

X-ENS Mathématiques A MP 2021 : un corrigé

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

Jérémy Larochette – Lycée Carnot – Dijon

12 avril 2021

Préliminaires

1. On a $z \in \mathbb{C}$ et $d \in \mathbb{N}$ tel que $z^d = 1$, alors $|z|^d = 1$ et $|z| \in \mathbb{R}^+$ donc $|z| = 1$.
2. On a $g \in \mathbf{GL}_n(\mathbb{C})$ d'ordre $d \in \mathbb{N}^*$, donc $g^d = I_n$ et $X^d - 1$ est un polynôme annulateur, scindé à racines toutes simples (les d racines d^e de l'unité) donc g est diagonalisable et ses valeurs propres sont parmi les racines du polynôme annulateur, donc sont des racines d^e de l'unité.
3. (a) Les multiples de q s'écrivent $k = q\ell$ avec $\ell \in \mathbb{Z}$ uniquement déterminé par k et q , et alors $1 \leq k = q\ell \leq m$ si et seulement si $\frac{1}{q} \leq \ell \leq \frac{m}{q}$ si et seulement si $1 \leq \ell \leq \left\lfloor \frac{m}{q} \right\rfloor$ avec $\ell \in \mathbb{Z}$.

Le nombre de multiples de q entre 1 et m est donc $\left\lfloor \frac{m}{q} \right\rfloor$.

- (b) Ainsi, la valuation q -adique de $m!$ avec q premier s'obtient en ajoutant les valuations q -adiques des entiers entre 1 et m , d'après la question précédente :

- les $\left\lfloor \frac{m}{q} \right\rfloor$ multiples de q fournissent chacun (au moins) un facteur q ,
- les $\left\lfloor \frac{m}{q^2} \right\rfloor$ multiples de q^2 fournissent chacun (au moins) un facteur q supplémentaire,
- les $\left\lfloor \frac{m}{q^3} \right\rfloor$ multiples de q^3 fournissent chacun (au moins) un facteur q supplémentaire,
- et ainsi de suite.

Le décompte s'arrête car la suite entière $\left(\left\lfloor \frac{m}{q^i} \right\rfloor \right)_{i \in \mathbb{N}^*}$ finit par s'annuler et on obtient la formule de Legendre (avec un nombre fini de termes non nuls) :

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

Autre rédaction possible : on peut dénombrer les entiers entre 1 et m ayant une valuation q -adique exactement égale à $i \in \mathbb{N}$: il s'agit des multiples de q^i qui ne sont pas multiples de q^{i+1} et qui sont au nombre de $\left\lfloor \frac{m}{q^i} \right\rfloor - \left\lfloor \frac{m}{q^{i+1}} \right\rfloor$, d'où la formule (les sommes étant toujours faussement infinies)

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

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

1. Soit $g \in \mathbf{GL}_2(\mathbb{Z})$ d'ordre fini d . Alors g est d'ordre d dans $\mathbf{GL}_n(\mathbb{C})$ et d'après les préliminaires, g est \mathbb{C} -diagonalisable et ses valeurs propres sont de module 1. Appelons-les λ et μ (comptées avec multiplicité) et on obtient alors $|\mathrm{Tr}(g)| = |\lambda + \mu| \leq |\lambda| + |\mu|$ donc $|\mathrm{Tr}(g)| \leq 2$.
2. Si les valeurs propres de g sont réelles, comme elles sont de module 1, elles valent 1 ou -1 . L'ordre de g étant celui d'une matrice diagonale à laquelle il est semblable, il suffit de traiter les quatre cas $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ d'ordre 1 et $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ d'ordre 2.

Finalement, si les valeurs propres de g sont réelles, g est d'ordre 1 ou 2.

3. On a $\chi_g = X^2 - \text{Tr}(g)X + \det g$ et toujours g \mathbb{C} -diagonalisable. Les racines sont les valeurs propres, nécessairement complexes conjuguées (car g à coefficients réels) $\lambda, \bar{\lambda}$ de module 1, donc $\det g = |\lambda|^2 = 1$.

De plus, vu la question 1, $\text{Tr } g \in \{0, \pm 1, \pm 2\}$.

Reste à ne garder que les cas où le polynôme caractéristique n'a pas de racine réelle, ce qui élimine $X^2 \pm 2X + 1$, $X^2 \pm X - 1$.

Finalement, $\chi_g \in \{X^2 + 1, X^2 + X + 1, X^2 - X + 1\}$.

