Préliminaire

1. S'il existe $k \in \mathbb{N}^*$ tel que $z^k = 1$, alors $|z|^k = 1$ puis $|z| = 1$ (puisque $|z| \in \mathbb{R}^+$).

2. Si $g \in G$ est d'ordre d, alors $g^d = I_n$, ainsi $P = X^d - 1$ est un polynôme annulateur scindé sur $\mathbb{C}$ et à racines simples donc g est diagonalisable, de plus les valeurs propres de g sont des racines de P en parciculier ce sont des racines $d-$ième de l'unité.

   (a) $\{k \in [\![1, m]\!] \text{ tel que } q \mid k\} = \{iq \ / \ 1 \leq iq \leq m\} = \left\{iq \ / \ 1 \leq i \leq \dfrac{m}{q}\right\}$, donc $\text{Card}\{k \in [\![1, m]\!] \text{ tel que } q$ $\left\lfloor \dfrac{m}{q} \right\rfloor$.

   (b) on va procéder par récurrence sur m,soi $m' = \left\lfloor \dfrac{m}{p} \right\rfloor$, alors $pm' \leq m < p(m'+1)$. En utilisant que $v_p(ab) = v_p(a) + v_p(b)$, puis que $v_p(k) = 0$ pour $pm' < k < p(m'+1)$, on a $v_p(m) = v_p(pm'!) + v_p((pm'+1)...(m)) = v_p(pm'!)$ puis $v_p(m!) = v_p((pm')!) = v_p(p \times (2p) \times ...(pm'))$ (si p ne divise pas k , $v_p(k) = 0$). Ceci donne que $v_p(m!) = m' + v_p(m'!) = \left\lfloor \dfrac{m}{p} \right\rfloor + v_p(m'!)$.
   Pour $m \leq p-1$ c'est immédiat. supposons la propriété vraie jusqu'a m, alors
   $v_p(m!) = m' + v_p(m'!) = m' + \sum_{i=1}^{+\infty} \left\lfloor \dfrac{m'}{p^i} \right\rfloor = \left\lfloor \dfrac{m}{p} \right\rfloor + \sum_{i=1}^{+\infty} \left\lfloor \dfrac{m'}{p^i} \right\rfloor$
   Il reste à vérifier que $\left\lfloor \dfrac{m'}{p^i} \right\rfloor = \left\lfloor \dfrac{m}{p^{i+1}} \right\rfloor$ qui immédiate à l'aide de l'inégalité $m' \leq \dfrac{m}{p} < m'+1$,
   donc $\dfrac{m'}{p^i} \leq \dfrac{m}{p^{i+1}} < \dfrac{m'}{p^i} + \dfrac{1}{p^i} \leq \dfrac{m'}{p^i} + 1$ puis on passe à la partie entière.

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

1. Si $g \in GL_2(\mathbb{Z})$ est d'ordre fini, $\chi_g = X^2 - tr(g)X + \det(g) \in \mathbb{Z}[X] \subset \mathbb{R}[X]$, donc alors g admet deux valeurs propres complexe $\lambda_1 = e^{i\alpha}$ et $\lambda_2 = e^{-i\alpha}$, ainsi $tr(g) = \lambda_1 + \lambda_2 = 2\cos(\alpha)$. $|tr(g)| \leq 2$.

2. les λ_i sont réelles et de module égal à 1, donc $\lambda_i \in \{-1, 1\}$, par suite $\lambda_i^2 = 1$. g étant diagonalisable, donc $g^2 = I_2$. Ainis d divise 2 par suite $d \in \{1, 2\}$.

