Première composition de mathématiques
ENS 2006 – MP

Notations et conventions

Soit G un groupe et soit S une partie de G. On appelle sous-groupe de G engendré par S l'intersection de tous les sous-groupes de G contenant S. On dit que S engendre G si le sous-groupe de G engendré par S est G.
Un élément g de G est *d'ordre fini* si le sous-groupe de G engendré par $\{g\}$ est fini. On appelle alors *ordre* de g le cardinal de ce sous-groupe. Si G est fini, le cardinal de tout sous-groupe de G divise le cardinal de G ; en particulier, tout élément de G est d'ordre fini et son ordre divise le cardinal de G.
Dans tout le problème, n est un entier naturel non nul. Soit $\mathbf{K}$ un corps ; on note

— $\mathcal{M}_n(\mathbf{K})$ la $\mathbf{K}$-algèbre des matrices carrées à n lignes à coefficients dans $\mathbf{K}$;

— $\mathrm{GL}_n(\mathbf{K})$ le groupe des éléments inversibles de $\mathcal{M}_n(\mathbf{K})$;

— I_n l'élément neutre de $\mathrm{GL}_n(\mathbf{K})$, c'est-à-dire la matrice identité de taille n ;

— $\mathrm{SL}_n(\mathbf{K})$ le groupe de $\mathrm{GL}_n(\mathbf{K})$ formé des matrices de déterminant 1 ;

— $\mathrm{SL}_n(\mathbf{Z})$ l'ensemble des matrices de $\mathrm{SL}_n(\mathbf{Q})$ à coefficients dans $\mathbf{Z}$.

Pour tous éléments distincts i et j de $\{1, \ldots, n\}$, on note $E_{i,j}$ l'élément de $\mathcal{M}_n(\mathbf{Q})$ dont tous les coefficients sont nuls, sauf celui de la i-ième ligne et de la j-ième colonne, qui vaut 1. On note $M_{i,j} = I_n + E_{i,j}$; c'est un élément de $\mathrm{SL}_n(\mathbf{Z})$.

PARTIE I - Le groupe $\mathrm{SL}_n(\mathbf{Z})$

1) Montrer que $\mathrm{SL}_n(\mathbf{Z})$ est un sous-groupe de $\mathrm{SL}_n(\mathbf{Q})$ (on pourra utiliser l'expression de l'inverse d'une matrice en fonction de sa comatrice).

2) Pour tous éléments distincts i et j de $\{1, \ldots, n\}$ et tout entier *relatif* m, calculer $(M_{i,j})^m$.

3) Soit M une matrice à n colonnes, non nécessairement carrée, à coefficients dans $\mathbf{Z}$. On appelle *opération élémentaire restreinte sur les colonnes de* M la multiplication à droite de M par une matrice $(M_{i,j})^m$, où $m \in \mathbf{Z}$ et où i et j sont des éléments distincts de $\{1, \ldots, n\}$. Comment s'expriment les colonnes de la matrice $M(M_{i,j})^m$ en fonction de celles de M ?

4) On suppose $n \geq 2$. Soit a_1, …, a_n des entiers relatifs. Montrer que l'on peut, par des opérations élémentaires restreintes sur les colonnes, transformer la matrice ligne $\begin{pmatrix} a_1 & a_2 & \cdots & a_n \end{pmatrix}$ en la matrice ligne $\begin{pmatrix} d & 0 & \cdots & 0 \end{pmatrix}$ où d est le pgcd positif de a_1, a_2, …, a_n.

5) Montrer que l'ensemble des matrices $M_{i,j}$, pour i et j distincts dans $\{1, \ldots, n\}$ engendre le groupe $\mathrm{SL}_n(\mathbf{Z})$.

6) Soit p un nombre premier, de sorte que $\mathbf{Z}/p\mathbf{Z}$ est un corps.

   a. Montrer que la réduction modulo p des coefficients d'une matrice permet de définir un morphisme de groupes
   $$\varphi_{n,p} \ : \mathrm{SL}_n(\mathbf{Z}) \to \mathrm{SL}_n(\mathbf{Z}/p\mathbf{Z}) \ .$$

   b. Montrer que $\varphi_{n,p}$ est surjectif (on pourra utiliser la question 4 et raisonner par récurrence sur n).

PARTIE II - Sous-groupes finis de $\mathrm{SL}_n(\mathbf{Z})$

7) Soit G un sous-groupe fini de $\mathrm{GL}_n(\mathbf{R})$.

a. Montrer que tout élément M de G est diagonalisable sur $\mathbf{C}$ et qu'on a

$$\mathrm{Tr}(M) = \mathrm{Tr}(M^{-1}) \quad \text{et} \quad |\mathrm{Tr}(M)| \leq n \ .$$

Quels sont les éléments de G de trace n ? Quels sont ceux de trace $-n$?

b. Soit U la matrice définie par

$$U = \sum_{M \in G} {}^{\mathrm{t}}MM \ .$$

Montrer que l'application $(X, Y) \mapsto {}^{\mathrm{t}}XUY$ définit un produit scalaire sur $\mathbf{R}^n$.

c. On munit $\mathbf{R}^n$ de ce produit scalaire. Montrer que les endomorphismes de $\mathbf{R}^n$ dont la matrice dans la base canonique est un élément de G sont orthogonaux pour ce produit scalaire.

8) Soit G un sous-groupe fini de $\mathrm{SL}_2(\mathbf{Z})$.

a. Montrer que le groupe G est cyclique (on pourra utiliser la question 7.c)).

b. Montrer que le cardinal de G est 1, 2, 3, 4 ou 6.

c. Déterminer tous les éléments de $\mathrm{SL}_2(\mathbf{Z})$ d'ordre 2.

d. Caractériser les éléments de $\mathrm{SL}_2(\mathbf{Z})$ d'ordre 3, puis 4, puis 6, à l'aide de leur trace.

e. Pour chaque g dans $\{1, 2, 3, 4, 6\}$, donner un exemple de sous-groupe de $\mathrm{SL}_2(\mathbf{Z})$ de cardinal g.

9) Soit M un élément de $\mathrm{SL}_3(\mathbf{Z})$ d'ordre fini. Déterminer les valeurs possibles de sa trace et déterminer l'ordre M en fonction de celle-ci.

10) Considérons des matrices carrées, à coefficients dans un corps $\mathbf{K}$, dont les lignes et les colonnes sont indexées par un ensemble fini I pas nécessairement ordonné. Si $M = (a_{i,j})_{i,j \in I}$ et $N = (b_{i,j})_{i,j \in I}$ sont de telles matrices, on définit la trace de M comme $\sum_{i \in I} a_{i,i}$, la somme $M + N$ comme la matrice $(a_{i,j} + b_{i,j})_{i,j \in I}$ et le produit MN comme la matrice $(c_{i,j})_{i,j \in I}$ où

$$c_{i,j} = \sum_{k \in I} a_{i,k} b_{k,j} \ .$$

On définit ainsi une $\mathbf{K}$-algèbre ; on notera $\mathcal{M}_I(\mathbf{K})$ cette algèbre et $\mathrm{GL}_I(\mathbf{K})$ le groupe de ses éléments inversibles. Si I est de cardinal n, le choix d'une bijection entre I et $\{1, \dots, n\}$ induit un isomorphisme de $\mathbf{K}$-algèbres entre $\mathcal{M}_I(\mathbf{K})$ et $\mathcal{M}_n(\mathbf{K})$. On identifiera en particulier $\mathrm{GL}_{\{1,\dots,n\}}(\mathbf{K})$ et $\mathrm{GL}_n(\mathbf{K})$.
Soit I et I' des ensembles finis, M et M' des éléments respectivement de $\mathcal{M}_I(\mathbf{R})$ et $\mathcal{M}_{I'}(\mathbf{R})$. On définit un élément $M \star M'$ de $\mathcal{M}_{I \times I'}(\mathbf{R})$ en posant $M = (a_{i,j})_{i,j \in I}$, $M' = (b_{i',j'})_{i',j' \in I'}$ et $M \star M' = (c_{(i,i'),(j,j')})_{(i,i'),(j,j') \in I \times I'}$ avec

$$c_{(i,i'),(j,j')} = a_{i,j} b_{i',j'} \ .$$

Enfin, pour tout entier r strictement positif, on définit un élément $M^{\star r}$ de $\mathcal{M}_{I^r}(\mathbf{R})$ par récurrence sur r en posant $M^{\star 1} = M$ et $M^{\star r} = M^{\star r-1} \star M$.

