}(X^\ell)$ et $\chi_M(X^\ell)$ sont congrus modulo ℓ.

Donc : $\boxed{\mathrm{Tr}(M^\ell) \equiv \mathrm{Tr}(M) \pmod{\ell}}$.

5. Soit $k \in \mathbb{N}$. Alors $g^{p^{k+1}} = (g^{p^k})^p$.

Or p est premier, donc d'après la question **4.c)**, $\mathrm{Tr}(g^{p^{k+1}}) \equiv \mathrm{Tr}(g^{p^k}) \pmod{p}$.

Or $g^{p^n} = I_n$ d'après le théorème de Lagrange dans G. De proche en proche, il vient :

$$\mathrm{Tr}(g) \equiv \mathrm{Tr}(g^p) \equiv \mathrm{Tr}(g^{p^2}) \equiv \cdots \equiv \mathrm{Tr}(g^{p^n}) \equiv \mathrm{Tr}(I_n) \equiv n \pmod{p}.$$

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

6. De même qu'à la question **I.1**, pour tout $h \in G$, $\mathrm{Sp}(h) \subset \mathbb{U}$, donc $\mathrm{Tr}(h) \in [-n, n]$.

Donc $|\mathrm{Tr}(g^\ell) - \mathrm{Tr}(g)| \leqslant 2n$.

Or d'après la question **4.c)**, $\mathrm{Tr}(g^\ell) \equiv \mathrm{Tr}(g) \pmod{\ell}$.

Donc $\mathrm{Tr}(g^\ell) = \mathrm{Tr}(g)$ ou $|\mathrm{Tr}(g^\ell) - \mathrm{Tr}(g)| \geqslant \ell > 2n$.

Puisque cette dernière inégalité est en contradiction la précédente, $\boxed{\mathrm{Tr}(g^\ell) = \mathrm{Tr}(g)}$.

7. Notons $q = \displaystyle\prod_{\substack{\ell \text{premier} \\ \ell \leqslant 2n \\ \ell \text{ ne divise pas } k}} \ell$.

7.a) Soit $r \leqslant 2n$ un nombre premier.

• Si r divise k, puisque $k \wedge p = 1$, donc $r \wedge p = 1$.

De même $k \wedge q = 1$, donc $r \wedge q = 1$. Ainsi, $r \mid k$ et $r \wedge p^r q = 1$, donc r ne divise pas $k + p^r q = m$.

• Si r ne divise pas k. Alors r est l'un des facteurs premiers de q.

Ainsi, r divise $p^r q$ mais ne divise pas k, donc r ne divise pas m.

Finalement, $\boxed{\text{tous les facteurs premiers de } m \text{ sont strictement supérieurs à } 2n}$.

7.b) Par le théorème de Lagrange dans G, $g^{p^r} = I_n$, donc $g^k = g^{k+p^r q}$.
Notons $\prod_{i=2}^{s} \ell_i = k + p^r q$ une décomposition en facteurs premiers.
D'après la question **7.a)**, les ℓ_i sont tous strictement supérieurs à $2n$. Alors :

$$\mathrm{Tr}(g^k) = \mathrm{Tr}(g^{k+p^r q}) = \mathrm{Tr}\left(g^{\prod_{i=1}^{r} \ell_i}\right) \underset{(1)}{=} \mathrm{Tr}\left(g^{\prod_{i=1}^{r-1} \ell_i}\right) = \cdots \underset{(2)}{=} \mathrm{Tr}(g)$$

(1) d'après la question **6** avec $g^{\prod_{i=1}^{r-1} \ell_i} \in G$ et $\ell_r > 2n$.
(2) en répétant l'étape précédente impliquant le résultat de la question **6**.
Finalement, $\boxed{\mathrm{Tr}(g^k) = \mathrm{Tr}(g)}$.

