Le groupe $\mathrm{SL}_n(\mathbb{Z})$

1. $\mathrm{SL}_n(\mathbb{Z}) \neq \emptyset$ car $I_n \in \mathrm{SL}_n(\mathbb{Z})$ et bien évidemment, $\mathrm{SL}_n(\mathbb{Z}) \subset \mathrm{SL}_n(\mathbb{Q})$,
$\mathrm{SL}_n(\mathbb{Z})$ est stable par produit car le produit de deux matrices à coefficients dans $\mathbb{Z}$ est une matrice à coefficients dans $\mathbb{Z}$ et le déterminant du produit est égal au produit des déterminants.
Si $M \in \mathrm{SL}_n(\mathbb{Z})$ alors M'^{T} (transposée de la matrice des cofacteurs) est encore dans $\mathrm{SL}_n(\mathbb{Z})$. Comme $MM'^{\mathrm{T}} = \det M . I_n$ alors $M'^{\mathrm{T}} = M^{-1}$.
Conclusion : $\mathrm{SL}_n(\mathbb{Z})$ est un sous-groupe de $\mathrm{SL}_n(\mathbb{Q})$. . . . . $\boxed{2}$

2. $E_{ij}^2 = 0$ donc $M_{ij}^m = I_n + mE_{ij}$ d'après la formule du binôme quand $m \in \mathbb{N}$. Cette relation est encore valable si $m = -p \in \mathbb{Z}^-$ car $(I_n + mE_{ij})M_{ij}^p = (I_n + mE_{ij})(I_n + pE_{ij}) = I_n$, d'où $I_n + mE_{ij} = M_{ij}^{-p} = M_{ij}^m$. . . . . $\boxed{1}$

3. Si $M = (C_1\ C_2\ \dots\ C_n)$ est l'écriture de M sous forme de colonnes alors $MM_{i,j}^m = (C_1\ C_2\ \dots\ C_j + mC_i\ \dots\ C_n)$ (la colonne C_j est remplacée par $C_j + mC_i$). . . . . $\boxed{1}$

4. Commençons par traiter le cas $n = 2$: on utilise l'algorithme d'Euclide.
(i) Si $a_1 \geqslant 0$ et $a_2 = 0$, c'est terminé.
(ii) Si $a_1 < 0$ et $a_2 = 0$ alors on effectue les opérations suivantes :

$$(a_1\ 0) \xrightarrow{C_2 \leftarrow C_2 + C_1} (a_1\ a_1) \xrightarrow{C_1 \leftarrow C_1 - 2C_2} (-a_1\ a_1) \xrightarrow{C_2 \leftarrow C_2 + C_1} (-a_1\ 0)$$

(iii) Si $a_2 \neq 0$ alors c'est là que commence l'algorithme d'Euclide : on écrit successivement

$$a_2 = q_1 a_1 + r_1,\ a_1 = q_2 r_1 + r_2,\ \dots, r_l = q_{l+2} r_{l+1} + r_{l+2},\ \dots, r_k = q_{k+2} r_{k+1}$$

où $r_l = q_{l+2} r_{l+1} + r_{l+2}$ est la division euclidienne de r_l par r_{l+1} et $r_{k+1} = d$, P.G.C.D. de a_2 et a_1. On fait alors les opérations qui suivent :

$$(a_1\ a_2) \xrightarrow{C_2 \leftarrow C_2 - q_1 C_1} (a_1\ r_1) \xrightarrow{C_1 \leftarrow C_1 - q_2 C_2} (r_2\ r_1) \dots (r_{2p}\ r_{2p\pm1}) \dots \begin{cases} (d\ 0) & 1 \\ (0\ d) & 2 \end{cases}$$

Dans le premier cas, c'est fini, dans le deuxième, on fait

$$(0\ d) \xrightarrow{C_1 \leftarrow C_1 + C_2} (d\ d) \xrightarrow{C_2 \leftarrow C_2 - C_1} (d\ 0).$$

Cas général : on utilise l'associativité du P.G.C.D., on obtiendra successivement $(d_1\ 0\ a_3\ \dots\ a_n)$ où $d_1 = a_1 \wedge a_2$ puis $(d_2\ 0\ 0\ a_4\ \dots\ a_n)$ où $d_2 = d_1 \wedge a_3 = a_1 \wedge a_2 \wedge a_3$ en opérant sur les premières et troisième colonnes et par une récurrence finie sur les colonnes suivantes $(d\ 0\ \dots\ 0)$. . . . . $\boxed{15}$

