ALGÈBRE - LEÇON 108 : EXEMPLES DE PARTIES GÉNÉRATRICES D'UN GROUPE. APPLICATIONS

SIMON RICHE

1. Commentaires du jury (rapport 2024)

La leçon doit être illustrée par des exemples de groupes très variés, dont il est indispensable de donner des parties génératrices. La description ensembliste du groupe engendré par une partie doit être connue et les groupes monogènes et cycliques doivent être évoqués.

Les groupes $\mathbf{Z}/n\mathbf{Z}$ fournissent des exemples naturels tout comme les groupes de permutations, les groupes linéaires ou leurs sous-groupes (par exemple $\mathrm{SL}_n(\mathbf{K})$, $\mathrm{O}_n(\mathbf{R})$ ou $\mathrm{SO}_n(\mathbf{R})$). Ainsi, on peut s'attarder sur l'étude du groupe des permutations avec différents types de parties génératrices en discutant de leur intérêt (ordre, simplicité de $\mathcal{A}_5$ par exemple). On peut, en utilisant des parties génératrices pertinentes, présenter le pivot de Gauss, le calcul de l'inverse ou du rang d'une matrice, le groupe des isométries d'un triangle équilatéral. Éventuellement, il est possible de discuter des conditions nécessaires et suffisantes pour que $(\mathbf{Z}/n\mathbf{Z})^\times$ soit cyclique ou la détermination de générateurs du groupe diédral.

On illustre comment la connaissance de parties génératrices s'avère très utile dans certaines situations, par exemple pour l'analyse de morphismes de groupes, ou pour montrer la connexité par arcs de certains sous-groupes de $\mathrm{GL}_n(\mathbf{R})$.

Pour aller plus loin, on peut s'intéresser à la présentation de certains groupes par générateurs et relations. Il est également possible de parler du logarithme discret et de ses applications à la cryptographie (algorithme de Diffie–Hellman, cryptosystème de El Gamal).

2. Plan

Comme pour beaucoup de leçons d'algèbre, [Pe] est une référence incontournable sur ce sujet.

2.1. **Ce qui doit apparaître.** Définition et description du sous-groupe engendré par une partie.

Définition d'une partie génératrice.

Groupes monogènes et cycliques.

Description des générateurs d'un groupe cyclique.

Théorème chinois.

Le groupe des inversibles d'un corps fini (ou, plus généralement, tout sous-groupe fini du groupe des inversibles d'un corps) est cyclique.

Parties génératrices classiques du groupe symétrique $\mathfrak{S}_n$.

Date: Année 2024–2025.

Applications : sous-groupe dérivé, $\mathfrak{A}_n$ est simple si $n \geq 5$, tout automorphisme de $\mathfrak{S}_n$ est intérieur si $n \neq 6$.

Le groupe $\mathrm{SL}_n(k)$ est engendré par les transvections, et $\mathrm{GL}_n(k)$ est engendré par les transvections et les dilatations.

Applications : centre de $\mathrm{SL}_n(k)$ et de $\mathrm{GL}_n(k)$, description des composantes connexes de $\mathrm{SL}_n(k)$ et $\mathrm{GL}_n(k)$ pour $k = \mathbb{R}$ et $\mathbb{C}$, sous-groupes dérivés de $\mathrm{SL}_n(k)$ et $\mathrm{GL}_n(k)$, simplicité de $\mathrm{PSL}_n(k)$ (sauf si $(n, k) = (2, \mathbb{F}_2)$ ou $(2, \mathbb{F}_3)$).

Générateurs de $\mathrm{O}_n(\mathbb{R})$ et $\mathrm{SO}_n(\mathbb{R})$.

Applications : $\mathrm{SO}_n(\mathbb{R})$ est connexe par arcs, $\mathrm{SO}_3(\mathbb{R})$ est simple.

2.2. **Ce qui peut apparaître.** Exemple du groupe diédral : cf. Partie 5.

