Préliminaires.

1. Soit $z \in \mathbb{C}$ une racine de l'unité. Il existe $d \in \mathbb{N}^*$ tel que $z^d = 1$. En prenant le module on a $|z|^d = |z^d| = 1$ et donc $|z| = 1$.

2. On a $g^d = \mathrm{I}_n$ et la matrice g est annulée par le polynôme $\mathrm{X}^d - 1$ qui est scindé à racines simples sur $\mathbb{C}$ avec pour racines les d racines d-ièmes de l'unité. Il en découle que g est diagonalisable et que ses valeurs propres sont des racines d-ièmes de l'unité.

3. **(a)** On demande de compter le nombre de multiples de q compris entre 1 et m. L'application $k \mapsto kq$ étant injective il y en a autant que d'entiers k vérifiant $1 \leqslant kq \leqslant m$ c'est-à-dire $\left\lfloor \dfrac{m}{q} \right\rfloor$.

(b) D'après (a), l'entier $d_k = \left\lfloor \dfrac{m}{q^k} \right\rfloor$ est le nombre de multiples de q^k compris entre 1 et m. Mais bien entendu, dans les d_1 multiples de q on trouve les d_2 multiples de q^2 qui contiennent eux mêmes les d_3 multiples de q^3 et ainsi de suite. Le nombre de multiples de q^k qui ne sont pas multiples de q^{k+1} est donc $d_k - d_{k+1}$ et chacun d'entre eux apporte une contribution de k à la valuation en q de $m!$. On a donc

$$\nu_q(m!) = \sum_{k=1}^{+\infty} k(d_k - d_{k+1}) = \sum_{k=1}^{+\infty} k d_k - \sum_{k=1}^{+\infty} (k-1) d_k = \sum_{k=1}^{+\infty} d_k = \sum_{k=1}^{+\infty} \left\lfloor \frac{m}{q^k} \right\rfloor$$

(le calcul est légitime car toutes les sommes sont finies).

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

1. D'après la question 2 des préliminaires g est diagonalisable et admet deux valeurs propres λ_1 et λ_2 qui sont des racines d-ièmes de l'unité et donc de module 1. On a donc $|\operatorname{Tr} g| = |\lambda_1 + \lambda_2| \leqslant |\lambda_1| + |\lambda_2| = 2$.

2. Si les valeurs propres sont réelles elles valent 1 ou -1. On a donc les cas suivants :

- Soit $\lambda_1 = \lambda_2 = 1$ et $g = \mathrm{I}_2$ qui est d'ordre $d = 1$.
- Soit $\lambda_1 = 1$ et $\lambda_2 = -1$ et g est semblable à $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$: c'est une symétrie et elle est d'ordre $d = 2$.
- Soit $\lambda_1 = \lambda_2 = -1$ et $g = -\mathrm{I}_2$ est aussi d'ordre 2.

3. Les valeurs propres de g n'étant pas réelles, conjuguées et de module 1, il existe un réel θ non nul modulo π tel que $\operatorname{Sp} g = \{e^{i\theta}, e^{-i\theta}\}$. On a alors $\det g = 1$ (produit des deux valeurs propres) et $\operatorname{Tr} g = 2\cos\theta$ qui ne peut valoir que $-1, 0, 1$ car pour avoir une trace égale à 2 (resp. -2) il faudrait que θ soit nul (resp. congru à π) modulo 2π. Le polynôme caractéristique de g est égal à $\mathrm{X}^2 - \operatorname{Tr}(g)\mathrm{X} + \det g$ et on a donc trois polynômes possibles, à savoir $\mathrm{X}^2 + 1$, $\mathrm{X}^2 + \mathrm{X} + 1$ et $\mathrm{X}^2 + \mathrm{X} - 1$.

4. Notons que si g admet une valeur propre réelle, la seconde valeur propre est aussi réelle puisque la trace est un entier. Les cas des questions 2 et 3 sont donc exhaustifs. Dans le cas où les valeurs propres sont réelles on a vu que les ordres possibles sont 1 et 2. Poursuivons l'étude du second cas en discutant selon le polynôme caractéristique.

