

X-ENS 2021 : épreuve A

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

Un corrigé

Préliminaires

1. Si z est une racine de l'unité, alors il existe d tel que $z^d = 1$ et on a donc $|z|^d = 1$. Comme $|z| \in \mathbb{R}^+$, le passage à la racine d -ième est licite et donne $|z| = 1$.

Les racines de l'unité sont de module 1

2. Si g est d'ordre d alors $X^d - 1$ annule g . Ainsi g est diagonalisable (car annulé par un polynôme scindé simple) et ses valeurs propres sont des racines de $X^d - 1$ et donc des racines de l'unité.

Si $g \in GL_n(\mathbb{C})$ est d'ordre d , alors g est diagonalisable à spectre inclus dans $\mathbb{U}_d$

3. (a) Les multiples de q dans $\llbracket 1, m \rrbracket$ sont les entiers qui s'écrivent pq avec $1 \leq pq \leq m$ c'est à dire $\frac{1}{q} \leq p \leq \frac{m}{q}$.
Comme $\frac{1}{q} \leq 1$, les entiers p convenables sont ceux de $\llbracket 1, \lfloor m/q \rfloor \rrbracket$. Comme deux entiers p différents donnent deux multiples différents, on conclut que

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

- (b) Dans $\llbracket 1, m \rrbracket$, il y a $\lfloor m/q^k \rfloor$ multiples de q^k et $\lfloor m/q^{k+1} \rfloor$ multiples de q^{k+1} . Il y a donc $\lfloor m/q^k \rfloor - \lfloor m/q^{k+1} \rfloor$ éléments de valuation q -adique valant k . Remarquons que ce nombre est nul pour k assez grand.

Puisque v_q est multiplicative ($v_q(ab) = v_q(a) + v_q(b)$) par unicité de la décomposition en produit de nombres premiers par exemple), on a

$$v_q(m!) = \sum_{a=1}^m v_q(a)$$

Dans cette somme, il y a $\lfloor m/q^k \rfloor - \lfloor m/q^{k+1} \rfloor$ entiers a qui apportent une contribution égale à k . On a donc (la somme est en fait finie)

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

Comme $\lfloor m/q^k \rfloor$ est nul pour k assez grand, on peut découper la somme et réindicer la seconde :

$$v_q(m!) = \sum_{k=1}^{\infty} k \left\lfloor \frac{m}{q^k} \right\rfloor - \sum_{k=2}^{\infty} (k-1) \left\lfloor \frac{m}{q^k} \right\rfloor$$

les termes se simplifient et il reste

$$v_q(m!) = \sum_{k=1}^{\infty} \left\lfloor \frac{m}{q^k} \right\rfloor$$

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

1. g est $\mathbb{C}$ -diagonalisable et sa trace est la somme de ses deux valeurs propres λ_1 et λ_2 (il suffit en fait d'avoir la trigonalisabilité qui est vraie pour toute matrice complexe). Comme $|\lambda_i| = 1$ (préliminaires), l'inégalité triangulaire donne

$$|\mathrm{Tr}(g)| \leq 2$$

2. Si les valeurs propres sont réelles, comme elles sont de module 1, elles valent 1 ou -1 . On a donc $g^2 = I_2$ et donc $d|2$.

$$\boxed{\text{Si } g \text{ est à valeurs propres réelles, son ordre vaut 1 ou 2}}$$

3. On suppose ici que les valeurs propres de g ne sont pas réelles. Comme g est réelle, ses valeurs propres sont conjuguées, disons $e^{i\theta}$ et $e^{-i\theta}$. La trace, qui vaut $2\cos(\theta)$, est entière et de module ≤ 2 et est donc dans $\{-2, -1, 0, 1, 2\}$.

