X-ENS 2021 MP maths A

Adrien JOSEPH

Préliminaires

1. On dispose de $d \in \mathbb{N}^*$ tel que $z^d = 1$. Donc $\left|z^d\right| = 1$, *i.e.* $|z|^d = 1$. Or $|z|$ est un réel positif. On en déduit que $\boxed{|z| = 1}$.

2. Comme $g^d = I_n$, $X^d - 1$ est un polynôme annulateur de g. On en déduit d'une part, comme le polynôme complexe $X^d - 1$ est scindé à racines simples, que $\boxed{g \text{ est diagonalisable}}$, et d'autre part que le spectre de g est inclus dans l'ensemble des racines de $X^d - 1$, *i.e.* $\boxed{\text{les valeurs propres de } g \text{ sont des racines } d\text{-ièmes de l'unité}}$.

3. (a) Montrons que $\{k \in [\![1, m]\!] \,;\, q \mid k\} = \left\{\ell q \,;\, \ell \in \left[\!\left[1, \left\lfloor \frac{m}{q} \right\rfloor\right]\!\right]\right\}$. Soit $k \in [\![1, m]\!]$ tel que $q \mid k$: on dispose de $\ell \in \mathbb{Z}$ tel que $k = \ell q$. Alors $\ell = \dfrac{k}{q} > 0$ donc, comme ℓ est entier, $\ell \geqslant 1$. D'autre part, $\ell = \dfrac{k}{q} \leqslant \dfrac{m}{q}$ donc, comme ℓ est entier, $\ell \leqslant \left\lfloor \dfrac{m}{q} \right\rfloor$. Finalement, $\{k \in [\![1, m]\!] \,;\, q \mid k\} \subset \left\{\ell q \,;\, \ell \in \left[\!\left[1, \left\lfloor \frac{m}{q} \right\rfloor\right]\!\right]\right\}$. Montrons l'autre inclusion : soit $\ell \in \left[\!\left[1, \left\lfloor \dfrac{m}{q} \right\rfloor\right]\!\right]$ et posons $k = \ell q$. Alors q divise k, et $0 < k \leqslant \dfrac{m}{q} q$, donc comme k est un entier, $1 \leqslant k \leqslant m$. D'où la seconde inclusion. On en déduit que l'application $\ell \in \left[\!\left[1, \left\lfloor \dfrac{m}{q} \right\rfloor\right]\!\right] \mapsto \ell q \in \{k \in [\![1, m]\!] \,;\, q \mid k\}$ est bien définie et surjective, et comme $q \neq 0$, elle est injective. C'est donc une bijection. On en déduit que $\boxed{\operatorname{card}(\{k \in [\![1, m]\!] \,;\, q \mid k\}) = \left\lfloor \dfrac{m}{q} \right\rfloor}$.

3. (b) Signalons que les sommes infinies manipulées dans cette question sont à support fini (seul un nombre fini de termes sont non nuls). On écrit :

$$v_q(m!) = v_q\left(\prod_{k=1}^{m} k\right) = \sum_{k=1}^{m} v_q(k) = \sum_{i=1}^{+\infty} i \operatorname{card}(\{k \in [\![1, m]\!] \,;\, v_q(k) = i\}).$$

Or, pour tout $i \in \mathbb{N}^*$, $\{k \in [\![1, m]\!] \,;\, q^i \mid k\} = \{k \in [\![1, m]\!] \,;\, v_q(k) = i\} \sqcup \{k \in [\![1, m]\!] \,;\, q^{i+1} \mid k\}$, la réunion étant disjointe. D'après la question précédente, on en déduit que pour tout $i \in \mathbb{N}^*$, $\operatorname{card}(\{k \in [\![1, m]\!] \,;\, v_q(k) = i\}) = \left\lfloor \dfrac{m}{q^i} \right\rfloor - \left\lfloor \dfrac{m}{q^{i+1}} \right\rfloor$. Ainsi (rappelons que les sommes sont à support fini) :

$$v_q(m!) = \sum_{i=1}^{+\infty} i \left(\left\lfloor \frac{m}{q^i} \right\rfloor - \left\lfloor \frac{m}{q^{i+1}} \right\rfloor \right) = \sum_{i=1}^{+\infty} i \left\lfloor \frac{m}{q^i} \right\rfloor - \sum_{i=0}^{+\infty} i \left\lfloor \frac{m}{q^{i+1}} \right\rfloor = \sum_{i=1}^{+\infty} i \left\lfloor \frac{m}{q^i} \right\rfloor - \sum_{i=0}^{+\infty} (i+1) \left\lfloor \frac{m}{q^{i+1}} \right\rfloor + \sum_{i=0}^{+\infty} \left\lfloor \frac{m}{q^{i+1}} \right\rfloor,$$

ce qui montre que $\boxed{v_q(m!) = \displaystyle\sum_{i=1}^{+\infty} \left\lfloor \frac{m}{q^i} \right\rfloor}$.

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

1. D'après les questions 1 et 2 des Préliminaires, g est diagonalisable et ses valeurs propres sont de module 1. En notant λ et μ ses valeurs propres (comptées avec multiplicité), on en déduit que $\operatorname{Tr}(g) = \lambda + \mu$ puis que $|\operatorname{Tr}(g)| \leqslant |\lambda| + |\mu| = 2$: $\boxed{|\operatorname{Tr}(g)| \leqslant 2}$.

2. En reprenant les notations de la question précédente, on dispose d'une matrice inversible $P \in \mathbf{GL}_2(\mathbb{C})$ telle que $g = P \operatorname{Diag}(\lambda, \mu) P^{-1}$. Puisque λ et μ sont réels et que leur module vaut 1, on en déduit que $\lambda^2 = \mu^2 = 1$. Donc $g^2 = P \operatorname{Diag}(\lambda^2, \mu^2) P^{-1} = P I_2 P^{-1} = I_2$, donc d divise 2 puis $\boxed{d \in \{1, 2\}}$.

3. On sait que $\chi_g = X^2 - \mathrm{Tr}(g)X + \det(g)$. Comme g n'a pas de valeurs propres réelles, le polynôme réel χ_g de degré 2 a un discriminant strictement négatif : $\mathrm{Tr}(g)^2 - 4\det(g) < 0$ Or, g étant diagonalisable, en reprenant les notations de la question 1, $\det(g) = \lambda\mu$. Comme λ et μ sont de module 1, on en déduit que $|\det(g)| = 1$, et comme $\det(g)$ est réel, $\det(g) \in \{-1, 1\}$. Sachant que $\mathrm{Tr}(g)^2 < 4\det(g)$, on en déduit que $\det(g) = 1$ puis que $\mathrm{Tr}(g)^2 < 4$, et comme $\mathrm{Tr}(g)$ est un entier, $\mathrm{Tr}(g) \in \{0, -1, 1\}$. Finalement, $\boxed{\chi_g \in \{X^2+1, X^2+X+1, X^2-X+1\}}$.