3. Si g n'a pas de valeurs propres réelles, comme on a $\chi_g \in \mathbb{Z}[X]$ et $|tr(g)| \leq 2$ et $|\det(g)| = |\lambda_1\lambda_2| = 1$. χ_g n'a pas de racines réelles, donc $\Delta = (tr(g))^2 - 4\det(g) < 0$. Ce qui donne que $(tr(g))^2 < 4$, donc $|tr(g)| \leq 1$ (puisque $tr(g) \in \mathbb{Z}$). D'où la discussion

   - Si $tr(g) = 0$, alors $\chi_g \in \{X^2+1, X^2-1\}$ mais X^2-1 à des racines réelles, donc $\chi_g = X^2+1$.
   - Si $tr(g) = 1$, $\chi_g \in \{X^2+X+1, X^2+X-1\}$.

4. Si $\chi_g = X^2 - 1$, c'est-à-dire g admet des racines réelles, alors $g^2 = I_2$, donc $d \in \{1, 2\}$.

   - Si $\chi_g = X^2+1$, alors $g^2 = -I_2$ puis $g^4 = I_2$ dans ce cas $d = 4$.
   - Si $\chi_g = X^2+X+1$, alors $g^3 - I_2 = (g^2 + g + I_2) = 0$, donc $g^3 = I_2$ dans ce cas $d = 3$.
   - Si $\chi_g = X^2-X+1$, alors $g^3 + I_2 = (g^2 - g + I_2) = 0$, donc $g^3 = -I_2$ puis $g^6 = I_2$ dans ce cas $d = 6$.

5. D'après les relations entre les racines et les coefficients d'un polynôme, on a:

$$a_k = (-1)^{n-k} \sum_{1\leq i_1\leq ...\leq i_{n-k}\leq n} z_{i_1}...z_{i_{n-k}}$$

Donc

$$|a_k| \leq \sum_{1\leq i_1\leq ...\leq i_{n-k}\leq n} |z_{i_1}|...\left|z_{i_{n-k}}\right| \leq \alpha^{n-k}\left(\sum_{1\leq i_1\leq ...\leq i_{n-k}\leq n} 1\right) = \binom{n}{n-k}\alpha^{n-k} = \binom{n}{k}\alpha^{n-k}.$$

6. Soit $A = \left\{\chi_g \text{ tel que } g \in GL_n(\mathbb{Z}) \text{ est d'ordre fini}\right\}$ et $B = [\![1, m]\!]^n$, où $m = \max\limits_{1\leq k\leq n-1}\binom{n}{k}$

Si $g \in GL_n(\mathbb{Z})$ est d'ordre fini, alors d'après la question précédente, les coefficients $a_i(g)$ de χ_g sont bornées et on a $|a_i(g)| \leq \binom{n}{k} \leq m$. ($\alpha_i(g) \leq 1$).

Soit $\phi : A \to B,\ \chi_g \mapsto (a_0(g), ..., a_{n-1}(g))$ est injective et B est fini, donc A est aussi fini.

7. Soit $H = \{d \in \mathbb{N}^* \text{ , il existe un élément } g \in GL_n(\mathbb{Z}) \text{ d'ordre } d\}$.

puisque $A = \left\{\chi_g \text{ tel que } g \in GL_n(\mathbb{Z}) \text{ est d'ordre fini}\right\}$ est fini, donc l'ensemble K des valeurs propres des éléments $g \in GL_n(\mathbb{Z})$ d'ordre fini est aussi fini. Les racines des éléments d'ordre fini sont des racines de l'unité, donc si H est infini, alors il suffit de choisir $d \in H$ tel que les racines de $X^d - 1$ soient toute dans $\mathbb{C}\backslash K$ (à l'exception de 1).

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

1. (a) g est d'ordre fini, donc diagonalisable, si $P \in GL_n(\mathbb{C})$ est telle que $P^{-1}gP$ =diag$(\lambda_1, ..., \lambda_n)$, alors $P^{-1}AP$ =diag$\left(\frac{\lambda_1 - 1}{m}, ..., \frac{\lambda_n - 1}{m}\right)$, donc A est diagonalsable.