- Si $\chi_g = \mathrm{X}^2 + 1$ alors g est semblable à $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ et on a $g^2 = -\mathrm{I}_2$ et $g^4 = \mathrm{I}_2$ de sorte que $d = 4$.
- Si $\chi_g = \mathrm{X}^2 + \mathrm{X} + 1$ alors g est semblable à $\begin{pmatrix} j & 0 \\ 0 & j^2 \end{pmatrix}$ et on a $g^3 = \mathrm{I}_2$: g est d'ordre 3.
- Si $\chi_g = \mathrm{X}^2 - \mathrm{X} + 1$ alors g est semblable à $\begin{pmatrix} -j & 0 \\ 0 & -j^2 \end{pmatrix}$ et on a $g^3 = -\mathrm{I}_2$, $g^2 \neq \mathrm{I}_2$ et $g^6 = \mathrm{I}_2$: g est d'ordre 6.

On peut conclure que l'ordre d d'une matrice de $\mathrm{GL}_2(\mathbb{Z})$ appartient à $\{1, 2, 3, 4, 6\}$. On peut noter que tous les ordres sont bien réalisables ce que l'énoncé ne demande pas : il suffit de prendre les matrices compagnons des polynômes en question.

5. On utilise les relations coefficients-racines pour un polynôme scindé. Comme P est unitaire on a, par inégalité triangulaire, $a_i = (-1)^{n-i}\sigma_{n-i}(z_1, \dots, z_n)$ et donc

$$|a_i| = |\sigma_{n-i}(z_1, \dots, z_n)| = \left| \sum_{\mathrm{I} \in \mathcal{P}_{n-i}([\![1,n]\!])} \prod_{i \in \mathrm{I}} z_i \right| \leqslant \sum_{\mathrm{I} \in \mathcal{P}_{n-i}([\![1,n]\!])} \prod_{i \in \mathrm{I}} |z_i| \leqslant \sum_{\mathrm{I} \in \mathcal{P}_{n-i}([\![1,n]\!])} \alpha^{n-i} = \binom{n}{i} \alpha^{n-i}$$

6. Si $g \in \mathrm{GL}_n(\mathbb{Z})$ est d'ordre fini alors son polynôme caractéristique est à coefficients entiers, unitaire, et toutes ses racines sont de module 1 (d'après la partie préliminaire). En posant $\chi_g = \mathrm{X}^n + a_{n-1}\mathrm{X}^{n-1} + \cdots + a_0$, la question précédente, avec $\alpha = 1$, montre que $|a_i| \leqslant \binom{n}{i}$ pour tout i. Il en découle que les coefficients de χ_g ne peuvent prendre qu'un nombre fini de valeurs et par suite l'ensemble des polynômes caractéristiques des éléments d'ordre fini de $\mathrm{GL}_n(\mathbb{Z})$ est fini.

7. Si $g \in \mathrm{GL}_n(\mathbb{Z})$ est d'ordre fini d alors son polynôme minimal π_g divise $\mathrm{X}^d - 1$ et divise aussi le polynôme caractéristique de g par le théorème de Cayley-Hamilton. Il découle de la question précédente que l'ensemble des polynômes minimaux des éléments d'ordre fini de $\mathrm{GL}_n(\mathbb{Z})$ est aussi fini. Pour chacun de ces polynômes P on choisit le plus petit entier d_P tel que P divise $\mathrm{X}^{d_\mathrm{P}} - 1$. L'ensemble des ordres finis possibles des éléments de $\mathrm{GL}_n(\mathbb{Z})$ est exactement l'ensemble fini de ces entiers d_P.

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

1. **(a)** La matrice g est diagonalisable avec pour valeurs propres des racines de l'unité et A, qui est un polynôme en g, est donc aussi diagonalisable. De plus les valeurs propres de A sont de la forme $\lambda = \dfrac{z-1}{m}$ où z est une valeur propre de g et vérifient donc $|\lambda| \leqslant \dfrac{2}{m} \leqslant \dfrac{2}{3} < 1$.

(b) Il existe $\mathrm{P} \in \mathrm{GL}_n(\mathbb{C})$ et D diagonale à coefficients diagonaux de module strictement inférieur à 1 tels que $\mathrm{A} = \mathrm{PDP}^{-1}$. Clairement $\mathrm{D}^k \longrightarrow 0$ et comme $\mathrm{A}^k = \mathrm{PD}^k\mathrm{P}^{-1}$, il en découle que la suite A^k tend vers 0 lorsque k tend vers l'infini. Mais par hypothèse A est une matrice à coefficients dans $\mathbb{Z}$ et toutes les matrices A^k sont encore dans $\mathcal{M}_n(\mathbb{Z})$. Comme une suite d'entiers qui converge vers 0 est nécessairement stationnaire, on en déduit que $\mathrm{A}^k = 0$ pour k assez grand, autrement dit que A est nilpotente.

