

Le groupe $SL_n(\mathbf{Z})$

- 1) La seule propriété non triviale est la stabilité par inversion ; elle résulte de la formule $M^{-1} = \frac{{}^t \text{com}(M)}{\det(M)}$.
- 2) $E_{ij}^2 = 0$ donc $M_{ij}^m = I_n + mE_{ij}$ d'après la formule du binôme quand $m \in \mathbf{N}$. Cette relation est encore valable si $m = -p \in \mathbf{Z}^-$ car $(I_n + mE_{ij})M_{ij}^p = (I_n + mE_{ij})(I_n + pE_{ij}) = I_n$, d'où $I_n + mE_{ij} = M_{ij}^{-p} = M_{ij}^m$.
- 3) $\text{col}_j(MM_{ij}^m) = \text{col}_j(M) + m\text{col}_i(M)$. Les autres colonnes sont inchangées.
- 4) Par associativité du pgcd, il suffit de prouver le résultat quand $n = 2$. Dans ce cas on utilise l'algorithme suivant, dérivé de l'algorithme d'Euclide :
 1. Si $a_1 \geq 0$ et $a_2 = 0$ il n'y a rien à faire.
 2. Si $a_1 < 0$ et $a_2 = 0$, on effectue successivement les opérations élémentaires $C_2 \leftarrow C_2 + C_1$, $C_1 \leftarrow C_1 - 2C_2$ et $C_2 \leftarrow C_2 + C_1$ qui transforment $(a_1, 0)$ en $(-a_1, 0)$.
 3. Si $a_2 \neq 0$, soit $a_1 = qa_2 + r$ la division euclidienne de a_1 par a_2 . Les opérations élémentaires $C_1 \leftarrow C_1 - qC_2$, $C_2 \leftarrow C_2 + C_1$, $C_1 \leftarrow C_1 - C_2$, $C_2 \leftarrow C_2 + C_1$ transforment (a_1, a_2) en $(-a_2, r) = (a'_1, a'_2)$ avec $|a'_2| < |a_2|$ et $\text{pgcd}(a'_1, a'_2) = \text{pgcd}(a_1, a_2)$.

En itérant l'étape 3 tant que possible, on aboutit en un nombre fini d'étapes à l'un des cas de terminaison 1 ou 2 puisque la suite des valeurs absolues du deuxième coefficient est à valeurs dans $\mathbf{N}$, strictement décroissante.

- 5) Il est clair que $M_{ij} \in SL_n(\mathbf{Z})$ pour tous i, j distincts. Notons G_n le sous-groupe de $SL_n(\mathbf{Z})$ engendré par les matrices M_{ij} . L'algorithme de la question précédente peut être généralisé à une matrice rectangulaire à coefficients entiers quelconque : si $M \in \mathcal{M}_{n,p}(\mathbf{Z})$ alors il existe une suite d'opérations élémentaires sur les colonnes qui transforme M en une matrice de la forme : $M_1 = \begin{pmatrix} d & 0 \dots 0 \\ X & N \end{pmatrix}$ avec $d \in \mathbf{N}$, $X \in \mathcal{M}_{n-1,1}(\mathbf{Z})$, $N \in \mathcal{M}_{n-1,p-1}(\mathbf{Z})$, et il existe une matrice $P \in G_n$ telle que $M_1 = MP$ (P est le produit des matrices des transformations effectuées). Dans le cas particulier où $M \in SL_n(\mathbf{Z})$, on a $\det(M_1) = d \det(N) = \det(M) = 1$ d'où $d_1 = 1$ et $N \in SL_{n-1}(\mathbf{Z})$.