4. On reste dans le cas de la question précédente.

- Soit $\chi_g = X^2 + 1$, alors g est semblable à $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ et est d'ordre 4 car $g^4 = I_2$ et $g^2 \neq I_2$.

- Soit $\chi_g = X^2 + X + 1$, alors g est semblable à $\begin{pmatrix} j & 0 \\ 0 & \bar{j} \end{pmatrix}$ et est d'ordre 3 car $g^3 = I_2$ et $g \neq I_2$.

- Soit $\chi_g = X^2 - X + 1$, alors g est semblable à $\begin{pmatrix} \omega & 0 \\ 0 & \bar{\omega} \end{pmatrix}$ avec $\omega = \frac{1 + i\sqrt{3}}{2} = e^{i\frac{\pi}{3}} \in \mathbb{U}_6$ et est d'ordre 6 car $g^6 = I_2$ et $g^3 \neq I_2$.

Remarque : L'ordre de g diagonalisable est le ppcm des ordres de ses valeurs propres.

Finalement, avec le résultat de la question 2, $d \in \{1, 2, 3, 4, 6\}$.

5. Soit $i \in \llbracket 0, n-1 \rrbracket$ et σ_{n-i} la $(n-i)^e$ fonction symétrique élémentaire en les z_k . Alors

$$|\sigma_{n-i}| = \left| \sum_{\substack{I \subset \llbracket 1, n \rrbracket \\ \text{card}(I) = n-i}} \left(\prod_{i \in I} z_i \right) \right| \leq \sum_{\substack{I \subset \llbracket 1, n \rrbracket \\ \text{card}(I) = n-i}} \left(\prod_{i \in I} |z_i| \right) \leq \sum_{\substack{I \subset \llbracket 1, n \rrbracket \\ \text{card}(I) = n-i}} \alpha^{n-i} = \binom{n}{n-i} \alpha^{n-i} = \binom{n}{i} \alpha^{n-i}$$

Le polynôme P étant à coefficients complexes non constant, il est scindé donc les relations coefficients-racines s'appliquent et on a $|a_i| = 1 \times |\sigma_{n-i}|$ (P est unitaire) d'où $|a_i| \leq \binom{n}{i} \alpha^{n-i}$.

6. Si $g \in \mathbf{GL}_n(\mathbb{Z})$ est d'ordre fini, alors ses valeurs propres sont de module 1 d'après les préliminaires, donc, en appliquant la question précédente à χ_g , polynôme unitaire de degré n , $\alpha = 1$ et pour tout $i \in \llbracket 0, n-1 \rrbracket$,

$$|a_i| \leq \binom{n}{i}.$$

Ainsi, $\{\chi_g \text{ tels que } g \in \mathbf{GL}_n(\mathbb{Z}) \text{ est d'ordre fini}\}$ est fini.

7. Comme dans les exemples précédent, l'ordre de $g \in \mathbf{GL}_n(\mathbb{Z})$ est déterminé par l'ordre de ses valeurs propres (c'est leur ppcm) car g est diagonalisable. Comme il y a un nombre fini de polynômes caractéristiques possibles pour $g \in \mathbf{GL}_n(\mathbb{Z})$, on en déduit qu'il y a un nombre fini d'ordres possibles pour $g \in \mathbf{GL}_n(\mathbb{Z})$, à n fixé.

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

1. (a) g étant diagonalisable dans \mathbb{C} d'après les préliminaires, on obtient directement que $A = \frac{1}{m}(g - I_n) \in \mathcal{M}_n(\mathbb{Z})$ l'est

(avec les mêmes matrices de passages) et si λ valeur propre de A , alors $\lambda = \frac{\mu - 1}{m}$ où μ valeur propre de g ,

donc nombre complexe de module 1 d'après les préliminaires, donc $|\lambda| \leq \frac{2}{m} < 1$ car $m > 2$.

(b) En écrivant $A = PDP^{-1}$ où $P \in \mathbf{GL}_n(\mathbb{C})$ et $D = \begin{pmatrix} \lambda_1 & & & (0) \\ & \ddots & & \\ & & \ddots & \\ (0) & & & \lambda_n \end{pmatrix}$, on a pour tout $k \in \mathbb{N}$,

$$A^k = P \begin{pmatrix} \lambda_1^k & & & (0) \\ & \ddots & & \\ & & \ddots & \\ (0) & & & \lambda_n^k \end{pmatrix} P^{-1} \text{ avec pour tout } i, \lambda_i^k \xrightarrow[k \rightarrow +\infty]{} 0 \text{ vu la question précédente. Donc } A^k \rightarrow 0.$$

Or, pour tout $k \in \mathbb{N}$, $A^k \in \mathcal{M}_n(\mathbb{Z})$, donc les suites de coefficients de A^k sont des suites entières convergentes, donc stationnaires et comme il y en a un nombre fini, on a un rang à partir duquel $A^k = 0$.