(c) Comme A est à la fois diagonalisable et nilpotente, elle est nulle et on a donc $g = \mathrm{I}_n$.

2. **(a)** Si $\mathrm{M} \in \mathcal{M}_n(\mathbb{Z})$ on notera $\overline{\mathrm{M}}$ la matrice de $\mathcal{M}_n(\mathbb{Z}/n\mathbb{Z})$ obtenue en réduisant les coefficients de M modulo m. L'application $\mathrm{M} \mapsto \overline{\mathrm{M}}$ est un morphisme (surjectif) d'anneaux de $\mathcal{M}_n(\mathbb{Z})$ dans $\mathcal{M}_n(\mathbb{Z}/n\mathbb{Z})$ et ce morphisme induit un morphisme de groupes de $\mathrm{GL}_n(\mathbb{Z})$ dans le groupe $\mathrm{GL}_n(\mathbb{Z}/m\mathbb{Z})$ des éléments inversibles de l'anneau $\mathcal{M}_n(\mathbb{Z}/n\mathbb{Z})$. La question précédente montre que ce morphisme restreint à G est injectif. En effet, si $g \in \mathrm{G}$ alors g est d'ordre fini puisque G est fini et si $\overline{g} = \overline{\mathrm{I}_n}$ cela signifie que la matrice $g - \mathrm{I}_n$ a tous ses coefficients divisibles par m. La question 1 s'applique et montre que $g = \mathrm{I}_n$.

(b) On peut appliquer ce qui précède avec $m = 3$. On a donc, pour tout sous-groupe fini G de $\mathrm{GL}_n(\mathbb{Z})$, la majoration $|\mathrm{G}| \leqslant |\mathrm{GL}_n(\mathbb{Z}/3\mathbb{Z})| \leqslant |\mathcal{M}_n(\mathbb{Z}/3\mathbb{Z})| = 3^{n^2}$.

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

1. **(a)** Soit $k \in [\![1, \ell-1]\!]$. On a $\ell\binom{\ell-1}{k-1} = k\binom{\ell}{k}$ donc ℓ divise $k\binom{\ell}{k}$. Mais comme ℓ est premier et $k < \ell$, les entiers ℓ et k sont premiers entre eux donc ℓ divise $\binom{\ell}{k}$ par le lemme de Gauss.

(b) Comme x et y sont deux éléments de R qui commutent on peut utiliser la formule du binôme de Newton et on a

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

en vertu de (a).

2. Soit $M \in \mathcal{M}_n(R)$ dont les colonnes sont notées $C_1, \dots, C_n$. Si l'une (au moins) des colonnes de M a tous ses coefficients dans l'idéal I alors le développement de $\det M$ selon cette colonne montre que $\det M \in I$. Notons alors $A_1, \dots, A_n$ les colonnes de A et $B_1, \dots, B_n$ les colonnes de B qui sont toutes à coefficients dans I par hypothèse. Si on développe le déterminant $\det(A+B) = \det(A_1 + B_1, \dots, A_n + B_n)$ par multilinéarité on obtient une somme de 2^n déterminants. Hormis $\det A$ tous les autres déterminants ont au moins une colonne B_i et sont donc dans I d'après la remarque initiale. On a donc bien $\det(A+B) - \det A \in I$.

3. Pour $P, Q \in \mathbb{Z}[X]$ on notera $P \equiv Q\ [\ell]$ lorsque $P - Q \in \ell\mathbb{Z}[X]$. La question 1.(b) appliquée avec $R = \mathbb{Z}[X]$ (qui est commutatif) montrer que pour tous P, Q dans $\mathbb{Z}[X]$ on a $(P+Q)^\ell \equiv P^\ell + Q^\ell\ [\ell]$. Une récurrence immédiate permet de généraliser cela à une somme finie quelconque de polynômes. Pour $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$ on a donc

$$P(X)^\ell \equiv \sum_{k=0}^{n} a_k^\ell X^{k\ell} \equiv \sum_{k=0}^{n} a_k X^{k\ell} = P(X^\ell)$$

la seconde congruence découlant du petit théorème de Fermat.