Montrons alors par récurrence sur $n \geq 2$ que $G_n = SL_n(\mathbf{Z})$: pour $n = 2$ et $M \in SL_2(\mathbf{Z})$, avec les notations ci-dessus on a $N = (1)$, soit $M_1 = I + xE_{21} = M_{21}^x \in G_2$, puis $M = M_1P^{-1} \in G_2$. Pour $n \geq 3$, toujours avec les mêmes notations, on a $N \in G_{n-1}$ par hypothèse de récurrence, donc la matrice $Q = \begin{pmatrix} 1 & 0 \dots 0 \\ (0) & N \end{pmatrix}$ appartient à G_n (c'est un produit de matrices élémentaires comme l'est N). Et $M_1Q^{-1} = \begin{pmatrix} 1 & 0 \dots 0 \\ X & I_{n-1} \end{pmatrix}$ appartient aussi à G_n car elle se déduit de I_n par addition à la première colonne de multiples entiers des autres colonnes. Finalement $M = (M_1Q^{-1})QP^{-1} \in G_n$, ce qui achève la démonstration.

6a) Évident.

- 6b) Il s'agit de prouver que si $M \in \mathcal{M}_n(\mathbf{Z})$ est telle que $\det(M) \equiv 1 \pmod{p}$ alors il existe $M' \in SL_n(\mathbf{Z})$ telle que $M \equiv M' \pmod{p}$ (c'est-à-dire les coefficients de $M - M'$ sont tous divisibles par p). On procède par récurrence sur n comme conseillé, sachant que le cas $n = 1$ est trivial. Soit donc $n \geq 2$ et $M \in \mathcal{M}_n(\mathbf{Z})$ telle que $\det(M) = 1 + kp$ avec $k \in \mathbf{Z}$. En reprenant la première partie de la réponse à la question 5, on considère une matrice $P \in G_n$ telle que $M_1 = MP$ soit de la forme $M_1 = \begin{pmatrix} d & 0 \dots 0 \\ X & N \end{pmatrix}$. Soit $d' = \det(N)$, donc $dd' = 1 + kp$. On considère la matrice $D = \begin{pmatrix} d'(1 - kp) & kp & 0 \dots 0 \\ -kp & d & \\ (0) & & I_{n-2} \end{pmatrix} \in SL_n(\mathbf{Z})$: on a $M_1D \equiv \begin{pmatrix} 1 & 0 \dots 0 \\ X' & N' \end{pmatrix} \pmod{p}$ où $X' = d'X$ et N' se déduit de N en multipliant sa première colonne par d . Donc $\det(N') = dd' = 1 + kp$, et par hypothèse de récurrence, N' est congrue modulo p à une matrice de $SL_{n-1}(\mathbf{Z})$. Il en résulte que M_1D est elle aussi congrue modulo p à une matrice de $SL_n(\mathbf{Z})$ et de même pour $M = (M_1D)D^{-1}P^{-1}$.

Sous-groupes finis de $SL_n(\mathbf{Z})$

7a) Si $M \in G$ alors $M^g = I_n$ où $g = \text{card}(G)$, donc M admet un annulateur scindé à racines simples sur $\mathbf{C}$; elle est $\mathbf{C}$ -diagonalisable et ses valeurs propres sont des racines g -èmes de l'unité. Les valeurs propres de M^{-1} sont les inverses, donc les conjugués, des valeurs propres de M , d'où $\text{tr}(M^{-1}) = \overline{\text{tr}(M)} = \text{tr}(M)$ puisque M est à coefficients réels. Enfin, $|\text{tr}(M)| \leq n$ (somme de n complexes de module 1), et il y a égalité si et seulement si toutes les valeurs propres de M sont égales ($\mathbf{R}^+$ -colinéaires et de mêmes modules), soit $M = \lambda I_n$ avec $\lambda \in U_g \cap \mathbf{R}$. En particulier le seul élément de G de trace n est la matrice I_n , et le seul éventuel élément de G de trace $-n$ est la matrice $-I_n$ pour autant qu'elle appartiennent à G .

7b) C'est une somme de matrices symétriques définies positives.

7c) Si $N \in G$ alors ${}^tNUN = \sum_{M \in G} {}^t(MN)(MN) = U$ car G est invariant par l'application $M \mapsto MN$. Ainsi, l'endomorphisme canoniquement associé à N conserve les produits scalaires des vecteurs de la base canonique de $\mathbf{R}^n$; c'est un endomorphisme orthogonal.