(c) Mais alors les valeurs propres de A^k , les λ_i^k , sont nulles, on en déduit donc que les valeurs propres de A sont nulles puis que A est nulle et enfin que $g = I_n$.

2. Notons $\overline{M} \in \mathcal{M}_n(\mathbb{Z}/m\mathbb{Z})$ la réduite modulo m de $M \in \mathcal{M}_n(\mathbb{Z})$, et $\phi : M \mapsto \overline{M}$, morphisme d'anneau.

Si $g, h \in G$ tel que $\phi(g) = \phi(h)$, ϕ étant un morphisme d'anneau, $\phi(gh^{-1}) = \phi(g)\phi(h)^{-1} = \overline{I_n} = \phi(I_n)$ d'où $\overline{gh^{-1} - I_n} = \phi(gh^{-1} - I_n) = \overline{0}$ donc m divise tous les coefficients de $gh^{-1} - I_n$.

Comme, de plus, $gh^{-1} \in G$ sous-groupe fini de $\mathbf{GL}_n(\mathbb{Z})$, gh^{-1} est d'ordre fini et la question précédente s'applique : $gh^{-1} = I_n$ donc $g = h$.

Ainsi ϕ induit une application injective de G sur $\mathcal{M}_n(\mathbb{Z}/m\mathbb{Z})$.

3. On en déduit que pour tout $m \geq 3$, $\text{card}(G) \leq \text{card}(\mathcal{M}_n(\mathbb{Z}/m\mathbb{Z})) = m^{n^2}$.

En particulier, pour $m = 3$, $\text{card}(G) \leq 3^{n^2}$.

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

1. (a) On remarque que $k \binom{\ell}{k} = \ell \binom{\ell-1}{k-1}$ donc ℓ divise $k \binom{\ell}{k}$ et comme ℓ est premier et ne divise pas k ,

$$\ell \text{ divise } \binom{\ell}{k}.$$

(Cette formule est hors-programme. On la retrouve soit en repassant par des factorielles, soit en dénombrant les couples (x, A) où $x \in A$ et A partie à k éléments de E de cardinal ℓ de deux manières différentes : en choisissant d'abord x puis $A \setminus \{x\}$ on obtient l'expression de droite, et en choisissant d'abord A puis $x \in A$ on obtient celle de gauche.

On peut aussi s'en passer en remarquant que ℓ divise $k! \binom{\ell}{k}$ et ℓ est premier avec $k!$, en utilisant le lemme de Gauß.)

(b) Soient $xy \in R$ tels que $xy = yx$. Alors la formule du binôme de Newton s'applique : $(x+y)^\ell = \sum_{k=0}^{\ell} \binom{\ell}{k} x^k y^{\ell-k}$.

Alors vu la question précédente et la structure d'anneau de R , pour tout $k \in \llbracket 1, \ell-1 \rrbracket$, $\binom{\ell}{k} x^k y^{\ell-k} \in \ell R$

$$\text{et donc } (x+y)^\ell - (x^\ell + y^\ell) = \sum_{k=1}^{\ell-1} \binom{\ell}{k} x^k y^{\ell-k} \in \ell R.$$

2. A est à coefficients dans R et B est à coefficients dans I . $\det(A+B) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^n (a_{i,\sigma(i)} + b_{i,\sigma(i)})$. En

développant les produits, on obtient une somme dont un terme est $\det A = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^n a_{i,\sigma(i)}$ et dont les

autres termes sont des produits de ± 1 , d'au moins un coefficient de B (appartenant à l'idéal I) et d'autres coefficients de A ou B appartenant à R . Ainsi, tous ces autres termes sont dans l'idéal I et donc, comme I est un sous-groupe additif de R , $\det(A+B) - \det A \in I$.

3. ℓ est un nombre premier et $P \in \mathbb{Z}[X]$. On montrer par récurrence forte sur le degré de P que $P(X^\ell) - P(X)^\ell \in \ell \mathbb{Z}[X]$.