8.a) Soit $k \in J_r$. Notons $k = ps + t$ avec $s, t \in \mathbb{N}$ et $t < p$ la division euclidienne de k par p.
Puisque $p \not| k$, $t \in [\![1,\, p-1]\!]$. Et bien sûr, $s = \left\lfloor \frac{k}{p} \right\rfloor \leqslant \left\lfloor \frac{p^r - 1}{p} \right\rfloor = \frac{p^r - p}{p} = p^{r-1} - 1$.
Réciproquement, pour tout $s \leqslant p^{r-1} - 1$ et $t \in [\![0,\, p-1]\!]$, $ps + t < p^r$ et $p \not| k$ donc $ps + t \in J_r$.
Ainsi, $\boxed{J_r = \bigcup_{0 \leqslant s \leqslant p^{r-1}-1} \{ps + t \text{ tels que } 1 \leqslant\leqslant p-1\}.}$

8.b) • Si $\zeta = 1$, alors $\sum_{j \in J_r} \zeta^j = \mathrm{Card}(J_r) = \boxed{p^{r-1}(p-1)}$.

• Si $\zeta \neq 1$ et $\zeta^p = 1$, alors d'après la question **8.a)**, $\sum_{j \in J_r} \zeta^j = \sum_{s=0}^{p^{r-1}-1} \sum_{t=1}^{p-1} \zeta^{ps+t} = \boxed{-p^{r-1}}$,
car pour tout s, $\sum_{t=1}^{p-1} \zeta^{ps+t} = \sum_{t=1}^{p-1} \zeta^t = \sum_{t=0}^{p-1} \zeta^t - 1 = 0 - 1$.

• Si $\zeta^p \neq 1$, alors ζ est d'ordre p^α avec $2 \leqslant \alpha \leqslant r$.
Notons $K_r = \{0,\, p,\, 2p,\, \cdots,\, p^r - p\}$ de sorte que $J_r = [\![0,\, p^r - 1]\!] \setminus K_r$.

– Puisque $(\zeta^p)^{p^{r-1}} = 1$, $\sum_{j=0}^{p^{r-1}-1} (\zeta^p)^j = 0$, donc $\sum_{j \in K_r} \zeta^j = 0$.

– De plus, $\zeta^{p^r} = 1$, donc $\sum_{j=0}^{p^r-1} \zeta^j = 0$.

Donc par différence, $\sum_{j \in J_r} \zeta^j = \boxed{0}$.

9. Soit $M \in \mathcal{M}_n(\mathbb{C})$ une matrice diagonale semblable à g (donc $\chi_M = \chi_g$, etc.).
Alors la matrice $N = \sum_{j \in J_r} M^j$ est diagonale.
D'après la question **8** (sachant que $\mathrm{Sp}(M) = \mathrm{Sp}(g)$) :
– les 1 sur la diagonale de M deviennent des $p^{r-1}(p-1)$ sur la diagonale de N,
– les valeurs propres d'ordre p de M deviennent des $-p^{r-1}$ sur la diagonale de N,
– les autres valeurs propres de M deviennent des 0 sur la diagonale de N.
Ainsi,

$$\mathrm{tr}(N) = n_0\, p^{r-1}(p-1) - n_1 p^{r-1}. \tag{1}$$

Mais d'après la question **7**, comme tous les entiers de J_r sont premiers avec p, il vient :

$$\forall j \in J_r,\ \mathrm{tr}(M^j) = \mathrm{tr}(g^j) = \mathrm{tr}(g) = \mathrm{tr}(M). \tag{2}$$

Par conséquent, $\mathrm{tr}(N) = p^{r-1}(p-1)\mathrm{tr}(M)$.
Finalement, en rapprochant (1) et (2), il vient :

$$\boxed{\mathrm{Tr}(g) = \mathrm{Tr}(M) = \frac{n_0\, p^{r-1}(p-1) - n_1 p^{r-1}}{p^{r-1}(p-1)} = n_0 - \frac{n_1}{p-1}}.$$