On a $\left|\frac{\lambda_i - 1}{m}\right| \leq \frac{|\lambda_i| + 1}{m} \leq \frac{2}{m} < 1$. ($|\lambda_i| = 1$ d'après préliminaire)

(b) Les coefficients de $g - I_n$ sont tous divisbles par m, donc $A \in \mathcal{M}_n(\mathbb{Z})$ .Soit $\alpha(A) = \max\limits_{\lambda\in \mathrm{Sp}(A)} |\lambda|$ où sp(A) est le spectre de A. On a $\alpha < 1$.Les valeurs propres de A^k sont les λ^k avec $\lambda \in$sp(A). on a $\alpha\left(A^k\right) \leq \alpha(A) = \beta$.D'après la question **5.partie 1.**, on a $\left|a_i\left(A^k\right)\right| \leq \binom{n}{k}\alpha^{n-k} = \binom{n}{k}\beta^{n-k}$.Comme $0 \leq \beta < 1$, donc la suite $\binom{n}{k}\beta^{n-k}$ tend vers 0 lorsque $k \to +\infty$, il existe donc un entier q tel que

$$\forall k \geq q\ , 0 \leq \binom{n}{k}\beta^{n-k} < 1.$$

Pour un tel choix on a $|a_i(A^q)| < 1$ avec $a_i(A^q) \in \mathbb{Z}$ (puisque $A \in \mathcal{M}_n(\mathbb{Z})$), donc $a_i(A^q) = 0$ pour $0 \leq i \leq n-1$ et par suite $\chi_{A^q} = X^n$, donc $(A^q)^n = 0$. On prend alors $k = qn$.

(c) A est nilpotente et diagonalisable son polynôme minimal est donc scindé à racines simples, donc égal à X par suite $A = 0$, c'est-à-dire que $g = I_n$.

2. (a) Notons $f : \mathcal{M}_n(\mathbb{Z}) \to \mathcal{M}_n(\mathbb{Z}/m\mathbb{Z})\ , A = (a_{ij})_{1\leq i,j\leq n} \mapsto \overline{A} = (\overline{a_{ij}})_{1\leq i,j\leq n}$ où $\overline{a}$ désigne la classe modulo m. Il est immédiat que f est un morphisme d'anneaux.
et que si $A \in G$, alors $f(A^{-1}) = f(A)^{-1}$.

Si $A, B \in G$ tel que $f(A) = f(B)$, alors $f(AB^{-1}) = f(I_n)$
Ce qui donne que $AB^{-1} - I_n \in \mathcal{M}_n(\mathbb{Z})$ et que les coefficients de $AB^{-1} - I_n$ sont tous divisibles par m. Comme $AB^{-1} \in G$ est d'ordre fini (puisque G l'est), d'après la question précédente, on a $AB^{-1} = I_n$ puis $A = B$.

(b) On applique ce que précède avec $m = 3$, on a $\phi : G \to \mathcal{M}_n(\mathbb{Z}/3\mathbb{Z})$ est injective et $\mathcal{M}_n(\mathbb{Z}/3\mathbb{Z})$ est fini de cardinal 3^{n^2}, donc G est fini et $\text{card}(G) \leq 3^{n^2}$.

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

1. (a) Découle de le relation $k\binom{\ell}{k} = \ell\binom{\ell-1}{k-1}$ et du fait que k et ℓ sont premiers entre eux pour $1 \leq k < \ell$.

(b) On a $xy = yx$, on peux donc utiliser la formuledu binôme

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

puis à l'aide de la question précédente, on a $(x+y)^\ell - x^\ell - y^\ell \in \ell R$.

