DM 12 - Matrices à coefficients entiers

1 Généralités et exemples

1. • $\mathcal{M}_n(\mathbb{Z})$ contient la matrice I_n, élément neutre de $\mathcal{M}_n(\mathbb{Q})$;
   • Si $A=(a_{i,j})_{i,j}$ et $B=(b_{i,j})_{i,j}$ sont dans $\mathcal{M}_n(\mathbb{Z})$, alors $A-B=(a_{i,j}-b_{i,j})_{i,j}$ aussi.
   • De même , $AB=\left(\sum_{j=1}^{n} a_{i,j}b_{j,k}\right)_{i,k}$ est dans $\mathcal{M}_n(\mathbb{Z})$.

   Donc $\mathcal{M}_n(\mathbb{Z})$ est un sous-anneau de $\mathcal{M}_n(\mathbb{Q})$.

2. On note $A=\begin{pmatrix}1&1\\0&1\end{pmatrix}$. Elle est inversible d'inverse $\begin{pmatrix}1&-1\\0&1\end{pmatrix}$ donc $A\in \mathrm{GL}_2(\mathbb{Z})$. De plus, pour tout $k\in\mathbb{N}$, $A^k=\begin{pmatrix}1&k\\0&1\end{pmatrix}$ (récurrence immédiate). Donc, les puissances A^k sont deux à deux distinctes dans $\mathrm{GL}_2(\mathbb{Z})$; en particulier $\mathrm{GL}_2(\mathbb{Z})$ est infini.

   On généralise pour $\mathrm{GL}_n(\mathbb{Z})$ en considérant $A=I_n+E_{1,2}$ (matrice de transvection). Alors A est inversible d'inverse $I_n-E_{1,2}$ et pour tout $k\in\mathbb{N}$, $A^k=I_n+kE_{1,2}$.

3. L'égalité $M^m=I_n$ se réécrit $M\times M^{m-1}=M^{m-1}M=I_n$. Donc, si $M^m=I_n$, M est inversible, d'inverse M^{m-1}.

4. L'inclusion $\mathrm{GL}_n(\mathbb{Z})\subset\mathcal{M}_n(\mathbb{Z})$ est vraie par définition. De plus, si $A\in\mathrm{GL}_n(\mathbb{Z})$, il existe $B\in\mathcal{M}_n(\mathbb{Z})$ tel que $AB=BA=I_n$. En particulier, $A,B\in\mathcal{M}_n(\mathbb{Q})$ donc $A\in\mathrm{GL}_n(\mathbb{Q})$. Donc, $\mathrm{GL}_n(\mathbb{Z})\subset\mathrm{GL}_n(\mathbb{Q})\cap\mathcal{M}_n(\mathbb{Z})$.

   La matrice $A=2I_n$ est dans $\mathrm{GL}_n(\mathbb{Q})\cap\mathcal{M}_n(\mathbb{Z})$ (son inverse est $\frac{1}{2}I_n$). Comme l'inverse de A n'est pas dans $\mathcal{M}_n(\mathbb{Z})$, $A\notin\mathrm{GL}_n(\mathbb{Z})$.

5. On suppose $A=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\mathcal{M}_2(\mathbb{Z})$. Si $\det A=ad-bc=\pm1$, on sait que A est inversible (dans $\mathrm{GL}_n(\mathbb{Q})$) et que $A^{-1}=\frac{1}{ad-bc}\begin{pmatrix}d&-b\\-c&a\end{pmatrix}=\pm\begin{pmatrix}d&-b\\-c&a\end{pmatrix}$. Donc, si $\det A=\pm1$, $A\in\mathrm{GL}_2(\mathbb{Z})$.

   Réciproquement, si $A\in\mathrm{GL}_2(\mathbb{Z})$, on a $\det A\in\mathbb{Z}$ et $\det A^{-1}\in\mathbb{Z}$. Or $\det A^{-1}=\frac{d}{ad-bc}\frac{a}{ad-bc}-\frac{-c}{ad-bc}\frac{-b}{ad-bc}=\frac{ad-bc}{(ad-bc)^2}=\frac{1}{\det A}$. Donc $\det A$ est un entier, dont l'inverse est entier. Donc $\det A=\pm1$.