- Le résultat est vrai pour des polynômes constants (éventuellement nul).

- Soit $n \in \mathbb{N}^*$ tel que le résultat soit vrai pour des polynômes de degré au plus $n-1$, et $P = \sum_{k=0}^n a_k X^k \in \mathbb{Z}[X]$

un polynôme de degré n .

Le polynôme $Q = \sum_{k=0}^{n-1} a_k X^k$ est de degré au plus $n-1$.

Alors $P(X^\ell) - P(X)^\ell = a_n X^{\ell n} + Q(X^\ell) - (a_n X^n + Q(X))^\ell$.

Or, d'après la question 1 (l'anneau $\mathbb{Z}[X]$ étant commutatif), on a $T \in \ell \mathbb{Z}[X]$ tel que

$$(a_n X^n + Q(X))^\ell - a_n^\ell X^{\ell n} - Q(X)^\ell = T.$$

Mais alors on a que

$$P(X^\ell) - P(X)^\ell = Q(X^\ell) - Q(X)^\ell + (a_n - a_n^\ell) X^{n\ell} - T$$

avec $Q(X^\ell) - Q(X)^\ell \in \ell\mathbb{Z}[X]$ par hypothèse de récurrence, $T \in \ell\mathbb{Z}[X]$ et $a_n^\ell \equiv a_n \pmod{\ell}$ d'après le petit théorème de Fermat donc $(a_n - a_n^\ell) X^{n\ell} \in \ell\mathbb{Z}[X]$.

Finalement, $P(X^\ell) - P(X)^\ell \in \ell\mathbb{Z}[X]$, ce qui établit la récurrence.

4. (a) On remarque que XI_n et $-M$ sont des éléments commutant de l'anneau $R = \mathcal{M}_n(\mathbb{Z}[X])$, on peut donc appliquer la question 1.(b) qui donne $(XI_n - M)^\ell - (X^\ell I_n + (-1)^\ell M^\ell) \in \ell R$.

Si ℓ est impair, on a bien $A \in \mathcal{M}_n(\mathbb{Z}[X])$ tel que $(XI_n - M)^\ell - (X^\ell I_n - M^\ell) = \ell A$.

Sinon, $\ell = 2$ et $(XI_n - M)^2 - (X^2 I_n - M^2) = \underbrace{(XI_n - M)^2 - (X^2 I_n + M^2)}_{\in 2\mathcal{M}_n(\mathbb{Z}[X])} + \underbrace{2M^2}_{\in 2\mathcal{M}_n(\mathbb{Z}[X])} \in 2\mathcal{M}_n(\mathbb{Z}[X])$

ce qui permet de conclure également.

- (b) $\ell\mathbb{Z}[X]$ étant un idéal de l'anneau commutatif $\mathbb{Z}[X]$, la question 2 nous donne, tous les coefficients de ℓA étant dans cet idéal,

$$\det((X^\ell I_n - M^\ell) + \ell A) - \det(X^\ell I_n - M^\ell) \in \ell\mathbb{Z}[X]$$

c'est-à-dire

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

soit encore

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

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

- (c) On a donc $\chi_{M^\ell}(X) - \chi_M(X)^\ell \in \ell\mathbb{Z}[X]$ et avec la question 3, $\chi_M(X)^\ell - \chi_M(X) \in \ell\mathbb{Z}[X]$.

On a donc $P \in \mathbb{Z}[X]$ tel que $\chi_{M^\ell}(X) = \chi_M(X) + \ell P$.

Alors, en égalant les coefficients de degré $(n-1)\cdot\ell$ et en réduisant modulo ℓ , on tire $\text{Tr}(M^\ell) \equiv \text{Tr}(M) \pmod{\ell}$.

5. Soit $g \in G$. En appliquant la question précédente à $M = g^{p^k} \in \mathcal{M}_n(\mathbb{Z})$ avec $k \in \mathbb{N}$ et au nombre premier $\ell = p$, on tire $\text{Tr}(g^{p^k}) \equiv \text{Tr}(g^{p^{k+1}}) \pmod{p}$. Ainsi, par transitivité, $\text{Tr}(g) \equiv \text{Tr}(g^{p^r}) \pmod{p}$.

Or G est d'ordre p^r donc $g^{p^r} = I_n$. Ainsi, $\text{Tr}(g) \equiv n \pmod{p}$.