- Si elle vaut ± 2 alors $\cos(\theta) = \pm 1$ et les valeurs propres sont entières et cela est exclu.
- Si elle vaut 0 alors $\cos(\theta) = 0$ et les valeurs propres sont i et $-i$. Le polynôme caractéristique vaut $X^2 + 1$.
- Si elle vaut 1 alors $\cos(\theta) = 1/2$ et les valeurs propres valent $-j$ et $-j^2$. Le polynôme caractéristique vaut $X^2 - X + 1$.
- Si elle vaut -1 alors $\cos(\theta) = -1/2$ et les valeurs propres valent j et j^2 . Le polynôme caractéristique vaut $X^2 + X + 1$.

$$\boxed{\text{Si } \mathrm{sp}(g) \cap \mathbb{R} = \emptyset \text{ alors } \chi_g \in \{X^2 + 1, X^2 + X + 1, X^2 - X + 1\}}$$

4. Dans le cas où il y a des valeurs propres réelles, $d \in \{1, 2\}$.
Dans l'autre cas, g est semblable dans $\mathbb{C}$ à $\mathrm{diag}(\lambda, \bar{\lambda})$ avec $\lambda \in \{i, j, -j\}$ et l'ordre vaut alors 4, 3 ou 6.

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

5. Comme P est unitaire, on a

$$X^n + \sum_{i=0}^{n-1} a_i X^i = \prod_{k=1}^n (X - z_k)$$

On développe le second membre :

$$\prod_{k=1}^n (X - z_k) = X^n + \sum_{j=1}^n (-1)^j b_j X^{n-j} \quad \text{avec} \quad b_j = \sum_{1 \leq i_1 < \dots < i_j \leq n} \prod_{k=1}^j z_{i_k}$$

et par identification des coefficients :

$$a_{n-j} = (-1)^j \sum_{1 \leq i_1 < \dots < i_j \leq n} \prod_{k=1}^j z_{i_k}$$

Dans cette somme, tous les termes sont en module plus petits que α^j et il y en a $\binom{n}{j}$. Ainsi (inégalité triangulaire)

$$|a_{n-j}| \leq \binom{n}{j} \alpha^j$$

Comme $\binom{n}{j} = \binom{n}{n-j}$, on conclut que

$$\boxed{\forall j \in \llbracket 0, n-1 \rrbracket, |a_j| \leq \binom{n}{j} \alpha^{n-j}}$$

6. Si $g \in GL_n(\mathbb{Z})$ est d'ordre fini, son polynôme caractéristique est à coefficients entiers et comme toutes les valeurs propres de χ_g sont de module 1, la question précédente montre que le coefficient de X^j est plus petit que $\binom{n}{j}$ en module et ne peut prendre que $2\binom{n}{j} + 1$ valeurs. Ainsi

$$\boxed{\{\chi_g \text{ tel que } g \in GL_n(\mathbb{Z}) \text{ est d'ordre fini}\} \text{ est fini}}$$

et son cardinal plus petit que le produit des $2\binom{n}{j} + 1$ pour $j \in \llbracket 0, n-1 \rrbracket$.

7. Les valeurs propres des éléments de $GL_n(\mathbb{Z})$ d'ordre fini ne peuvent donc prendre qu'un nombre fini de valeurs (nombre fini de polynômes caractéristiques n'ayant eux-mêmes qu'un nombre fini de racines). De plus chacune de ces valeurs propres est une racine de l'unité.

En notant m le plus grand entier tel qu'il existe une racine d'un χ_g envisageable possédant une racine dans $\mathbb{U}_m$, on est donc assuré que l'ordre d d'un élément $GL_n(\mathbb{Z})$ d'ordre fini est plus petit que m .

$$\boxed{\{d \in \mathbb{N}, \exists g \in GL_n(\mathbb{Z}) \text{ d'ordre } d\} \text{ est fini}}$$

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

1. (a) g étant d'ordre fini d est semblable à $\text{diag}(\lambda_1, \dots, \lambda_n)$ avec $\lambda_i \in \mathbb{U}_d$. Ainsi, A est semblable (par la même matrice de passage) à $\text{diag}(\mu_1, \dots, \mu_n)$ où $\mu_k = \frac{\lambda_k - 1}{m}$. On remarque que $|\mu_k| \leq \frac{2}{m} < 1$.