   Remarque : plus généralement, si $A,B\in\mathcal{M}_2(\mathbb{Z})$, $\det(AB)=\det(A)\det(B)$. On généralisera...

6. **Matrices de permutation.**

(a) Comme P_σ est une matrice avec uniquement des coefficients 0 et 1, elle appartient à $\mathcal{M}_n(\mathbb{Z})$. Pour montrer que $P_\sigma \in \mathrm{GL}_n(\mathbb{Z})$, il suffit de montrer que $P_\sigma P_{\sigma^{-1}} = P_{\sigma^{-1}} P_\sigma = I_n$. Cela résulte de l'égalité : $\forall \sigma, \tau \in \mathcal{S}_n, P_{\sigma\circ\tau} = P_\sigma P_\tau$, montrée à la question suivante.

(b) Montrons que $\forall \sigma, \tau \in \mathcal{S}_n, P_{\sigma\circ\tau} = P_\sigma P_\tau$. Soient $\sigma, \tau \in \mathcal{S}_n$. Soient $i, k \in [\![1, n]\!]$. On calcule :

$$\begin{aligned}[P_\sigma P_\tau]_{i,k} &= \sum_{j=1}^{n} [P_\sigma]_{i,j}[P_\tau]_{j,k} \\ &= \sum_{j=1}^{n} \delta_{i,\sigma(j)}\delta_{j,\tau(k)} \\ &= \delta_{i,\sigma(\tau(k))}.\end{aligned}$$

Donc, $\forall i, k \in [\![1, n]\!]$, $[P_\sigma P_\tau]_{i,k} = [P_{\sigma\circ\tau}]_{i,k}$. Donc $P_\sigma P_\tau = P_{\sigma\circ\tau}$. En prenant $\tau = \sigma^{-1}$, cela montre que P_σ est inversible d'inverse $P_{\sigma^{-1}}$ (laissé en suspens à la question précédente), donc $P_\sigma \in \mathrm{GL}_n(\mathbb{Z})$. Donc, $\Psi : \mathcal{S}_n \to \mathrm{GL}_n(\mathbb{Z})$ est un morphisme de groupes.
Pour montrer que Ψ est injective, on étudie son noyau. Si une permutation $\sigma \in \mathcal{S}_n$ est dans $\mathrm{Ker}\,\Psi$, alors $P_\sigma = I_n$, donc $\forall i, j \in [\![1, n]\!]$, $\delta_{i,\sigma(j)} = \delta_{i,j}$. En prenant $i = j$, on obtient que $\forall j \in [\![1, n]\!]$, $\delta_{j,\sigma(j)} = 1$, c'est-à-dire $\sigma(j) = j$. Donc $\sigma = \mathrm{id}_{[\![1,n]\!]}$. Donc $\mathrm{Ker}\,\Psi = \{\mathrm{id}_{[\![1,n]\!]}\}$, donc Ψ est injective.

7. **Groupe diédral D_{12}.**

(a) Soit $f \in D_{12}$. Les images $f(1)$ et $f(\alpha)$ doivent être des sommets de H tels que $|f(\alpha) - f(1)| = |\alpha - 1|$. Cette quantité est la longueur d'un côté de H ; il est clair géométriquement que les diagonales de H sont strictement plus grandes que la longueur d'un côté (et on peut le montrer en calculant la longueur des diagonales) ; donc $f(\alpha)$ et $f(1)$ sont des sommets consécutifs.
On a aussi $|f(\alpha^2) - f(\alpha)| = |\alpha^2 - \alpha| = 1 - \alpha$. Donc, $f(\alpha)$ et $f(\alpha^2)$ sont aussi des sommets consécutifs de H. Par injectivité, on doit aussi avoir $f(1) \neq f(\alpha^2)$, donc $f(\alpha^2)$ est nécessairement l'unique sommet adjacent à $f(\alpha)$, qui n'est pas $f(1)$.
En réitérant le raisonnement avec α^3, α^4 et α^5, on en déduit que f est entièrement déterminée par les images de $f(1)$ et $f(\alpha)$.