6. g et g^ℓ appartenant au groupe fini G , ils sont d'ordre fini. Donc d'après les préliminaires, ils sont diagonalisables dans \mathbb{C} de valeurs propres toutes de module 1. Alors $|\text{Tr}(g)| \leq n$ et $|\text{Tr}(g^\ell)| \leq n$ sur le même principe que 1.1.

Ainsi, $\text{Tr}(g^\ell) - \text{Tr}(g) \in [-n, n] \subset]-\frac{\ell}{2}, \frac{\ell}{2}[$ et $\text{Tr}(g^\ell) \equiv \text{Tr}(g) \pmod{\ell}$ par 4.

Donc $\text{Tr}(g^\ell) = \text{Tr}(g)$.

7. (a) Soit $q \leq 2n$ est un diviseur premier de m . Alors
- soit q divise k , est donc différent de p , et va diviser $m - k$ donc sera l'un des $\ell \leq 2n$ premiers ne divisant pas k , ce qui est contradictoire,
 - soit q ne divise pas k , et, étant l'un des ℓ , divise $m - k$ puis divise $k = m - (m - k)$ ce qui est aussi contradictoire.

C'est donc que tous les facteurs premiers de m sont $> 2n$.

- (b) En itérant la question 6 à tous les diviseurs premier de m (toutes les puissance de g étant encore dans G), on tire alors $\text{Tr}(g^m) = \text{Tr}(g)$.

Mais comme $m \equiv k \pmod{p^r}$ et $g^{p^r} = I_n$, $g^m = g^k$.

Ainsi, $\text{Tr}(g^k) = \text{Tr}(g)$.

8. (a) Soit $k \in \llbracket 1, p^r - 1 \rrbracket$ tel que p ne divise pas k .

Par division euclidienne par p , on a $s, t \in \mathbb{Z}$ tels que $k = ps + t$ et $0 \leq t \leq p - 1$.

Mais comme $p \nmid k$, $t \neq 0$ et comme $0 < k < p^r$, $-p < -t < ps < p^r - t < p^r$ donc $-1 < s < p^{r-1}$ et $s \in \mathbb{Z}$ donc $s \in \llbracket 0, p^{r-1} - 1 \rrbracket$. Ainsi,

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

Réciproquement, si $k \in \bigcup_{s=0}^{p^{r-1}-1} \{ps + t \text{ tels que } 1 \leq t \leq p - 1\}$, alors $k = ps + t$ avec $s \in \llbracket 0, p^{r-1} - 1 \rrbracket$ et $t \in \llbracket 1, p - 1 \rrbracket$ donc p ne divise pas k et $1 = p \cdot 0 + 1 \leq k \leq p(p^{r-1} - 1) + p - 1 = p^r - 1$ donc $k \in J_r$.

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

(b) On prend $\zeta \in \mathbb{C}$ tel que $\zeta^{p^r} = 1$. D'après la question précédente, $\sum_{j \in J_r} \zeta^j = \sum_{s=0}^{p^{r-1}-1} \sum_{t=1}^{p-1} \zeta^{ps+t}$.

• Si $\zeta = 1$, on obtient $\sum_{j \in J_r} 1^j = \sum_{s=0}^{p^{r-1}-1} \sum_{t=1}^{p-1} 1 = p^{r-1}(p-1)$.

• Si ζ est d'ordre p , on obtient $\sum_{j \in J_r} \zeta^j = \sum_{s=0}^{p^{r-1}-1} \sum_{t=1}^{p-1} \zeta^t = \sum_{s=0}^{p^{r-1}-1} \left(\frac{1-1}{1-\zeta} - 1 \right)$ donc $\sum_{j \in J_r} \zeta^j = -p^{r-1}$.

• Sinon, l'ordre de p divisant p^r et p étant premier, $\zeta^p \neq 1$ et, en notant $S = \sum_{t=1}^{p-1} \zeta^t$,

$$\sum_{j \in J_r} \zeta^j = S \times \sum_{s=0}^{p^{r-1}-1} (\zeta^p)^s = S \frac{1 - (\zeta^p)^{p^{r-1}}}{1 - \zeta^p} = S \frac{1 - \zeta^{p^r}}{1 - \zeta^p} = 0$$

donc $\sum_{j \in J_r} \zeta^j = 0$.

9. Notons ζ_1, \dots, ζ_n les valeurs propres de g comptées avec multiplicité. Comme G est de cardinal p^r , elles vérifient toutes $\zeta_i^{p^r} = 1$.