10. D'après la question **5**, $\mathrm{Tr}(g) \equiv n \pmod p$.
Par ailleurs, on a déjà dit que $\mathrm{Tr}(g) \in [-n,\, n]$, donc :

$$\mathrm{Tr}(g) = \{n - pv\ ;\ v \in \mathbb{N}\}. \tag{1}$$

Cherchons la valeur v la plus grande possible, donc cherchons à minimiser $\mathrm{Tr}(g)$.
Posons $a = \left\lfloor \dfrac{n}{p-1} \right\rfloor$, puis $b = n - (p-1)a$.
L'entier $\mathrm{Tr}(g)$ est supérieur à la trace obtenue si toutes les valeurs propres étaient d'ordre p, donc :

$$\mathrm{Tr}(g) \geqslant -\frac{n}{p-1}.$$

Mais comme $\mathrm{Tr}(g)$ est un entier, il vient :

$$\mathrm{Tr}(g) \geqslant -\left\lfloor \frac{n}{p-1} \right\rfloor = -a. \tag{2}$$

Confrontons (1) et (2). Les entiers v possibles dans (1) doivent vérifier $n - pv \geqslant -a$, donc :

$$v \leqslant \frac{n+a}{p} = \frac{(p-1)a + b + a}{p} = a + \frac{b}{p} < a + 1.$$

Finalement,

$$\boxed{\mathrm{Tr}(g) \in \{n - pv\ ;\ 0 \leqslant v \leqslant a\}.}$$

Rem. *Un exemple simple où la trace de g est négative est donnée par la matrice :*

$$\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$$

qui engendre un groupe d'ordre 3, donc un 3-sous-groupe de $\mathbf{GL}_2(\mathbb{Z})$.

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

1.a) Notons $c = \mathrm{Card}(G)$.

- Tout d'abord, f est un projecteur car :

$$f \circ f = \frac{1}{c^2}\left(\sum_{g\in G} g\right)\left(\sum_{h\in G} h\right) = \frac{1}{c^2}\sum_{g\in G}\left(\sum_{h\in G} gh\right) = \frac{1}{c^2}\sum_{g\in G}\left(\sum_{h'\in G} h'\right) = f$$

où l'on a posé le changement de variables $h' = gh$, possible car l'application $h \mapsto gh$ réalise une bijection de G dans G.

- Notons $I = \{x \in \mathbb{C}^n \ ; \ \forall g \in G, \ g(x) = x\}$. Nous voulons montrer que $\mathrm{Ker}\,(f - I_n) = I$.

L'inclusion $I \subset \mathrm{Ker}\,(f - I_n)$ est évidente : si $x \in I$, alors $f(x) = \dfrac{1}{c}\displaystyle\sum_{g\in G} g(x) = \frac{c}{c}x = x$.

Réciproquement, soient $x \in \mathrm{Ker}\,(f - I_n)$ et $g \in G$. Vérifions que $x \in \mathrm{Ker}\,(g - I_n)$.
Or, par le même changement de variables que précédemment,

$$g(x) = g(f(x)) = \frac{1}{c}\sum_{g\in G} g \circ h(x) = \frac{1}{c}\sum_{h'\in G} h'(x) = f(x) = x.$$

Donc : $\forall x \in G, \ x \in \mathrm{Ker}\,(g - I_n)$. Donc $x \in I$. Ainsi $\mathrm{Ker}\,(f - I_n) \subset I$.

Finalement, $\boxed{f \text{ est un projecteur d'image } \{x \in \mathbb{C}^n \ ; \ \forall g \in G, \ g(x) = x\}}$.

1.b) En diagonalisant un projecteur f, on s'aperçoit que sa trace est égal à $\dim(E_1(f))$, donc à son rang.
Ainsi $\mathrm{Tr}(f) \in \mathbb{Z}$, puis par linéarité de la trace,

$$\boxed{\sum_{g\in G} \mathrm{Tr}(g) \in \mathrm{Card}(G)\mathbb{Z}}.$$

2.

(i) $\mathrm{Tr}(g \otimes h) = \displaystyle\sum_{i=1}^{n} \mathrm{Tr}(g_{ii}h) = \sum_{i=1}^{n} g_{ii}\mathrm{Tr}(h) = \mathrm{Tr}(g)\mathrm{Tr}(h)$. Donc $\boxed{\mathrm{Tr}(g \otimes h) = \mathrm{Tr}(g)\mathrm{Tr}(h)}$.