(b) D'après ce qui précède, il y a au maximum 12 choix pour un élément f de D_{12} : d'abord 6 choix pour l'image $f(1)$, puis 2 choix pour l'image $f(\alpha)$, qui doit être un des deux sommets consécutifs de $f(1)$.
De plus, on connait dans D_{12} les 12 éléments suivants : les 6 rotations de centre 0 et d'angle $\dfrac{2k\pi}{6}$, pour $k \in [\![0, 5]\!]$; les 3 symétries axiales d'axe joignant deux sommets oppposés ; les 3 symétries axiales d'axe joignant les milieux de deux côtés opposés.
Donc, D_{12} est de cardinal 12.

(c) On calcule rapidement que :

- $1 = 1 + 0\alpha$;
- $\alpha = 0 + \alpha$;
- $\alpha^2 = -1 + \alpha$;
- $\alpha^3 = - + 0\alpha$;
- $\alpha^4 = 0 - \alpha$;
- $\alpha^5 = 1 - \alpha$.

(d) Soit $h \in H$. On a $h = a_h 1 + b_h \alpha$. Notons r la permutation de H définie par $r(\alpha^k) = \alpha^{k+1}$. Alors,

$$r(h) = \alpha h = \alpha(a_h 1 + b_h \alpha) = a_h \alpha + b_h \alpha^2 = a_h r(1) + b_h r(\alpha).$$

Notons s la permutation de H définie par $s(\alpha^k) = \alpha^{-k}$. Alors,

$$s(h) = \bar{h} = \overline{a_h 1 + b_h \alpha} = a_h 1 + b_h \alpha^{-1} = a_h s(1) + b_h s(\alpha).$$

(*car a_h et b_h sont entiers, donc réels.*)

On montre aisément que l'ensemble des $f \in D_{12}$ qui vérifient $\forall h \in H, f(h) = a_h f(1) + b_h f(\alpha)$ est un sous-groupe de D_{12}. Comme il contient r et s et que $\langle r, s\rangle = D_{12}$, on en déduit que l'égalité est vraie pour tout $f \in D_{12}$.

(e) Comme pour tout $h \in H, a_h, b_h \in \mathbb{Z}$, Φ est bien définie comme application à valeurs dans $\mathscr{M}_2(\mathbb{Z})$. Montrons que pour tout $f, g \in D_{12}$, $\Phi(g \circ f) = \Phi(g)\Phi(f)$, ce qui montrera à la fois que Φ est à valeurs dans $\mathrm{GL}_2(\mathbb{Z})$ (en prenant $g = f^{-1}$) et que Φ est un morphisme de groupes.

Soient $f, g \in D_{12}$. On a

$$g \circ f(1) = g(\alpha_{f(1)} 1 + \beta_{f(1)} \alpha) = \alpha_{f(1)} g(1) + \beta_{f(1)} g(\alpha),$$

d'après la question précédente. Comme $g(1) = \alpha_{g(1)} 1 + \beta_{g(1)} \alpha$ et que $g(\alpha) = \alpha_{g(\alpha)} 1 + \beta_{g(\alpha)} \alpha$, on obtient :

$$g \circ f(1) = \big(\alpha_{f(1)} \alpha_{g(1)} + \beta_{f(1)} \alpha_{g(\alpha)}\big) 1 + \big(\alpha_{f(1)} \beta_{g(1)} + \beta_{f(1)} \beta_{g(\alpha)}\big) \alpha.$$

Par un calcul analogue, on trouve que :

$$g \circ f(\alpha) = \big(\alpha_{f(\alpha)} \alpha_{g(1)} + \beta_{f(\alpha)} \alpha_{g(\alpha)}\big) 1 + \big(\alpha_{f(\alpha)} \beta_{g(1)} + \beta_{f(\alpha)} \beta_{g(\alpha)}\big) \alpha.$$