Mais pour tout $k \in J_r$, $\text{Tr}(g^k) = \text{Tr}(g)$ d'après 7., et comme toutes ces matrices sont diagonalisable, on a pour tout $k \in J_r$, $\text{Tr}(g) = \sum_{i=1}^n \zeta_i^k$.

Donc $\text{Tr}(g) = \frac{1}{\text{card}(J_r)} \sum_{j \in J_r} \left(\sum_{i=1}^n \zeta_i^j \right) = \frac{1}{\text{card}(J_r)} \sum_{i=1}^n \left(\sum_{j \in J_r} \zeta_i^j \right)$. Le cas $\zeta = 1$ donne $\text{card}(J_r) = p^{r-1}(p-1)$

et, en distinguant les trois cas de la question précédente, on obtient

$$\text{Tr}(g) = \frac{1}{p^{r-1}(p-1)} (n_0 p^{r-1} (p-1) - n_1 p^{r-1} + (n - n_0 - n_1) \cdot 0)$$

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

10. D'après 5, on a $v \in \mathbb{Z}$ tel que $\text{Tr}(g) = n - pv$.

Comme vu en 6, $\text{Tr}(g) \leq n$ donc $v \geq 0$.

Et avec la question précédente, $n - \text{Tr}(g) = pv = n - n_0 + \frac{n_1}{p-1}$ avec $n_0 \geq 0$ et $n_1 \leq n$, donc $pv \leq n + \frac{n}{p-1} = p \frac{n}{p-1}$ donc $v \leq \frac{n}{p-1}$ et $v \in \mathbb{N}$ donc $v \leq a = \left\lfloor \frac{n}{p-1} \right\rfloor$.

Finalement, $\text{Tr}(g) \in \{n - pv, 0 \leq v \leq a\}$.

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

1. (a) On calcule $f^2 = f \times f = \frac{1}{\text{card}(G)} \sum_{g,h \in G} gh$ mais pour tout $g \in G$, $\begin{matrix} G & \longrightarrow & G \\ h & \longmapsto & h' = gh \end{matrix}$ est une bijection

(translation) de réciproque $\begin{matrix} G & \longrightarrow & G \\ h' & \longmapsto & h = g^{-1}h' \end{matrix}$ donc $f^2 = \frac{1}{\text{card}(G)^2} \sum_{g,h' \in G} h' = \frac{\text{card}(G)}{\text{card}(G)^2} \sum_{h' \in G} h' = f$

donc f est un projecteur sur F son image ou, de manière équivalente, l'espace de ses invariants.

Or si pour tout $g \in G$, $g(x) = x$ alors $f(x) = \frac{1}{\text{card}(G)} \text{card}(G)x = x$ donc $\{x \in \mathbb{C}^n \mid \forall g \in G, g(x) = x\} \subset F$ et, réciproquement, si $x \in F = \text{Im } f$, on a $x' \in \mathbb{C}^n$ tel que $x = f(x') = \frac{1}{\text{card}(G)} \sum_{h \in G} h(x')$ et alors, si $g \in G$,

$$g(x) = \frac{1}{\text{card}(G)} \sum_{h \in G} gh(x') = \frac{1}{\text{card}(G)} \sum_{h' \in G} h'(x') = f(x') = x$$

via la bijection précédente.

Donc f est la projection sur $\{x \in \mathbb{C}^n \mid \forall g \in G, g(x) = x\}$.

(b) Par linéarité de la trace, on tire $\text{card}(G) \cdot \text{Tr}(f) = \sum_{g \in G} \text{Tr}(g)$ et comme f est un projecteur, sa trace est égale

à son rang donc est un entier. Donc $\sum_{g \in G} \text{Tr}(g)$ est un entier multiple de $\text{card}(G)$.

2. (i) Soient $g \in \mathbf{GL}_n(\mathbb{C})$ et $h \in \mathbf{GL}_k(\mathbb{C})$. $\text{Tr}(g \otimes h) = \sum_{i=1}^n \left(\sum_{j=1}^k g_{i,i} h_{j,j} \right) = \sum_{i=1}^n g_{i,i} \sum_{j=1}^k h_{j,j} = \text{Tr}(g) \text{Tr}(h)$.