8a) D'après la question précédente, G est un sous-groupe du groupe des rotations pour le produit scalaire associé à U . Si $g = \text{card}(G)$, G est isomorphe à un sous-groupe de U_g . Or les sous groupes d'un groupe cyclique sont cycliques, donc G l'est aussi par isomorphisme.

8b) Pour $M \in G$, l'endomorphisme canoniquement associé à M est une rotation d'angle θ et $2 \cos \theta = \text{tr}(M) \in \llbracket -2, 2 \rrbracket$. Donc $\theta \in \{0, \pm\pi/3, \pm\pi/2, \pm 2\pi/3, \pi\} + 2\pi\mathbf{Z}$, ce qui prouve que l'ordre de M est 1, 2, 3, 4 ou 6. Il en va de même du cardinal de G puisque c'est un groupe cyclique.

8c) Si M est une telle matrice alors $G = \{I, M\}$ est un sous-groupe fini de $SL_2(\mathbf{Z})$ auquel on peut appliquer le discours précédent. En particulier, $\text{ord}(M) = 2 \implies \text{tr}(M) = -2 \implies M = -I_2$. Réciproquement, $-I_2$ convient.

8d) De même, $\text{ord}(M) = 3 \implies \text{tr}(M) = -1$ et réciproquement, si $\text{tr}(M) = -1$ alors $\chi_M(M) = M^2 + M + I_2 = 0$ donc $M^3 = I_2$ et $M \neq I_2$ vu sa trace, d'où $\text{ord}(M) = 3$. On montre de même que $\text{ord}(M) = 4 \iff \text{tr}(M) = 0$ et $\text{ord}(M) = 6 \iff \text{tr}(M) = 1$.

8e) 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 : $\{I_2\}$, $\{\pm I_2\}$, $\{I_2, J, J^2\}$, $\{\pm I_2, \pm K\}$, $\{\pm I_2, \pm J, \pm J^2\}$.

9) Soit $M \in SL_3(\mathbf{Z})$ d'ordre fini et G le groupe engendré par M . Si U désigne la matrice définie en **7b** alors M est une matrice orthogonale positive pour le produit scalaire associé, donc représente une rotation dont l'angle θ vérifie $1 + 2 \cos \theta = \text{tr}(M) \in \llbracket -1, 3 \rrbracket$.

Pour $\text{tr}(M) = -1$ on a $\theta \equiv \pi \pmod{2\pi}$ et $\text{ord}(M) = 2$.
 Pour $\text{tr}(M) = 0$ on a $\theta \equiv \pm \frac{2}{3}\pi \pmod{2\pi}$ et $\text{ord}(M) = 3$.
 Pour $\text{tr}(M) = 1$ on a $\theta \equiv \pm \frac{1}{2}\pi \pmod{2\pi}$ et $\text{ord}(M) = 4$.
 Pour $\text{tr}(M) = 2$ on a $\theta \equiv \pm \frac{1}{3}\pi \pmod{2\pi}$ et $\text{ord}(M) = 6$.
 Pour $\text{tr}(M) = 3$ on a $\theta \equiv 0 \pmod{2\pi}$ et $\text{ord}(M) = 1$.

Il reste à vérifier qu'il existe effectivement des matrices dans $SL_3(\mathbf{Z})$ ayant les traces indiquées : il suffit pour cela de prendre les matrices trouvées à la question précédente et de les compléter par un 1 en bas à droite.

10a) $\text{tr}(M * M') = \text{tr}(M) \text{tr}(M')$.

10b) $(MN) * (M'N') = (MM') * (NN')$.

10c) Résulte de la relation précédente.

11a) Pour $N \in G$ on a $NS = S$ (cf. **7c**), d'où $S^2 = gS$. Donc S/g est une matrice de projection, de trace entière égale à son rang, d'où $\text{tr}(S) = g \text{rg}(S)$.