5. Soit $M \in \mathrm{SL}_n(\mathbb{Z})$, comme $\det M = 1$ alors, en développant selon n'importe quelle ligne, on prouve que le P.G.C.D. des éléments d'une même ligne vaut 1. On note G_n le groupe engendré par les matrices $M_{i,j}$, on remarque que c'est un sous-groupe de $\mathrm{SL}_n(\mathbb{Z})$. L'objectif ici est de prouver que $G_n = \mathrm{SL}_n(\mathbb{Z})$.
En faisant les opérations de la question précédente sur la première ligne de M alors on a $MC_1 = M_1 = \begin{pmatrix} 1 & 0 & \dots & 0 \\ a'_{21} & a'_{22} & \dots & a'_{2n} \\ \vdots & & & \\ a'_{n1} & a'_{n2} & & a'_{nn} \end{pmatrix}$ où C_1 est un produit de matrices $M_{i,j}$ donc appartient à G_n.

On peut ensuite opérer sur la deuxième ligne de M_1 à partir de la deuxième colonne pour obtenir la matrice $MC_1C_2 = M_2 = \begin{pmatrix} 1 & 0 & \dots & 0 \\ a'_{21} & d_2 & \dots & 0 \\ \vdots & & M''_2 & \\ a'_{n1} & a''_{n2} & & \end{pmatrix}$ où d_2 est le P.G.C.D. des termes $a'_{22}, \dots, a'_{2n}$. En fait $d_2 = 1$ car $\det(MC_1C_2) = 1 = \underbrace{d_2}_{\in\mathbb{N}} \times \underbrace{\det M''_2}_{\in\mathbb{Z}}$. La première colonne est inchangée car les opérations élémentaires que l'on a faites ont concerné les colonnes 2 à n.

En appliquant cet algorithme aux autres lignes, on trouve une matrice triangulaire inférieure $M_n = MC = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ m_{ij} & & 1 \end{pmatrix}$ où $C \in G_n$. On retranche à la k-ième colonne, la dernière multipliée par m_{nk}, pour $k \in [\![1, n-1]\!]$, la dernière ligne ne comporte alors que des 0 sauf sur la diagonale. On reprend le même processus avec les autres lignes, finalement on obtient la matrice I_n.

On aura $C^{\mathrm{T}}M^{\mathrm{T}} = D$ où $D \in G_n$ soit $M = D^{\mathrm{T}}C^{-1} \in G_n$ car G_n est stable par transposition et par inversion.

Conclusion : on avait $G_n \subset \mathrm{SL}_n(\mathbb{Z})$ et on vient de prouver l'inclusion inverse donc $\mathrm{SL}_n(\mathbb{Z})$ est engendré par les matrices $M_{i,j}$. .... $\boxed{10}$

6. a) $\mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z})$ est bien un groupe, on fait la même démonstration que pour la question **1** et on utilise l'expression du produit dans $\mathcal{M}_n(\mathbb{K})$ pour n'importe quel corps $\mathbb{K}$. $\boxed{0}$

b) On veut prouver que si $\overline{M} \in \mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z})$ alors il existe une matrice $M \in \mathrm{SL}_n(\mathbb{Z})$ telle que $\overline{M} = \varphi_{n,p}(M)$. En d'autres termes, si $N \in \mathcal{M}_n(\mathbb{Z})$ est telle que $\det N \equiv 1[p]$ alors il existe $M \in \mathrm{SL}_n(\mathbb{Z})$ telle que $N \equiv M[p]$.