Générateurs de $\mathrm{O}(q)$ et $\mathrm{O}^+(q)$ pour q une forme quadratique non dégénérée générale. [1]

Simplicité de $\mathrm{PO}_n^+(\mathbb{R})$ pour $n \geq 5$. [2]

Description de $(\mathbb{Z}/n\mathbb{Z})^\times$ (en expliquant que ce groupe s'identifie aux automorphismes de $(\mathbb{Z}/n\mathbb{Z}, +)$), condition pour qu'il soit cyclique. (Ce résultat est énoncé dans [Pe, p. 84] ; sa démonstration ne fait intervenir que le contenu de [Pe, Chap. I, §7].)

Théorème de structure des groupes abéliens finis (ou de type fini).

Engendrement de $\mathrm{SL}_2(\mathbb{Z})$ par les matrices $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. [3]

Présentation d'un groupe par générateurs et relations. Exemples classiques.

3. Quelques questions bêtes auxquelles il faut absolument savoir répondre rapidement

(1) À quelle condition un produit de deux groupes cycliques est cyclique ? (Référence si nécessaire : [Go, §I.2.5, Exercice 4].)

(2) Que peut-on dire des représentations complexes d'un groupe monogène ?

(3) Montrer que si $n \geq 3$ le groupe $\mathfrak{A}_n$ est engendré par les familles suivantes :

   (a) les produits de 2 transpositions ;

   (b) les 3-cycles ;

   (c) les éléments de la forme σ^2 pour $\sigma \in \mathfrak{S}_n$.

   (Référence : pour les deux premiers cas, voir [Go, §I.2.5, Exercice 7]. Le troisième cas est proposé en exercice dans [Pe, p. 40].)

1. Voir [Pe, Chap. VIII].
2. Voir [Pe, Chap. VI, §7].
3. Voir [FGN1, Ex. 2.19] ou [FGN2, Ex. 3.15].

4. Exercices

4.1. **Groupes linéaires.**

Exercice 1. Montrer que si p est un nombre premier, le morphisme $\mathrm{SL}_n(\mathbb{Z}) \to \mathrm{SL}_n(\mathbb{F}_p)$ induit par la réduction modulo p est surjectif pour tout n.

Référence : [CG1, p. 61]. (Cet énoncé est en fait vrai plus généralement pour le morphisme $\mathrm{SL}_n(\mathbb{Z}) \to \mathrm{SL}_n(\mathbb{Z}/m\mathbb{Z})$ pour tout $m \geq 2$, cf. Exercice 10 de la fiche de la leçon 120.)

Exercice 2. Dans cet exercice on propose deux variantes d'énoncés concernant les morphismes de $\mathrm{GL}_n(k)$ vers un groupe abélien.

(1) Soit k un corps, soit $n \geq 1$, et soit $j \in \mathbb{Z}$. Le but de cette question est de montrer que si $\rho : \mathrm{GL}_n(k) \to k^\times$ est un morphisme de groupes tel que
$$\rho(\mathrm{diag}(\lambda, 1, \cdots, 1)) = \lambda^j$$
pour tout $\lambda \in k$ (où $\mathrm{diag}(\mu_1, \cdots, \mu_n)$ désigne la matrice diagonale de coefficients $\mu_1, \cdots, \mu_n$), alors $\rho(M) = \det(M)^j$ pour tout $M \in \mathrm{GL}_n(k)$.
   (a) Montrer que pour toute matrice diagonale M on a $\rho(M) = \det(M)^j$.
   (b) Montrer que ρ vaut 1 sur les matrices de transvection. (*Indication* : on pourra utiliser le comportement des matrices de transvection par rapport au produit.)
   (c) Conclure.