a. Calculer la trace de $M \star M'$ en fonction de celles de M et M'.

b. Soit N et N' des éléments respectivement de $\mathcal{M}_I(\mathbf{R})$ et $\mathcal{M}_{I'}(\mathbf{R})$. Exprimer la matrice $(MN)\star(M'N')$ en fonction des matrices $M\star M'$ et $N\star N'$.

c. Soit r un entier strictement positif. Montrer qu'en associant à M la matrice $M^{\star r}$, on définit un morphisme de groupes

$$\psi_r \ : \mathrm{GL}_I(\mathbf{R}) \to \mathrm{GL}_{I^r}(\mathbf{R}) \ .$$

11) Soit G un sous-groupe fini de $\mathrm{GL}_n(\mathbf{R})$ de cardinal g. On pose

$$S = \sum_{M\in G} M \ .$$

a. Montrer que la trace de S est un entier divisible par g (on pourra calculer S^2).

b. Soit r un entier strictement positif. Décrire le noyau de la restriction à G du morphisme de groupes

$$\psi_r \ : \mathrm{GL}_n(\mathbf{R}) \to \mathrm{GL}_{\{1,\ldots,n\}^r}(\mathbf{R})$$

défini à la question 10.c) (on pourra étudier la trace des éléments de ce noyau).

c. Montrer que pour tout entier naturel r, la somme $\displaystyle\sum_{M\in G}\mathrm{Tr}(M)^r$ est un entier divisible par g.

12) Soit G un sous-groupe fini de $\mathrm{SL}_n(\mathbf{Z})$ de cardinal g.

a. Soit $\{t_0, t_1, \ldots, t_s\}$ l'ensemble des traces (distinctes) des éléments de G, avec $t_0 = n = \mathrm{Tr}(I_n)$. Montrer que

$$(n-t_1)\cdots(n-t_s)$$

est un entier divisible par g (on pourra poser $P = (X-t_1)\cdots(X-t_s)$ et considérer la somme $\displaystyle\sum_{M\in G} P(\mathrm{Tr}(M))$).

b. En déduire que g divise $(2n)!$ et que si n est impair, g divise $(2n-1)!$.

c. Si $n=3$, montrer que g divise 24 (on pourra utiliser la question 9).

13) a. Construire pour chaque entier n supérieur ou égal à 2 un sous-groupe de $\mathrm{SL}_n(\mathbf{Z})$ de cardinal $2^{n-1}n!$ (si T est l'ensemble des vecteurs colonnes à n lignes dont tous les coefficients sont nuls sauf un qui vaut ± 1, on pourra considérer les matrices qui appliquent l'ensemble T dans lui-même).

b. En déduire le cardinal maximal d'un sous-groupe fini de $\mathrm{SL}_3(\mathbf{Z})$.

14) Soit p un nombre premier et soit M un élément de $\mathrm{SL}_n(\mathbf{Z})$ d'ordre p. On note m le pgcd positif de tous les coefficients de $M - I_n$.

a. Montrer que m divise p (on pourra écrire $M = I_n + mN$ et développer $(I_n+mN)^p$).

b. Montrer qu'on a soit $m=1$, soit $m=p=2$.

15) Soit G un sous-groupe fini de $\mathrm{SL}_n(\mathbf{Z})$ de cardinal g.

a. Montrer que la restriction à G du morphisme de groupes $\varphi_{n,3} : \mathrm{SL}_n(\mathbf{Z}) \to \mathrm{SL}_n(\mathbf{Z}/3\mathbf{Z})$ défini dans la question 6.a) est injective.

b. En déduire que g divise $\dfrac{1}{2}(3^n-1)(3^n-3)\cdots(3^n-3^{n-1})$.

c. Si $n=4$, montrer que g divise 5760.

16) Montrer que tout groupe fini de cardinal g est isomorphe à un sous-groupe de $\mathrm{SL}_g(\mathbf{Z})$.

PARTIE III - Morphismes de groupes et $\mathrm{SL}_n(\mathbf{Z})$

17) Montrer qu'il existe un morphisme de groupes surjectif

$$\mathrm{SL}_2(\mathbf{Z}) \to \mathbf{Z}/2\mathbf{Z}$$

(on pourra montrer que $\mathrm{SL}_2(\mathbf{Z}/2\mathbf{Z})$ est isomorphe à un groupe de permutations).

18) On suppose dans cette question $n \geq 3$.

a. Soit i, j et k des éléments deux à deux distincts de $\{1, \ldots, n\}$. Calculer le produit

$$M_{i,j} M_{j,k} (M_{i,j})^{-1} (M_{j,k})^{-1} .$$

b. Soit G un groupe commutatif. Montrer que tout morphisme de groupes $\mathrm{SL}_n(\mathbf{Z}) \to G$ est constant.

19) Soit G un groupe engendré par une partie finie et soit H un groupe fini.

a. Montrer qu'il y a un nombre fini de morphismes de groupes de G dans H.

b. Soit $u : G \to G$ un morphisme de groupes surjectif. Montrer que pour tout morphisme de groupes $v : G \to H$, on a $\mathrm{Ker}(u) \subset \mathrm{Ker}(v)$.

20) En déduire que tout morphisme de groupes surjectif $\mathrm{SL}_n(\mathbf{Z}) \to \mathrm{SL}_n(\mathbf{Z})$ est bijectif.

PREMIÈRE COMPOSITION DE MATHÉMATIQUES – ENS 2006 – MP

PARTIE I - Le groupe $\mathrm{SL}_n(\mathbf{Z})$

1) Puisque $\mathbf{Z}$ est inclus dans $\mathbf{Q}$, $\mathrm{SL}_n(\mathbf{Z})$ est inclus dans $\mathrm{SL}_n(\mathbf{Q})$. Puisque l'identité est à coefficients entiers et est de déterminant 1, I_n appartient à $\mathrm{SL}_n(\mathbf{Z})$, qui n'est donc pas vide. Soit P et Q dans $\mathrm{SL}_n(\mathbf{Z})$. Comme ce sont des éléments de $\mathrm{SL}_n(\mathbf{Q})$, P^{-1} et PQ sont dans $\mathrm{SL}_n(\mathbf{Q})$, et donc appartiennent à $\mathrm{SL}_n(\mathbf{Z})$ si et seulement s'ils sont à coefficients entiers.