- Le cas $n = 1$ est immédiat.
- On suppose la propriété vraie à l'ordre n.
  Soit $N \in \mathcal{M}_{n+1}(\mathbb{Z})$ telle que $\det N \equiv 1[p]$. D'après la question **4**, on sait qu'il existe $C \in \mathrm{SL}_{n+1}(\mathbb{Z})$ telle que $NC = \begin{pmatrix} d & 0 & \dots & 0 \\ \vdots & & N' & \end{pmatrix}$ avec $d\underbrace{\det N'}_{\Delta'} = 1 + kp$.
  En faisant la manipulation de la question **4** alors la première ligne de la matrice NC va se transformer de la manière suivante :
  $$\begin{aligned} (d\ 0\ \dots) &\xrightarrow{C_2 \leftarrow C_2 + \Delta' C_1} (d\ 1+kp\ \dots) \\ &\xrightarrow{C_1 \leftarrow C_1 - dC_2} (-dkp\ 1+kp\ \dots) \\ &\xrightarrow{C_1 \leftarrow C_1 + C_2} (1+kp-dkp\ 1+kp) \\ &\xrightarrow{C_2 \leftarrow C_2 - C_1} (1+kp-dkp\ -dkp\ \dots) \end{aligned}$$
  d'où, si $C' \in \mathrm{SL}_n(\mathbb{Z})$ est la matrice qui correspond à toutes ces manipulations, on aura $NC' \equiv \begin{pmatrix} 1 & 0 & \dots \\ \vdots & & N'' \end{pmatrix}$ et $\det N'' \equiv 1[p]$, on applique alors la récurrence à N''.
  Finalement, on a $NC'' \equiv D[p]$ où $D \in \mathrm{SL}_n(\mathbb{Z})$ (D est une matrice triangulaire inférieure et tous ses termes diagonaux sont égaux à 1).
  On en déduit $N \equiv C''^{-1}D[p]$ car $\varphi_{n+1,p}$ est un morphisme de groupes... $\boxed{15}$

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

7. a)
- (M), le sous-groupe de G engendré par M est fini donc il existe $k \in \mathbb{N}^*$ tel que $M^k = I_n$. $X^k - 1$ est un polynôme annulateur de M qui est scindé, à racines simples sur $\mathbb{C}$ donc M est diagonalisable sur $\mathbb{C}$. .... $\boxed{1}$
- Toutes les valeurs propres de M sont racines de $X^k - 1$ donc $\mathrm{Tr}(M) = \sum_{j=1}^{n} \lambda_j$ où les λ_j sont des complexes de module 1 donc $\overline{\lambda_j} = \dfrac{1}{\lambda_j}$ et $M = \overline{M}$ car M est à coefficients réels d'où
$$\mathrm{Tr}(M) = \mathrm{Tr}(\overline{M}) = \sum_{j=1}^{n} \overline{\lambda_j} = \sum_{j=1}^{n} \frac{1}{\lambda_j} = \mathrm{Tr}(M^{-1}) \qquad \boxed{1}$$
- $|\mathrm{Tr}(M)| \leqslant \sum_{j=1}^{n} |\lambda_j| = n$. .... $\boxed{0}$
- $\mathrm{Tr}(M) = n \Leftrightarrow \sum_{j=1}^{n} \lambda_j = n$ et, en prenant les parties réelles, $\sum_{j=1}^{n} \mathrm{Re}(\lambda_j) = n$. Comme $\lambda_j = x_j + iy_j$ avec $x_j^2 + y_j^2 = 1$ alors $x_j \leqslant 1$ donc $x_j = 1$ et $y_j = 0$. M est une matrice diagonalisable qui n'a que 1 comme valeur propre, c'est donc l'identité. De même pour $\mathrm{Tr}(M) = -n$.
Conclusion : $\mathrm{Tr}(M) = n \Leftrightarrow M = I_n$ et $\mathrm{Tr}(M) = -n \Leftrightarrow M = -I_n$ (à condition que $-I_n \in G$). .... $\boxed{2}$

b) U est symétrique définie positive en tant que somme de matrices symétriques définies positives (en effet, $X^{\mathrm{T}} M^{\mathrm{T}} M X = \|MX\|^2 \geqslant 0$ et, comme M est inversible, si $X \neq 0$ alors $MX \neq 0$ donc $\|MX\|^2 > 0$). .... $\boxed{1}$

c) Soit $f \in \mathcal{L}(\mathbb{R}^n)$, N sa matrice élément de G alors
$$N^{\mathrm{T}} U N = \sum_{M \in G} (MN)^{\mathrm{T}} MN = \sum_{M \in G} M^{\mathrm{T}} M = U$$
car $M \mapsto MN$ est une bijection de G donc f est orthogonal pour ce produit scalaire.
.... $\boxed{2}$