Donc $\Phi(g \circ f) = \begin{pmatrix} \alpha_{f(1)} \alpha_{g(1)} + \beta_{f(1)} \alpha_{g(\alpha)} & \alpha_{f(\alpha)} \alpha_{g(1)} + \beta_{f(\alpha)} \alpha_{g(\alpha)} \\ \alpha_{f(1)} \beta_{g(1)} + \beta_{f(1)} \beta_{g(\alpha)} & \alpha_{f(\alpha)} \beta_{g(1)} + \beta_{f(\alpha)} \beta_{g(\alpha)} \end{pmatrix}$. Donc,

$$\Phi(g \circ f) = \begin{pmatrix} \alpha_{g(1)} & \alpha_{g(\alpha)} \\ \beta_{g(1)} & \beta_{g(\alpha)} \end{pmatrix} \begin{pmatrix} \alpha_{f(1)} & \alpha_{f(\alpha)} \\ \beta_{f(1)} & \beta_{f(\alpha)} \end{pmatrix} = \Phi(g)\Phi(f).$$

Pour montrer l'injectivité de Φ, on considère $f \in \operatorname{Ker} \Phi$. On a donc $\begin{pmatrix} \alpha_{f(1)} & \alpha_{f(\alpha)} \\ \beta_{f(1)} & \beta_{f(\alpha)} \end{pmatrix} = I_2$, ce qui revient à dire que $f(1) = 1$ et que $f(\alpha) = \alpha$. Au vu de la description des éléments de D_{12}, ceci implique que $f = \mathrm{id}_H$.

2 Ordre des éléments de $\mathrm{GL}_2(\mathbb{Z})$

1. Notons $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. On a donc $\operatorname{Tr} A = a + d$ et $\det A = ad - bc$. On calcule :

$$\begin{aligned} \chi_A(A) &= A^2 - (\operatorname{Tr} A) A + (\det A) I_2 \\ &= \begin{pmatrix} a^2 + bc & ab + bd \\ ac + cd & bc + d^2 \end{pmatrix} - (a + d) \begin{pmatrix} a & b \\ c & d \end{pmatrix} + (ad - bc) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ \chi_A(A) &= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}. \end{aligned}$$

2. Il existe $V \in \mathscr{M}_{2,1}(\mathbb{C}) - \{0\}$ tel que $AV = \lambda V$ ssi il existe $V \in \mathscr{M}_{2,1}(\mathbb{C}) - \{0\}$ tel que $(A - \lambda I_2)V = 0$ ssi $(A - \lambda I_2)$ est non inversible.
C'est équivalent à $\det(A - \lambda I_2) = 0$. Or,

$$\det(A - \lambda I_2) = (a - \lambda)(d - \lambda) - bc = \lambda^2 - (a + d)\lambda + ad - bc = \chi_A(\lambda).$$

Donc λ est racine de χ_A ssi il existe $V \in \mathscr{M}_{2,1}(\mathbb{C}) - \{0\}$ tel que $AV = \lambda V$.
On considère donc un tel V. On a $AV = \lambda V$, donc par récurrence immédiate : $A^k V = \lambda^k V$, pour tout $k \in \mathbb{N}$. En particulier, pour $k = m$: $V = A^m V = \lambda^m V$. Comme V est non nul, ceci implique $\lambda^m = 1$.

3. La trace de A est un entier car $A \in \mathscr{M}_2(\mathbb{Z})$. De plus, comme $\chi_A = X^2 - (\operatorname{Tr} A)X + \det A$, $\operatorname{Tr} A$ est la somme des deux racines (éventuellement confondues, éventuellement complexes) de χ_A. Or, la question précédente, montre qu'une racine de χ_A est une racine de l'unité, donc de module 1. En notant λ_1, λ_2 les racines de χ_A, on a donc :

$$|\operatorname{Tr}(A)| = |\lambda_1 + \lambda_2| \leq |\lambda_1| + |\lambda_2| = 2.$$

Donc $\operatorname{Tr} A \in [\![-2, 2]\!]$.

4. Comme $A \in \mathrm{GL}_2(\mathbb{Z})$, on sait que $\det A = \pm 1$. De plus, on vient de montrer que $\operatorname{Tr} A \in [\![-2, 2]\!]$. On distingue maintenant selon le nombre de racines réelles de χ_A.