   Puisque le déterminant et le produit matriciel sont des expressions polynomiales à coefficients entiers en fonction des termes des matrices considérées, PQ est à coefficients entiers et le déterminant et donc aussi les cofacteurs de P sont des entiers. Il en résulte que la comatrice de P est à coefficients entiers. Comme $\det(P) = 1$, la transposée de la comatrice de P est également son inverse et donc les coefficients de P^{-1} sont entiers. Par caractérisation des sous-groupes, on en déduit que $\boxed{\mathrm{SL}_n(\mathbf{Z}) \text{ est un sous-groupe de } \mathrm{SL}_n(\mathbf{Q}).}$

2) Soit i et j deux éléments distincts de $\{1, \ldots, n\}$. La matrice $E_{i,j}$ est alors nilpotente d'ordre 2 et donc, $(I_n - E_{i,j})(I_n + E_{i,j}) = I_n$, i.e. $M_{i,j}^{-1}$ existe et vaut $I_n - E_{i,j}$. Puisque l'identité commute avec toute matrice, on peut appliquer la formule du binôme de Newton et, en tenant compte de la nilpotence d'ordre 2, il vient, pour tout entier relatif m, $\boxed{(M_{i,j})^m = I_n + mE_{i,j}.}$

3) D'après la formule précédente, et puisqu'on a affaire à une opération élémentaire sur les colonnes d'une matrice au sens habituel dans $\mathrm{SL}_n(\mathbf{R})$,

   les colonnes de $M(M_{i,j})^m$ sont celles de M à l'exception de la j-ième à laquelle on a additionné m fois la i-ième colonne de M.

4) On note M la matrice ligne $\begin{pmatrix} a_1 & \ldots & a_n \end{pmatrix}$. Soit i et j deux éléments distincts de $\{1, \ldots, n\}$ avec $0 < |a_i| \leq |a_j|$. D'après ce qui précède, on peut, par des opérations élémentaires restreintes sur les colonnes, transformer a_j en $a_j \pm a_i$ et en particulier choisir le signe de sorte que ce terme soit de valeur absolue égale à $|a_j| - |a_i|$, et donc faire décroître la somme des valeurs absolues des coefficients de M. Puisque cette somme est un entier positif, on ne peut le faire décroître strictement indéfiniment, i.e. on peut, par des opérations élémentaires restreintes sur les colonnes, transformer M en une matrice dont au plus un terme est non nul. Quitte à multiplier par $M_{i,1}M_{1,i}^{-1}$, on peut supposer que tous les termes, sauf peut-être le premier, sont nuls. Puisqu'on a $n \geq 2$, quitte à multiplier par $M_{1,2}^{-1}M_{2,1}^{2}M_{2,1}^{-1}$, on peut supposer que le premier terme est positif.

   Par ailleurs une opération élémentaire restreinte sur les colonnes ne modifie pas le pgcd des coefficients d'une matrice ligne, puisque l'idéal de $\mathbf{Z}$ engendré par ces coefficients est le même. On en déduit que l'on peut, par des opérations élémentaires restreintes sur les colonnes, transformer la matrice ligne $\begin{pmatrix} a_1 & a_2 & \ldots & a_n \end{pmatrix}$ en la matrice ligne

   $\boxed{\begin{pmatrix} d & 0 & \ldots & 0 \end{pmatrix} \text{ où } d \text{ est le pgcd positif de } a_1, a_2, \ldots, a_n.}$

5) Pour i et j des entiers distincts dans $[\![1, n]\!]$, $M_{i,j}$ appartient à $\mathrm{SL}_n(\mathbf{Z})$, ainsi qu'il est affirmé dans le préambule, puisqu'il s'agit d'une matrice triangulaire de diagonale identiquement égale à 1, à coefficients égaux à 0 ou 1. Le groupe G que ces matrices engendrent contient donc tout produit de ces matrices, élevées à des puissances relatives, ainsi que les inverses de ses éléments. Il en résulte que si l'on peut, par des opérations élémentaires restreintes sur les colonnes, transformer M en l'identité, alors on dispose de A dans G tel que $MA = I_n$ et donc

$M = A^{-1}$, et M appartient à G. On remarque enfin que G est inclus dans $\mathrm{SL}_n(\mathbf{Z})$ puisque ce dernier est un groupe contenant toutes les matrices $M_{i,j}$.

Soit M dans $\mathrm{SL}_n(\mathbf{Z})$. On note $\begin{pmatrix} a_1 & a_2 & \cdots & a_n \end{pmatrix}$ sa première ligne. D'après ce qui précède on dispose de A dans G tel que $\begin{pmatrix} a_1 & a_2 & \cdots & a_n \end{pmatrix} A = \begin{pmatrix} d & 0 & \cdots & 0 \end{pmatrix}$, où d est le pgcd positif de a_1, a_2, …, a_n. La matrice MA est alors triangulaire par blocs et son déterminant est donc un multiple entier de d. Puisqu'on a affaire à des matrices de $\mathrm{SL}_n(\mathbf{Z})$, puisque $G \subset \mathrm{SL}_n(\mathbf{Z})$, il en résulte que d divise 1, puis $d = 1$ par positivité.

Par récurrence immédiate sur k dans $[\![2, n]\!]$, en travaillant sur les colonnes de k à n, on en déduit qu'on peut, par des opérations élémentaires restreintes sur les colonnes, transformer M en une matrice triangulaire inférieure de diagonale identiquement égale à 1.

En multipliant à droite par des matrices de la forme $M_{n,i}^a$, on peut transformer la matrice précédente en une matrice de même type ayant une dernière ligne formée de 0 à l'exception du terme diagonal. Encore une fois par récurrence immédiate descendante sur k dans $[\![2, n]\!]$, on peut transformer cette matrice en une matrice dont les $n+1-k$ dernières lignes sont formées de 0 à l'exception des termes diagonaux. Pour $k = 2$, finalement, on obtient que l'on peut transformer M en l'identité. Par conséquent l'ensemble des matrices $M_{i,j}$, pour i et j distincts dans $\{1, \ldots, n\}$, $\boxed{\text{engendre le groupe } \mathrm{SL}_n(\mathbf{Z}).}$

6) a. Puisque le déterminant est une fonction polynomiale à coefficients entiers des termes d'une matrice, le morphisme canonique φ_p de $\mathbf{Z}$ dans $\mathbf{Z}/p\mathbf{Z}$ induit une application $\Phi_{n,p}$ de $\mathcal{M}_n(\mathbf{Z})$ dans $\mathcal{M}_n(\mathbf{Z}/p\mathbf{Z})$ compatible au déterminant, i.e. $\overline{\det(M)} = \det(\Phi_{n,p}(M))$ pour tout M dans $\mathcal{M}_n(\mathbf{Z})$. En particulier, φ_p induit aussi une application $\varphi_{n,p}$ de $\mathrm{SL}_n(\mathbf{Z})$ dans $\mathrm{SL}_n(\mathbf{Z}/p\mathbf{Z})$. Comme le produit matriciel est une fonction polynomiale à coefficients entiers des termes des matrices, il est également compatible au morphisme canonique précédent, i.e. $\boxed{\varphi_{n,p} \text{ est un morphisme de groupes.}}$

b. Soit $(\mathbf{H}_k)$ le prédicat sur k dans $\mathbf{N}^*$: $\varphi_{k,p}$ est surjectif. Pour $k = 1$, les groupes SL_n sont réduits à leurs éléments neutres et donc $(\mathbf{H}_1)$ est vrai.