4. Remarquons que comme χ_g est un polynôme réel, on a l'alternative suivante : ses racines sont réelles ou sont complexes non réelles conjuguées, donc les questions 2 et 3 traitent tous les cas. Pour répondre à la question 4, on peut donc distinguer les quatre cas suivants.

- *Cas 1 : les valeurs propres de g sont réelles.* Alors d'après la question 2, $d \in \{1, 2\}$.
- *Cas 2 :* $\chi_g = X^2 + 1$. Alors $\chi_g = (X - i)(X + i)$, donc g est semblable à $\mathrm{Diag}(i, -i)$, donc g^4 est semblable à $\mathrm{Diag}(i^4, (-i)^4)$, *i.e.* g^4 est semblable à I_2 donc est égale à I_2, donc d divise 4 : $d \in \{1, 2, 4\}$ (notons que comme g est semblable à $\mathrm{Diag}(i, -i)$, $d \notin \{1, 2\}$, donc $d = 4$, mais cela nous sera inutile).
- *Cas 3 :* $\chi_g = X^2 + X + 1$. Alors $\chi_g = (X - j)(X - \overline{j})$, donc g est semblable à $\mathrm{Diag}(j, \overline{j})$, donc g^3 est semblable à $\mathrm{Diag}(j^3, \overline{j}^3) = I_2$, donc $g^3 = I_2$ *i.e.* d divise 3 : $d \in \{1, 3\}$ (de même, on peut montrer que $d = 3$).
- *Cas 4 :* $\chi_g = X^2 - X + 1$. Alors $\chi_g = (X - e^{i\pi/3})(X - e^{-i\pi/3})$, donc g est semblable à $\mathrm{Diag}(e^{i\pi/3}, e^{-i\pi/3})$, donc g^6 est semblable à I_2, donc $g^6 = I_2$ *i.e.* d divise 6 : $d \in \{1, 2, 3, 6\}$ (de même, on peut montrer que $d = 6$).

Finalement, $\boxed{d \in \{1, 2, 3, 4, 6\}}$.

5. Le polynôme complexe P étant scindé, on peut utiliser les relations coefficients/racines, qui assurent que pour tout $i \in [\![0, n-1]\!]$: $(-1)^{n-i}a_i = \displaystyle\sum_{1 \leqslant k_1 < \cdots < k_{n-i} \leqslant n} z_{k_1} \dots z_{k_{n-i}}$, donc $|a_i| \leqslant \displaystyle\sum_{1 \leqslant k_1 < \cdots < k_{n-i} \leqslant n} |z_{k_1}| \dots |z_{k_{n-i}}| \leqslant \displaystyle\sum_{1 \leqslant k_1 < \cdots < k_{n-i} \leqslant n} \alpha^{n-i} = \alpha^{n-i}\binom{n}{n-i}$. On en déduit que $\boxed{\text{pour tout } i \in [\![0, n-1]\!],\ |a_i| \leqslant \binom{n}{i}\alpha^{n-i}}$.

6. Soit $g \in \mathbf{GL}_n(\mathbb{Z})$ d'ordre fini. Notons que χ_g est un polynôme unitaire de degré n : écrivons $\chi_g = X^n + \displaystyle\sum_{i=0}^{n-1} a_i X^i$. D'après les questions 1 et 2 des Préliminaires, les valeurs propres de g sont de module 1. La question précédente assure alors que pour tout $i \in [\![0, n-1]\!]$, $|a_i| \leqslant \binom{n}{i}$. Or, comme g est une matrice à coefficients entiers, $\chi_g \in \mathbb{Z}[X]$. On en déduit que

$$\{\chi_g\,;\, g \in \mathbf{GL}_n(\mathbb{Z}) \text{ est d'ordre fini}\} \subset \left\{ X^n + \sum_{i=0}^{n-1} a_i X^i\,;\, (a_0, \dots, a_{n-1}) \in \prod_{i=0}^{n-1} \left[\!\left[-\binom{n}{i}, \binom{n}{i} \right]\!\right] \right\}.$$

Comme ce dernier ensemble est fini, on a bien montré que l'ensemble $\boxed{\{\chi_g\,;\, g \in \mathbf{GL}_n(\mathbb{Z}) \text{ est d'ordre fini}\} \text{ est fini}}$.

7. Soit $g \in \mathbf{GL}_n(\mathbb{Z})$ d'ordre fini. Notons $z_1, \dots, z_n$ ses valeurs propres (comptées avec multiplicité). D'après la question 2 des Préliminaires, g est diagonalisable et ses valeurs propres sont des racines de l'unité. Donc pour tout $k \in \mathbb{Z}$, g^k est semblable à $\mathrm{Diag}(z_1^k, \dots, z_n^k)$ et $g^k = I_n$ si et seulement si pour tout $i \in [\![1, n]\!]$, $z_i^k = 1$ si et seulement si pour tout $i \in [\![1, n]\!]$, l'ordre de z_i divise k. Ainsi, l'ordre de g est le PPCM des ordres des z_i. En notant f l'application qui, à tout polynôme complexe P non nul dont toutes les racines sont des racines de l'unité, associe l'entier $f(P)$ égal au PPCM des ordres des racines de P, on en déduit que :

$$\{d \in \mathbb{N}\,;\, \exists g \in \mathbf{GL}_n(\mathbb{C}) \text{ d'ordre } d\} \subset \{f(\chi_g)\,;\, g \in \mathbf{GL}_n(\mathbb{Z}) \text{ est d'ordre fini}\}.$$

Comme d'après la question précédente, l'ensemble $\{\chi_g\,;\, g \in \mathbf{GL}_n(\mathbb{Z}) \text{ est d'ordre fini}\}$ est fini, on en déduit que l'ensemble $\boxed{\{d \in \mathbb{N}\,;\, \exists g \in \mathbf{GL}_n(\mathbb{C}) \text{ d'ordre } d\} \text{ est fini}}$.

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

1. (a) D'après les questions 1 et 2 des Préliminaires, g est diagonalisable et ses valeurs propres, notées $z_1, \dots, z_n$ (comptées avec multiplicité), sont de module 1 : on dispose d'une matrice inversible $P \in \mathbf{GL}_n(\mathbb{C})$ telle que $g = P\,\mathrm{Diag}(z_1, \dots, z_n)P^{-1}$. Alors $A = P\,\mathrm{Diag}((z_1 - 1)/m, \dots, (z_n - 1)/m)P^{-1}$, donc $\boxed{A \text{ est diagonalisable sur } \mathbb{C}}$, et comme pour tout $i \in [\![1, n]\!]$, $\left|\dfrac{z_i - 1}{m}\right| \leqslant \dfrac{|z_i| + 1}{m} = \dfrac{2}{m} < 1$, $\boxed{\text{les valeurs propres de } A \text{ sont de module strictement inférieurs à } 1}$.