4. **(a)** On applique la question 1.(b) avec l'anneau $R = \mathcal{M}_n(\mathbb{Z}[X])$. La matrice XI_n et la matrice $-M$ commutent et on a donc

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

Cela donne directement le résultat souhaité si ℓ est impair. Mais si $\ell = 2$ il reste encore vrai puisque

$$(XI_n - M)^2 - (X^2 I - M^2) = 2M^2 - 2XM \in 2\mathcal{M}_n(\mathbb{Z}[X])$$

(b) On applique maitenant la question 2 avec l'anneau commutatif $R = \mathbb{Z}[X]$ et l'idéal $I = \ell\mathbb{Z}[X]$. On a donc

$$\chi_M(X)^\ell - \chi_{M^\ell}(X^\ell) = \det(XI_n - M)^\ell - \det(X^\ell I_n - M^\ell) \in \ell\mathbb{Z}[X]$$

en prenant $A = X^\ell I_n - M^\ell$ et $B = (XI_n - M)^\ell - (X^\ell I_n - M^\ell)$ avec les notations de la question 2.

(c) Avec la question 3 on a donc $\chi_{M^\ell}(X^\ell) \equiv \chi_M(X)^\ell \equiv \chi_M(X^\ell)$. La trace d'une matrice de $\mathcal{M}_n(\mathbb{Z})$ est l'opposé du coefficient de X^{n-1} dans le polynôme caractéristique. On a donc $\operatorname{Tr} M^\ell \equiv \operatorname{Tr} M\ [\ell]$.

5. Soit $g \in G$. Par le théorème de Lagrange on a $g^{p^r} = I_n$. En itérant le résultat de 4.(c) avec $\ell = p$ on a donc modulo p

$$\operatorname{Tr}(g) \equiv \operatorname{Tr}(g^p) \equiv \operatorname{Tr}(g^{p^2}) \equiv \cdots \equiv \operatorname{Tr}(g^{p^r}) = \operatorname{Tr}(I_n) = n$$

6. D'après 4.(c) on a $\operatorname{Tr}(g^\ell) \equiv \operatorname{Tr}(g)[\ell]$ puisque ℓ est premier. Mais comme les valeurs propres de g (et donc celles de g^ℓ aussi) sont de module 1 on a $|\operatorname{Tr} g| \leqslant n$. Ainsi, $\operatorname{Tr}(g^\ell) - \operatorname{Tr} g$ est un entier de $[\![-2n, 2n]\!]$ et il est divisible par $\ell > 2n$. C'est donc qu'il est nul et $\operatorname{Tr}(g^\ell) = \operatorname{Tr}(g)$.

7. **(a)** Soit q un nombre premier $\leqslant 2n$. Si q ne divise pas k alors il divise le produit et par conséquent il ne divise pas m. Si q divise k alors il n'est pas égal à p et ne divise par $m - k$ donc ne divise pas m. Ainsi, tous les facteurs premiers de m sont $> 2n$.

(b) Si $g \in G$ et si q_1, q_2 sont deux nombres premiers $> 2n$ on a $\operatorname{Tr}(g) = \operatorname{Tr}(g^{q_1}) = \operatorname{Tr}(g^{q_1 q_2})$ en appliquant deux fois le résultat de la question 6, une fois avec g et la seconde fois avec g^{q_1} qui reste dans le groupe G. En itérant cela on a donc $\operatorname{Tr}(g^m) = \operatorname{Tr}(g)$ pour tout $g \in G$ où m est l'entier de la question (a). Mais comme l'ordre de g divise p^r on a clairement $g^m = g^k$ pour tout $g \in G$.

8. **(a)** J_r est l'ensemble des entiers de 0 à $p^r - 1$ non congrus à 0 modulo p, ou encore l'ensemble des entiers naturels de quotient par p strictement inférieur à p^{r-1} et de reste entre 1 et $p-1$. Si on partionne cet ensemble selon la valeur du quotient s, on obtient que J_r est la réunion disjointe de $p^{r-1} - 1$ parties qui sont les $I_s = \{ps + t, 1 \leqslant t \leqslant p-1\}$.