(2) Soit k un corps, soit $n \geq 1$, et supposons que $k \neq \mathbb{F}_2$ si $n = 2$. Soit G un groupe abélien, et soit $\rho : \mathrm{GL}_n(k) \to G$ un morphisme de groupes.
   (a) Montrer qu'il existe un morphisme de groupes $\tau : k^\times \to G$ tel que $\rho = \tau \circ \det$. (*Indication* : on pourra utiliser le résultat de l'Exercice 5 ci-dessous.)
   (b) Montrer que si k est fini et $G = k^\times$, alors il existe $q \in \mathbb{Z}$ tel que $\rho(M) = \det(M)^q$ pour tout $M \in \mathrm{GL}_n(k)$.

Référence : pour la deuxième variante, voir [Go, Chap. 3, §6, Problème 10].

Exercice 3. Soit k un corps, et soit $n \in \mathbb{Z}_{\geq 1}$. Pour $i, j \in \{1, \cdots, n\}$ et $\lambda \in k$, on pose
$$T_{i,j}(\lambda) = I_n + \lambda E_{i,j} \quad \in \mathrm{M}_n(k).$$

(1) Soit $M \in \mathrm{M}_n(k)$. Montrer que $\mathrm{rg}(M) = 1$ si et seulement si M est conjuguée soit à $\lambda E_{1,1}$ pour un $\lambda \in k^\times$, soit à $E_{1,2}$.

(2) Soit $M \in \mathrm{GL}_n(k)$. Montrer que les conditions suivantes sont équivalentes :
   (a) M est conjuguée à $T_{1,2}(1)$;
   (b) M est conjuguée à $T_{1,2}(\lambda)$ pour un $\lambda \in k^\times$;
   (c) $\mathrm{rg}(M - I_n) = 1$ et le polynôme caractéristique de M est $(X-1)^n$.

(3) On suppose que k est de caractéristique $p > 0$ et que $n = 2$. Montrer que $M \in \mathrm{GL}_2(k)$ est d'ordre p si et seulement si M est conjuguée à $T_{1,2}(1)$. En déduire que tout automorphisme de $\mathrm{GL}_2(k)$ stabilise la classe de conjugaison de $T_{1,2}(1)$.

Référence : Sujet MG 2013.

Exercice 4. (1) Soit G un groupe tel que $\mathscr{D}(G) = G$. Montrer que si $H \subset G$ est un sous-groupe tel que $G = H \cdot Z(G)$, alors $H = G$.

(2) Montrer que si k est un corps et n un entier positif tel que

$$(k, n) \notin \{(\mathbb{F}_2, 2), (\mathbb{F}_2, 3)\},$$

alors les sous-groupes distingués stricts de $\mathrm{SL}_n(k)$ sont exactement les sous-groupes de son centre.

(3) Que peut-on dire dans les cas $(k, n) = (\mathbb{F}_2, 2)$ et $(k, n) = (\mathbb{F}_2, 3)$?

Référence : `https://perso.univ-rennes1.fr/matthieu.romagny/agreg/exo/sous_groupes_distingues_de_SLn_et_GLn.pdf`.

Exercice 5. Montrer que $\mathscr{D}(\mathrm{GL}_n(k)) = \mathrm{SL}_n(k)$ dans les cas suivants :

(1) si k est de caractéristique différente de 2 ;

(2) si k est de cardinal au moins 4.

(3) si $n \geq 3$.

Qu'en est-il dans la seule configuration non couverte par ces différents cas (c'est-à-dire $n = 2$, $k = \mathbb{F}_2$) ?

Indications :

(1) dans le premier cas on pourra remarquer que la matrice $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^2$ est conjuguée à $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$;

(2) dans le deuxième cas, on pourra considérer le produit

$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \lambda^{-1} & 0 \\ 0 & \lambda \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1}$$

pour un $\lambda \in k$ différent de 1, 0 et -1 ;

(3) dans le troisième cas on pourra considérer le produit

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}^{-1}.$$

Référence : [Pe, Chap. IV, §3].

Exercice 6. Montrer que si $k \neq \mathbb{F}_2$, alors le groupe $\mathrm{GL}_n(k)$ est engendré par les matrices inversibles diagonalisables.