8. a) Les endomorphismes de $\mathbb{R}^2$ dont les matrices appartiennent au groupe G sont donc des rotations pour le produit scalaire défini par U (ce ne sont pas des symétries car leur déterminant vaut 1). Comme G est fini, on sait que $r^{\mathrm{Card}\, G} = \mathrm{Id}_{\mathbb{R}^2}$ donc G est isomorphe à un sous groupe de $\mathbb{U}_{\mathrm{Card}\, G}$. Comme tout sous-groupe d'un groupe cyclique est cyclique alors G est cyclique. .... $\boxed{4}$

b) Si λ_1 et λ_2 désignent les valeurs propres d'un élément M qui engendre G alors on sait que $|\lambda_1 + \lambda_2| = |2\cos\theta| \leqslant 2$. On aura ainsi 5 possibilités correspondant à $\lambda_1 + \lambda_2 \in \{-2, -1, 0, 1, 2\}$ ($\lambda_1 + \lambda_2 = \mathrm{Tr}(M) \in \mathbb{Z}$).
- $\lambda_1 + \lambda_2 = 2$ alors $M = I_2$, $G = \{I_2\}$
- $\lambda_1 + \lambda_2 = -2$ alors $M = -I_2$, $G = \{\pm I_2\}$,
- $\cos\theta = \frac{1}{2}$ alors $\theta = \pm\frac{\pi}{3}$, G est d'ordre 6,
- $\cos\theta = -\frac{1}{2}$ alors $\theta = \pm\frac{2\pi}{3}$, G est d'ordre 3,
- $\cos\theta = 0$ alors $\theta = \pm\dfrac{\pi}{2}$, G est d'ordre 4.

.... $\boxed{4}$

Il est à noter que l'on a étudié toutes les possibilités pour G.

c) Si M est d'ordre 2 alors $G = \{I_1, M\}$ est un sous-groupe fini de $\mathrm{SL}_2(\mathbb{Z})$ auquel on peut appliquer le résultat précédent donc $M = -I_2$. La réciproque est évidente. $\boxed{2}$

d) Si l'ordre de G vaut 3 alors $\mathrm{Tr}(M)=-1$ vu le **b**, réciproquement, si $\mathrm{Tr}(M)=-1$ alors $M^2+M+I_2=0$ donc $M^3=I_2$ et $M\neq I_2$ donc l'ordre de M vaut 3.
Si l'ordre de M vaut 4 alors $\mathrm{Tr}(M)=0$, réciproquement, si $\mathrm{Tr}(M)=0$ alors $M^2+I_2=0$ donc $M^4=I_2$, l'ordre de M vaut 4.
$\mathrm{Card}\,G=6\Leftrightarrow\mathrm{Tr}(M)=1$ de même. .... $\boxed{4}$

e) On note $J=\begin{pmatrix}0&-1\\1&-1\end{pmatrix}$ et $K=\begin{pmatrix}0&-1\\1&0\end{pmatrix}$. Les groupes suivants conviennent :

$$\begin{array}{lll}
G=(I_2) & =\{I_2\}, & \mathrm{Card}\,G=1,\\
G=(-I_2) & =\{\pm I_2\}, & \mathrm{Card}\,G=2,\\
G=(J) & =\{I_2,J,J^2\}, & \mathrm{Card}\,G=3,\\
G=(K) & =\{\pm I_2,\pm K\}, & \mathrm{Card}\,G=4,\\
G=(-J) & =\{\pm I_2,\pm J,\pm J^2\}, & \mathrm{Card}\,G=6.
\end{array}$$
.... $\boxed{3}$

9. A priori on a $\mathrm{Tr}(M)\in[\![-3,3]\!]$ mais on sait que l'endomorphisme associé à M est une rotation pour le produit scalaire défini par U donc $\mathrm{Tr}(M)=1+2\cos\theta\in[\![-1,3]\!]$. . $\boxed{1}$

Pour $\mathrm{Tr}(M)=-1$ on a $\theta\equiv\pi \mod 2\pi$ et $\mathrm{ord}\,(M)=2$.
Pour $\mathrm{Tr}(M)=0$ on a $\theta\equiv\pm\frac{2}{3}\pi \mod 2\pi$ et $\mathrm{ord}\,(M)=3$.
Pour $\mathrm{Tr}(M)=1$ on a $\theta\equiv\pm\frac{1}{2}\pi \mod 2\pi$ et $\mathrm{ord}\,(M)=4$.
Pour $\mathrm{Tr}(M)=2$ on a $\theta\equiv\pm\frac{1}{3}\pi \mod 2\pi$ et $\mathrm{ord}\,(M)=6$.
Pour $\mathrm{Tr}(M)=3$ on a $\theta\equiv 0 \mod 2\pi$ et $\mathrm{ord}\,(M)=1$.