Par définition le morphisme canonique φ_p est surjectif et donc $\Phi_{k,p}$ l'est aussi pour tout entier strictement positif k puisqu'on a affaire à des produits cartésiens.

Soit maintenant k dans $\mathbf{N}^*$ tel que $(\mathbf{H}_k)$ soit vrai et A dans $\mathrm{SL}_{k+1}(\mathbf{Z}/p\mathbf{Z})$. Soit alors M dans $\mathcal{M}_{k+1}(\mathbf{Z})$ un antécédent de A par $\Phi_{k+1,p}$. D'après la question précèdente, on a donc $\overline{\det(M)} = \det(A)$ et donc $\det(M) \equiv 1 \pmod p$.

On reprend les notations des questions 4) et 5). On dispose alors d'un élément g de G tel que Mg soit triangulaire, en relaxant la condition $d = 1$ sur chaque ligne. Comme $\det(g) = 1$, on a donc $\det(Mg) = \det(M) \equiv 1 \pmod p$ et donc tous les éléments diagonaux de Mg sont inversibles modulo p et leur produit est égal à 1 modulo p. On note d le premier terme de la diagonale de Mg. Comme d est inversible modulo p, par relation de Bézout, on dispose de u et v dans $\mathbf{Z}$ tels que $du - pv = 1$. On considère alors la matrice diagonale par blocs h donnée par (en convenant qu'il n'y a pas de bloc inférieur si $k = 1$)

$$h = \left(\begin{array}{cc|c} u & p & \\ v & d & \\ \hline & & I_{k-1} \end{array}\right)$$

de sorte que h est à coefficients entiers et de déterminant 1, i.e. $h \in \mathrm{SL}_n(\mathbf{Z})$. Comme, de plus, $\Phi_{k+1,p}(h)$ est une matrice triangulaire inférieure, on en déduit que $\Phi_{k+1,p}(Mgh)$ aussi. De plus son premier terme diagonal est du, i.e. est congru à 1 modulo p. On décompose alors Mgh par blocs de taille 1 et k

$$Mgh = \left(\begin{array}{c|c} du & X \\ \hline Y & N \end{array}\right)$$

et, comme $\Phi_{k+1,p}(Mgh)$ est triangulaire inférieure avec 1 comme premier terme diagonal, $\Phi_{k,p}(N) \in \mathrm{SL}_k(\mathbf{Z}/p\mathbf{Z})$. Par hypothèse de récurrence, on dispose de M' dans $\mathrm{SL}_n(\mathbf{Z}/p\mathbf{Z})$ tel que $\varphi_{k,p}(M') = N$. Soit alors la matrice diagonale par blocs k donnée par

$$k = \left(\begin{array}{c|c} 1 & \\ \hline & M' \end{array}\right) .$$

Alors k est à coefficients entiers et de déterminant 1, donc appartient à $\mathrm{SL}_{k+1}(\mathbf{Z})$. De plus $\Phi_{k+1,p}(Mghk^{-1})$ est triangulaire inférieure avec une diagonale identiquement égale à 1. Il en résulte que $\Phi_{k+1,p}(Mghk^{-1})$ appartient à l'image de $\varphi_{k+1,p}$ puisqu'un antécédent peut être choisi triangulaire inférieur à diagonale identiquement égal à 1, dans $\mathcal{M}_n(\mathbf{Z})$ et donc aussi dans $\mathrm{SL}_n(\mathbf{Z})$. Soit f un tel antécédent. On a donc $\Phi_{k+1,p}(Mghk^{-1}) = \Phi_{k+1,p}(f)$ et donc aussi $A = \Phi_{k+1,p}(M) = \Phi_{k+1,p}(fkh^{-1}g^{-1})$ et, comme $fkh^{-1}g^{-1}$ est dans $\mathrm{SL}_n(\mathbf{Z})$ en tant que produit d'éléments et d'inverses de tels éléments, il vient $A = \varphi_{k+1,p}(fkh^{-1}g^{-1})$. Par conséquent $\varphi_{k+1,p}$ est surjectif.

Le principe de récurrence permet de conclure que $\boxed{\varphi_{n,p} \text{ est surjectif.}}$

PARTIE II - Sous-groupes finis de $\mathrm{SL}_n(\mathbf{Z})$

7) a. Soit M dans G. D'après le théorème de Lagrange, M est annulé par le polynôme $X^{|G|} - 1$, qui est simplement scindé sur $\mathbf{C}$. Il en résulte que $\boxed{M \text{ est diagonalisable sur } \mathbf{C}.}$

Soit D diagonale telle que $D^{|G|} - 1$, alors les éléments diagonaux de D sont ses valeurs propres, donc des racines de l'unité, et donc $D^{-1} = \overline{D}$. Soit alors P dans $\mathrm{GL}_n(\mathbf{C})$ tel que $P^{-1}MP$ soit diagonal. Il vient $P^{-1}M^{-1}P = \overline{P^{-1}MP}$ et donc, puisque la trace est invariante par conjugaison et compatible à la conjugaison complexe,

$$\mathrm{Tr}(M^{-1}) = \mathrm{Tr}(P^{-1}M^{-1}P) = \mathrm{Tr}(\overline{P^{-1}MP}) = \overline{\mathrm{Tr}(P^{-1}MP)} = \overline{\mathrm{Tr}(M)} = \mathrm{Tr}(M)$$

puisque M est réel, i.e. $\boxed{\mathrm{Tr}(M) = \mathrm{Tr}(M^{-1}).}$

De plus comme la diagonale de $P^{-1}MP$ est formée d'éléments de module 1, par inégalité triangulaire, il vient $\boxed{|\mathrm{Tr}(M)| \leq n.}$

Le cas d'égalité dans l'inégalité triangulaire correspondant au cas où tous les nombres sont positivement liés, puisqu'ils sont tous de même module, il vient D scalaire, et donc aussi M. Par conséquent $\boxed{\text{le seul élément de } G \text{ de trace } n \text{ est } I_n.}$

De plus $\boxed{G \text{ contient au plus un élément de trace } -n, \text{ à savoir } -I_n.}$

b. Soit M dans G et X dans $\mathbf{R}^n$. La matrice ${}^{\mathrm{t}}MM$ est alors symétrique réelle. On a ${}^{\mathrm{t}}X\,{}^{\mathrm{t}}MMX = \|MX\|^2$. D'après la question précédente, le spectre de M ne contient pas 0, et donc M est inversible. Il en résulte que $(X,Y) \mapsto {}^{\mathrm{t}}X\,{}^{\mathrm{t}}MMY$ est un produit scalaire sur $\mathbf{R}^n$. Une somme de produits scalaires en étant un aussi $\boxed{(X,Y) \mapsto {}^{\mathrm{t}}XUY \text{ définit un produit scalaire sur } \mathbf{R}^n.}$

c. On note $\langle \cdot \mid \cdot \rangle$ le produit scalaire précédent. Soit N dans G, x dans $\mathbf{R}^n$ et X la matrice colonne associée à x dans la base canonique. Soit enfin f l'endomorphisme de $\mathbf{R}^n$ dont la matrice dans la base canonique est N. On a

$$\langle x \mid x \rangle = {}^{\mathrm{t}}XUX \quad \text{et} \quad \langle f(x) \mid f(x) \rangle = {}^{\mathrm{t}}X\,{}^{\mathrm{t}}NUNX \ .$$