$$\boxed{A \text{ est } \mathbb{C}\text{-diagonalisable à valeurs propres de module } < 1}$$

- (b) Avec les notations précédentes (et comme $(P^{-1}BP)^k = P^{-1}B^kP$), il existe une matrice inversible $P \in GL_n(\mathbb{C})$ telle que

$$A^k = P^{-1} \text{diag}(\mu_1^k, \dots, \mu_n^k) P$$

La matrice diagonale est de limite nulle quand $k \rightarrow +\infty$ (car $|\mu_k| < 1$ pour tout k) et par théorèmes d'opération, $A^k \rightarrow 0$.

Ceci signifie que toutes les suites de coefficients $(A^k[i, j])$ sont de limite nulle.

Mais A étant à coefficients entiers, il en est de même de A^k et ainsi A^k est nulle pour k assez grand (à coefficients entiers en module < 1).

$$\boxed{A \text{ est nilpotente}}$$

- (c) $g - I_n$ est donc une matrice nilpotente et 0 est sa seule valeur propre. Comme c'est une matrice diagonalisable, elle est nulle.

$$\boxed{g = I_n}$$

2. (a) Notons φ l'application de réduction modulo m des coefficients.

Supposons avoir $g_1, g_2 \in G$ tels que $\varphi(g_1) = \varphi(g_2)$.

D'après les propriétés dans l'anneau $\mathbb{Z}/m\mathbb{Z}$ et avec la formule du produit matriciel, on a $\varphi(A)\varphi(B) = \varphi(AB)$. Ainsi,

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

et, φ étant un morphisme additif,

$$\varphi(g_1^{-1}g_2 - I_n) = \varphi(0)$$

$g = g_1^{-1}g_2$ vérifie les hypothèses de la question 1 de la partie 2 ($g \in G$ car G est un groupe et comme G est fini, A est d'ordre fini diviseur de $|G|$; de plus, on vient de voir que tous les coefficients de $g - I_n$ sont multiples de m). Ainsi $g = I_n$ et $g_1 = g_2$.

La réduction modulo m est injective de G dans $\mathcal{M}_n(\mathbb{Z}/m\mathbb{Z})$

- (b) Ceci est vrai en particulier pour $m = 3$ et G est donc de cardinal plus petit que $\mathcal{M}_n(\mathbb{Z}/3\mathbb{Z})$, c'est à dire

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

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

1. (a) Soit $k \in [1, \ell - 1]$. On a

$$k! \binom{\ell}{k} = \ell(\ell - 1) \dots (\ell - k + 1) \in \mathbb{N}$$

Ainsi $\ell | \binom{\ell}{k} k!$. Or, $\ell \wedge k = 1$ quand $1 \leq k \leq \ell - 1$ (car ℓ est premier) et donc $\ell \wedge k! = 1$ (par exemple, car ℓ n'intervient dans la décomposition en produit de facteur premier d'aucun des facteurs de la factorielle). Par lemme de Gauss, on conclut que $\ell | \binom{\ell}{k}$.

$$\forall k \in [1, \ell - 1], \ell | \binom{\ell}{k}$$

- (b) Si x et y commutent, on peut utiliser la formule du binôme. En isolant les termes extrêmes, on obtient

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

Avec la question précédente, on peut écrire

$$(x + y)^\ell - x^\ell - y^\ell = \ell \sum_{k=1}^{\ell-1} \alpha_k x^k y^{\ell-k} \quad \text{avec } \alpha_k \in \mathbb{N}$$

Comme R est un anneau, la somme est élément de R et ainsi

$$\forall x, y \in R, xy = yx \implies (x + y)^\ell - x^\ell - y^\ell \in \ell R$$

2. Notons $C_i(M)$ la colonne numéro i d'une matrice M . On a alors

$$\det(A_1 + A_2) = \det(C_1(A_1) + C_1(A_2), \dots, C_n(A_1) + C_n(A_2))$$

Par multilinéarité du déterminant, on en déduit que

$$\det(A_1 + A_2) = \sum_{i_1, \dots, i_n \in \{1, 2\}} \det(C_1(A_{i_1}), \dots, C_n(A_{i_n}))$$

Dans cette somme, on a 2^n termes.