1. (b) Notons pour tout $i \in [\![1,n]\!]$, $\lambda_i = (z_i-1)/m$. Pour tout $k \in \mathbb{N}$, $A^k = P\,\mathrm{Diag}(\lambda_1^k,\dots,\lambda_n^k)P^{-1}$. Comme pour tout $i \in [\![1,n]\!]$, $|\lambda_i| < 1$, la suite de matrices $(\mathrm{Diag}(\lambda_1^k,\dots,\lambda_n^k))_{k\in\mathbb{N}}$ converge vers 0. Or, puisque les applications « multiplication à gauche par P » et « multiplication à droite par P^{-1} » sont linéaires et que $\mathcal{M}_n(\mathbb{C})$ est de dimension finie, ces deux applications sont continues, donc la suite $(P\,\mathrm{Diag}(\lambda_1^k,\dots,\lambda_n^k)P^{-1})_{k\in\mathbb{N}}$ converge vers $P\times 0\times P^{-1}$, *i.e.* A^k converge vers 0. On en déduit que les n^2 suites des coefficients de A^k convergent vers 0. Or, comme A est par hypothèse une matrice entière, ces n^2 suites sont des suites d'entiers. On en déduit que toutes ces suites sont nulles à partir d'un certain rang, donc en prenant le maximum de ces n^2 rangs, ceci montre qu'$\boxed{\text{il existe } k\in\mathbb{N} \text{ tel que } A^k = 0}$.

1. (c) Notons Π_A le polynôme minimal de A. La question précédente assure que Π_A divise X^k, donc on dispose de $\ell \in \mathbb{N}$ tel que $\Pi_A = X^\ell$. Or, d'après la question (a), A est diagonalisable, donc Π_A est scindé à racines simples. On en déduit que $\Pi_A = X$, et comme $\Pi_A(A) = 0$, $A = 0$. Donc $\boxed{g = I_n}$.

2. (a) Soit $(g,h) \in G^2$ tel que les réductions modulo m des coefficients de g et h soient égales : on dispose de $B \in \mathcal{M}_n(\mathbb{Z})$ telle que $g - h = mB$. En multipliant à gauche par h^{-1} et en notant $A = h^{-1}B$, on a donc : $A = (h^{-1}g - I_n)/m$. Or $h^{-1}g$ et h^{-1} sont des éléments du groupe fini $G \subset \mathbf{GL}_n(\mathbb{C})$, donc $h^{-1}g$ est une matrice entière d'ordre fini et h^{-1} est une matrice entière. Donc $h^{-1}B$ est aussi une matrice entière *i.e.* $A \in \mathcal{M}_n(\mathbb{Z})$. D'autre part, $m \geqslant 3$. On peut donc appliquer la question précédente : $A = 0$. Comme $g - h = mhA$, on en déduit que $g = h$. D'où $\boxed{\text{l'injectivité demandée}}$.

2. (b) En particulier G s'injecte dans l'ensemble $\mathcal{M}_n(\mathbb{Z}/3\mathbb{Z})$, qui est de cardinal 3^{n^2}. Ainsi, $\boxed{\mathrm{card}(G) \leqslant 3^{n^2}}$.

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

1. (a) Soit $k \in [\![1,\ell-1]\!]$. On remarque que $k\binom{\ell}{k} = k\dfrac{\ell!}{k!(\ell-k)!} = \dfrac{\ell!}{(k-1)!(\ell-k)!} = \ell\dfrac{(\ell-1)!}{(k-1)!(\ell-k)!} = \ell\binom{\ell-1}{k-1}$ donc ℓ divise $k\binom{\ell}{k}$. Or, comme $k \in [\![1,\ell-1]\!]$ et ℓ est un nombre premier, ℓ et k sont premiers entre eux. D'après le lemme de Gauss, on en déduit que $\boxed{\binom{\ell}{k} \text{ est un multiple de } \ell}$.

1. (b) Soit $(x,y) \in R^2$ tel que $xy = yx$. D'après la formule du binôme de Newton, $(x+y)^\ell = \displaystyle\sum_{k=0}^{\ell}\binom{\ell}{k}x^{\ell-k}y^k$ donc $(x+y)^\ell - (x^\ell + y^\ell) = \displaystyle\sum_{k=1}^{\ell-1}\binom{\ell}{k}x^{\ell-k}y^k$. La question précédente assure alors que $\boxed{(x+y)^\ell - (x^\ell+y^\ell) \in \ell R}$.

2. On écrit : $\det(A+B)-\det(A) = \displaystyle\sum_{\sigma\in\mathfrak{S}_n}\varepsilon(\sigma)\left(\prod_{i=1}^{n}\left(a_{i,\sigma(i)}+b_{i,\sigma(i)}\right) - \prod_{i=1}^{n}a_{i,\sigma(i)}\right)$. Or, pour tout $\sigma \in \mathfrak{S}_n$, le développement de $\displaystyle\prod_{i=1}^{n}\left(a_{i,\sigma(i)}+b_{i,\sigma(i)}\right)$ donne 2^n termes (de n facteurs chacun) ; parmi eux, seul le terme $\displaystyle\prod_{i=1}^{n}a_{i,\sigma(i)}$ ne contient aucun facteur issu de B : les 2^n-1 autres termes font apparaître, parmi leurs n facteurs, au moins un coefficient $b_{j,\sigma(j)}$ venant de B, et comme B est inclus dans l'idéal I, ces 2^n-1 termes appartiennent à I : $\displaystyle\prod_{i=1}^{n}\left(a_{i,\sigma(i)}+b_{i,\sigma(i)}\right) - \prod_{i=1}^{n}a_{i,\sigma(i)} \in I$. Comme I est un sous-groupe de R, on en déduit que finalement que $\displaystyle\sum_{\sigma\in\mathfrak{S}_n}\varepsilon(\sigma)\left(\prod_{i=1}^{n}\left(a_{i,\sigma(i)}+b_{i,\sigma(i)}\right) - \prod_{i=1}^{n}a_{i,\sigma(i)}\right) \in I$, *i.e.* $\boxed{\det(A+B)-\det(A) \in I}$.