2. On a $\det(A+B) - \det(A) = \sum_{\sigma \in \mathcal{S}_n} \left(\prod_{i=1}^{n} \left(a_{\sigma(i),i} + b_{\sigma(i),i} \right) - \prod_{i=1}^{n} a_{\sigma(i),i} \right)$.Il suffit de montrer que si $(a_1, ..., a_k) \in I^k$ et $(b_1, ..., b_k) \in R^k$, alors

$$\Delta_k = (a_1 + b_1) ... (a_k + b_k) - a_1 ... a_k \in I$$

On a $(a_1 + b_1) ... (a_k + b_k) = \sum_{j=0}^{k} \left(\sum_{i_1 < ... < i_j \ ; \ i_{j+1} < .. i_k} b_{i_1} ... b_{i_j} a_{i_{j+1}} ... a_{i_k} \right)$

$= a_1 ... a_k + \sum_{j=1}^{k} \left(\sum_{i_1 < ... < i_j \ ; \ i_{j+1} < .. i_k} b_{i_1} ... b_{i_j} a_{i_{j+1}} ... a_{i_k} \right)$ et comme I est un idéal, la deuxième somme est un élément de I, donc $\Delta_k \in I$

3. Dans cette question considérons l'anneau $R = \mathbb{Z}[X]$. ℓ étant premier donc par récurrence sur m, on pour toute famille de polynômes $P_1, ..., P_m$ d'éléments de $\mathbb{Z}[X]$ $(P_1 + ... + P_m)^\ell - P_1^\ell - ... P_m^\ell \in \ell\mathbb{Z}[X]$.
Si $P = \sum_{i=0}^{k} a_i X^i$, alors $(P(X))^\ell - \sum_{i=0}^{k} (a_i X^i)^\ell \in \ell\mathbb{Z}[X] \quad (*)$.ℓ étant premier, donc d'après le théorème de Fermet $a_i^\ell - a_i \in \ell\mathbb{Z}$.Donc $\sum_{i=0}^{k} (a_i X^i)^\ell - \sum_{i=0}^{k} a_i X^{i\ell} \in \mathbb{Z}[X] \quad (**)$, puis par sommation de $(*)$ et $(**)$, on a $(P(X))^\ell - P\left(X^\ell\right) \in \ell\mathbb{Z}[X]$.

4. (a) Dans l'anneau $\mathcal{M}_n(\mathbb{Z}[X])$ les éléments XI_n et M commutent, on peux donc utiliser la formule du binôme, on a donc

$$\begin{aligned} (XI_n - M)^\ell &= \sum_{i=0}^{\ell} \binom{\ell}{i} X^{\ell-i} (-1)^i M^i \\ &= X^\ell I_n + (-1)^\ell M^\ell + \sum_{i=1}^{\ell-1} \binom{\ell}{i} X^{\ell-i} (-1)^i M^i \end{aligned}$$

$\binom{\ell}{i}$ est divisible par par ℓ, donc

$$\begin{aligned}(XI_n - M)^\ell &= \sum_{i=0}^{\ell}\binom{\ell}{i}X^{\ell-i}(-1)^i M^i \\ &= X^\ell I_n + (-1)^\ell M^\ell + \ell\left(\sum_{i=1}^{\ell-1}\frac{1}{\ell}\binom{\ell}{i}X^{\ell-i}(-1)^i M^i\right)\end{aligned}$$

$A = \left(\sum_{i=1}^{\ell-1}\frac{1}{\ell}\binom{\ell}{i}X^{\ell-i}(-1)^i M^i\right) \in \mathcal{M}_n(\mathbb{Z}[X])$.

Reste à discuter si $\ell = 2$ ou ℓ est impair.

Dans le premier cas $(XI_n - M)^2 = X^2 I_n - 2XM + M^2$ c'est donc vraie.

Si ℓ est impair, alors $(XI_n - M)^\ell - \left(X^\ell I_n - M^\ell\right) + \ell A$.

(b) Considérons l'idéal $I = \ell\mathbb{Z}[X]$ de l'anneaux $\mathbb{Z}[X]$, alors d'après la question, on a $\chi_{M^\ell}\left(X^\ell\right) - (\chi(X))^\ell = \det\left(X^\ell I_n - M^\ell\right) - (\det(XI_n - M))^\ell \in \ell\mathcal{M}_n(\mathbb{Z}[X])$

Donc d'après la question **3.partie 3**, on a $\chi_{M^\ell}\left(X^\ell\right) - (\chi(X))^\ell \in \ell\mathbb{Z}[X]$.