- Celui pour lequel $i_1 = \dots = i_n = 1$ et qui vaut $\det(A_1)$.
- Ceux pour lequel $\exists p, i_p = 2$. Dans un tel terme, le développement par rapport à la colonne p donne

$$\det(C_1(A_{i_1}), \dots, C_n(A_{i_n})) = \sum_{k=1}^n (-1)^{p+k} c_k A_2[k, p]$$

où les c_k sont des déterminants d'éléments de $\mathcal{M}_{n-1}(R)$ et donc des éléments de R . Si tous les coefficients de A_2 sont dans I , cette somme est dans I (car I est un idéal donc sous-groupe additif et stable par multiplication par un élément de R).

Ainsi, si tous les coefficients de A_2 sont dans I , $\det(A_1 + A_2) - \det(A_2)$ est dans I comme somme de tels éléments.

Si tous les coefficients de B sont dans I , alors $\det(A + B) - \det(A) \in I$

3. Montrons par récurrence (sur n) que dans l'anneau commutatif $\mathbb{Z}[X]$,

$$(A_1 + \cdots + A_n)^\ell - (A_1^\ell + \cdots + A_n^\ell) \in \ell\mathbb{Z}[X]$$

- Le résultat est immédiat au rang $n = 1$.
- Supposons le résultat vrai à un rang $n \geq 1$. Soient $A_1, \dots, A_{n+1} \in \mathbb{Z}[X]$. On a alors (avec 1(b) et par commutativité de l'anneau)

$$\left(\sum_{k=1}^{n+1} A_k\right)^\ell - \left(\left(\sum_{k=1}^n A_k\right)^\ell + A_{n+1}^\ell\right) \in \ell\mathbb{Z}[X]$$

Par hypothèse de récurrence,

$$(A_1 + \cdots + A_n)^\ell - (A_1^\ell + \cdots + A_n^\ell) \in \ell\mathbb{Z}[X]$$

Il reste à sommer pour obtenir le résultat au rang $n + 1$.

Soit alors $P \in \mathbb{Z}[X]$. On peut l'écrire $P = a_0 + a_1X + \cdots + a_dX^d$ et ainsi

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

C'est à dire que $P(X)^\ell - P(X^\ell) \in \ell\mathbb{Z}[X]$. Ainsi (passage à l'opposé)

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

4. (a) XI_n et M sont des éléments de l'anneau $R = \mathcal{M}_n(\mathbb{Z}[X])$ et ces éléments commutent ($(XI_n)M = M(XI_n) = XM$). On peut ainsi utiliser 1(b) avec $x = XI_n$ et $y = -M$:

$$(XI_n - M)^\ell - (X^\ell I_n + (-1)^\ell M^\ell) \in \ell R$$

Si $\ell \geq 3$ alors, ℓ étant premier, ℓ est impair et $(-1)^\ell = -1$. Ainsi

$$\exists A \in \mathcal{M}_n(\mathbb{Z}[X]), (XI_n - M)^\ell - (X^\ell I_n - M^\ell) = \ell A$$

Dans le cas où $\ell = 2$, on remarque que $(X^2 I_n + M) - (X^2 I_n - M) = 2M \in 2R$ et le résultat demeure vrai.