Puisque G est un groupe, l'application $M \mapsto MN$ est une bijection de G sur lui-même, d'inverse donné par $M \mapsto MN^{-1}$. Il vient alors

$${}^{\mathrm{t}}NUN = \sum_{M \in G} {}^{\mathrm{t}}N\,{}^{\mathrm{t}}MMN = \sum_{M \in G} {}^{\mathrm{t}}(MN)MN = \sum_{M \in G} {}^{\mathrm{t}}MM = U$$

et donc

$${}^{\mathrm{t}}X\,{}^{\mathrm{t}}NUNX = {}^{\mathrm{t}}XUX\,,$$

i.e. $\boxed{f \text{ est un endomorphisme orthogonal pour ce produit scalaire.}}$

8) a. Soit (e) une base orthonormée de $\mathbf{R}^2$ pour le produit scalaire de la question 7.b). Soit M dans G et f l'endomorphisme dont la matrice dans la base canonique est M. Alors la matrice de f dans (e) est orthogonale, d'après ce qui précède, et donc si P est la matrice de passage de la base canonique à la base (e), $P^{-1}MP$ appartient à $\mathcal{O}_2(\mathbf{R})$. Comme M est de déterminant 1, il en va de même pour ses conjugués, et donc l'automorphisme intérieur de $\mathrm{GL}_2(\mathbf{R})$ associé à P est un isomorphisme entre G et un sous-groupe fini du groupe commutatif $\mathcal{SO}_2(\mathbf{R})$, lui-même isomorphe à $\mathbf{U}$, groupe des unités complexes. À tout sous-groupe fini G de $\mathrm{SL}_2(\mathbf{Z})$ et toute matrice de passage P de la base canonique à une matrice orthogonale pour le produit scalaire associé à G dans la question précédente, on peut donc associer une application $\varphi_{G,P}$ déterminée par

$$G \xhookrightarrow{i_P} \mathcal{SO}_2(\mathbf{R}) \xrightarrow{\sim} \mathbf{U}$$

où i_P désigne l'automorphisme intérieur $M \mapsto P^{-1}MP$. D'après le théorème de Lagrange, on en déduit que G est isomorphe à un sous-groupe du groupe cyclique des racines $|G|$-ièmes de l'unité. Comme ce dernier est de cardinal $|G|$, $\varphi_{G,P}$ induit un isomorphisme entre G et $\mathbf{U}_{|G|}$, groupe des racines $|G|$-ièmes de l'unité, et en particulier $\boxed{G \text{ est cyclique.}}$

b. On reprend les notations précédentes en fixant P. Comme la trace est invariante par conjugaison et que la trace d'une rotation d'angle θ est $2\cos(\theta)$, on a, pour tout M dans G, $\mathrm{Tr}(M) = 2\,\mathrm{Re}(\varphi_{G,P}(M))$.

Soit M un générateur de G. Sa trace est entière et comprise entre -2 et 2, d'après 7.a), et donc $\mathrm{Re}(\varphi_{G,P}(M))$ appartient à $\left\{-1, -\dfrac{1}{2}, 0, \dfrac{1}{2}, 1\right\}$. On en déduit que $\varphi_{G,P}(M)$ appartient à $\{-1, j, j^2, \pm i, -j, -j^2, 1\}$ où j est une racine primitive troisième de l'unité. Comme l'ordre de G est celui de M qui est celui de $\varphi_{G,P}(M)$, $\boxed{\text{le cardinal de } G \text{ est 1, 2, 3, 4 ou 6.}}$

Remarque : on peut raisonner directement. Le polynôme caractéristique de M est unitaire, de terme constant égal à 1 (le déterminant de M) et est donc déterminé par sa trace. En notant Φ_k le polynôme cyclotomique d'indice k, χ_M fait partie donc partie des cinq polynômes suivants : $(X-1)^2$, X^2-X+1, X^2+1, X^2+X+1 et $(X+1)^2$, i.e. Φ_1^2, Φ_6, Φ_4, Φ_3 ou Φ_2^2. Il en résulte que les racines de l'unité qui sont racines d'un de ces polynômes sont les racines d'ordre 1, 2, 3, 4 ou 6.

c. Soit M dans $\mathrm{SL}_2(\mathbf{Z})$ d'ordre 2. On note G le groupe engendré par M, qui est donc un sous-groupe fini d'ordre 2 de $\mathrm{SL}_2(\mathbf{Z})$. D'après ce qui précède la trace de M est donc égale à -2 et son polynôme caractéristique est donc $(X+1)^2$. Comme M est diagonalisable, son polynôme minimal est $X+1$, i.e. $M=-I_2$. Comme $-I_2$ est effectivement d'ordre 2, $\boxed{\text{le seul élément de } \mathrm{SL}_2(\mathbf{Z}) \text{ d'ordre 2 est } -I_2.}$

d. Soit M un élément d'ordre fini de $\mathrm{SL}_2(\mathbf{Z})$ d'ordre supérieur à 3. On considère le groupe cyclique G engendré par M. D'après l'étude faite en 8.b), l'ordre de M est caractérisé par sa trace, qui appartient alors à $\{-1,0,1\}$.

Réciproquement si la trace de M appartient à $\{-1,0,1\}$, alors le polynôme caractéristique de M fait partie de X^2+X+1, X^2+1 ou X^2-X+1 et donc M est annulé par un diviseur de X^3-1, X^4-1 ou X^6-1 respectivement. Ces trois polynômes sont simplement scindés sur $\mathbf{C}$ avec comme racines des racines de l'unité, donc M est diagonalisable sur $\mathbf{C}$ et ses valeurs propres sont des racines de l'unité, et en particulier M est d'ordre fini. Au final, parmi les éléments de $\mathrm{SL}_2(\mathbf{Z})$

$\boxed{\text{ceux d'ordre 3 sont ceux de trace } -1\text{, ceux d'ordre 4 sont ceux de trace nulle, ceux d'ordre 6 sont ceux de trace 1.}}$

e. Pour $g=1$, $G=\{I_2\}$ convient. Pour $g=2$, $G=\{\pm I_2\}$ convient. Pour $g\geq 3$, on peut prendre pour M la matrice compagnon associée à son polynôme minimal (qui est aussi son polynôme caractéristique). D'où les sous-groupes d'ordres 1, 2, 3, 4 et 6 respectivement

$$\boxed{\{I_2\},\quad \{\pm I_2\},\quad \left\{\begin{pmatrix}0&1\\-1&-1\end{pmatrix}^k \,\middle|\, 0\leq k\leq 2\right\},\quad \left\{\begin{pmatrix}0&1\\-1&0\end{pmatrix}^k \,\middle|\, 0\leq k\leq 3\right\} \quad\text{et}\quad \left\{\begin{pmatrix}0&1\\-1&1\end{pmatrix}^k \,\middle|\, 0\leq k\leq 5\right\}.}$$

9) Soit M un élément de $\mathrm{SL}_3(\mathbf{Z})$ d'ordre fini et G le groupe cyclique qu'il engendre. On reprend l'étude de la question 8 : on note (e) une base orthonormée de $\mathbf{R}^3$ pour le produit scalaire défini à la question 7.b) et P la matrice de passage de la base canonique à la base (e). Alors $P^{-1}MP$ appartient à $\mathcal{SO}_3(\mathbf{R})$ et admet donc un vecteur propre unitaire X pour la valeur propre 1. Soit alors Q la matrice de passage de (e) à une base orthonormée ayant X comme premier vecteur. Alors $(PQ)^{-1}MPQ$ appartient à $\mathcal{SO}_3(\mathbf{R})$ et se décompose par blocs avec un bloc de taille 1 égal à 1 et un bloc U de taille 2 dans $\mathcal{SO}_2(\mathbf{R})$, et ce dernier bloc caractérise M. On obtient à nouveau un isomorphisme entre G et un sous-groupe de $\mathbf{U}$, tel qu'on ait $\mathrm{Tr}(M)=\mathrm{Tr}((PQ)^{-1}MPQ)=1+\mathrm{Tr}(U)=1+2\,\mathrm{Re}(u)$, si u est le nombre complexe associé à M par cet isomorphisme. De plus l'ordre de M est celui de u dans $\mathbf{U}$.