   - Si χ_A a une racine réelle double, celle-ci est 1 ou -1 d'aprs la question précédente. Et alors $\chi_A = P_1$ ou P_2.
   - Si χ_A a deux racines réelles distinctes, ce sont nécessairement -1 et 1 et $\chi_A = P_3$.
   - Si χ_A n'a pas de racines réelles, ses racines sont complexes conjuguées. Notons-les λ et $\bar{\lambda}$. Alors $|\operatorname{Tr} A| = |\lambda + \bar{\lambda}| < |\lambda| + |\bar{\lambda}| = 2$ donc $\operatorname{Tr} A = \pm 1$ et $\det A = \lambda\bar{\lambda} = 1$. Donc $\chi_A = P_4$, P_5 ou P_6.

5. On pose :

   - $A_1 = I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$;
   - $A_2 = -I_2$;
   - $A_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$;
   - $A_4 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$;
   - $A_5 = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$;
   - $A_6 = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$.

   En calculant trace et déterminant, on constate que pour chaque $i \in [\![1, 6]\!]$, $\chi_{A_i} = P_i$. Et chaque $A_i \in \mathscr{M}_2(\mathbb{Z})$. Il suffit donc de montrer que chacun des A_i est d'ordre fini. Des calculs rapides montrent que l'ordre de A_1 est 1 ; l'ordre de A_2 et A_3 est 2 ; l'ordre de A_4 est 4 ; l'ordre de A_5 est 6 et l'ordre de A_6 est 3.

6. Soit $A \in \mathrm{GL}_2(\mathbb{Z})$ une matrice d'ordre fini, noté m. On a donc $A^m = I_2$. De plus, on sait que $\chi_A(A) = 0$ et on sait que χ_A est l'un des 6 polynômes énumérés précédemment. On raisonne selon la valeur de χ_A :

   - Si $\chi_A = P_1$, on a $(A - I)^2 = 0$. Or,

   $$A^m = ((A - I) + I)^m = \sum_{k=0}^{m} \binom{m}{k} (A - I)^k = I + m(A - I).$$

   On en déduit donc, comme $m \geq 1$, que $A - I = 0$, donc $A = I_2$ et A est d'ordre 1.

- De même, si $\chi_A = P_2$, on montre que $A = -I_2$.
- Si $\chi_A = P_3$, on a $A^2 - I_2 = 0$, donc A est d'ordre fini divisant 2 (en fait 2).
- Si $\chi_A = P_4$, on a $A^2 + I_2 = 0$. Donc $A^4 - I_2 = (A^2 + I_2)(A^2 - I_2) = 0$. Donc A est d'ordre fini divisant 4 (en fait 4).
- Si $\chi_A = P_5$, on montre que $A^6 = I_2$. En effet,

  $$X^6 - 1 = (X^2 - 1)(X^4 + X^2 + 1) = (X^2 - 1)(X^2 - X + 1)(X^2 + X + 1).$$

  Donc, comme $\chi_A(A) = 0$ et que $X^6 - 1$ est factorisable par χ_A, $A^6 - I_2 = 0$. Donc A est d'ordre fini divisant 6 (en fait 6).
- Si $\chi_A = P_6$, on a de même (en plus simple) :

  $$A^3 - I_2 = (A - I_2)(A^2 + A + I_2) = 0,$$

  donc $A^3 = I_2$ et A est d'ordre fini divisant 3 (en fait 3).

Remarque : il y a une différence de traitement entre les deux premiers cas et les autres. Pour les 4 derniers cas, il suffit de connaître χ_A pour montrer que A est d'ordre fini. Pour les deux premiers, ce n'est pas suffisant puisque I_2 et $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ ont le même polynôme caractéristique, mais que les deux matrices ont respectivement un ordre égal à 1 et à l'infini. Ceci sera plus clair l'an prochain, avec l'étude de la réduction des endomorphismes.

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

1. (a) On note r le minimum des valuations p-adiques des coefficients de $M - I_n$ (comme $M \neq I_n$, $M - I_n$ a au moins un coefficient non nul et donc r est fini). Par hypothèse, $r \geq 1$. On note $N = p^{-r}(M - I_n)$. On a $N \in \mathcal{M}_n(\mathbb{Z})$ (car tout coefficient de $M - I_n$ est divisible par p^r) et $N \notin p\mathcal{M}_n(\mathbb{Z})$ (car au moins un coefficient de $M - I_n$ n'est pas divisible par p^{r+1}). Donc r et N conviennent.