Pour trouver des matrices qui conviennent dans chacun des cas ci-dessus, il suffit de prendre $M=\begin{pmatrix}N&0\\0&1\end{pmatrix}$ où N est l'une des matrices de la question **8.e**. .... $\boxed{3}$

10. a) On a immédiatement

$$\mathrm{Tr}(M\star M')=\sum_{(i,i')\in I\times I'}a_{i,i}b_{i',i'}=\sum_{i\in I}a_{i,i}\sum_{i'\in I'}b_{i',i'}=\mathrm{Tr}(M)\,\mathrm{Tr}(M').$$
$\boxed{1}$

b) Soit $M=(a_{i,j})$, $N=(b_{i,j})$, $M'=(a'_{i',j'})$, $N'=(b'_{i',j'})$ et $(MN)\star(M'N')=(c_{(i,i'),(j,j')})$ alors

$$c_{(i,i'),(j,j')}=\sum_{k\in I}a_{i,k}b_{k,j}\times\sum_{k'\in I'}a'_{i',k'}b'_{k',j'}=\sum_{(k,k')\in I\times I'}(a_{i,k}a'_{i',k'})\times(b_{k,j}b'_{k',j'})$$

donc $(MN)\star(M'N')=(M\star M')(N\star N')$. .... $\boxed{1}$

c) Évident en utilisant les deux résultats précédents. .... $\boxed{0}$

11. a) Classique, on a $S^2=\sum\limits_{(M,N)\in G^2}MN=gS$ car $M\mapsto MN$ est une bijection de G.

On remarque alors que $\dfrac{1}{g}S$ est un projecteur et comme la trace d'un projecteur est un entier (égal à son rang) alors $\mathrm{Tr}(S)=g\,\mathrm{Rg}(S)$ donc la trace de S est un entier divisible par g. .... $\boxed{2}$

b) $M\in\mathrm{Ker}\,\psi_r\Leftrightarrow M^{*r}=I_{[\![1,n]\!]^r}$ donc $\mathrm{Tr}(M)^r=n^r$. On en déduit que $\mathrm{Tr}(M)=\pm n$ donc $M=\pm I_n$ vu la question **7.a**.
Conclusion : $\mathrm{Ker}\,\psi_r=\{I_n\}$ si r est impair ou si $-I_n\notin G$, $\mathrm{Ker}\,\psi_r=\{\pm I_n\}$ si r est pair et si $-I_n\in G$. .... $\boxed{2}$

c) Si $\mathrm{Ker}\,\psi_r=\{I_n\}$ alors $G_r=\{M^{*r},\ M\in G\}$ est un sous-groupe de $\mathrm{GL}_{[\![1,n]\!]^r}(\mathbb{R})$ de même cardinal que G donc, en appliquant le résultat du **a** à $S_r=\sum\limits_{M\in G}M^{*r}$, on en déduit que g divise $\sum\limits_{M\in G}\mathrm{Tr}(M)^r$.
Si $\mathrm{Ker}\,\psi_r=\{-I_n,I_n\}$ alors si $M\in G$, $-M\in G$, $g=2g'$ où $g'=\mathrm{Card}\,G_r$. On pose

$S_r = \sum_{M_r \in G_r} M_r = \frac{1}{2} \sum_{M \in G} M^{*r}$, g' divise $\mathrm{Tr}(S_r)$ donc on arrive à la même conclusion que ci-dessus. . . . . $\boxed{4}$