Comme la trace de M est entière et que u est de module 1, il vient $\boxed{\mathrm{Tr}(M) \in [\![-1, 3]\!]}$ et, comme en question 8.b), u appartient à $\{-1, j, j^2, \pm i, -j, -j^2, 1\}$ et donc M est d'ordre 1, 2, 3, 4 ou 6. Réciproquement on peut construire des matrices ayant cet ordre en choisissant une matrice par bloc avec un 1 et un bloc comme construit en 8.e). On en conclut que $\boxed{\text{l'ordre de } M \text{ est 1, 2, 3, 4 ou 6 selon que } \mathrm{Tr}(M) \text{ vaut } 3,\ -1,\ 0,\ 1 \text{ ou } 2.}$

10) a. On a

$$\mathrm{Tr}(M \star M') = \sum_{(i,i') \in I \times I'} a_{(i,i)} b_{(i',i')} = \left(\sum_{i \in I} a_{(i,i)}\right)\left(\sum_{i' \in I'} b_{(i',i')}\right)$$

et donc $\boxed{\mathrm{Tr}(M \star M') = \mathrm{Tr}(M)\,\mathrm{Tr}(M').}$

b. On pose $N = (c_{i,j})_{i,j \in I}$ et $N' = (d_{i',j'})_{i',j' \in I'}$. Pour $(i,j) \times (i',j')$ dans $I^2 \times (I')^2$, il vient

$$\sum_{(k,k') \in I \times I'} \left(a_{(i,k)} b_{(i',k')}\right)\left(c_{(k,j)} d_{(k',j')}\right) = \left(\sum_{k \in I} a_{(i,k)} c_{(k,j)}\right)\left(\sum_{k' \in I'} b_{(i',k')} d_{(k',j')}\right)$$

et donc $\boxed{(MN) \star (M'N') = (M \star M') \cdot (N \star N').}$

c. L'élément neutre de $\mathrm{GL}_I(\mathbf{R})$ pour la multiplication est la matrice ayant des 1 sur la diagonale, i.e. $a_{i,i} = 1$ pour tout i dans I, et des 0 ailleurs. Par définition on en déduit que son image par ψ_r est l'élément neutre de $\mathrm{GL}_{I^r}(\mathbf{R})$.

Par ailleurs, par récurrence immédiate et en utilisant ce qui précède, on a $(MN)^{\star r} = M^{\star r} \cdot N^{\star r}$. En particulier si M appartient à $\mathrm{GL}_I(\mathbf{R})$ on a $(MM^{-1})^{\star r} = M^{\star r} \cdot (M^{-1})^{\star r}$ et donc ψ_r est à valeurs dans $\mathrm{GL}_{I^r}(\mathbf{R})$. La formule précédente montre alors que

$\boxed{\psi_r \text{ est un morphisme de groupes de } \mathrm{GL}_I(\mathbf{R}) \text{ dans } \mathrm{GL}_{I^r}(\mathbf{R}).}$

11) a. Puisque, pour tout M dans G, la multiplication à gauche par M est une bijection de G sur lui-même, d'inverse donné par la multiplication à gauche par M^{-1}, il vient

$$S^2 = \sum_{M \in G} \sum_{N \in G} MN = \sum_{M \in G} \sum_{N \in G} N = gS$$

et donc $\dfrac{1}{g} S$ est un projecteur. Il en résulte que sa trace est égale à son rang et donc $\mathrm{Tr}(S) = g \,\mathrm{rg}\left(\dfrac{1}{g} S\right)$. En particulier, $\boxed{\mathrm{Tr}(S) \text{ est un entier divisible par } g.}$

b. Soit M dans G tel que $\psi_r(M)$ est le neutre de de $\mathrm{GL}_{\{1,\ldots,n\}^r}(\mathbf{R})$. En particulier $\mathrm{Tr}(\psi_r(M)) = n^r$ et donc, en utilisant 10.a), $|\mathrm{Tr}(M)| = n$. Il en résulte, d'après 7.a),

$\boxed{M = I_n \text{ si } r \text{ est impair et } M = \pm I_n \text{ sinon.}}$

c. Pour $r = 0$, en convenant que si $\mathrm{Tr}(M) = 0$, alors $\mathrm{Tr}(M)^r = 1$, il vient $\displaystyle\sum_{M \in G} \mathrm{Tr}(M)^r = \sum_{M \in G} 1 = g$. Pour r dans $\mathbf{N}^*$, on a, comme en 11.a) et en utilisant 10.b),

$$\left(\sum_{M \in G} M^{*r}\right)^2 = \sum_{M \in G} \sum_{N \in G} (MN)^{*r} = g \sum_{N \in G} N^{*r}$$

et donc $\dfrac{1}{g}\displaystyle\sum_{M\in G} M^{*r}$ est un projecteur et sa trace est un entier égal à son rang. En tenant compte de 10.a) et du cas $r=0$, on en déduit que, pour tout entier naturel r, $\boxed{\displaystyle\sum_{M\in G}\mathrm{Tr}(M)^r \text{ est un entier divisible par } g.}$

Remarque : on peut aussi choisir un isomorphisme entre $\mathrm{GL}_{\{1,\dots,n\}^r}(\mathbf{R})$ et $\mathrm{GL}_{n^r}(\mathbf{R})$ et obtenir un morphisme de groupes ι_r entre G et un sous-groupe de $\mathrm{GL}_{n^r}(\mathbf{R})$. Alors, d'après 10.a),

$$\sum_{M\in G}\mathrm{Tr}(M)^r = \mathrm{Card}\,\mathrm{Ker}(\iota_r)\sum_{N\in\iota_r(G)}\mathrm{Tr}(N)$$

ce qui, d'après 11.a), est un multiple entier de $\mathrm{Card}\,\mathrm{Ker}(\iota_r)\times\mathrm{Card}\,\mathrm{Im}(\iota_r)$, donc de g. Mais il faut alors justifier ces calculs.