   (b) On a $M^m = I_n$ donc

   $$I_n = (I_n + p^r N)^m = \sum_{k=0}^{m} \binom{m}{k} p^{rk} N^k.$$

   (car I_n et $p^r N$ commutent)

   Donc, $mp^r N = -\sum_{k=2}^{m} \binom{m}{k} p^{rk} N^k = -p^{2r} \sum_{k=2}^{m} \binom{m}{k} p^{r(k-2)} N^k$. Donc $mp^r N \in p^{2r}\mathcal{M}_n(\mathbb{Z})$.

   En divisant par p^r, on a donc $mN \in p^r \mathcal{M}_n(\mathbb{Z})$. Comme $N \notin p\mathcal{M}_n(\mathbb{Z})$, un des coefficients de N n'est pas divisible par p, donc est premier avec p. Comme m fois ce coefficient est divisible par p^r, p^r divise m. En particulier, p divise m.

(c) $(M')^k = I_n \iff M^{pk} = I_n \iff m \mid pk \iff m' \mid k$. Donc M' est d'ordre m'. On calcule :

$$\begin{aligned} M' &= M^p \\ &= (I_n + p^r N)^p \\ &= \sum_{k=0}^{p} \binom{p}{k} p^{rk} N^k \\ &= I_n + p^{r+1} N + \sum_{k=2}^{p} \binom{p}{k} p^{rk} N^k \\ &= I_n + p^{r+1} \left(N + \sum_{k=2}^{p} \binom{p}{k} p^{r(k-1)-1} N^k \right). \end{aligned}$$

On pose $N' = N + \sum_{k=2}^{p} \binom{p}{k} p^{r(k-1)-1} N^k$. Pour $k \in [\![2, p-1]\!]$, p divise $\binom{p}{k}$. Pour $k = p$, on a $r(p-1) - 1 \geq 2r - 1 \geq 1$ car p est supposé ≥ 3. Donc, p divise tous les coefficients des matrices dans la somme. Donc, les coefficients de N' sont congrus à ceux de N modulo p. En particulier, $N' \in \mathcal{M}_n(\mathbb{Z}) - p\mathcal{M}_n(\mathbb{Z})$ et $M' = I_n + p^{r+1} N'$.

(d) M' vérifie les mêmes hypothèses que M ($M' \neq I_n$ d'après la conclusion de la question précédente), donc le même raisonnement donne $p \mid m'$, c'est-à-dire $p^2 \mid m$. En réitérant, on obtient que $p^k \mid m$, pour tout $k \in \mathbb{N}$. Comme m est supposé ≥ 1, c'est absurde.
Donc $M - I_n \notin p\mathcal{M}_n(\mathbb{Z})$.

2. On a $\phi(I_n) = I_n$, où I_n désigne à gauche la matrice identité de $\mathcal{M}_n(\mathbb{Z})$ et à droite celle de $\mathcal{M}_n(\mathbb{Z}/p\mathbb{Z})$.

Soient $M, N \in \mathcal{M}_n(\mathbb{Z})$. On a :

$$\phi(M+N) = \overline{M+N} = (\overline{m_{i,j} + n_{i,j}})_{i,j} = (\overline{m_{i,j}}_{i,j} + \overline{n_{i,j}})_{i,j} = \overline{M} + \overline{N} = \phi(M) + \phi(N).$$

Soient $i, k \in [\![1, n]\!]$. On a :

$$\phi(MN)_{i,k} = \overline{MN}_{i,k} = \sum_{j=1}^{n} \overline{m_{i,j} n_{j,k}} = \sum_{j=1}^{n} \overline{m_{i,j}} \times \overline{n_{j,k}} = \left(\overline{M} \times \overline{N}\right)_{i,k} = [\phi(M)\phi(N)]_{i,k}.$$

Donc $\phi(MN) = \phi(M)\phi(N)$. Donc ϕ est un morphisme d'anneaux.