(c) On a $\chi_{M^\ell}(X) = X^n - tr\left(M^\ell\right)X^{n-1} + ...$, donc

$$\chi_{M^\ell}\left(X^\ell\right) - (\chi(X))^\ell = \left(X^{\ell n} - tr\left(M^\ell\right)X^{\ell(n-1)} + ...\right) - \left(X^n - tr(M)X^{n-1} + ...\right)^\ell$$

le coefficient de $X^{\ell(n-1)}$ est $tr\left(M^\ell\right) - (tr(M))^\ell \in \ell\mathbb{Z}$ d'après la question précédente.

Donc $tr\left(M^\ell\right) \equiv (tr(M))^\ell \mod(\ell)$ puis par le théorème de Fermat, on a $tr\left(M^\ell\right) \equiv (tr(M)) \mod(\ell)$ (puisque ℓ est premier).

5. Soit $g \in G$, d'après la question **4.c,** on a $tr(g^p) \equiv tr(g) \mod(\ell)$ puis par récurrence, on a $tr\left(g^{p^i}\right) \equiv tr(g) \mod(\ell)$ pour tout $i \in \mathbb{N}^*$. En particulier pour $i = r$, on a $g^{p^r} = I_n$, donc $tr(g) \equiv n \mod(p)$.

6. D'après la question **4.(c) partie 3**, ℓ divise $tr\left(g^k - g\right)$. Il suffit donc de montrer que $\left|tr\left(g^k - g\right)\right| < \ell$. Si $\mathrm{sp}(g) = \{\lambda_i, i = 1, 2, ..., n\}$, on a pour tout i ,alors $\left|\lambda_i^k - \lambda_i\right| \leq |\lambda_i| + |\lambda_i|^k \leq 2$, donc $\left|tr\left(g^k - g\right)\right| \leq \sum_{i=1}^{n}\left|\lambda_i^k - \lambda_i\right| \leq 2n < \ell$. D'où la conclusion

7. (a) $m = k + p^r\prod_{\ell\in A}\ell$ où $A = \{\ell \text{ premier}, \ell \leq 2n \text{ et } \ell \text{ ne divise pas } k\}$. Supposons que m admet un facteur premiers $q \in A$, alors q divise $p^r\prod_{\ell\in A}\ell$ et m, donc divise k absurde.

(b) Posons $m = p_1^{\alpha_1}...p_s^{\alpha_s}$ les diviseurs premiers de m, on a d'après la question précédente $p_i > 2n$.

Par itération de la question **6,** on a $tr\left(g^{\ell^i}\right) = tr(g)$ pour tout $i \in \mathbb{N}^*$ et ℓ premier >2n

Par récurrence alors sur s, on a $tr(g^m) = tr\left(g'^{p_s^{\alpha_s}}\right) = tr\left(g^{m'}\right)$ où $m = m'p_s^{\alpha_s}$

puis hypothèse de récurrene, donnc que $tr(g^m) = tr(g)$.

On a $g^m = g^k.\left(g^{p^r}\right)^d$ où $d = \prod_{\ell\in A}\ell$ (A déja défini)

Ce qui donne que $g^m = g^k$ (G étant d'ordre p^r, donc $g^{p^r} = I_n$). Ce qui permet de conclure que $tr(g^m) = tr\left(g^k\right)$.

8. (a) On effectue la division euclidienne de k par p, $k = ps + r$ avec $0 \leq r \leq p - 1$

p ne divise pas k si et seulement si $1 \leq r \leq p - 1$. on a $ps \leq p^{r-1}$, donc $s \leq p^{r-1} - 1$.