12. a) Comme G est un sous-groupe de $\mathrm{SL}_n(\mathbb{R})$ alors les t_i sont des entiers donc le polynôme P est à coefficients entiers. On sait ensuite que I_n est le seul élément de G de trace égale à n donc $P(\mathrm{Tr}(M)) = 0$ pour tous les autres éléments de G. Si on pose $P = \sum_{k=0}^{s} a_k X^s$ alors

$$\begin{aligned}\sum_{M \in G} P(\mathrm{Tr}(M)) &= \sum_{k=0}^{s} a_k \left(\sum_{M \in G} \mathrm{Tr}(M)^r \right) = mg,\ m \in \mathbb{N}^* \\ &= P(\mathrm{Tr}(I_n)) = P(n)\end{aligned}$$

donc $P(n)$ est un entier divisible par g. . . . . $\boxed{4}$

b) Comme les $t_i \in [\![-n, n-1]\!]$ alors $\prod_{k=1}^{s}(n - t_k)$ divise $\prod_{l=-n}^{n-1}(n-l) = (2n)!$ donc g divise $(2n)!$. . . . . $\boxed{2}$
Si n est impair alors $-I_n \notin G$ car $\det(-I_n) = -1$ donc on peut reprendre le produit ci-dessus à partir de $l = -n+1$ et conclure g divise $(2n-1)!$. . . . . $\boxed{1}$

c) Si $n = 3$ alors, vu la question **9**, -2 n'est pas une valeur possible pour la trace d'un élément de G donc g divise $(2n-2)! = 24$. . . . . $\boxed{3}$

13. a) Soit $\sigma \in \mathfrak{S}_n$, on considère $\mathcal{M}_\sigma = \{M \in \mathrm{GL}_n(\mathbb{Z}) \mid MT_i = \pm T_{\sigma_i}\}$. $\mathcal{M}_\sigma$ est la réunion de deux ensembles de même cardinal, $\mathcal{M}_\sigma^+$, ensemble des matrices de déterminant 1 et $\mathcal{M}_\sigma^-$, ensemble des matrices de déterminant -1. Or $\mathrm{Card}\,\mathcal{M}_\sigma = 2^n$ donc $\mathrm{Card}\,\mathcal{M}_\sigma^+ = 2^{n-1}$.
Soit $G = \bigcup_{\sigma \in \mathfrak{S}_n} M_\sigma^+$ alors $\mathrm{Card}\,G = 2^{n-1}n!$ et G est l'ensemble des matrices de $\mathrm{SL}_n(\mathbb{Z})$ qui conservent T qui est bien un sous-groupe de $\mathrm{SL}_n(\mathbb{Z})$. . . . . $\boxed{4}$

b) Le cardinal maximal cherché est donc 24. . . . . $\boxed{0}$

14. a) On a $M^p = I_n$ donc

$$(I_n + mN)^p = I_n + pmN + m^2 H = I_n$$

donc, en simplifiant par $m \neq 0$, $pN = -mH$ or les coefficients de la matrice N sont premiers dans leur ensemble donc il existe des $a_{ij} \in \mathbb{Z}$ tels que $\sum_{i,j} a_{ij} n_{ij} = 1$ (où $N = (n_{ij})$. On a alors $-m \sum_{i,j} a_{ij} h_{ij} = p$ i.e. m divise p. . . . . $\boxed{4}$

b) On a donc soit $m = 1$ soit $m = p$.
Si $p \geqslant 3$ et $m = p$ alors, en reprenant le calcul ci-dessus, on obtient $p^2 N = -\sum_{k=2}^{p} p^k \binom{p}{k} N^k = p^3 K$ car $p | \binom{p}{k}$ pour $k \in [\![1, p-1]\!]$ ce qui est impossible.
Conclusion : $m = 1$ ou $m = p = 2$. . . . . $\boxed{3}$

15. a) Si $g = 1$, c'est immédiat, supposons $g \geqslant 2$. On sait que, pour tout élément M de G, on a $M^g = I_n$ donc l'ordre q de M est un diviseur de g.
Supposons que $\varphi_{n,3}(M) \equiv I_n[3]$, $M \neq I_n$. Si p est un diviseur premier de q alors $M^{q/p}$ est d'ordre p. On a $\varphi_{n,3}(M^{q/p}) \equiv I_n[3]$ donc $M^{q/p} = I_n + 3N$, d'où, si $N \neq 0$, $3|m$ (question **14.a**) ce qui est impossible (question **14.b**).