3. On applique ici la question 1 (b) à l'anneau commutatif $\mathbb{Z}[X]$. Notons que l'on peut aisément démontrer par récurrence sur k que pour tout $k \in \mathbb{N}^*$ et pour tout $P_1,\dots,P_k \in \mathbb{Z}[X]$, $(P_1+\cdots+P_k)^\ell - (P_1^\ell+\cdots+P_k^\ell) \in \ell\mathbb{Z}[X]$, l'hérédité venant précisément de la propriété établie à la question 1 (b). Soit $P \in \mathbb{Z}[X]$. Écrivons $P = \displaystyle\sum_{k=0}^{N}a_kX^k$. Alors d'après la propriété que l'on vient d'énoncer, on dispose de $Q \in \mathbb{Z}[X]$ tel que $\left(\displaystyle\sum_{k=0}^{N}a_kX^k\right)^\ell = \sum_{k=0}^{N}a_k^\ell X^{k\ell} + \ell Q$. Donc $P\big(X^\ell\big) - P(X)^\ell =$

$-\sum_{k=0}^{N}(a_k^\ell - a_k)X^{k\ell} - \ell Q$. Or, ℓ étant un nombre premier, le petit théorème de Fermat assure que pour tout $k \in [\![0, N]\!]$, $a_k^\ell - a_k \in \ell\mathbb{Z}$. On conclut finalement que $\boxed{P(X^\ell) - P(X)^\ell \in \ell\mathbb{Z}[X]}$.

4. (a) Comme XI_n et $-M$ commutent, la question 1 (b) appliquée à l'anneau $\mathcal{M}_n(\mathbb{Z}[X])$ assure que $(XI_n - M)^\ell - \big((XI_n)^\ell + (-M)^\ell\big) \in \ell\mathcal{M}_n(\mathbb{Z}[X])$. Si ℓ est impair, on en déduit que $(XI_n - M)^\ell - \big(X^\ell I_n - M^\ell\big) \in \ell\mathcal{M}_n(\mathbb{Z}[X])$. Sinon, comme ℓ est un nombre premier, $\ell = 2$ et $(XI_n - M)^2 - \big(X^2 I_n - M^2\big) = 2\big(M^2 - XM\big) \in 2\mathcal{M}_n(\mathbb{Z}[X])$. Dans tous les cas, on a bien établi $\boxed{\text{l'existence d'une matrice } A \in \mathcal{M}_n(\mathbb{Z}[X]) \text{ telle que } (XI_n - M)^\ell - \big(X^\ell I_n - M^\ell\big) = \ell A}$.

4. (b) On applique ici la question 2 à l'anneau commutatif $\mathbb{Z}[X]$ et à l'idéal $\ell\mathbb{Z}[X]$. On pose $M_1 = (XI_n - M)^\ell$ et $M_2 = \big(X^\ell I_n - M^\ell\big) - (XI_n - M)^\ell$. D'après la question précédente, tous les coefficients de M_2 sont dans $\ell\mathbb{Z}[X]$. La question 2 assure alors que $\det(M_1 + M_2) - \det(M_1) \in \ell\mathbb{Z}[X]$ *i.e.* $\det\big(X^\ell I_n - M^\ell\big) - \det\big((XI_n - M)^\ell\big) \in \ell\mathbb{Z}[X]$. Or $\det\big(X^\ell I_n - M^\ell\big) = \chi_{M^\ell}\big(X^\ell\big)$ et $\det\big((XI_n - M)^\ell\big) = (\det(XI_n - M))^\ell = \chi_M(X)^\ell$. Finalement, $\boxed{\chi_{M^\ell}\big(X^\ell\big) - \chi_M(X)^\ell \in \ell\mathbb{Z}[X]}$.

4. (c) Comme $M \in \mathcal{M}_n(\mathbb{Z})$, on dispose de polynômes à coefficients entiers R_1 et R_2 de degré strictement inférieur à $n-1$ tels que $\chi_M(X) = X^n - \mathrm{Tr}(M)X^{n-1} + R_1(X)$ et $\chi_{M^\ell}(X) = X^n - \mathrm{Tr}\big(M^\ell\big)X^{n-1} + R_2(X)$. Alors $\chi_{M^\ell}\big(X^\ell\big) = X^{\ell n} - \mathrm{Tr}\big(M^\ell\big)X^{\ell n-\ell} + R_2\big(X^\ell\big)$. D'autre part, d'après la question 3, on dispose de $Q_1 \in \mathbb{Z}[X]$ tel que $\chi_M(X)^\ell = \chi_M\big(X^\ell\big) + \ell Q_1$, donc $\chi_M(X)^\ell = X^{\ell n} - \mathrm{Tr}(M)X^{\ell n-\ell} + R_1\big(X^\ell\big) + \ell Q_1\big(X^\ell\big)$. Enfin, d'après la question précédente, on dispose de $Q_2 \in \mathbb{Z}[X]$ tel que $\chi_{M^\ell}\big(X^\ell\big) - \chi_M(X)^\ell = \ell Q_2$. Finalement :

$$X^{\ell n} - \mathrm{Tr}\big(M^\ell\big)X^{\ell n-\ell} + R_2\big(X^\ell\big) - \big(X^{\ell n} - \mathrm{Tr}(M)X^{\ell n-\ell} + R_1\big(X^\ell\big) + \ell Q_1\big(X^\ell\big)\big) = \ell Q_2$$

i.e.

$$\big(\mathrm{Tr}(M) - \mathrm{Tr}\big(M^\ell\big)\big)X^{\ell n-\ell} + R_2\big(X^\ell\big) - R_1\big(X^\ell\big) = \ell\big(Q_1\big(X^\ell\big) + Q_2\big).$$

Ainsi, les coefficients du polynôme $\big(\mathrm{Tr}(M) - \mathrm{Tr}\big(M^\ell\big)\big)X^{\ell n-\ell} + R_2\big(X^\ell\big) - R_1\big(X^\ell\big)$ sont des multiples de ℓ. Comme $R_1\big(X^\ell\big)$ et $R_2\big(X^\ell\big)$ sont de degré strictement inférieur à $n\ell - \ell$, on en déduit que $\boxed{\mathrm{Tr}(M) - \mathrm{Tr}\big(M^\ell\big) \text{ est un multiple de } \ell}$.