11b) Pour $M = (a_{ij}) \in GL_n(\mathbf{R})$ et $i_1, \dots, i_r, j_1, \dots, j_r \in \llbracket 1, n \rrbracket^r$ on a $(M^{*r})_{(i_1, \dots, i_r), (j_1, \dots, j_r)} = a_{i_1, j_1} \times \dots \times a_{i_r, j_r}$. Donc si $M^{*r} = I_{n^r}$ alors pour $i, j \in \llbracket 1, n \rrbracket$ on a $a_{ij} \times a_{i1}^{r-1} = \delta_{ij}$ (symbole de Kronecker). En particulier tous les a_{ii} sont non nuls et égaux à un même réel λ avec $\lambda^r = 1$, et tous les a_{ij} tels que $i \neq j$ sont nuls. Ainsi,

$M \in \text{Ker } \psi_r \implies M = \lambda I_n$ avec $\lambda = \pm 1$ et $\lambda^r = 1$. On en déduit que $\text{Ker } \psi_r = \{\pm I_n\}$ quand $-I_n \in G$ et r est pair, et $\text{Ker } \psi_r = \{I_n\}$ dans tous les autres cas.

11c) $\sum_{M \in G} \text{tr}(M)^r = \sum_{M \in G} \text{tr}(M^{*r}) = \sum_{N \in \psi_r(G)} \text{tr}(N) \times \text{card}(\psi_r^{-1}(N)) = \text{card}(\text{Ker } \psi_r) \sum_{N \in \psi_r(G)} \text{tr}(N)$. D'après **11a** cette dernière somme est un multiple de $\text{card}(\psi_r(G))$, donc $\sum_{M \in G} \text{tr}(M)^r$ est un multiple de $\text{card}(\text{Ker } \psi_r) \text{card}(\psi_r(G)) = g$.

12a) $P \in \mathbb{Z}[X]$ car les traces des éléments de G sont entières. Avec la question précédente, on déduit que $\sum_{M \in G} P(\text{tr}(M))$ est un entier divisible par g . Or cette somme est égale à $P(n)$ car G contient exactement une matrice de trace $t_0 = n$ d'après **7a**.

12b) Les traces t_i sont des entiers distincts appartenant à $[-n, n-1]$, dont $(n - t_1) \dots (n - t_s)$ est un diviseur de $(n - (-n)) \dots (n - (n-1)) = (2n)!$. On peut retirer le facteur $2n$ dans le cas g impair car $-I_n \notin G$ d'après le théorème de Lagrange, donc aucun t_i n'est égal à $-n$.

12c) Pour $n = 3$ on ne peut pas avoir $t_i = -n + 1 = -2$ d'après **9**. Il reste donc $(2n - 2)! = 24$.

13a) Soit G l'ensemble des matrices $n \times n$ telles que chaque ligne et chaque colonne contient un unique coefficient non nul, égal à ± 1 . G est un sous-groupe de $\mathcal{O}(n, \mathbb{R})$ de cardinal $2^n n!$ (fait bien connu ou vérification immédiate). La restriction du déterminant à G est un morphisme de groupes à valeurs dans $\{-1, 1\}$, surjectif. Donc $G \cap \text{SL}_n(\mathbb{Z})$ est un sous-groupe de $\text{SL}_n(\mathbb{Z})$ de cardinal $\frac{1}{2} \text{card}(G) = 2^{n-1} n!$.

13b) Le cardinal maximal est 24 au vu des deux question précédentes.

14a) D'après la formule du binôme, $I_n = (I_n + mN)^p = I_n + pmN + m^2H$ avec $H \in \mathcal{M}_n(\mathbb{Z})$. Donc les coefficients de pmN sont divisibles par m^2 et $m \neq 0$ car M n'est pas d'ordre 1, ce qui implique que les coefficients de pN sont divisibles par m . Donc m divise aussi le pgcd des coefficients de pN , et ce pgcd est p puisque le pgcd des coefficients de N est 1.