Conclusion : on a $M^{q/p} = I_n$ avec $q/p < q$ ce qui est impossible là encore car $\operatorname{ord}(M) = q$ donc $M = I_n$. . . . . $\boxed{5}$

b) $\varphi_{n,3}(G)$ est un sous-groupe de $\mathrm{SL}_n(\mathbb{Z}/3\mathbb{Z})$ de même cardinal que G.
Or on sait que $\operatorname{Card}\mathrm{GL}_n(\mathbb{Z}/3\mathbb{Z}) = (3^n-1)(3^n-3^2)(\ldots)(3^n-3^{n-1})$, en effet, il suffit de dénombrer les familles libres à n éléments dans $(\mathbb{Z}/3\mathbb{Z})^n$:
pour le premier vecteur, on a 3^n-1 choix (on prend n'importe quel vecteur non nul),
pour le deuxième vecteur, on choisit un vecteur non proportionnel au premier, ce qui donne 3^n-3 choix (on a enlevé tous les vecteurs portés par la droite engendrée par le premier vecteur),
pour le k-ième vecteur, on a 3^n-3^{k-1} choix (il faut enlever les vecteurs qui appartiennent à l'espace vectoriel engendré par les $k-1$ premiers vecteurs).
On peut alors faire une partition de $\mathrm{GL}_n(\mathbb{Z}/3\mathbb{Z})$ selon le déterminant : soit il vaut 1, soit il vaut $-1 = 2$. Par symétrie, chaque ensemble de la partition a le même nombre d'éléments donc

$$g|\operatorname{Card}\mathrm{SL}_n(\mathbb{Z}/3\mathbb{Z}) = \frac{1}{2}(3^n-1)(3^n-3)(\ldots)(3^n-3^{n-1}). \qquad \boxed{5}$$

c) $5760 = 80\times72$, on sait que g divise $40\times78\times72\times54 = 80\times72\times2\times3^4\times13$ vu la question précédente et qu'il divise aussi $8! = 80\times72\times7$ donc il divise leur P.G.C.D. qui est 5760. . . . . $\boxed{2}$

16. Soit $G = \{a_1, a_2, \ldots, a_n\}$ si $a \in G$ alors $a * a_i = a_j$ et l'application $i \in [\![1,g]\!] \mapsto j \in [\![1,g]\!]$ est une bijection σ. Soit $\varphi\ : a \in G \mapsto \sigma \in \mathfrak{S}_g$, on vérifie que φ est bien un morphisme de groupes injectif.
Si maintenant on considère $\psi\ : \sigma \in \mathfrak{S}_g \mapsto P_\sigma \in \mathrm{GL}_g(\mathbb{Z})$ où P_σ est la matrice de permutation associée à σ alors $\theta = \psi\circ\varphi$ est un morphisme de groupe injectif de G dans l'ensemble des matrices inversibles dans $\mathcal{M}_g(\mathbb{Z})$ (de déterminant ±1).

- Si g est impair alors $\theta(a)^g = I_n$ donc $\det\theta(a)^g = 1$ soit $\theta(g) \in \mathrm{SL}_n(\mathbb{Z})$ et par conséquent $\theta(G)$ est un sous-groupe de $\mathrm{SL}_n(\mathbb{Z})$ isomorphe à G.
- Si g est pair, cela pose plus de problèmes...
  On remarque que l'hyperplan $H = \{(x_1,\ldots,x_g) \in \mathbb{Q}^g \text{ tq } x_1+\cdots+x_g = 0\}$ est stable par toutes les applications $\theta(a)$. Ceci permet de co-trigonaliser par blocs les matrices $\theta(a)$ à l'aide d'une base de $\mathbb{Q}^g$ commençant par une base de H.
  Plus précisément, soit $P = \begin{pmatrix} I_{n-1} & (0) \\ -1\cdots-1 & 1\end{pmatrix}$: si $a \in G$ alors la matrice $P^{-1}\theta(a)P$ est de la forme $P^{-1}\theta(a)P = \begin{pmatrix} N(a) & X \\ 0\ldots0 & y\end{pmatrix}$ avec $X \in \mathcal{M}_{g-1,1}(\mathbb{Z})$ et $y \in \mathbb{Z}$. Puisque $\theta(a) \in \mathrm{GL}_g(\mathbb{Z})$, on a $N(a) \in \mathrm{GL}_{g-1}(\mathbb{Z})$ et l'application $a \mapsto N(a)$ est un morphisme de groupes de G dans $\mathrm{GL}_{g-1}(\mathbb{Z})$. Ce morphisme est injectif car si $N(a) = I_{g-1}$ alors $\theta(a)$ induit l'identité sur H, et aussi sur la droite vectorielle engendrée par le vecteur $(1,\ldots,1)$ qui est supplémentaire de H dans $\mathbb{Q}^g$, donc $\theta(a) = \mathrm{Id}_{Q^g}$ ce qui implique $a = 1_G$. On note alors $Q(a) = \begin{pmatrix} N(a) & (0) \\ 0\ldots0 & \det(N(a))\end{pmatrix}$: l'application $a \mapsto Q(a)$ est un morphisme de groupes de G dans $SL_g(\mathbb{Z})$, injectif. . . . . $\boxed{20}$