5. Montrons par récurrence sur k que pour tout $k \in \mathbb{N}$, $\mathrm{Tr}\Big(g^{p^k}\Big) \equiv \mathrm{Tr}(g) \pmod p$. L'initialisation est claire. Prouvons l'hérédité. Soit $k \in \mathbb{N}$ tel que $\mathrm{Tr}\Big(g^{p^k}\Big) \equiv \mathrm{Tr}(g) \pmod p$. Puisque $g \in G$ et que G est un groupe, $g^{p^k} \in G$, et comme $G \subset M_n(\mathbb{Z})$, $g^{p^k} \in M_n(\mathbb{Z})$. Rappelons enfin que p est un nombre premier. La question précédente assure alors que

$$\mathrm{Tr}\Big(\Big(g^{p^k}\Big)^p\Big) \equiv \mathrm{Tr}\Big(g^{p^k}\Big) \pmod p \quad \textit{i.e.} \quad \mathrm{Tr}\Big(g^{p^{k+1}}\Big) \equiv \mathrm{Tr}\Big(g^{p^k}\Big) \pmod p.$$

On en déduit que $\mathrm{Tr}\Big(g^{p^{k+1}}\Big) \equiv \mathrm{Tr}(g) \pmod p$, d'où l'hérédité. Finalement, pour tout $k \in \mathbb{N}$, $\mathrm{Tr}\Big(g^{p^k}\Big) \equiv \mathrm{Tr}(g) \pmod p$, et en particulier $\mathrm{Tr}\Big(g^{p^r}\Big) \equiv \mathrm{Tr}(g) \pmod p$. Or, comme g est un élément du groupe fini G de cardinal p^r, l'ordre de g divise p^r, donc $g^{p^r} = I_n$, donc $\mathrm{Tr}\Big(g^{p^r}\Big) = n$. On en déduit que $\boxed{\mathrm{Tr}(g) \equiv n \pmod p}$.

6. Puisque $g \in G$ et que $G \subset M_n(\mathbb{Z})$, $g \in M_n(\mathbb{Z})$. La question 4 assure alors que $\mathrm{Tr}\big(g^\ell\big) \equiv \mathrm{Tr}(g) \pmod \ell$. D'autre part, d'après les questions 1 et 2 des Préliminaires, g est diagonalisable et ses valeurs propres sont de module 1. Ainsi, en notant $z_1, \dots, z_n$ ses valeurs propres (comptées avec multiplicité), $\mathrm{Tr}(g) = \sum_{i=1}^{n} z_i$ puis $|\,\mathrm{Tr}(g)| \leqslant \sum_{i=1}^{n} |z_i| = n$. Comme G est un groupe, on a aussi $g^\ell \in G$, donc d'après ce qui précède $\big|\mathrm{Tr}\big(g^\ell\big)\big| \leqslant n$. On en déduit que $\big|\mathrm{Tr}\big(g^\ell\big) - \mathrm{Tr}(g)\big| \leqslant 2n$, donc comme $2n < \ell$, $\big|\mathrm{Tr}\big(g^\ell\big) - \mathrm{Tr}(g)\big| < \ell$. Finalement, $\mathrm{Tr}\big(g^\ell\big) - \mathrm{Tr}(g)$ est un multiple de ℓ strictement compris entre $-\ell$ et ℓ. D'où $\mathrm{Tr}\big(g^\ell\big) - \mathrm{Tr}(g) = 0$ *i.e.* $\boxed{\mathrm{Tr}\big(g^\ell\big) = \mathrm{Tr}(g)}$.

7. (a) Notons $u = \prod_{\substack{\ell \text{ premier} \\ \ell \leqslant 2n \\ \ell \text{ ne divise pas } k}} \ell$. Soit q un nombre premier inférieur ou égal à $2n$. Distinguons les deux cas suivants.

- *Cas 1 : q ne divise pas k.* Alors q divise $p^r u$. Or q ne divise pas k. Donc q ne divise pas m.

- *Cas 2 : q divise k.* Alors pour tout nombre premier ℓ qui ne divise pas k, $q \neq \ell$, donc comme q et ℓ sont des nombres premiers, q et ℓ sont premiers entre eux. Donc q est premier avec $p^r u$ (rappelons que p ne divise pas k). Comme $q \neq 1$, on en déduit que q ne divise pas $p^r u$. Comme q divise k, q ne divise pas m.

Ainsi, dans tous les cas, q ne divise pas m. Finalement, $\boxed{\text{les facteurs premiers de } m \text{ sont strictement supérieurs à } 2n}$.

7. (b) On conserve la notation de la question précédente pour u. Soit $g \in G$. On a déjà vu (cf. question 5) que l'ordre de g divise p^r, donc $g^{p^r u} = I_n$ puis $g^m = g^k$. D'après la question précédente et la question 6 :

$$\forall q \text{ facteur premier de } m, \quad \forall h \in G, \quad \mathrm{Tr}(h^q) = \mathrm{Tr}(h). \tag{1}$$

Écrivons $m = q_1^{\alpha_1} \dots q_s^{\alpha_s}$ la décomposition en facteurs premiers de m. Alors

$$\mathrm{Tr}(g^m) = \mathrm{Tr}\Big(g^{q_1^{\alpha_1}\dots q_s^{\alpha_s}}\Big) = \mathrm{Tr}\Big(\Big(g^{q_1^{\alpha_1}\dots q_s^{\alpha_s-1}}\Big)^{q_s}\Big) = \mathrm{Tr}\Big(g^{q_1^{\alpha_1}\dots q_s^{\alpha_s-1}}\Big),$$

la dernière égalité venant de la relation (1) appliquée au facteur premier q_s de m et à l'élément $g^{q_1^{\alpha_1}\dots q_s^{\alpha_s-1}}$ du groupe G. On montre ainsi par récurrence finie que $\mathrm{Tr}(g^m) = \mathrm{Tr}\Big(g^{q_1^{\alpha_1}\dots q_{s-1}^{\alpha_{s-1}}}\Big)$ puis encore par récurrence finie que $\mathrm{Tr}(g^m) = \mathrm{Tr}(g)$. Comme $g^m = g^k$, on a finalement montré que $\boxed{\mathrm{Tr}\big(g^k\big) = \mathrm{Tr}(g)}$.

8. (a) Soit $k \in J_r$. On effectue la division euclidienne de k par p : on dispose d'un unique couple $(s,t) \in \mathbb{Z}^2$ tel que $k = ps + t$ et $t \in [\![0, p-1]\!]$. Comme p ne divise pas k, le reste t n'est pas nul : $t \in [\![1, p-1]\!]$. D'autre part, $k \geqslant 0$ donc $ps + t \geqslant 0$ donc $ps \geqslant -t > -p$ donc $s > -1$ et $s \geqslant 0$. Enfin, $k \leqslant p^r$ donc $ps + t \leqslant p^r$ donc $ps \leqslant p^r - t < p^r$ donc $s < p^{r-1}$ et $s \leqslant p^{r-1} - 1$. Finalement, $J_r \subset \bigsqcup_{0 \leqslant s \leqslant p^{r-1}-1} \{ps + t\,;\, t \in [\![1, p-1]\!]\}$ (la réunion est disjointe par unicité de la division euclidienne). Inversement, soit $(s,t) \in \mathbb{Z}^2$ tel que $0 \leqslant s \leqslant p^{r-1} - 1$ et $1 \leqslant t \leqslant p - 1$. Alors p ne divise pas t, et comme p divise ps, p ne divise pas $ps + t$. D'autre part, $ps + t \geqslant t \geqslant 1$ et $ps + t \leqslant p(p^{r-1} - 1) + p - 1 = p^r - 1$. Finalement, on a établi la seconde inclusion. On conclut que $\boxed{J_r = \bigsqcup_{0 \leqslant s \leqslant p^{r-1}-1} \{ps + t\,;\, t \in [\![1, p-1]\!]\}}$.