- (b) D'après la question 3 utilisée avec $P = \chi_M$, on a

$$\chi_M(X^\ell) - (\chi_M(X))^\ell \in \ell\mathbb{Z}[X] \tag{*}$$

On se place dans l'anneau commutatif $R = \mathbb{Z}[X]$ et on utilise la question 2 avec $I = \ell\mathbb{Z}[X]$ (idéal engendré par le polynôme constant ℓ) et $B = (XI_n - M)^\ell - (X^\ell I_n - M^\ell)$ qui s'écrit ℓA et dont tous les coefficients sont donc dans I . Cette question donne

$$\det((X^\ell I_n - M^\ell) + B) - \det(X^\ell I_n - M^\ell) \in I$$

c'est à dire

$$\det((XI_n - M)^\ell) - \det(X^\ell I_n - M^\ell) \in I$$

ou encore

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

En soustrayant les relations (*) et (**), on a donc

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

(c) On a d'une part

$$\chi_{M^\ell}(X^\ell) = X^{\ell n} - \text{Tr}(M^\ell)X^{\ell(n-1)} + \cdots + (-1)^n \det(M^\ell)$$

$$\chi_M(X) = X^n - \text{Tr}(M)X^{n-1} + \cdots + (-1)^n \det(M)$$

et d'autre part avec la question 3,

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

Ainsi avec la question précédente

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

Tous les coefficients de $\chi_{M^\ell}(X^\ell) - (\chi_M(X))^\ell$ sont des multiples de ℓ . C'est en particulier le cas du coefficient de $X^{(n-1)\ell}$ et ainsi

$$\boxed{\text{Tr}(M^\ell) \equiv \text{Tr}(M) \pmod{\ell}}$$

5. On peut appliquer ceci à $g \in G$ et $\ell = p$:

$$\text{Tr}(g^p) = \text{Tr}(g) \pmod{p}$$

mais aussi à g^p :

$$\text{Tr}(g^{p^2}) = \text{Tr}(g^p) \pmod{p}$$

On a donc

$$\text{Tr}(g^{p^2}) = \text{Tr}(g) \pmod{p}$$

On montre de même par une récurrence non détaillée que

$$\forall k \in \mathbb{N}^*, \text{Tr}(g^{p^k}) = \text{Tr}(g) \pmod{p}$$

L'ordre de g dans G divise le cardinal de G et est donc une puissance de p (puisque p est premier). Il existe ainsi k tel que $g^{p^k} = I_n$. On en conclut que

$$\boxed{\forall g \in G, \text{Tr}(g) \equiv n \pmod{p}}$$

6. La question 4(c) montre que g et g^ℓ (tous deux dans G) ont des traces égales modulo ℓ (et même égale à n modulo ℓ).

Or, la trace d'un élément de G est un entier de module $\leq n$ (puisque les valeurs propres sont toutes de module ≤ 1).

On a donc $\text{Tr}(g^\ell) - \text{Tr}(g)$ qui est un multiple de ℓ dans $[-2n, 2n]$. On peut en déduire que

$$\boxed{\text{Si } \ell > 2n \text{ est premier, } \text{Tr}(g^\ell) = \text{Tr}(g)}$$

7. (a) Supposons, par l'absurde, que m possède un facteur premier $\ell \leq 2n$.

Si ℓ ne divise pas k , il est dans le produit de définition de m et donc divise ce produit. Comme il divise aussi m , il divise k et c'est impossible.

Si ℓ divise k alors comme il divise m il divise $m - k$. Et comme il ne divise pas le produit dans la définition de m (par unicité de la décomposition en produit de premiers), il divise p^r et est donc égal à p . Ce qui contredit l'hypothèse que k n'est pas divisible par p .

$$\boxed{\text{Tous les facteurs premiers de } m \text{ sont } > 2n}$$

- (b) L'ordre de g étant un diviseur du cardinal de G , $g^{p^r} = 1$ et donc $g^k = g^m$.
Or, $m = \ell_1 \dots \ell_q$ où les ℓ_i sont des nombres premiers tous $> 2n$.
La question 6 donne

$$\text{Tr}(g^m) = \text{Tr}((g^{\ell_1 \dots \ell_{q-1}})^{\ell_q}) = \text{Tr}(g^{\ell_1 \dots \ell_{q-1}})$$

et en itérant le processus (et donc en fait à l'aide d'une récurrence sur le nombre q de facteurs), g^m et g ont même trace. Ainsi

$$\boxed{\forall g \in G, \text{Tr}(g^k) = \text{Tr}(g) \text{ quand } p \text{ ne divise pas } k}$$

8. (a) Procédons par double inclusion.