(b) On a $\sum_{j\in J_r}\zeta^j = \sum_{s=0}^{p^{r-1}-1}\zeta^{ps}\left(\sum_{t=1}^{p-1}\zeta^t\right)$

- Si $\zeta = 1$, alors $\zeta^{ps}\left(\sum_{t=1}^{p-1}\zeta^j\right) = p-1$, donc

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

- Si ζ est d'ordre p, alors $\zeta^p = 1$, donc $\zeta^{ps}\left(\sum_{t=1}^{p-1}\zeta^t\right) = \left(\sum_{t=0}^{p-1}\zeta^t\right) - 1 = \frac{1-\zeta^p}{1-\zeta} - 1 = -1$, ce qui donne

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

- Sinon

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

D'autre part $\left(\sum_{s=0}^{p^{r-1}-1}\zeta^{ps}\right) = \frac{1-\zeta^{p\left(p^{r-1}\right)}}{1-\zeta^p} = \frac{1-\zeta^{p^r}}{1-\zeta^p} = 0$, d'où le résultat.

9. (a) Par le résultat de la question **7.c partie 3**, on a $tr\left(g^k\right) = tr(g)$ pour tout $k \in J_r$, donc $\sum_{k\in J_r} tr\left(g^k\right) = \sum_{k\in J_r} tr(g) = \text{card}(J_r)\, tr(g)\,.\,\text{card}(J_r) = p^r - \text{card}\{k \text{ tel que } p \mid k \text{ et } k \le p^r\} = p^r - p^{r-1}$, puis puis **8.b,** $\sum_{k\in J_r} tr\left(g^k\right) = \sum_{k\in J_r} tr\left(g^k\right) = \sum_{k\in J_r}\left(\sum_{\zeta\in \text{sp}(g)}\zeta^k\right) = n_0 p^{r-1}(p-1) - n_1 p^{r-1}$

Ce qui donne $tr(g) = n_0 - \frac{n_1}{p-1}$.

(b) Il suffit de montrer que $\frac{n - tr(g)}{p}$ est un entier compris entre 0 et a.

$n - tr(g)$ est divisble par p (d'après la question **partie 3.5)**
D'autre part

$$n - tr(g) = n - n_0 + \frac{n_1}{p-1} \le n - n_0 + \frac{n}{p-1} \le n + \frac{n}{p-1} = \frac{np}{p-1}$$

Donc $\frac{n - tr(g)}{p} \le \frac{n}{p-1} \le a$. D'autre part $|tr(g)| \le n$ (puisque les valeurs propres sont de modules 1), donc $0 \le \frac{n - tr(g)}{p} \le a$.

Partie 4. Cardinaux des p-sous-groupes de $\text{GL}_n(\mathbb{C})$

1. Soit G un sous-groupe fini de $GL_n(\mathbb{C})$, $f = \frac{1}{\text{card}(G)}\sum_{g\in G} g$.

(a) On a $f^2 = \left(\frac{1}{\text{card}\,(G)}\right)^2 \sum_{g_1\in G}\left(\sum_{g_2\in G} g_1g_2\right)$. D'autre part, pour tout $g \in G$, l'application $G \to G, h \mapsto gh$ est injective et G est fini donc bijective. En conséquence on a $\{gh;\ h \in G\} = G$ et donc $\left(\sum_{g_2\in G} g_1g_2\right) = \left(\sum_{g\in G} g\right)$ =card$(G) \times f$. On a alors

$$f^2 = \left(\frac{1}{\text{card}\,(G)}\right)^2 \sum_{g_1\in G}\left(\sum_{g_2\in G} g_1g_2\right) = \left(\frac{1}{\text{card}\,(G)}\right)^2 \sum_{g_1\in G} card\,(G) \times f$$

Donc $f^2 = f$.
Si $\forall g \in G$, alors $g\,(x) = x$, alors $f\,(x) = x$.
Notons qu'au passage, on a montrer que pour tout $g \in G$, $f \circ g = g \circ f = f$, cette remarque servira pour établir la réciproque.
Réciproquement
On a pour tout $g \in G$, $f \circ g = g \circ f = f$, donc si $f\,(x) = x$, alors $g\,(f\,(x)) = x$, par suite $g\,(x) = x$.
En conclusion f est le projecteur sur $\{x \in \mathbb{C}^n / \forall g \in G, g\,(x) = x\}$.