Morphismes de groupes et $\mathrm{SL}_n(\mathbb{Z})$

17. On sait déjà (question **6.b**) qu'il existe un morphisme surjectif de $\mathrm{SL}_2(\mathbb{Z})$ sur $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$. Or on peut décrire ce dernier ensemble :

$$\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z}) = \left\{ \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}}_{=I_2}, \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}_{=A_1}, \underbrace{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}}_{=A_2}, \underbrace{\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}}_{=A_3}, \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}}_{=A_4}, \underbrace{\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}}_{=A_5} \right\}$$

et on remarque que $A_1^2 = A_2^2 = A_3^2 = I_2$, $A_4^2 = A_5$ et $A_5 = A_4^2$, si on pose $\psi(A_1) = t_{1,2}$, $\psi(A_2) = t_{1,3}$, $\psi(A_3) = t_{2,3}$, $\psi(A_4) = (1,3,2)$ et $\psi(A_5) = (1,2,3)$ alors ψ est un morphisme surjectif de $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$ sur $\mathfrak{S}_3$.
Pour conclure, il suffit de prendre $\varepsilon\ : \sigma \in \mathfrak{S}_3 \mapsto \varepsilon(\sigma)$ signature de σ. $\varepsilon \circ \psi \circ \varphi$ est alors un morphisme surjectif de $\mathrm{SL}_2(\mathbb{Z})$ sur $\{-1, 1\} \sim \mathbb{Z}/2\mathbb{Z}$. 4

18. **a)** Par un calcul simple, on trouve $M_{ij}M_{jk}M_{ij}^{-1}M_{jk}^{-1} = M_{ik}$. 1

b) Si φ est un tel morphisme, alors $\varphi(M_{ik}) = \varphi(M_{ij})\varphi(M_{jk})\varphi(M_{ij})^{-1}\varphi(M_{jk})^{-1} = 1_G$. Les M_{ik} engendrant $\mathrm{SL}_n(\mathbb{Z})$, on en déduit $\varphi(M) = 1_G$ pour toute matrice $M \in \mathrm{SL}_n(\mathbb{Z})$.
Conclusion : tout morphisme de $\mathrm{SL}_n(\mathbb{Z})$ sur G est constant. 1

19. **a)** Soit $\{a_1, \dots, a_p\}$ la partie génératrice de G, on sait alors que tout morphisme φ de G dans H est déterminé de manière unique par $\varphi(a_i)$, $i \in [\![1, p]\!]$. Comme H est fini, il n'y a qu'un choix fini pour chaque valeur de $\varphi(a_i)$ donc il n'y a qu'un nombre fini de morphismes de G dans H (nombre majoré par $\operatorname{Card} H^p$). 1

b) Soit E l'ensemble des morphismes de G dans H. L'application $\psi\ : f \mapsto f \circ u$ de E dans E est injective car u est surjectif, et donc bijective car E est fini. Ainsi tout élément v de E est de la forme $v = f \circ u$ avec $f \in E$, d'où $\operatorname{Ker} u \subset \operatorname{Ker} v$. 4

20. On prend $H = \mathbb{Z}/p\mathbb{Z}$, $v = \varphi_{n,p}$ alors $\operatorname{Ker} u \subset \operatorname{Ker} \varphi_{n,p}$ soit $u(M) = I_n \Rightarrow M \equiv I_n[p]$ i.e. p divise tous les coefficients de la matrice $u(M) - I_n \in \mathcal{M}_n(\mathbb{Z})$ et ceci n'est possible que si $u(M) = I_n$.
Conclusion : u est injective donc bijective, i.e. tout morphisme de groupe surjectif de $\mathrm{SL}_n(\mathbb{Z})$ sur $\mathrm{SL}_n(\mathbb{Z})$ est bijectif. 7