(b) Le résultat est clair si $\zeta = 1$. Si ζ est d'ordre p, en particulier $\zeta \neq 1$ et $\displaystyle\sum_{j=0}^{p^{r-1}-1} \zeta^j = 0$. Comme par ailleurs, $\zeta^p = 1$, la somme $\displaystyle\sum_{j=0}^{p-1} \zeta^j$ est nulle et $\displaystyle\sum_{j\in \mathrm{I}_s} \zeta^j = \sum_{t=1}^{p-1} \zeta^t = -1$, si bien que $\displaystyle\sum_{j\in \mathrm{J}_r} \zeta^r = -p^{r-1}$ puisque s peut prendre p^{r-1} valeurs possibles. Il reste le cas $\zeta^p \neq 1$. On a alors

$$\sum_{j\in \mathrm{J}_r} \zeta^j = \sum_{t=1}^{p-1} \zeta^t \sum_{s=0}^{p^{r-1}-1} (\zeta^p)^s = \sum_{t=1}^{p-1} \zeta^t \frac{\zeta^{p^r}-1}{\zeta^p - 1} = 0$$

puisque $\zeta^{p^r} = 1$.

9. On a $\displaystyle\sum_{\substack{0\leqslant k\leqslant p^r-1\\ p\nmid k}} \mathrm{Tr}(g^k) = \sum_{\substack{0\leqslant k\leqslant p^r-1\\ p\nmid k}} \mathrm{Tr}(g) = (p^r - p^{r-1})\,\mathrm{Tr}\, g = p^{r-1}(p-1)\,\mathrm{Tr}(g)$. Or $\displaystyle\sum_{\substack{0\leqslant k\leqslant p^r-1\\ p\nmid k}} \mathrm{Tr}(g^k) = \mathrm{Tr}\left(\sum_{k\in \mathrm{J}_r} g^k\right)$, et si on diagonalise g dans une base adaptée, la matrice $\displaystyle\left(\sum_{k\in \mathrm{J}_r} g^k\right)$ est aussi diagonalisée et on retrouve sur la diagonale des sommes $\displaystyle\sum_{k\in \mathrm{J}_r} \zeta^k$, avec ζ valeur propre de g. On a donc sur la diagonale $p^{r-1}(p-1)$ qui apparaît n_0 fois et $-p^{r-1}$ qui apparaît n_1 fois, les autres coefficients étant nuls. Ainsi

$$p^{r-1}(p-1)\,\mathrm{Tr}(g) = \sum_{\substack{0\leqslant k\leqslant p^r-1\\ p\nmid k}} \mathrm{Tr}(g^k) = n_0 p^{r-1}(p-1) - n_1 p^{r-1},$$

ce qui donne $\mathrm{Tr}(g) = n_0 - \dfrac{n_1}{p-1}$.

10. On a $|\,\mathrm{Tr}\, g| \leqslant n$ donc $\dfrac{n - \mathrm{Tr}\, g}{p} \in \mathbb{N}$ d'après la question 5. Par ailleurs, si on pose

$$v = \frac{n-\mathrm{Tr}\, g}{p} = \frac{1}{p}\left(\frac{n_1}{p-1} + n - n_0\right) \leqslant \frac{1}{p}\left(\frac{n-n_0}{p-1} + n - n_0\right) = \frac{n-n_0}{p-1} \leqslant \frac{n}{p-1},$$

on a bien $\mathrm{Tr}\, g = n - pv$ avec $0 \leqslant v \leqslant a = \left\lfloor \dfrac{n}{p-1} \right\rfloor$.

4 Cardinaux des p-sous-groupe de $\mathrm{GL}_n(\mathbb{Z})$.

1. **(a)** Si $g_0 \in \mathrm{G}$, $g_0 f = \dfrac{1}{|\mathrm{G}|}\displaystyle\sum_{g\in \mathrm{G}} g_0 g = \frac{1}{|\mathrm{G}|}\sum_{g'\in \mathrm{G}} g' = f$ car $g \longmapsto g' = g_0 g$ est une permutation du groupe G. Donc $f\circ f = \dfrac{1}{|\mathrm{G}|}\displaystyle\sum_{g\in \mathrm{G}} g\circ f = \frac{1}{|\mathrm{G}|}\sum_{g\in \mathrm{G}} f = f$ et f est un projecteur. Notons $\mathrm{F} = \{x \in \mathbb{C} | \forall g \in \mathrm{G}, g(x) = x\}$. Clairement tout vecteur de F est laissé fixe par f. Réciproquement, si $x \in \mathrm{Im}\, f$, on a $f(x) = x$ et donc $g(f(x)) = g(x)$ mais aussi $g(f(x)) = f(x) = x$ puisque $gf = f$. Donc $x \in \mathrm{F}$. On conclut que $\mathrm{Im}\, f = \mathrm{F}$.