- Soit $s \in \llbracket 0, p^{r-1} - 1 \rrbracket$ et soit $t \in \llbracket 1, p - 1 \rrbracket$. On a alors $1 \leq ps + t \leq p^r - p + (p - 1) = p^r - 1$. De plus, p ne divisant pas t , il ne divise pas $ps + t$.
- Soit $x \in J_r$. Une division euclidienne donne $x = ps + t$ avec $0 \leq t \leq p - 1$. Comme p ne divise pas x , $t \neq 0$ et donc $t \in \llbracket 1, p - 1 \rrbracket$. De plus, $s = \frac{x-t}{p}$ et donc $-1 < -\frac{p-2}{p} \leq s \leq \frac{p^r-1}{p} < p^{r-1}$ et comme s est entier, $s \in \llbracket 0, p^{r-1} - 1 \rrbracket$.

$$\boxed{J_r = \bigcup_{0 \leq s \leq p^{r-1}-1} \{ps + t \text{ tels que } 1 \leq t \leq p - 1\}}$$

- (b) Par unicité de la division euclidienne, deux couples (s, t) comme ci-dessus donnent deux éléments différents de J_r . On a donc

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

La valeur des sommes géométriques dépend du fait que la raison est ou non égale à 1.

Si $\zeta = 1$, les deux raisons ζ et ζ^p valent 1 et le produit des sommes vaut $(p - 1)p^{r-1}$.

Sinon si $\zeta^p = 1$, la seconde somme vaut p^{r-1} et on a par ailleurs $\sum_{t=0}^{p-1} \zeta^t = 0$ et donc la première somme vaut -1 .

Sinon, la deuxième somme vaut $\frac{\zeta^{p^r}-1}{\zeta^p-1} = 0$.

Finalement,

$$\boxed{\sum_{j \in J_r} \zeta^j = \begin{cases} p^{r-1}(p - 1) & \text{si } \zeta = 1 \\ -p^{r-1} & \text{si } \zeta \text{ est d'ordre } p \\ 0 & \text{sinon} \end{cases}}$$

9. Notons $\lambda_1, \dots, \lambda_n$ les valeurs propres de g comptées avec multiplicité. Celles de g^k sont donc les $\lambda_1^k, \dots, \lambda_n^k$ (ce que l'on voit, par exemple, en se plaçant dans une base de trigonalisation). La trace d'une matrice étant la somme des valeurs propres complexes comptées avec multiplicité, on a

$$\forall k \in \mathbb{N}, \text{Tr}(g^k) = \sum_{i=1}^n \lambda_i^k$$

Quand $k \in J_r$, toutes ces traces sont égales à celle de g (question 7). En sommant les relations, on a donc

$$\text{Card}(J_r) \text{Tr}(g) = \sum_{i=1}^n \sum_{k \in J_r} \lambda_i^k$$

Dans cette somme, les termes peuvent valoir $p^{r-1}(p-1)$ (cas $\lambda_i = 1$) ou $-p^{r-1}$ (cas λ_i d'ordre p) et 0 sinon. On a donc

$$\text{Card}(J_r)\text{Tr}(g) = (n_0 - \frac{n_1}{p-1})p^{r-1}(p-1)$$

Comme $\text{Card}(J_r) = p^{r-1}(p-1)$ (comme mentionné en question précédente avec l'unicité de la division euclidienne), on a

$$\boxed{\text{Tr}(g) = n_0 - \frac{n_1}{p-1}}$$

10. Comme les valeurs propres sont de multiplicité plus petite que n , on a

$$-\frac{n}{p-1} \leq \text{Tr}(g) = n_0 - \frac{n_1}{p-1} \leq n$$

On en déduit que

$$0 \leq \frac{n - \text{Tr}(g)}{p} \leq \frac{n}{p-1}$$

Or, p divise $n - \text{Tr}(g)$ (question 5) et la quantité centrale ci-dessus est entière. Elle est donc dans $\llbracket 0, \left\lfloor \frac{n}{p-1} \right\rfloor \rrbracket$.