(b) f est un projecteur, donc $Tr\,(f)$ =rg$(f) \in \mathbb{N}$(où rg désigne le rang). Ce qui donne que

$$\sum_{g\in G} tr\,(g) = rg\,(f) \times \text{card}\,(G) \in \mathbb{N}$$

2. (a) i. immédiate $tr\,((g \otimes h)) = \sum_{i=1}^{n} tr\,(g_{ii}h) = \sum_{i=1}^{n} g_{ii}tr\,(h) = tr\,(g)\,tr\,(h)$.

ii. Posons $(g \otimes h)\,(g' \otimes h') = (c_{ij})_{1\le i,j\le n}$ où c_{ij} sont des matrices (écriture par blocs). On a $c_{ij} = \sum_{k=1}^{n} g_{ik}hg'_{kj}h' = \sum_{k=1}^{n} g_{ik}g'_{kj}hh'$ c'est le bloc d'indice (i,j) de $(gg' \otimes hh')$. D'où l'égalité.

iii. Il suffit de remarquer que $(g \otimes h)\,(g^{-1} \otimes h^{-1}) = gg^{-1} \otimes hh^{-1} = I_n \otimes I_p = I_{np}$.

3. (a) Supposons que $\varphi^{-1}\,(\{\gamma'\}) \neq \emptyset$. Soit $\gamma \in \varphi^{-1}\,(\{\gamma'\})$, alors $x \in \varphi^{-1}\,(\{\gamma'\})$ si et seulement si $\varphi\,(x) = \gamma' = \varphi\,(\gamma)$ ce qui est équivalent à $\varphi\,(\gamma^{-1}x) = e_{\Gamma'}$ ou encore à $\gamma^{-1}x \in \ker\,(\varphi) = H$, donc $\varphi^{-1}\,(\{\gamma'\}) = \gamma H$.

(b) Remarquons d'abord que si $\gamma' \notin \varphi\,(\Gamma)$, alors $\varphi^{-1}\,(\{\gamma'\}) = \emptyset$. La famille $(\varphi^{-1}\,(\gamma'))_{\gamma'\in\varphi(\Gamma)}$ est une partition de Γ, donc $\text{card}(\Gamma) = \sum_{\gamma'\in\varphi(\Gamma)} \text{card}\varphi^{-1}\,(\{\gamma'\})$

D'autre part γH est équipotent à H (l'application $h \mapsto \gamma h$ est une bijection)
Donc $\text{card}(\Gamma) = \sum_{\gamma'\in\varphi(\Gamma)} \text{card}\varphi^{-1}\,(\{\gamma'\}) = \sum_{\gamma'\in\varphi(\Gamma)} \text{card}\ H$ =card$(\varphi\,(\Gamma)) \times$card$(H)$.

4. (a) φ_s est un morphisme découle de la question **2.**
Posons $\Gamma = G$ et $\Gamma' = \varphi_s\,(G)$, alors φ_s induit sur G un morphisme de Γ sur Γ' de noyau $H = \ker\,(\varphi_s) \cap G$. Γ et Γ' étant finis, alors à par la question **3.b de la partie 4**, on a:

$$\text{card}\,(G) = \text{card}\,(\varphi_s\,(G)) \times \text{card}\,(\ker\,(\varphi_s) \cap G)$$