(ii) Soient $g, g' \in \mathbf{GL}_n(\mathbb{C})$, $h, h' \in \mathbf{GL}_k(\mathbb{C})$, $i, j \in \llbracket 1, n \rrbracket$. On note $[g \otimes h]_{i,j} = g_{i,j} h$ le bloc (i, j) de $g \otimes h$. Alors, par produit par blocs,

$$[(g \otimes h)(g' \otimes h')]_{i,j} = \sum_{\ell=1}^n [g \otimes h]_{i,\ell} [g' \otimes h']_{\ell,j} = \sum_{\ell=1}^n g_{i,\ell} h \times g'_{\ell,j} h' = [gg']_{i,j} hh' = [gg' \otimes hh']_{i,j}$$

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

(iii) Soient $g \in \mathbf{GL}_n(\mathbb{C})$ et $h \in \mathbf{GL}_k(\mathbb{C})$. D'après le calcul précédent, $(g \otimes h)(g^{-1} \otimes h^{-1}) = gg^{-1} \otimes hh^{-1} = I_n \otimes I_k = I_{nk}$ donc $g \otimes h$ est inversible à droite donc inversible soit $g \otimes h \in \mathbf{GL}_{nk}(\mathbb{C})$ et $(g \otimes h)^{-1} = g^{-1} \otimes h^{-1}$.

3. (a) Supposons $\varphi^{-1}(\{\gamma'\})$ non vide et donnons-nous $\gamma \in \varphi^{-1}(\{\gamma'\})$ c'est-à-dire $\gamma \in \Gamma$ tel que $\varphi(\gamma) = \gamma'$. Alors $x \in \varphi^{-1}(\{\gamma'\}) \iff \varphi(x) = \gamma' = \varphi(\gamma) \iff \varphi(x\gamma^{-1}) = e_\Gamma \iff x\gamma^{-1} \in \ker \varphi = H \iff x \in \gamma H$

donc $\varphi^{-1}(\{\gamma'\}) = \emptyset$ ou $\varphi^{-1}(\{\gamma'\}) = \gamma H$, avec $\gamma \in \varphi^{-1}(\{\gamma'\})$ quelconque.

(b) Or les $\varphi^{-1}(\{\gamma'\})$ pour $\gamma' \in \gamma(\Gamma)$ forment une partition de Γ (recouvrement disjoint par des parties non vides) : $\Gamma = \bigsqcup_{\gamma' \in \gamma(\Gamma)} \varphi^{-1}(\{\gamma'\})$ donc $\text{card}(\Gamma) = \sum_{\gamma' \in \gamma(\Gamma)} \text{card}(\varphi^{-1}(\{\gamma'\}))$.

Et, d'après la question précédente, si $\gamma' \in \gamma(\Gamma)$, alors on a $\gamma \in \Gamma$ tel que $\varphi^{-1}(\{\gamma'\}) = \gamma H$, en bijection avec H (avec par exemple la translation $h \in H \mapsto \gamma h$) donc pour tout γ' , $\text{card}(\varphi^{-1}(\{\gamma'\})) = \text{card}(H)$.

Finalement, $\text{card}(\Gamma) = \text{card}(\gamma(\Gamma)) \text{card}(H)$.

4. (a) Soient $g, h \in \mathbf{GL}_n(\mathbb{C})$. on montre par récurrence sur $s \in \mathbb{N}^*$ que $\varphi_s(gh^{-1}) = \varphi_s(g)\varphi_s(h)^{-1}$.

- En effet, pour $s = 1$, cela s'écrit simplement $gh^{-1} = gh^{-1}$.
- Soit $s \geq 1$ pour lequel c'est vrai. Alors, par définition et hypothèse de récurrence,

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

Donc par (ii) et (iii), $\varphi_{s+1}(gh^{-1}) = (\varphi_s(g) \otimes g)(\varphi_s(h) \otimes h)^{-1} = \varphi_{s+1}(g)\varphi_{s+1}(h)^{-1}$ ce qui établit la récurrence : φ_s est un morphisme de groupes.