8. (b) Notons que, dans la question précédente, on a remarqué que la réunion $J_r = \bigsqcup_{0 \leqslant s \leqslant p^{r-1}-1} \{ps + t\,;\, t \in [\![1, p-1]\!]\}$ est disjointe.

- Si $\zeta = 1$, comme $\mathrm{card}(J_r) = \sum_{0 \leqslant s \leqslant p^{r-1}-1} \mathrm{card}([\![1, p-1]\!]) = (p-1)p^{r-1}$, on a bien $\sum_{j \in J_r} \zeta^j = p^{r-1}(p-1)$.
- Si $\zeta \neq 1$. Alors

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

  Ainsi, si ζ est d'ordre p alors $\sum_{j \in J_r} \zeta^j = \frac{\zeta - 1}{1 - \zeta} \sum_{s=0}^{p^{r-1}-1} 1 = -p^{r-1}$. En revanche, si ζ n'est pas d'ordre p, alors comme $\zeta^{p^r} = 1$, l'ordre de ζ divise p^r, donc est une puissance de p, et comme cet ordre n'est ni égal à 1 ni égal à p, il est strictement supérieur à p et $\zeta^p \neq 1$. Ainsi $\sum_{j \in J_r} \zeta^j = \frac{\zeta - \zeta^p}{1 - \zeta} \frac{1 - (\zeta^p)^{p^{r-1}}}{1 - \zeta^p} = \frac{\zeta - \zeta^p}{1 - \zeta} \frac{1 - \zeta^{p^r}}{1 - \zeta^p} = 0$.

D'où $\boxed{\text{le résultat demandé}}$.

9. On a déjà vu (cf. question 5) que l'ordre de g divise p^r, donc d'après la question 2 des Préliminaires, toutes les valeurs propres de g sont des racines p^r-ièmes de l'unité. Notons $\zeta_{n_0+1}, \dots, \zeta_{n_0+n_1}$ les valeurs propres de g d'ordre p (comptées avec multiplicité), et $\zeta_{n_0+n_1+1}, \dots, \zeta_n$ les valeurs propres de g d'ordre strictement supérieur à p (comptées avec multiplicité). Pour tout $j \in J_r$, p ne divise pas k, donc d'après la question 7 (b), $\mathrm{Tr}\big(g^j\big) = \mathrm{Tr}(g)$. Ainsi,

$$\mathrm{Tr}(g) = \frac{1}{\mathrm{card}(J_r)} \sum_{j \in J_r} \mathrm{Tr}\big(g^j\big) = \frac{1}{\mathrm{card}(J_r)} \sum_{j \in J_r} \left(n_0 + \sum_{i=n_0+1}^{n_0+n_1} \zeta_i^j + \sum_{i=n_0+n_1+1}^{n} \zeta_i^j \right)$$

donc, en appliquant la question précédente :

$$\mathrm{Tr}(g) = n_0 + \frac{1}{\mathrm{card}(J_r)} \sum_{i=n_0+1}^{n_0+n_1} \sum_{j\in J_r} \zeta_i^j + \frac{1}{\mathrm{card}(J_r)} \sum_{i=n_0+n_1+1}^{n} \sum_{j\in J_r} \zeta_i^j = n_0 + \frac{1}{p^{r-1}(p-1)} \sum_{i=n_0+1}^{n_0+n_1} (-p^{r-1}).$$

Finalement, $\boxed{\mathrm{Tr}(g) = n_0 - \dfrac{n_1}{p-1}}$.

10. Posons $v = \dfrac{n - \mathrm{Tr}(g)}{p}$. D'après la question 5, $v \in \mathbb{Z}$. Par ailleurs, d'après la question précédente, $\mathrm{Tr}(g) = n_0 - \dfrac{n_1}{p-1}$. On en déduit d'une part que $\mathrm{Tr}(g) \leqslant n_0 \leqslant n$, donc $v \geqslant 0$, et que $\mathrm{Tr}(g) = n_0 - \dfrac{n_1}{p-1} \geqslant -\dfrac{n_1}{p-1} \geqslant -\dfrac{n}{p-1}$, donc $0 \leqslant n + (p-1)\,\mathrm{Tr}(g)$ puis $(p-1)n - (p-1)\,\mathrm{Tr}(g) \leqslant np$. D'où $v \leqslant \dfrac{n}{p-1}$ puis $v \leqslant a$. Finalement, $\boxed{\mathrm{Tr}(g) = n - pv \text{ avec } v \in [\![0, a]\!]}$.

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

1. (a) Remarquons que $f^2 = \dfrac{1}{\mathrm{card}(G)^2} \displaystyle\sum_{g\in G} \sum_{h\in G} gh$. Or, pour tout $g \in G$, l'application $h \in G \mapsto gh \in G$ est une bijection (d'inverse la multiplication à gauche par g^{-1}), donc $\displaystyle\sum_{h\in G} gh = \sum_{g'\in G} g'$. Ainsi, $f^2 = \dfrac{1}{\mathrm{card}(G)^2} \displaystyle\sum_{g\in G} \sum_{g'\in G} g' = \dfrac{1}{\mathrm{card}(G)} \sum_{g'\in G} g' = f$, donc $\boxed{f \text{ est un projecteur}}$. Montrons que $\mathrm{Im}(f) = \displaystyle\bigcap_{g\in G} \mathrm{Ker}(g - I_n)$. Pour tout $y \in \displaystyle\bigcap_{g\in G} \mathrm{Ker}(g - I_n)$, on a : pour tout $g \in G$, $g(y) = y$ donc $f(y) = \dfrac{1}{\mathrm{card}(G)} \displaystyle\sum_{g\in G} g(y) = \dfrac{1}{\mathrm{card}(G)} \sum_{g\in G} y = y$ donc $y \in \mathrm{Im}(f)$. D'autre part, pour tout $x \in \mathrm{Im}(f)$, comme f est un projecteur, $f(x) = x$, donc pour tout $g \in G$, $g(x) = g(f(x)) = g\left(\dfrac{1}{\mathrm{card}(G)} \displaystyle\sum_{h\in G} h(x)\right) = \dfrac{1}{\mathrm{card}(G)} \left(\sum_{h\in G} gh\right)(x) = \dfrac{1}{\mathrm{card}(G)} \displaystyle\sum_{g'\in G} g'(x) = f(x) = x$, donc $x \in \displaystyle\bigcap_{g\in G} \mathrm{Ker}(g - I_n)$. Finalement, $\boxed{\mathrm{Im}(f) = \displaystyle\bigcap_{g\in G} \mathrm{Ker}(g - I_n)}$.