(*Indication* : on pourra remarquer que

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \alpha^{-1} & \alpha^{-1} \\ 0 & 1 \end{pmatrix}$$

si $\alpha \in k^\times$.)

Référence : [FGN2, Ex. 3.2].

4.2. **Groupes symétriques.**

Exercice 7. Décrire les sous-groupes distingués de $\mathfrak{S}_n$. (On pourra commencer par le cas $n \geq 5$.)

Référence : [Pe, p. 30].

Exercice 8. (1) Soit $n \geq 2$. Déterminer tous les morphismes de groupes de $\mathfrak{S}_n$ vers $\mathbb{C}^\times$. (*Réponse* : il n'y en a que 2 : le morphisme trivial et la signature.)

(2) En déduire quelles sont les représentations complexes de dimension 1 de $\mathfrak{S}_n$.

Exercice 9. Fixons $\sigma \in \mathfrak{S}_n$, et considérons

$$Z_{\mathfrak{S}_n}(\sigma) = \{\tau \in \mathfrak{S}_n \mid \sigma\tau = \tau\sigma\}.$$

(1) Montrer que si $\tau \in Z_{\mathfrak{S}_n}(\sigma)$, alors τ permute les supports des cycles apparaissant dans la décomposition de σ en produit de cycles à supports disjoints.

(2) Pour tout $j \geq 1$, notons a_j le nombre de cycles de longueur j dans la décomposition de σ en produit de cycles à supports disjoints. Montrer que

$$|Z_{\mathfrak{S}_n}(\sigma)| = \prod_{j \geq 1} a_j! j^{a_j}.$$

(3) En déduire le cardinal de la classe de conjugaison de σ.

Référence : [CG2, Chap. XIII, §§C.1.3–C.1.6].

Exercice 10. Le but de cet exercice est de calculer le nombre minimal de transpositions nécessaire pour écrire un élément de $\mathfrak{S}_n$ comme produit de transpositions. On propose 2 méthodes légèrement différentes. Pour $\sigma \in \mathfrak{S}_n$, on notera :

- $N_{\mathrm{c}}(\sigma)$ le nombre de cycles apparaissant dans la décomposition de σ en produit de cycles à supports disjoints (en comptant les cycles de longueur 1) ;
- $N_{\mathrm{o}}(\sigma)$ le nombre d'orbites de l'action du sous-groupe de $\mathfrak{S}_n$ engendré par σ sur $\{1, \cdots, n\}$;
- $N_{\mathrm{r}}(\sigma)$ le nombre minimal de transpositions nécessaire pour écrire σ comme produit de transpositions.

(1) Rappeler pourquoi $N_{\mathrm{c}}(\sigma) = N_{\mathrm{o}}(\sigma)$.

(2) Montrer que tout m-cycle s'écrit comme un produit de $m-1$ transpositions (pour $1 \leq m \leq n$).

(3) En déduire que $N_{\mathrm{r}}(\sigma) \leq n - N_{\mathrm{c}}(\sigma)$.

(4) *Première méthode* pour démontrer que $N_{\mathrm{r}}(\sigma) \geq n - N_{\mathrm{c}}(\sigma)$.

  (a) Montrer que pour toute transposition τ et tout $\sigma \in \mathfrak{S}_n$ on a $N_{\mathrm{c}}(\tau \circ \sigma) = N_{\mathrm{c}}(\sigma) \pm 1$.

  (b) En déduire que pout tout σ on a $N_{\mathrm{c}}(\sigma) \geq n - N_{\mathrm{r}}(\sigma)$ et conclure.

(5) *Deuxième méthode* pour démontrer que $N_{\mathrm{r}}(\sigma) \geq n - N_{\mathrm{c}}(\sigma)$. On fixe un corps k.