$$\boxed{\forall g \in G, \text{Tr}(g) \in \{n - pv, v \in \llbracket 0, \left\lfloor \frac{n}{p-1} \right\rfloor \rrbracket\}}$$

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

1. (a) On a

$$f^2 = \frac{1}{\text{card}(G)^2} \sum_{g_1 \in G} \sum_{g_2 \in G} g_1 g_2$$

Pour tout $g_1 \in G$, $g \mapsto g_1 g$ est injective et va de G dans G qui est fini. C'est donc une bijection. Ci-dessus, la somme intérieure est constante et ainsi

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

On a montré que

$$\boxed{f \text{ est un projecteur}}$$

C'est, comme tout projecteur, un projecteur sur $\text{Im}(f) = \ker(f - I_n)$ (de direction $\ker(f)$).

(b) La trace étant linéaire, on a

$$\sum_{g \in G} \text{Tr}(g) = \text{card}(G) \text{Tr}(f)$$

et comme f est un projecteur, la trace de f est un entier (égal au rang de f). Ainsi

$$\boxed{\sum_{g \in G} \text{Tr}(g) \text{ est un entier divisible par } \text{card}(G)}$$

2. La trace d'une matrice définie par blocs, comme $g \otimes h$, est la somme des traces des blocs. Ici, le i -ième bloc diagonale a pour trace $g_{i,i} \text{Tr}(h)$ (linéarité de la trace). En sommant, on a donc

$$\boxed{\text{tr}(g \otimes h) = \text{Tr}(g) \text{Tr}(h)}$$

Le calcul par blocs montre que $(g \otimes h)(g' \otimes h')$ est bloc diagonale avec le bloc en position (i, j) qui vaut

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

On a donc

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

En particulier,

$$(g \otimes h)(g^{-1} \otimes h^{-1}) = I_n \otimes I_k = I_{nk}$$

ce qui montre que

$$g \otimes h \in GL_{nk}(\mathbb{C}) \text{ et } (g \otimes h)^{-1} = g^{-1} \otimes h^{-1}$$

3. (a) Supposons que $\varphi^{-1}(\{\gamma'\})$ soit non vide et notons γ un de ses éléments.
On a alors $h \in \varphi^{-1}(\{\gamma'\}) \iff \varphi(h) = \gamma' = \varphi(\gamma) \iff \varphi(\gamma^{-1}h) = 1 \iff \gamma^{-1}h \in \ker(\varphi)$.
Ainsi

$$\text{Si } \varphi^{-1}(\{\gamma'\}) \neq \emptyset, \exists g \in \Gamma, \varphi^{-1}(\{\gamma'\}) = \gamma \ker(\varphi)$$

- (b) Tous les éléments de l'image de φ ont ainsi $\text{card}(H)$ antécédents. On a ainsi une partition de Γ formée de parties toutes de cardinal $\text{card}(H)$ et en nombre $\text{card}(\text{Im}(\varphi))$ (ce sont les classes d'équivalences dans la relation sur Γ définie par $g_1 \sim g_2 \iff \varphi(g_1) = \varphi(g_2)$).

$$\text{card}(\Gamma) = \text{card}(\varphi(\Gamma))\text{card}(H)$$

4. (a) Montrons par récurrence que

$$(g_1 g_2)^{(s)} = g_1^{(s)} g_2^{(s)}$$

- C'est immédiat pour $s = 1$ (c'est la définition de $g^{(s)}$).
- Supposons le résultat vrai jusqu'au rang $s \geq 1$. On a alors

$$\begin{aligned} (g_1 g_2)^{(s+1)} &= (g_1 g_2)^{(s)} \otimes (g_1 g_2) \\ &= (g_1^{(s)} g_2^{(s)}) \otimes (g_1 g_2) \\ &= (g_1^{(s)} \otimes g_1)(g_2^{(s)} \otimes g_2) \\ &= g_1^{(s+1)} g_2^{(s+1)} \end{aligned}$$