1. (b) Comme f est un projecteur, $\mathrm{Tr}(f) = \mathrm{rg}(f)$, donc $\dfrac{1}{\mathrm{card}(G)} \displaystyle\sum_{g\in G} \mathrm{Tr}(g) = \mathrm{rg}(f)$ *i.e.* $\displaystyle\sum_{g\in G} \mathrm{Tr}(g) = \mathrm{rg}(f)\,\mathrm{card}(G)$. On en déduit que $\boxed{\displaystyle\sum_{g\in G} \mathrm{Tr}(g) \text{ est un entier divisible par } \mathrm{card}(G)}$.

2. (i) On calcule : $\mathrm{Tr}(g \otimes h) = \displaystyle\sum_{i=1}^{n} g_{i,i}\,\mathrm{Tr}(h)$ donc $\boxed{\mathrm{Tr}(g \otimes h) = \mathrm{Tr}(g)\,\mathrm{Tr}(h)}$.

2. (ii) On utilise la formule du produit matriciel par blocs : pour tout $(i, j) \in [\![1, n]\!] \times [\![1, k]\!]$, le j-ième bloc de la ligne-bloc numéro i de la matrice $(g \otimes h)(g' \otimes h')$ est

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

qui est le j-ième bloc de la ligne-bloc numéro i de la matrice par blocs $(gg') \otimes (hh')$, donc $\boxed{(g \otimes h)(g' \otimes h') = (gg') \otimes (hh')}$.

2. (iii) D'après la question précédente, $(g \otimes h)\left(g^{-1} \otimes h^{-1}\right) = \left(gg^{-1}\right) \otimes \left(hh^{-1}\right) = I_n \otimes I_k = I_{nk}$, ce qui prouve (on travaille dans l'anneau des matrices carrées $\mathcal{M}_{nk}(\mathbb{C})$) que $\boxed{g \otimes h \in \mathbf{GL}_{nk}(\mathbb{C}) \text{ et } (g \otimes h)^{-1} = g^{-1} \otimes h^{-1}}$.

3. (a) Supposons que $\varphi^{-1}(\{\gamma'\})$ n'est pas vide : on dispose de $\gamma \in \Gamma$ tel que $\varphi(\gamma) = \gamma'$. Alors pour tout $\delta \in \Gamma$, on a : $\delta \in \varphi^{-1}(\{\gamma'\})$ si et seulement si $\varphi(\delta) = \gamma'$ si et seulement si $\varphi(\delta) = \varphi(\gamma)$ si et seulement si $\varphi(\gamma^{-1}\delta)$ est le neutre de Γ si et seulement si $\gamma^{-1}\delta \in H$ si et seulement si $\delta \in \gamma H$. D'où $\varphi^{-1}(\{\gamma'\}) = \gamma H$. Finalement, $\boxed{\varphi^{-1}(\{\gamma'\}) \text{ est vide ou il existe } \gamma \in \Gamma \text{ tel que } \varphi^{-1}(\{\gamma'\}) = \gamma H}$.

3. (b) Remarquons que $\Gamma = \bigsqcup_{\gamma' \in \varphi(\Gamma)} \varphi^{-1}(\{\gamma'\})$, la réunion étant disjointe (on partitionne les éléments de Γ selon leur image par φ). Donc $\text{card}(\Gamma) = \sum_{\gamma' \in \varphi(\Gamma)} \text{card}(\varphi^{-1}(\{\gamma'\}))$. Or, par définition, pour tout $\gamma' \in \varphi(\Gamma)$, $\varphi^{-1}(\{\gamma'\})$ n'est pas vide donc, d'après la question précédente, est en bijection avec H, donc de cardinal $\text{card}(H)$. Ainsi $\text{card}(\Gamma) = \sum_{\gamma' \in \varphi(\Gamma)} \text{card}(H)$, ce qui montre que $\boxed{\text{card}(\Gamma) = \text{card}(\varphi(\Gamma))\,\text{card}(H)}$.

4. (a) Montrons par récurrence sur s que pour tout $s \in \mathbb{N}^*$, φ_s est un morphisme de groupes. L'initialisation est claire. Prouvons l'hérédité. Soit $s \in \mathbb{N}^*$ tel que φ_s est un morphisme de groupes. Soit $(g,h) \in \mathbf{GL}_n(\mathbb{C})^2$. On calcule : $\varphi_{s+1}(gh) = (gh)^{(s+1)} = (gh)^{(s)} \otimes gh = \varphi_s(gh) \otimes gh$. Ainsi, d'après l'hypothèse de récurrence, $\varphi_{s+1}(gh) = \varphi_s(g)\varphi_s(h) \otimes gh = g^{(s)}h^{(s)} \otimes gh$. D'après la question 2 (ii), on en déduit que $\varphi_{s+1}(gh) = (g^{(s)} \otimes g)(h^{(s)} \otimes h) = g^{(s+1)}h^{(s+1)} = \varphi_{s+1}(g)\varphi_{s+1}(h)$. Finalement, φ_{s+1} est un morphisme de groupes. D'où l'hérédité. On conclut que $\boxed{\text{pour tout } s \in \mathbb{N}^*,\ \varphi_s \text{ est un morphisme de groupes}}$. On peut aussi montrer par récurrence (en utilisant la question 2 (i) pour l'hérédité) que pour tout $s \in \mathbb{N}^*$ et pour tout $g \in G$, $\text{Tr}\left(g^{(s)}\right) = \text{Tr}(g)^s$. Donc pour tout $s \in \mathbb{N}^*$, $\sum_{g \in G} \text{Tr}(g)^s = \sum_{g \in G} \text{Tr}\left(g^{(s)}\right) = \sum_{g \in G} \text{Tr}(\varphi_s(g))$. Notons $\psi_s : G \to \varphi_s(G)$ l'application qui à tout $g \in G$ associe $\varphi_s(g)$. Remarquons que ψ_s est un morphisme de groupes entre les groupes finis G et $\varphi_s(G)$. On a donc

$$\sum_{g \in G} \text{Tr}(g)^s = \sum_{g \in G} \text{Tr}(\psi_s(g)) = \sum_{g' \in \varphi_s(G)} \text{card}(\psi_s^{-1}(\{g'\}))\,\text{Tr}(g').$$

Or, pour tout $g' \in \varphi_s(G)$, $\psi_s^{-1}(\{g'\})$ n'est par définition pas vide donc, d'après la question 3 (b), est de cardinal $\text{card}(\text{Ker}(\psi_s))$. Ainsi $\sum_{g \in G} \text{Tr}(g)^s = \text{card}(\text{Ker}(\psi_s)) \sum_{g' \in \varphi_s(G)} \text{Tr}(g')$. Comme $\text{Ker}(\psi_s) = G \cap \text{Ker}(\varphi_s)$, on a finalement : $\boxed{\sum_{g \in G} \text{Tr}(g)^s = \text{card}(G \cap \text{Ker}(\varphi_s)) \sum_{g' \in \varphi_s(G)} \text{Tr}(g')}$.