(b) Comme f est un projecteur, en prenant une base du noyau de f et une base de $\mathrm{Im}\, f$, on obtient par concaténation une base de $\mathbb{C}^n$ dans laquelle la matrice de f est diagonale avec des zéros et des un sur la diagonale. La trace de f est donc égale au rang de f et il s'agit en particulier d'un entier. Par conséquent $\displaystyle\sum_{g\in \mathrm{G}} \mathrm{Tr}(g) = |\mathrm{G}|\,\mathrm{Tr}(f)$ est un entier divisible par $|\mathrm{G}|$.

2. (i) La trace de $g\otimes h$ est $\mathrm{Tr}(g\otimes h) = \displaystyle\sum_{i=1}^{n} g_{ii}\,\mathrm{Tr}\, h = \mathrm{Tr}\, g\,\mathrm{Tr}\, h$.

(ii) Pour une matrice M de taille nk écrite sous forme de n^2 blocs de taille k, on note $[\mathrm{M}]_{ij}$ le bloc d'indice (i, j) :

$$[(g \otimes h)(g' \otimes h')]_{ij} = \sum_{l=1}^{n} g_{il} h g'_{lj} h' = \left(\sum_{l=1}^{n} g_{il} g'_{lj} \right) hh' = [gg']_{ij} hh' = [(gg') \otimes (hh')]_{ij}.$$

(iii) On a $(g \otimes h)(g^{-1} \otimes h^{-1}) = (gg^{-1} \otimes hh^{-1}) = \mathrm{I}_n \otimes \mathrm{I}_k = \mathrm{I}_{nk}$. On en déduit que $(g \otimes h)$ est inversible d'inverse $g^{-1} \otimes h^{-1}$.

3. **(a)** Supposons que γ' ait un antécédant γ. Alors pour y dans Γ, on a

$$y \in \varphi^{-1}(\gamma') \iff \varphi(y) = \gamma' = \varphi(\gamma) \iff \varphi(y)\varphi(\gamma)^{-1} = e_{\Gamma'} \iff y\gamma^{-1} \in \operatorname{Ker}\varphi = \mathrm{H} \iff y \in \gamma\mathrm{H}.$$

Donc $\varphi^{-1}(\gamma') = \gamma\mathrm{H}$.

(b) Le groupe Γ est la réunion disjointe des $\varphi^{-1}(\gamma')$ pour γ' décrivant l'image de φ. Or chaque de ces parties est de cardinal $|\mathrm{H}|$ puisque H et γH sont en bijection par $x \longmapsto \gamma x$. Donc $|\Gamma| = |\mathrm{H}|.|\operatorname{Im}\varphi|$.

4. **(a)** Vérifions que φ_s est un morphisme de groupes par récurrence sur s. C'est trivial si $s = 1$. Si $s \geqslant 2$, φ_{s-1} est un morphisme de groupes par hypothèse de récurrence et en particulier si $g \in \mathrm{GL}_n(\mathbb{C})$, $g^{(s-1)} \in \mathrm{GL}_{n^{s-1}}(\mathbb{C})$ et avec 2(iii), $g^{(s)}$ est bien dans $\mathrm{GL}_{n^s}(\mathbb{C})$. Pour $g, h \in \mathrm{GL}_n(\mathbb{C})$, on a

$$\varphi_s(gh) = (gh)^{(s-1)} \otimes (gh) = g^{(s-1)} h^{(s-1)} \otimes (gh) = (g^{(s-1)} \otimes g)(h^{(s-1)} \otimes h) = g^{(s)} h^{(s)} = \varphi_s(g)\varphi_s(h),$$

ce qui prouve que φ_s est un morphisme de groupes.
Par une récurrence immédiate, $\operatorname{Tr}(g^{(s)}) = \operatorname{Tr}(g)^s$ si bien que $\sum_{g \in \mathrm{G}} \operatorname{Tr}(g^{(s)}) = \sum_{g \in \mathrm{G}} \operatorname{Tr}(g)^s$. Dans cette somme, on va rassembler les $g^{(s)}$ qui sont égaux à un certain $g' \in \varphi_s(\mathrm{G})$. Combien y en a t-il ? En reprenant le travail du 3a, il y en a autant que $\operatorname{Card}\ \operatorname{Ker}\varphi_{s\,|\mathrm{G}} = \operatorname{Card}\ (\operatorname{Ker}\varphi_s \cap \mathrm{G})$. Ainsi,

$$\sum_{g \in \mathrm{G}} \operatorname{Tr}(g)^s = \sum_{g \in \mathrm{G}} \operatorname{Tr}(g^{(s)}) = \sum_{g' \in \varphi_s(\mathrm{G})} \operatorname{Tr}(g') \operatorname{Card}\ (\operatorname{Ker}\varphi_s \cap \mathrm{G}) = \operatorname{Card}\ (\operatorname{Ker}\varphi_s \cap \mathrm{G}) \sum_{g' \in \varphi_s(\mathrm{G})} \operatorname{Tr}(g').$$