14b) Si $m \neq 1$ alors $m = p$ car p est premier. Supposons $p > 2$. Alors $I_n = (I_n + pN)^p = I_n + p^2N + \binom{p}{2}p^2N^2 + \dots + p^pN^p$ et toutes les matrices à partir de $\binom{p}{2}p^2N^2$ sont divisibles par p^3 tandis que p^2N ne l'est pas ; c'est absurde.

15a) Supposons $\varphi_{n,3}$ non injective et considérons $M \in \text{Ker } \varphi_{n,3}$ avec $M \neq I$. Soit q l'ordre de M et p un diviseur premier de q . Donc $M^{q/p}$ appartient à $\text{SL}_n(\mathbb{Z})$, est d'ordre p , et $M \equiv I_n \pmod{3}$ donc $M^{q/p} \equiv I_n \pmod{3}$. Ainsi, avec les notations de la question précédente on a $3 \mid m$, ce qui est absurde.

15b) $\text{GL}_n(\mathbb{Z}/3\mathbb{Z})$ est de cardinal $c = (3^n - 1) \dots (3^n - 3)$ (dénombrement classique des bases dans un ev de dimension finie sur un corps fini). Comme le déterminant, de $\text{GL}_n(\mathbb{Z}/3\mathbb{Z})$ dans $(\mathbb{Z}/3\mathbb{Z})^* = \{1 \pmod{3}, -1 \pmod{3}\}$, est surjectif, on a $\text{card}(\text{SL}_n(\mathbb{Z}/3\mathbb{Z})) = c/2$ et on vient de voir que G est isomorphe à un sous-groupe de $\text{SL}_n(\mathbb{Z}/3\mathbb{Z})$, d'où $\text{card}(G)$ divise $c/2$ d'après le théorème de Lagrange.

15c) En réunissant les résultats des questions **12b** et **15b**, on voit que g divise le pgcd de $6!$ et de $(3^4 - 1) \dots (3^4 - 3^3)/2$, et ce pgcd vaut 5760.

16) Soit $G = \{a_1, \dots, a_g\}$ un groupe fini de cardinal g . Si $i, j \in [1, g]$, on note $i * j$ l'entier défini par $a_i \cdot a_j = a_{i*j}$. Pour $a_i \in G$ soit l'application linéaire $\varphi(a_i) : \begin{cases} \mathbb{Q}^g & \longrightarrow \mathbb{Q}^g \\ (x_1, \dots, x_g) & \longmapsto (x_{1*i}, \dots, x_{g*i}) \end{cases}$ et soit $M(a_i)$ la matrice de $\varphi(a_i)$ dans la base canonique de $\mathbb{Q}^g$. On vérifie aisément que $a \mapsto M(a)$ est un morphisme de groupes de G dans $\text{GL}_g(\mathbb{Z})$ et qu'il est injectif. Ce morphisme répond à la question quand g est impair, car les éléments de G sont alors d'ordres impairs, donc les matrices $M(a)$ aussi, et une matrice de $\text{GL}_g(\mathbb{Z})$ d'ordre impair a un déterminant égal à 1. Par contre si g est pair, on ne peut pas garantir que $M(a) \in \text{SL}_g(\mathbb{Z})$ et ça peut être faux (par exemple si G est un groupe cyclique).

Dans le cas général, avec $g \geq 2$, on remarque que l'hyperplan $H = \{(x_1, \dots, x_g) \in \mathbb{Q}^g \text{ tq } x_1 + \dots + x_g = 0\}$ est stable par toutes les applications $\varphi(a)$. Ceci permet de co-trigonaliser par blocs les matrices $M(a)$ à l'aide d'une base

de $\mathbb{Q}^g$ commençant par une base de H . Plus précisément, soit $P = \begin{pmatrix} I_{n-1} & (0) \\ -1 \dots -1 & 1 \end{pmatrix}$: si $a \in G$ alors la matrice