4. (b) Ainsi $\sum_{g \in G} \text{Tr}(g)^s = \text{card}(\psi_s(G))\,\text{card}(\text{Ker}(\psi_s)) \dfrac{1}{\text{card}(\varphi_s(G))} \sum_{g' \in \varphi_s(G)} \text{Tr}(g')$. Or, d'après la question 3 (b), on sait que $\text{card}(\psi_s(G))\,\text{card}(\text{Ker}(\psi_s)) = \text{card}(G)$. Donc $\sum_{g \in G} \text{Tr}(g)^s = \text{card}(G) \dfrac{1}{\text{card}(\varphi_s(G))} \sum_{g' \in \varphi_s(G)} \text{Tr}(g')$. Or, comme $\varphi_s(G)$ est un sous-groupe fini de $\mathbf{GL}_{n^s}(\mathbb{C})$, la question 1 (b) assure que $\dfrac{1}{\text{card}(\varphi_s(G))} \sum_{g' \in \varphi_s(G)} \text{Tr}(g')$ est un entier. Finalement, $\boxed{\sum_{g \in G} \text{Tr}(g)^s \text{ est un entier divisible par } \text{card}(G)}$.

5. (a) La question précédente assure pour tout $s \in \mathbb{N}^*$, $\sum_{g \in G} \text{Tr}(g)^s$ est un entier divisible par $\text{card}(G)$. On remarque que si $s = 0$, alors $\sum_{g \in G} \text{Tr}(g)^s = \text{card}(G)$ donc $\sum_{g \in G} \text{Tr}(g)^s$ est aussi un entier divisible par $\text{card}(G)$. Ainsi,

$$\forall s \in \mathbb{N}, \quad \sum_{g \in G} \text{Tr}(g)^s \in \text{card}(G)\mathbb{Z}. \tag{2}$$

Remarquons que $P \in \mathbb{Z}[X]$: écrivons $P = \sum_{s=0}^{a} k_s X^s$, où $k_0, \dots, k_a \in \mathbb{Z}$. Alors $\sum_{g \in G} P(\text{Tr}(g)) = \sum_{g \in G} \sum_{s=0}^{a} k_s\,\text{Tr}(g)^s = \sum_{s=0}^{a} k_s \sum_{g \in G} \text{Tr}(g)^s$. D'après la relation (2), on en déduit donc que $\sum_{g \in G} P(\text{Tr}(g))$ est un entier divisible par $\text{card}(G)$. Or, $\sum_{g \in G} P(\text{Tr}(g)) = P(\text{Tr}(I_n)) + \sum_{g \in G \setminus \{I_n\}} P(\text{Tr}(g))$. Remarquons que pour tout $g \in G$, d'après les questions 1 et 2 des Préliminaires, g est diagonalisable et ses valeurs propres sont de module 1, et en notant $z_1, \dots, z_n$ ses valeurs propres (comptées avec multiplicité), si $\text{Tr}(g) = n$, alors $0 = n - \text{Tr}(g) = n - \text{Re}(\text{Tr}(g)) = \sum_{k=1}^{n}(1 - \text{Re}(z_k))$, et comme pour tout $k \in [\![1,n]\!]$, $1 - \text{Re}(z_k) \geqslant 1 - |z_j| = 0$, on a : pour tout $k \in [\![1,n]\!]$, $1 - \text{Re}(z_k) = 0$ donc (rappelons que z_k est de module

1) $z_k = 1$, donc finalement $g = I_n$. Par contraposée, pour tout $g \in G \setminus \{I_n\}$, $\mathrm{Tr}(g) \neq n$, donc d'après la question 10 de la partie 3, $\mathrm{Tr}(g) \in \{\tau_j \,;\, j \in [\![1, a]\!]\}$, et $P(\mathrm{Tr}(g)) = 0$. Comme $\mathrm{Tr}(I_n) = n$, on en déduit finalement que $\displaystyle\sum_{g\in G} P(\mathrm{Tr}(g)) = P(n)$, puis que $\boxed{P(n) \text{ est un entier divisible par } \mathrm{card}(G)}$.

5. (b) D'après la question précédente, p^r divise $\displaystyle\prod_{j=1}^{a}(n - \tau_j) = \prod_{j=1}^{a}(pj) = p^a a!$, donc $v_p(p^r) \leqslant v_p(p^a a!) = v_p(p^a) + v_p(a!)$. D'où $\boxed{r \leqslant a + v_p(a!)}$.

6. (a) D'après la question précédente et la question 3 (b) des Préliminaires, $r \leqslant a + \displaystyle\sum_{i=1}^{+\infty}\left\lfloor \frac{a}{p^i}\right\rfloor \leqslant a + \sum_{i=1}^{+\infty}\frac{a}{p^i} = a\frac{p}{p-1}$. Or, $a \leqslant \dfrac{n}{p-1}$. D'où $\boxed{r \leqslant \dfrac{pn}{(p-1)^2}}$.

6. (b) On sait que $\mathrm{card}(G) = p^r = \exp(r \ln p)$, donc d'après la question précédente, $\mathrm{card}(G) \leqslant \exp\left(\dfrac{np\ln p}{(p-1)^2}\right)$. Montrons que $\dfrac{p\ln p}{(p-1)^2} \leqslant 2\ln 2$. On pose $u :]1, +\infty[\to \mathbb{R}$ la fonction qui à $x \in]1, +\infty[$ associe $\dfrac{x\ln x}{(x-1)^2} \in \mathbb{R}$. La fonction u est dérivable et pour tout $x \in]1, +\infty[$, $u'(x) = -\dfrac{x\ln x + \ln x - x + 1}{(x-1)^3}$. En posant $v : [1, +\infty[\to \mathbb{R}$ la fonction qui à $x \in [1, +\infty[$ associe $x\ln x + \ln x - x + 1 \in \mathbb{R}$, v est dérivable et pour tout $x \in [1, +\infty[$, $v'(x) = \ln x + \dfrac{1}{x} \geqslant 0$, donc v est croissante, donc $v \geqslant v(1) = 0$. Ainsi $u' \leqslant 0$, donc u est décroissante. Comme p est un nombre premier, $p \geqslant 2$, donc $u(p) \leqslant u(2)$ *i.e.* $\dfrac{p\ln p}{(p-1)^2} \leqslant 2\ln 2$. Finalement, $\mathrm{card}(G) \leqslant \exp(2n\ln 2)$, donc $\boxed{\mathrm{card}(G) \leqslant 4^n}$.