Ceci traduit exactement que

$$\varphi_s \text{ est un morphisme de groupes}$$

Notons φ la restriction de φ_s à G . On a vu que l'on peut regrouper les éléments de G selon la valeur de leur image par φ et que chaque groupe a le même nombre $\text{card}(\ker(\varphi))$ éléments. Ainsi

$$\sum_{g \in G} \varphi(g) = \text{card}(\ker(\varphi)) \sum_{g' \in \varphi(G)} g'$$

En passant à la trace, opération linéaire,

$$\sum_{g \in G} \text{Tr}(g^s) = \text{card}(\ker(\varphi)) \sum_{g' \in \varphi(G)} \text{Tr}(g')$$

Comme $\ker(\varphi) = \ker(\varphi_s) \cap G$, et comme $\text{Tr}(g^s) = \text{Tr}(g)^s$ (récurrence avec 2(i))

$$\sum_{g \in G} \text{Tr}(g)^s = \text{card}(\ker(\varphi_s) \cap G) \sum_{g' \in \varphi_s(G)} \text{Tr}(g')$$

- (b) Comme $\varphi_s(G)$ est un sous-groupe fini de $GL_n(\mathbb{C})$, la question 1 montre que la somme du membre de droite est un entier divisible par $\text{card}(\varphi_s(G))$.

Par ailleurs, la question 3 donne

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

et ainsi

$$\sum_{g \in G} \text{Tr}(g)^s = \frac{\text{card}(G)}{\text{card}(\varphi_s(G))} \sum_{g' \in \varphi_s(G)} \text{Tr}(g')$$

est un multiple de $\text{card}(G)$ (le quotient qui reste à droite est entier avec le premier argument).

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

5. (a) La partie 3 indique que pour $g \in G$, $\text{Tr}(g)$ est égal à n ou à l'un des τ_i pour $1 \leq i \leq n$. Cette trace n'est égal à 1 que si toutes les valeurs propres de g valent 1. En effet, dans ce cas le module de la somme des valeurs propres vaut n et on est dans un cas d'égalité pour l'égalité triangulaire et toutes les valeurs propres valent 1 ou -1 et ce second cas est exclu (la trace vaudrait $-n$).

Avec l'expression factorisée de P , on a donc

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

Ecrivons maintenant P sous forme développée $\alpha_n X^n + \alpha_{n-1} X^{n-1} + \dots + \alpha_0 X$. On a alors

$$\sum_{g \in G} P(\text{Tr}(g)) = \sum_{k=0}^n \left(\alpha_k \sum_{g \in G} \text{Tr}(g)^k \right)$$

Avec la question 4, tous les termes à droite sont multiples de $\text{card}(G)$ quand $k \geq 1$. C'est aussi le cas si $k = 0$. En effet, le terme vaut alors $\alpha_0 \text{card}(G)$ et

$$\alpha_0 = (-1)^a \prod_{i=1}^a \tau_i \in \mathbb{Z}$$

On a donc montré que

$$P(n) \text{ est un multiple de } \text{card}(G)$$

- (b) On a donc p^r diviseur de $P(n) = p^a a!$. En passant aux valuations p -adiques,

$$r \leq a + v_p(a!)$$

6. (a) Avec l'identité des la question 3 des préliminaires,

$$r \leq a + \sum_{i=1}^{\infty} \frac{a}{p^i} = a \left(1 + \frac{1}{p-1} \right) \leq \frac{n}{p-1} \left(\frac{p}{p-1} \right)$$

et ainsi,

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

(b) On a ainsi

$$\text{card}(G) = p^r \leq \exp\left(n \frac{p \ln(p)}{(p-1)^2}\right)$$

L'étude de $x \mapsto x \ln(x) - \ln(4)(x-1)^2$ montre que cette fonction décroît sur $[2, +\infty[$ et comme elle vaut 0 en 2, elle est négative. Ainsi, la quantité dans l'exponentielle ci-dessus est plus petite que $\ln(4)$. On a donc

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