(ii) Par produit par blocs de taille (k, k), pour tout $(i, j) \in [\![1,\, n]\!]^2$, le (i, j)-ème bloc de taille (k, k) de $(g \otimes h)(g' \otimes h')$ vaut :

$$\sum_{k=0}^{n} (g_{ik}h)(g'_{kj}h') = \left(\sum_{k=0}^{n} g_{ik}g'_{kj}\right) hh'$$

et l'on reconnaît le (i, j)-ème bloc de $gg' \otimes hh'$, donc $\boxed{(g \otimes h)(g' \otimes h') = gg' \otimes hh'}$.

(iii) D'après (ii),

$$(g \otimes h)(g^{-1} \otimes h^{-1}) = gg^{-1} \otimes hh^{-1} = I_n \otimes I_n = \mathrm{diag}(I_k, I_k, \cdots, I_k) = I_{nk}.$$

donc $\boxed{(g \otimes h) \in \mathbf{GL}_{nk}(\mathbb{C}) \text{ et } (g \otimes h)^{-1} = g^{-1} \otimes h^{-1}}$.

3.a) Supposons que $\varphi^{-1}(\{\gamma'\})$ n'est pas vide : soit $\gamma \in \Gamma$ tel que $\varphi(\gamma) = \gamma'$. Soit $\gamma'' \in \Gamma$.

$$\begin{aligned}
\gamma'' \in \varphi^{-1}(\{\gamma'\}) &\iff \varphi(\gamma'') = \gamma' = \varphi(\gamma) \\
&\iff \varphi(\gamma^{-1}\gamma'') = 1_{\Gamma'} \\
&\iff \gamma^{-1}\gamma'' \in H \\
&\iff \gamma'' \in \gamma H
\end{aligned}$$

Donc :

$$\boxed{\varphi^{-1}(\{\gamma'\}) = \varnothing \text{ ou } \exists \gamma \in \Gamma \mid \varphi^{-1}(\{\gamma'\}) = \gamma H}.$$

3.b) Considérons la relation d'équivalence $\mathcal{R}$ dans Γ selon le sous-groupe H :

$$\forall \gamma,\, \gamma' \in \Gamma,\ \gamma \mathcal{R} \gamma' \iff \gamma' \in \gamma H.$$

Alors, les classes d'équivalence sont les γH avec $\gamma \in \Gamma$, chacune de cardinal $\mathrm{Card}(H)$.
En choisissant dans chaque classe d'équivalence un représentant et en notant E l'ensemble de ces représentants, on obtient la partition suivante de Γ :

$$\Gamma = \bigsqcup_{\gamma \in E} \gamma H.$$

Passons aux cardinaux, sachant que H et γH sont en bijection :

$$\mathrm{Card}(\Gamma) = \mathrm{Card}\,(E)\,\mathrm{Card}(H). \tag{1}$$

Enfin, E est en bijection avec l'ensemble des classes d'équivalence, lui-même en bijection avec $\varphi(\Gamma)$ car, en utilisant la question **3.a)** :

$$\begin{array}{rcl} \forall \gamma,\, \gamma' \in \Gamma,\ \gamma \mathcal{R} \gamma' & \iff & \gamma' \in \gamma H \\ & \iff & \gamma' H \in \gamma H \\ & \iff & \varphi(\gamma) = \varphi(\gamma'). \end{array}$$

Donc (1) devient :

$$\boxed{\mathrm{Card}(\Gamma) = \mathrm{Card}\,(\varphi(\Gamma))\,\mathrm{Card}(H)}.$$

4.a) Remarquons que l'application φ_s est bien définie grâce à la question **2.(iii)**.