Puis en notant $\psi_s : G \rightarrow \mathbf{GL}_{n^s}(\mathbb{C})$ le morphisme de groupes induit par φ_s sur G ,

$$\sum_{g \in G} \text{Tr}(g)^s = \sum_{g \in G} \text{Tr}(g^{(s)}) = \sum_{g \in G} \text{Tr}(\psi_s(g))$$

Or comme dans la question précédente, le noyau de ψ_s étant $H = \ker \psi_s = G \cap \ker \varphi_s$, chaque élément de $\psi_s(G) = \varphi_s(G)$ possède exactement $\text{card}(G \cap \ker \varphi_s)$ antécédents dans G , donc

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

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

(b) On applique la question 3 au morphisme de groupe ψ_s directement :

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

ce qui donne avec la question précédente
$$\text{card}(\varphi_s(G)) \sum_{g \in G} \text{Tr}(g)^s = \text{card}(G) \sum_{g' \in \varphi_s(G)} \text{Tr}(g').$$

Or d'après la question 1, le groupe $\varphi_s(G)$ étant fini car G l'est, $\sum_{g' \in \varphi_s(G)} \text{Tr}(g')$ est un entier divisible par

$\text{card}(\varphi_s(G))$: on a donc $p \in \mathbb{Z}$ tel que $\sum_{g' \in \varphi_s(G)} \text{Tr}(g') = \text{card}(\varphi_s(G))p$. Puis, comme $\text{card}(\varphi_s(G)) \neq 0$ car

$G \neq \emptyset$, $\sum_{g \in G} \text{Tr}(g)^s = p \text{card}(G)$ et donc
$$\boxed{\sum_{g \in G} \text{Tr}(g)^s \text{ est un entier divisible par } \text{card}(G) .}$$

5. (a) On a $P \in \mathbb{Z}[X]$.

D'après la question 4, pour tout $s \in \mathbb{N}^*$, $\text{card}(G)$ divise $\sum_{g \in G} \text{Tr}(g)^s$. C'est encore vrai pour $s = 0$ (la

somme vaut alors $\text{card}(G)$). Donc $\text{card}(G)$ divise $\sum_{g \in G} P(\text{Tr}(g))$.

Or, d'après la partie précédente, toute trace d'un élément de g est de la forme $n - pv$ avec $0 \leq v \leq a$.

Si $v \neq 0$, alors $\text{Tr}(g)$ est une racine de P et $P(\text{Tr}(g)) = 0$. Sinon, $P(\text{Tr}(g)) = P(n)$.

Finalement, $\sum_{g \in G} P(\text{Tr}(g)) = P(n) \times k$ où k désigne le nombre d'éléments de g donc la trace vaut n .

Mais en reprenant le raisonnement de la partie précédente, le cas où la trace vaut n n'est atteint que pour $n_0 = n$, c'est-à-dire lorsque 1 est la seule valeur propre (car $\text{Tr}(g) \leq n_0 \leq n$). Donc le seul élément convenant est $g = I_n$ et $k = 1$.

Finalement,
$$\boxed{\text{card}(G) \text{ divise } P(n).}$$

(b) Or $P(n) = \prod_{j=1}^a (n - (n - pj)) = p^a a!$ et $\text{card}(G) = p^r$. On a donc
$$\boxed{v_p(\text{card}(G)) = r \leq v_p(P(n)) = a + v_p(a!).}$$

6. (a) On a $a \leq \frac{n}{p-1}$ et, par les préliminaires, $a + v_p(a!) = a + \sum_{i=1}^{+\infty} \left\lfloor \frac{a}{p^i} \right\rfloor = \sum_{i=0}^{+\infty} \left\lfloor \frac{a}{p^i} \right\rfloor$. Par croissance de la partie

entière, tout étant positif, et la série géométrique étant convergente, $r \leq \sum_{i=0}^{+\infty} \frac{a}{p^i} = \frac{a}{1 - \frac{1}{p}} \leq p \frac{\frac{n}{p-1}}{p-1}$ donc

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

(b) Ainsi, avec $p \geq 2$, $\text{card}(G) = p^r \leq \left(p^{\frac{p}{(p-1)^2}} \right)^n$ avec $p^{\frac{p}{(p-1)^2}} = \exp \frac{p \ln p}{(p-1)^2} = \exp \left[\left(1 + \frac{2}{p-1} + \frac{1}{(p-1)^2} \right) \frac{\ln p}{p} \right]$.

Mais comme $\left(1 + \frac{2}{p-1} + \frac{1}{(p-1)^2} \right)_{p \geq 2}$ est positive et décroissante, $x \mapsto \frac{\ln x}{x}$ se dérive en $x \mapsto \frac{1 - \ln x}{x^2}$

donc $\left(\frac{\ln p}{p} \right)_{p \geq 2}$ décroissante positive puis $\left(\frac{p \ln p}{(p-1)^2} \right)_{p \geq 2}$ décroît et donc $\text{card}(G) \leq \left(2^{\frac{2}{(2-1)^2}} \right)^n$ et donc

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

Fin du corrigé