Comme tout morphisme d'anneaux, ϕ induit un isomorphisme du groupe des inversibles de l'anneau de départ, vers le groupe des inversibles de l'anneau à l'arrivée ; donc de $\mathrm{GL}_n(\mathbb{Z})$ dans $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$.

3. Soit G un sous-groupe fini de $\mathrm{GL}_n(\mathbb{Z})$. Alors, $\phi_{|G} : G \to \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ est un morphisme de groupes, par restriction. Soit $M \in G$ tel que $M \in \mathrm{Ker}\,\phi$. Alors $\overline{M} = I_n$ (matrice identité à coefficients dans $\mathbb{Z}/p\mathbb{Z}$). Cela revient à dire que $M - I_n \in p\mathcal{M}_n(\mathbb{Z})$. Or, comme M est élément d'un groupe fini, son ordre est fini. D'après la question 1., seule $M = I_n$ vérifie alors $M - I_n \in p\mathcal{M}_n(\mathbb{Z})$. Donc, $\mathrm{Ker}\,\phi_{|G} = \{I_n\}$, donc ϕ est injective.

Ainsi, G est en bijection avec $\phi(G) \in \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z}) \subset \mathcal{M}_n(\mathbb{Z}/p\mathbb{Z})$. Comme $|\mathcal{M}_n(\mathbb{Z}/p\mathbb{Z})| = p^{n^2}$, on a $|G| \leq p^{n^2}$. En particulier, $|G| \leq 3^{n^2}$.

4. On commence par compter le nombre de produits xy égaux à $\bar{0}$, $\bar{1}$ et $\bar{2}$, avec $x, y \in \mathbb{Z}/3\mathbb{Z}$. Il y a 9 produits xy ; 5 valent $\bar{0}$ (dès que x ou y est nul), 2 valent $\bar{1}$ ($\bar{1}\times\bar{1}$ et $\bar{2}\times\bar{2}$) et 2 valent $\bar{2}$ ($\bar{1}\times\bar{2}$ et $\bar{2}\times\bar{1}$).

   Soit alors $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathscr{M}_2(\mathbb{Z}/3\mathbb{Z})$. M est inversible ssi $\det M \neq \bar{0}$ ssi $ad \neq bc$. Avec le comptage fait ci-dessus et le principe de soustraction, on compte

$$3^4 - 5^2 - 2^2 - 2^2 = 48$$

   telles matrices. Donc $|\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})| = 48$.
   D'après la question précédente, il existe un morphisme injectif ϕ de G dans $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$. Alors, $|G| = |\phi(G)|$ et par le théorème de Lagrange, $|\phi(G)|$ divise $|\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})| = 48$.

5. On calcule $A^2 = \begin{pmatrix} \bar{1} & \bar{1} \\ \bar{1} & \bar{2} \end{pmatrix}$, puis $A^4 = (A^2)^2 = \begin{pmatrix} \bar{2} & \bar{0} \\ \bar{0} & \bar{2} \end{pmatrix}$ et finalement $A^8 = (A^4)^2 = I_2$. La dernière égalité montre que l'ordre de A divise 8, comme A, A^2 et A^4 sont différentes de I_2, cet ordre est exactement 8.

   Considérons maintenant $B \in \mathrm{GL}_2(\mathbb{Z})$ d'ordre fini. D'après l'exercice précédent, B est d'ordre 1, 2, 3, 4 ou 6. Donc $\phi_3(B)^k = I_2$, pour un $k \in \{1,2,3,4,6\}$. Donc, l'ordre de $\phi_3(B) \in \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ est un diviseur d'un élément dans $\{1,2,3,4,6\}$, donc est un élément de $\{1,2,3,4,6\}$. En particulier, $\phi_3(B)$ n'est pas d'ordre 8.

   Ainsi, la matrice A ne peut pas être dans l'image $\phi_3(G)$, si G est un sous-groupe fini de $\mathrm{GL}_2(\mathbb{Z})$. Donc, $\phi_3(G)$ est un sous-groupe strict de $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$. Donc $|G| = |\phi_3(G)|$ est un diviseur strict de 48.