12) a. On pose $P=(X-t_1)\cdots(X-t_s)$ et on note $P=\displaystyle\sum_{k=0}^{s}a_kX^k$. Alors, puisque les traces d'éléments de G sont entières, P est à coefficients entiers relatifs et il vient

$$\sum_{M\in G}P(\mathrm{Tr}(M)) = \sum_{k=0}^{s}a_k\sum_{M\in G}\mathrm{Tr}(M)^r\in g\mathbf{Z}$$

d'après la question précédente. Comme P s'annule sur $\{t_1,\dots,t_s\}$ et que la seule matrice de G de trace égale à n est I_n, d'après 7.a), il vient $P(n)\in g\mathbf{Z}$, i.e.
$\boxed{(n-t_1)\cdots(n-t_s) \text{ est un entier divisible par } g.}$

b. D'après 7.a) les termes du produit précédent sont des entiers naturels compris entre 1 et $2n$, et ne peuvent être égaux à $2n$ que si G contient $-I_n$, ce qui est impossible si n est impair. On en déduit : $\boxed{g \text{ divise } (2n)! \text{ et même, si } n \text{ est impair, } g \text{ divise } (2n-1)!.}$

c. D'après 9), si $n=3$, $\{t_1,\dots,t_s\}\subset[\![-1,2]\!]$ et donc g divise $4!$, i.e. $\boxed{g \text{ divise } 24.}$

13) a. Soit n un entier supérieur ou égal à 2. Soit H l'ensemble des matrices diagonales à coefficients dans le groupe $\{\pm1\}$. C'est un sous-groupe de $\mathrm{GL}_n(\mathbf{R})$ isomorphe à $\{\pm1\}^n$. Soit K le groupe des matrices de permutations d'ordre n. C'est un sous-groupe de $\mathrm{GL}_n(\mathbf{R})$ isomorphe à $\mathfrak{S}_n$. On montre que HK est un sous-groupe de $\mathrm{GL}_n(\mathbf{R})$. Il est non vide car contient I_n. Soit (h,h') et (k,k') deux couples d'éléments de H et K respectivement, alors khk^{-1} est la matrice obtenue à partir de h en permutant ses lignes et colonnes selon la permutation associée à k et donc c'est un élément de H. Il en résulte que kh appartient à HK puisque $kh=\left(khk^{-1}\right)k$. En particulier $k^{-1}h^{-1}\in HK$ et donc HK est stable par passage à l'inverse. De plus $h'k'hk=h'(k'hk'^{-1})k'k$ et donc HK est stable par produit. Il en résulte que HK est un sous-groupe de $\mathrm{GL}_n(\mathbf{R})$. De plus, comme $H\cap K=\{I_n\}$, l'écriture d'un élément de HK sous la forme hk est unique et donc HK est de cardinal $2^nn!$.

De plus H et K sont formés de matrices à coefficients entiers et de déterminant dans ±1, donc HK aussi. Enfin il y a 2^{n-1} éléments de déterminant fixé (dans $\{\pm1\}$) dans H. Ainsi à k fixé dans K, correspondent exactement 2^{n-1} éléments de H tels que hk appartienne à $\mathrm{SL}_n(\mathbf{Z})$ et donc $HK\cap\mathrm{SL}_n(\mathbf{Z})$ est un sous-groupe de $\mathrm{SL}_n(\mathbf{Z})$ de $\boxed{\text{cardinal } 2^{n-1}n!.}$

b. D'après le deux questions précédentes

$\boxed{\text{le cardinal maximal d'un sous-groupe fini de } \mathrm{SL}_3(\mathbf{Z}) \text{ est } 24.}$

14) a. On pose $N = \dfrac{1}{m}(M - I_n)$ et alors N est à coefficients entiers par définition de m et le pgcd positif de ses coefficients est 1. Comme I_n et N commutent, il vient

$$0 = M^p - I_n = (I_n + mN)^p - I_n = pmN + \sum_{k=2}^{p} \binom{p}{k} m^k N^k$$

et donc

$$pN = -m \sum_{k=2}^{p} \binom{p}{k} m^{k-2} N^k\,,$$

de sorte que les coefficients de pN sont tous divisibles par m, puisque tous les termes qui interviennent sont entiers ou à coefficients entiers. Comme le pgcd positif des coefficients de N est 1, celui de pN est p et donc $\boxed{m \text{ divise } p.}$

b. D'après ce qui précède, si $m \neq 1$, alors $m = p$ puisque p est premier. D'où

$$pN = -p \sum_{k=2}^{p} \binom{p}{k} p^{k-2} N^k = -p^2 \frac{p-1}{2} N^2 - p^2 \sum_{k=3}^{p} \binom{p}{k} p^{k-3} N^k\,,$$

et donc, si $p \neq 2$, p^2 divise tous les coefficients du membre de droite car p est impair et donc $\dfrac{p-1}{2}$ est entier. Ceci est contradictoire avec le fait que le pgcd positif des coefficients de pN est p, et donc $\boxed{\text{soit } m = 1, \text{ soit } m = p = 2.}$

15) a. On remarque que $G \cap \mathrm{Ker}(\varphi_{n,3})$ est un groupe. Soit M dans ce groupe, r son ordre et p un diviseur premier de r. Alors $M^{r/p}$ est d'ordre p et appartient à $G \cap \mathrm{Ker}(\varphi_{n,3})$. En particulier 3 divise tous les coefficients de $M^{r/p} - I_n$, ce qui contredit le résultat précédent. Il en résulte que r n'admet aucun diviseur premier, i.e. $r = 1$ et donc $M = I_n$. Par conséquent $\boxed{\text{la restriction à } G \text{ de } \varphi_{n,3} \text{ est injective.}}$

b. Se donner un élément de $\mathrm{GL}_n(\mathbf{Z}/3\mathbf{Z})$, c'est se donner une base de $(\mathbf{Z}/3\mathbf{Z})^n$. Or étant donné k vecteurs de $(\mathbf{Z}/3\mathbf{Z})^n$ (avec $0 \leq k < n$) formant une famille libre, ils engendrent un espace de dimension k, donc de cardinal 3^k, et on dispose de $3^n - 3^k$ vecteurs indépendants de cette famille. Par application récursive du principe des bergers, on en déduit que le cardinal de $\mathrm{GL}_n(\mathbf{Z}/3\mathbf{Z})$ est $\displaystyle\prod_{k=0}^{n-1} (3^n - 3^k)$.

De plus la matrice diagonale n'ayant que des coefficients diagonaux égaux à $\overline{1}$, sauf le premier égal à $-\overline{1}$, est de déterminant $-\overline{1}$. Enfin, par multiplicativité du déterminant, la multiplication par cette matrice échange $\mathrm{SL}_n(\mathbf{Z}/3\mathbf{Z})$ avec son complémentaire dans $\mathrm{GL}_n(\mathbf{Z}/3\mathbf{Z})$. Il en résulte que $\mathrm{SL}_n(\mathbf{Z}/3\mathbf{Z})$ est de cardinal la moitié de celui de $\mathrm{GL}_n(\mathbf{Z}/3\mathbf{Z})$. Comme G et $\varphi_{n,3}(G)$ sont isomorphes, par injectivité de $\varphi_{n,3}$, ils ont même cardinal et celui-ci divise celui de $\mathrm{SL}_n(\mathbf{Z}/3\mathbf{Z})$ d'après le théorème de Lagrange. On en conclut que

$$\boxed{g \text{ divise } \frac{1}{2}(3^n - 1)(3^n - 3) \cdots (3^n - 3^{n-1}).}$$

c. On déduit de la question précédente et de 12.b) que, si $n = 4$, g divise $8!$ et $\frac{1}{2}80\times 78\times 72\times 54$, autrement dit $2^7 \times 3^2 \times 5 \times 7$ et $2^8 \times 3^6 \times 5 \times 13$. Il divise également leur pgcd, à savoir $2^7 \times 3^2 \times 5$, i.e. $\boxed{g \text{ divise } 5760.}$

16) Puisque tout élément d'un groupe est régulier, il définit une permutation de G par translation à gauche donnée par : $h \mapsto (k \mapsto hk)$. Cette application est un morphisme injectif de groupes de G dans $\mathfrak{S}_G$. Une bijection entre G et $[\![1, g]\!]$ induit un isomorphisme de groupes de $\mathfrak{S}_G$ sur $\mathfrak{S}_n$. Enfin l'application qui à une permutation associe sa matrice de permutation est un morphisme injectif de groupes de $\mathfrak{S}_n$ dans $\mathcal{O}_n(\mathbf{R})$. On obtient ainsi un morphisme injectif de groupes de G dans $\mathcal{O}_n(\mathbf{R})$, noté α. L'image de α est formée de matrices à coefficients entiers et de déterminant ± 1.