D'autre part, on a pour tout $h \in G$, $tr\,(\varphi_s\,(g)) = tr\left(g^{(s)} \otimes g\right) = tr\left(g^{(s)}\right) tr\,(g)$ ce qui donne par récurrence qie $tr\,(\varphi_s\,(g)) = (tr\,(g))^s$. De cette relation on tire que

$$\sum_{g\in G} tr\,(\varphi_s\,(g)) = \sum_{g\in G} (tr\,(g))^s$$

(b) $\varphi_s(G)$ est un groupe (comme image d'un groupe par un morphisme), donc par le résultat de la question **4.1.b)**, on a $\sum_{g' \in \varphi_s(G)} (tr(g'))$ est un entier divisible par $\text{card}(\varphi_s(G))$, donc $\sum_{g\in G} (tr(g))^s = \text{card}(G \cap \ker \varphi_s) \times \sum_{g' \in \varphi_s(G)} (tr(g'))$ est divisble par $\text{card}(G \cap \ker \varphi_s) \times \text{card}(\varphi_s(G)) = \text{card}(G)$.

5. (a) $P(X) = \prod_{j=1}^{n} (X - r_j) = X^n + a_{n-1}X^{n-1} + ... + a_0$.

$$\begin{aligned} \sum_{g\in G} P(tr(g)) &= \sum_{g\in G} \left((tr(g))^n + a_{n-1}(tr(g))^{n-1} + ... + a_0 \right) \\ &= \sum_{g\in G} (tr(g))^n + a_{n-1} \sum_{g\in G} (tr(g))^{n-1} + ... + \sum_{g\in G} a_0 \end{aligned}$$

Donc $\sum_{g\in G} P(tr(g)) = \sum_{g\in G} (tr(g))^n + a_{n-1} \sum_{g\in G} (tr(g))^{n-1} + ... + \sum_{g\in G} a_0$.
D'autre part $\sum_{g\in G} a_0 = a_0 \text{ card}(G)$ et $\text{card}(G)$ divise $\sum_{g\in G} (tr(g))^s$ pour tout $s \geq 1$, donc $\text{card}(G)$ divise $\sum_{g\in G} P(tr(g)) = P(n)$. ($tr(g) = n \bmod (p)$).

(b) $\text{card}(G) = p^r$ divise $P(n) = p^a(a!)$, donc $r \leq v_p(p^a(a!)) = a + v_p(a!)$.

6. (a) On a $v_p(a!) = \sum_{j=1}^{+\infty} \left\lfloor \frac{a}{p^j} \right\rfloor \leq \sum_{j=1}^{+\infty} \frac{a}{p^j}$, donc

$$r \leq a + \sum_{j=1}^{+\infty} \frac{a}{p^j} = \sum_{j=0}^{+\infty} \frac{a}{p^j} = \frac{a}{1 - \frac{1}{p}} = \frac{ap}{p-1} \leq \frac{np}{(p-1)^2} \text{ puisque } a \leq \frac{n}{p-1}$$

(b) On a $\text{card}(G) = p^r \leq p^{\frac{pn}{(p-1)^2}} = \left(p^{\frac{p}{(p-1)^2}} \right)^n$. Il suffit donc de montrer que $p^{\frac{p}{(p-1)^2}} \leq 4$

Pour étudier la monotonie de $p \mapsto p^{\frac{p}{(p-1)^2}} = \exp\left(\frac{p \ln p}{(p-1)^2} \right)$, considérons la fonction $\phi : t \mapsto \frac{t \ln(t)}{(t-1)^2} = \frac{\ln(t)}{t-1} \times \frac{t}{t-1}$

La fonction $t \mapsto \ln t$ est concave donc $t \mapsto \frac{\ln t}{t-1}$ est décroissante . La fonction $t \mapsto \frac{t}{t-1}$ est aussi décoissante et les deux fonctions sont positives et décroissantes sur $[2, +\infty[$, donc $t \mapsto \frac{t \ln(t)}{(t-1)^2} = \frac{\ln(t)}{t-1} \times \frac{t}{t-1}$ est décroissante sur $[2, +\infty[$, donc $\theta : p \mapsto \left(p^{\frac{p}{(p-1)^2}} \right)^n$ est décroissante donc $\theta(p) \leq \theta(2) = 4^n$.