• Montrons par récurrence sur $s \geqslant 1$ que φ_s est un morphisme de groupes.
Lorsque $s = 1$, $\varphi_1 = \mathrm{id}_{\mathbf{GL}_n(\mathbb{C})}$, qui est bien un morphisme de groupe.
Soit $s \geqslant 2$. Supposons le résultat acquis au rang $s-1$.
Alors pour tout $g, h \in \mathbf{GL}_n(\mathbb{C})$,

$$\begin{array}{rcll} g^{(s)} h^{(s)} & = & (g^{(s-1)} \otimes g)(h^{(s-1)} \otimes h) & \text{(par définition de } \varphi_s) \\ & = & (g^{(s-1)} h^{(s-1)}) \otimes (gh) & \text{(d'après la question } \mathbf{2.(ii)}) \\ & = & (gh)^{(s-1)} \otimes (gh) & \text{(par hypothèse de récurrence)} \\ & = & (gh)^{(s)} & \text{(par définition de } \varphi_s) \end{array}$$

Ceci conclut la récurrence et montre que $\boxed{\varphi_s \text{ est un morphisme de groupes}}$.

• Notons $\varphi_s|_G$ la restriction de φ_s au sous-groupe G de $\mathbf{GL}_n(\mathbb{C})$.
Considérons la classe d'équivalence $\mathcal{R}$ selon le sous-groupe $\mathrm{Ker}\left(\varphi_s|_G\right) = G \cap \mathrm{Ker}\,(\varphi_s)$.
Choisissons un ensemble E de représentants dans G des classes d'équivalence. Alors :

$$\varphi_s \text{ induit une bijection de } E \text{ sur } \mathrm{Im}(\varphi_s|_G) = \varphi_s(G). \tag{1}$$

Comme à la question **3.b)**, on obtient la partition :

$$G = \bigsqcup_{g' \in E} g' \mathrm{Ker}\left(\varphi_s|_G\right) \tag{2}$$

Il vient alors :

$$\begin{array}{rcll} \displaystyle\sum_{g \in G} \mathrm{Tr}(g)^s & = & \displaystyle\sum_{g \in G} \mathrm{Tr}(g^{(s)}) & \text{(d'après la question } \mathbf{2.(i)}) \\ & = & \displaystyle\sum_{g' \in E} \sum_{g \in g' \mathrm{Ker}\left(\varphi_s|_G\right)} \mathrm{Tr}(g^{(s)}) & \text{(d'après (2))} \\ & = & \mathrm{Card}(\mathrm{Ker}\left(\varphi_s|_G\right)) \displaystyle\sum_{g' \in E} \mathrm{Tr}(g'^{(s)}) & \text{(car } \varphi_s \text{ est constante sur } g'\mathrm{Ker}\left(\varphi_s|_G\right)) \\ & = & \boxed{\mathrm{Card}(G \cap \mathrm{Ker}\,(\varphi_s)) \displaystyle\sum_{g'' \in \varphi_s(G)} \mathrm{Tr}(g'')} & \text{(d'après (1))} \end{array}$$

4.b) D'après la question **1.b)** appliquée au groupe $\varphi_s(G)$,

$$\sum_{g'' \in \varphi_s(G)} \mathrm{Tr}(g'') \text{ est un multiple de } \mathrm{Card}(\varphi_s(G)).$$

Donc $\mathrm{Card}(G \cap \mathrm{Ker}\,(\varphi_s)) \sum_{g'' \in \varphi_s(G)} \mathrm{Tr}(g'')$ est un multiple de $\mathrm{Card}(G \cap \mathrm{Ker}\,(\varphi_s))\mathrm{Card}(\varphi_s(G))$.

Or :

* $\mathrm{Card}(G \cap \mathrm{Ker}\,(\varphi_s)) \sum_{g'' \in \varphi_s(G)} \mathrm{Tr}(g'') = \sum_{g \in G} \mathrm{Tr}(g)^s$ d'après la question **4.a)** ;

* $\mathrm{Card}(G \cap \mathrm{Ker}\,(\varphi_s))\mathrm{Card}(\varphi_s(G)) = \mathrm{Card}(G)$ d'après la question **3.b)** appliquée à $\varphi_s|_G$.

Donc :

$$\boxed{\sum_{g \in G} \mathrm{Tr}(g)^s \text{ est un multiple de } \mathrm{Card}(G)}.$$

5.a) Pour tout $s \in \mathbb{N}$, notons K_s l'entier tel que $\sum_{g \in G} \mathrm{Tr}(g)^s = K_s \mathrm{Card}(G)$.