$P^{-1}M(a)P$ est de la forme $P^{-1}M(a)P = \begin{pmatrix} N(a) & X \\ 0 \dots 0 & y \end{pmatrix}$ avec $X \in \mathcal{M}_{g-1,1}(\mathbb{Z})$ et $y \in \mathbb{Z}$. Puisque $M(a) \in \text{GL}_g(\mathbb{Z})$, on a $N(a) \in \text{GL}_{g-1}(\mathbb{Z})$ et l'application $a \mapsto N(a)$ est un morphisme de groupes de G dans $\text{GL}_{g-1}(\mathbb{Z})$. Ce morphisme

est injectif car si $N(a) = I_{g-1}$ alors $\varphi(a)$ induit l'identité sur H , et aussi sur la droite vectorielle engendrée par le vecteur $(1, \dots, 1)$ qui est supplémentaire de H dans $\mathbf{Q}^g$, donc $\varphi(a) = \text{id}_{\mathbf{Q}^g}$ ce qui implique $a = 1_G$. On note alors $Q(a) = \begin{pmatrix} N(a) & (0) \\ 0 \dots 0 & \det(N(a)) \end{pmatrix}$: l'application $a \mapsto Q$ est un morphisme de groupes de G dans $\text{SL}_g(\mathbf{Z})$, injectif.

Morphismes de groupes et $\text{SL}_n(\mathbf{Z})$

- 17)** Une matrice $M \in \text{SL}_2(\mathbf{Z}/2\mathbf{Z})$ représente un isomorphisme linéaire de $(\mathbf{Z}/2\mathbf{Z})^2$ et cet isomorphisme induit une permutation σ_M de $E = (\mathbf{Z}/2\mathbf{Z})^2 \setminus \{0(\text{mod } 2), 0(\text{mod } 2)\}$. L'application $M \mapsto \sigma_M$ est un morphisme injectif de $\text{SL}_2(\mathbf{Z}/2\mathbf{Z})$ dans le groupe symétrique S_E , donc c'est un isomorphisme car les deux groupes ont même cardinal fini (6). Alors l'application φ de $\text{SL}_2(\mathbf{Z})$ dans $\mathbf{Z}/2\mathbf{Z}$ qui à $M \in \text{SL}_2(\mathbf{Z})$ associe $0(\text{mod } 2)$ si $\sigma_{M(\text{mod } 2)}$ est une permutation paire et $1(\text{mod } 2)$ sinon, est un morphisme surjectif de $\text{SL}_2(\mathbf{Z})$ dans $\mathbf{Z}/2\mathbf{Z}$, d'après la question 6b.
- 18a)** $M_{ij}M_{jk}M_{ij}^{-1}M_{jk}^{-1} = M_{ik}$.
- 18b)** 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 $\text{SL}_n(\mathbf{Z})$, on en déduit $\varphi(M) = 1_G$ pour toute matrice $M \in \text{SL}_n(\mathbf{Z})$.
- 19a)** Soit G_1 une partie génératrice finie de G . Un morphisme de G dans H est connu dès qu'on connaît sa restriction à G_1 , et il y a un nombre fini de telles restrictions.
- 19b)** Soit E l'ensemble des morphismes de G dans H . L'application $f \mapsto f \circ u$ 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 $\text{Ker } u \subset \text{Ker } v$.
- 20)** $\text{SL}_n(\mathbf{Z})$ est engendré par une partie finie (l'ensemble des M_{ij}) donc on peut lui appliquer le résultat précédent : si u est un morphisme surjectif de $\text{SL}_n(\mathbf{Z})$ dans lui-même alors $\text{Ker } u$ est inclus dans tous les noyaux des morphismes de $\text{SL}_n(\mathbf{Z})$ dans un groupe fini. En particulier, en considérant le morphisme $\varphi_{n,p}$ avec p premier, on voit que si $M \in \text{Ker } u$ alors $M \equiv I_n \pmod{p}$ pour tout nombre premier p , ce qui implique $M = I_n$. Ainsi, u est injectif et donc bijectif.

Fin du problème