On note $(e_i)_{1\le i\le n}$ la base canonique de $\mathbf{R}^n$ et $(u_i)_{1\le i\le n}$ la base (u) de $\mathbf{R}^n$ donnée par $u_1 = \sum_{k=1}^{n} e_k$ et, pour $i \geq 2$, $u_i = e_i - e_1$. Soit alors Q la matrice de passage de la base canonique à (u) et i_Q l'automorphisme intérieur de $\mathrm{GL}_n(\mathbf{R})$ donné par $P \mapsto QPQ^{-1}$. Les formules, pour σ dans $\mathfrak{S}_n$ et i dans $[\![2, n]\!]$,

$$\sum_{k=1}^{n} e_{\sigma(k)} = u_1 \quad \text{et} \quad e_{\sigma(i)} - e_{\sigma(1)} = \left(e_{\sigma(i)} - e_1\right) - \left(e_{\sigma(1)} - e_1\right)$$

montrent que $i_Q \circ \alpha$ est un morphisme injectif de groupes de G dans $\mathrm{GL}_n(\mathbf{R})$ dont l'image est formée de matrices à coefficients entiers de déterminant ± 1, diagonales par blocs avec un premier bloc égal à (1) et un bloc de taille $n - 1$.

Pour h dans G on pose $\beta(h)$ la matrice diagonale dont le premier terme diagonal est égal à $\det(\alpha(h))$ et tous les autres sont égaux à 1, de sorte qu'on a $\det(\beta(h)) = \det(\alpha(h))$. Par composition de morphismes, β est un morphisme de groupes et par construction les images de α et de β commutent entre elles. On en déduit qu'en posant $\varphi(h) = \alpha(h)\beta(h)$, on obtient un morphisme de groupes. En effet, pour h et k dans G, on a

$$\varphi(h)\varphi(k) = \alpha(h)\beta(h)\alpha(k)\beta(k) = \alpha(h)\alpha(k)\beta(h)\beta(k) = \alpha(hk)\beta(hk) = \varphi(hk)$$

et, de plus, $\det(\varphi(h)) = \det(\alpha(h))^2 = 1$ et donc φ est un morphisme à valeurs dans $\mathrm{SL}_n(\mathbf{Z})$. C'est un morphisme injectif car α l'est et que celui-ci est déterminé par le second bloc, de taille $n - 1$, de φ.

Par conséquent $\boxed{G \text{ est isomorphe à un sous-groupe de } \mathrm{SL}_g(\mathbf{Z}).}$

PARTIE III - Morphismes de groupes et $\mathrm{SL}_n(\mathbf{Z})$

17) Puisque $(\mathbf{Z}/2\mathbf{Z})^2$ est de cardinal 4, il admet trois vecteurs non nuls et donc tout élément de $\mathrm{GL}_2(\mathbf{Z}/2\mathbf{Z})$ permute entre eux ces trois éléments. On en déduit un morphisme injectif de groupes de $\mathrm{GL}_2(\mathbf{Z}/2\mathbf{Z})$ dans $\mathfrak{S}_3$. Comme toute famille de deux vecteurs distincts et non nuls de $(\mathbf{Z}/2\mathbf{Z})^2$ en forme une base, ce dernier admet six bases, ce qui est donc aussi le cardinal de son groupe linéaire. Par cardinalité, on en déduit $\mathrm{GL}_2(\mathbf{Z}/2\mathbf{Z}) \simeq \mathfrak{S}_3$. Comme le seul scalaire non nul de $\mathbf{Z}/2\mathbf{Z}$ est son élément neutre on a aussi $\mathrm{GL}_2(\mathbf{Z}/2\mathbf{Z}) = \mathrm{SL}_2(\mathbf{Z}/2\mathbf{Z})$

et on dispose donc d'un isomorphisme de groupes s entre $\mathrm{SL}_2(\mathbf{Z}/2\mathbf{Z})$ et $\mathfrak{S}_3$. Par surjectivité de l'homomorphisme signature ε et, d'après 6.b), de $\varphi_{n,2}$, on en déduit que $\varepsilon \circ s \circ \varphi_{n,2}$ est $\boxed{\text{un morphisme de groupes surjectif de } \mathrm{SL}_2(\mathbf{Z}) \text{ dans } \mathbf{Z}/2\mathbf{Z}.}$

18) a. Soit i, j et k des éléments deux à deux distincts de $\{1,\dots,n\}$. Par définition, on a $M_{i,j}M_{j,k} = I_n + E_{i,j} + E_{j,k} + E_{i,k}$ et donc son inverse est $I_n - E_{i,j} - E_{j,k} - E_{i,k}$ puisqu'on a affaire à des indices distincts deux à deux. Pour la même raison, le produit de ces deux matrices est $I + E_{i,k}$, i.e. $\boxed{M_{i,j}M_{j,k}(M_{i,j})^{-1}(M_{j,k})^{-1} = M_{i,k}.}$

b. Soit φ un morphisme de groupes de $\mathrm{SL}_n(\mathbf{Z})$ dans G. Puisque n est supérieur à 3, pour tous i et k d'élements distincts de $\{1,\dots,n\}$ on dispose d'un j dans le même ensemble et distinct de i et k. D'après ce qui précède et par commutativité de G, il vient

$$\varphi(M_{i,k}) = \varphi(M_{i,j})\varphi(M_{j,k})\varphi(M_{i,j})^{-1}\varphi(M_{j,k})^{-1} = 1_G$$

et donc, en utilisant 5), $\boxed{\varphi \text{ est constant.}}$

19) a. Soit S une partie génératrice finie de G. Alors l'application de $\mathrm{Hom}(G,H)$ dans H^S qui à un morphisme de groupes de G dans H associe sa restriction à S est injective. Comme H et S sont finis, H^S l'est aussi et donc, par injectivité, $\boxed{\mathrm{Hom}(G,H) \text{ est fini.}}$

b. Soit φ l'application de $\mathrm{Hom}(G,H)$ dans lui-même définie par $\varphi(f) = f \circ u$. Par surjectivité de u, φ est injective et donc, par finitude de $\mathrm{Hom}(G,H)$, bijective. Il en résulte que, pour tout morphisme de groupes v de G dans H, on dispose de f dans $\mathrm{Hom}(G,H)$ tel que $v = f \circ u$ et il en résulte $\boxed{\mathrm{Ker}(u) \subset \mathrm{Ker}(v).}$

20) Soit φ un endomorphisme de groupes surjectif de $\mathrm{SL}_n(\mathbf{Z})$ et M dans son noyau. Soit p un nombre premier. D'après 5) et 19.b), M appartient au noyau de $\varphi_{n,p}$ puisque $\mathrm{SL}_n(\mathbf{Z}/p\mathbf{Z})$ est un groupe fini et donc p divise tous les coefficients de $M - I_n$. Comme ce résultat est vrai pour tout nombre premier p, les coefficients de $M - I_n$ sont tous nuls et donc $M = I_n$, i.e. φ est injectif. Il en résulte qu'il est $\boxed{\text{bijectif.}}$