(b) Comme $\varphi_s(\mathrm{G})$ est un sous-groupe de $\mathrm{GL}_{n^s}(\mathbb{C})$ la question 1.(b) montre que $\sum_{g' \in \varphi_s(\mathrm{G})} \operatorname{Tr}(g')$ est un multiple entier de $\operatorname{Card}\varphi_s(\mathrm{G})$ qui s'écrit $\mathrm{K}\operatorname{Card}\varphi_s(\mathrm{G})$ avec $\mathrm{K} \in \mathbb{Z}$. Donc on a

$$\sum_{g \in \mathrm{G}} \operatorname{Tr}(g)^s = \mathrm{K}\operatorname{Card}\ (\operatorname{Ker}\varphi_s \cap \mathrm{G}) \operatorname{Card}\varphi_s(\mathrm{G}) = \mathrm{K}\operatorname{Card}\mathrm{G},$$

en vertu de 3.(b).

5. **(a)** Par le résultat de la partie 3, chaque $\mathrm{P}(\operatorname{Tr}(g))$ est nul sauf pour $g = \mathrm{I}_n$: en effet si $\operatorname{Tr} g = n$, comme les valeurs propres distinctes ou confondues de g ont une partie réelle inférieur ou égale à 1, cette partie réelle vaut exactement 1 et comme elle sont de module 1, elles sont égales toutes à 1 : g étant diagonalisable, $g = \mathrm{I}_n$ et $\sum_{g \in \mathrm{G}} \mathrm{P}(\operatorname{Tr}(g)) = \mathrm{P}(n)$. Si l'on écrit $\mathrm{P} = c_0 + c_1\mathrm{X} + \cdots + c_a\mathrm{X}^a$, on a par 4.(b)

$$\mathrm{P}(n) = c_0|\mathrm{G}| + c_1 \sum_{g \in \mathrm{G}} \operatorname{Tr}(g) + \cdots + c_a \sum_{g \in \mathrm{G}} \operatorname{Tr}(g)^a \equiv 0\ \ [|\mathrm{G}|]$$

et $\mathrm{P}(n)$ est divisible par $|\mathrm{G}|$.

(b) On a $r = \nu_p(|\mathrm{G}|) \leqslant \nu_p(\mathrm{P}(n)) = \nu_p(p^a a!) = a + \nu_p(a!)$.

6. **(a)** Par la formule de la partie I on a $\nu_p(a!) \leqslant \sum_{i \geqslant 2} \frac{a}{p^i} = \frac{a}{p-1}$ et comme $a \leqslant \frac{n}{p-1}$,

$$r \leqslant \frac{n}{p-1} + \frac{a}{p-1} \leqslant \frac{n}{p-1} + \frac{n}{(p-1)^2} = \frac{pn}{(p-1)^2}.$$

(b) Ainsi, la majoration ontenue est $|\mathrm{G}| = p^r \leqslant p^{\frac{pn}{(p-1)^2}} = \exp\left(\dfrac{p\ln p}{(p-1)^2}n\right)$. Considérons sur $[2,+\infty[$, la fonction de classe C^∞, $x \longmapsto \dfrac{x\ln x}{(x-1)^2}$. Sa dérivée est $x \longmapsto \dfrac{x - x\ln x - \ln x - 1}{(x-1)^3}$. La dérivée du numérateur $x \longmapsto x - x\ln x - \ln x - 1$ est $x \longmapsto -\dfrac{1}{x} - \ln x < 0$. Donc ce numérateur décroît et comme en 2, il vaut $1 - 2\ln 2 - \ln 2 < 0$, la dérivée reste strictement négative sur $[2,+\infty[$. Cette étude de fonction prouve que f atteint son maximum en 2. Comme $p \geqslant 2$, on en déduit

$$|\mathrm{G}| \leqslant \exp(2\ln 2n) = 4^n.$$