Par ailleurs, notons $(p_s)_s$ les coefficients de P : $P = \sum_{s=0}^{a} p_s X^s$.

Alors, $\mathrm{Card}(G)$ divise $\sum_{g \in G} P(\mathrm{Tr}(g))$ car :

$$\begin{aligned}
\sum_{g \in G} P(\mathrm{Tr}(g)) &= \sum_{g \in G} \sum_{s=0}^{a} p_s \mathrm{Tr}(g)^s \\
&= \sum_{s=0}^{a} p_s \sum_{g \in G} \mathrm{Tr}(g)^s \\
&= \sum_{s=0}^{a} p_s K_s \mathrm{Card}(G) \quad \text{(d'après la question } \mathbf{4.b)}\text{)}
\end{aligned}$$

De plus, $\mathrm{Tr}(I_n) = n$. Par contre, si $g \in G \setminus \{I_n\}$ alors : 1 n'est pas valeur propre de multiplicité n (ceci découle de la diagonalisabilité de g),
donc $\mathrm{Tr}(g) < n$ (car les valeurs propres autres que 1 sont de partie réelle < 1),
donc il existe $j \in [\![1, a]\!]$ tel que $\mathrm{Tr}(g) = n - pj$ d'après la question **III.10**,
donc $P(\mathrm{Tr}(g)) = 0$.
Par conséquent :

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

En confrontant ces deux calculs de $\sum_{g \in G} P(\mathrm{Tr}(g))$, on obtient finalement que :

$$\boxed{\mathrm{Card}(G) \text{ divise } P(n)}.$$

5.b) En exploitant la divisibilité obtenue question **5.a)**, on obtient cette autre divisibilité :

$$p^r = \mathrm{Card}(G) \mid P(n) = \prod_{j=1}^{a} (n - (n - pj)) = \prod_{j=1}^{a} (pj) = p^a\, a!$$

En passant à la p-valuation, il vient :

$$r = v_p(p^r) \leqslant v_p(p^a a!) = a + v_p(a),$$

d'où :

$$\boxed{r \leqslant a + v_p(a).}$$

6.a) D'après la question **3.b)** des préliminaires,

$$v_p(a!) = \sum_{i=1}^{\infty} \left\lfloor \frac{a}{p^i} \right\rfloor \leqslant \sum_{i=0}^{\infty} \frac{a}{p^i} = \frac{a}{1 - \frac{1}{p}} = \frac{pa}{p-1}.$$

Or $a = \left\lfloor \dfrac{n}{p-1} \right\rfloor \leqslant \dfrac{n}{p-1}$, donc :

$$\boxed{r \leqslant \frac{pn}{(p-1)^2}}$$

6.b) En multipliant l'inégalité de la question **6.a)** par $\ln(p)$, on obtient :

$$r \ln(p) \leqslant n \frac{p \ln(p)}{(p-1)^2}.$$

Etudions la fonction $f : x \mapsto \dfrac{x \ln(x)}{(x-1)^2}$ sur $[2, +\infty[$.

Elle est dérivable sur $\mathbb{R}_+^*$ de dérivée : $f'(x) = \dfrac{x - 1 - (x+1)\ln(x)}{(x-1)^3}$.

Cette dérivée est clairement négative sur $[4, +\infty[$, en utilisant le fait que $\ln(4) > 1$.

Donc le maximum de f sur $\mathbb{N} \setminus \{0, 1\}$ existe et est réalisé en 2, 3 ou 4.

Or $f(2) = \ln(4) > 1$, $f(3) = \dfrac{3\ln(3)}{4} < 1$ et $f(4) = \dfrac{4\ln(4)}{9} < 1$ (car $\ln(4) = 2\ln(2) < 2$).

Donc le maximum de f sur $\mathbb{N} \setminus \{0, 1\}$ vaut $\ln(4)$.

Donc, pour tout nombre premier p, $r \ln(p) \leqslant n \ln(4)$.

En passant à l'exponentielle, il vient :

$$\boxed{\mathrm{Card}(G) = p^r \leqslant 4^n}.$$