  (a) Montrer que si V un k-espace vectoriel de dimension finie et si $H_1, \cdots, H_r$ sont des hyperplans de V, alors

$$\dim(H_1 \cap \cdots \cap H_r) \geq \dim(V) - r.$$

(b) On note $\rho : \mathfrak{S}_n \to \mathrm{GL}_n(k)$ le morphisme de groupes envoyant une permutation sur la matrice de permutation correspondante. Montrer que pour tout $\sigma \in \mathfrak{S}_n$ on a

$$\dim \ker(\rho(\sigma) - \mathrm{id}) = N_{\mathrm{c}}(\sigma).$$

(c) Montrer que pour tout $\sigma \in \mathfrak{S}_n$ on a

$$\dim \ker(\rho(\sigma) - \mathrm{id}) \geq n - N_{\mathrm{r}}(\sigma),$$

et conclure.

(6) En déduire que le nombre minimal de transpositions nécessaires pour engendrer $\mathfrak{S}_n$ est $n-1$.

Référence : pour une autre méthode permettant de démontrer ce résultat, on pourra consulter [FGN1, Ex. 2.19].

Exercice 11 (Présentation du groupe symétrique par générateurs et relations)**.** Soit $n \geq 2$. Pour $i \in \{1, \cdots, n-1\}$ on on note s_i la transposition $(i, i+1)$. On note Γ_n le groupe donné par la présentation avec générateurs $r_1, \cdots, r_{n-1}$ et les relations suivantes :

- $r_i^2 = e$ pour tout $i \in \{1, \cdots, n-1\}$;
- $r_i r_j = r_j r_i$ pour tous $i, j \in \{1, \cdots, n-1\}$ tels que $|i-j| \geq 2$;
- $r_i r_{i+1} r_i = r_{i+1} r_i r_{i+1}$ pour tout $i \in \{1, \cdots, n-2\}$.

Le but de cet exercice est de montrer que l'application envoyant chaque r_i sur s_i induit un isomorphisme de groupes entre Γ_n et $\mathfrak{S}_n$.

(1) (a) Montrer que les éléments $(s_i : i \in \{1, \cdots, n-1\})$ vérifient les relations ci-dessus dans $\mathfrak{S}_n$.

(b) En déduire que l'application envoyant chaque r_i sur s_i induit un morphisme de groupes surjectif de Γ_n vers $\mathfrak{S}_n$.

(2) Pour tout $k \in \{1, \cdots, n-1\}$, on note H_k le sous-groupe de Γ_n engendré par $r_1, \cdots, r_k$. On note aussi $H_0 = \{e\}$. Montrer par récurrence sur k que pour tout $k \in \{0, \cdots, n-2\}$ on a

$$H_{k+1} = H_k \cup H_k r_{k+1} H_k.$$

(*Indication* : on pourra montrer que $H_k \cup H_k r_{k+1} H_k$ est stable par multiplication à gauche par chacun des r_j pour $j \in \{1, \cdots, k+1\}$.)

(3) Dans cette question on va montrer (encore par récurrence sur k) que pour tout $k \in \{0, \cdots, n-2\}$ on a $[H_{k+1} : H_k] \leq k+2$.

(a) Vérifier le cas $k = 0$.

(b) À partir de maintenant on fixe $k \in \{0, \cdots, n-3\}$ et on suppose que $[H_{k+1} : H_k] \leq k+2$. On note $\gamma_1, \cdots, \gamma_{k+2}$ une famille d'éléments de H_{k+1} tels que

$$H_{k+1} = \bigcup_{i=1}^{k+2} \gamma_i H_k.$$

Montrer que

$$\{g r_{k+2} g^{-1} : g \in H_{k+1}\} = \{\gamma_i r_{k+2} \gamma_i^{-1} : i \in \{1, \cdots, k+2\}\}.$$

(c) En déduire que

$$H_{k+2} = H_{k+1} \cup \bigcup_{i=1}^{k+2} \gamma_i r_{k+2} \gamma_i^{-1} \cdot H_{k+1}.$$

(*Indication* : on pourra utiliser la question (2).)

(d) En déduire que $[H_{k+2} : H_{k+1}] \leq k+3$ et conclure.

(4) Montrer que $|\Gamma_n| \leq n!$ et conclure.

Référence : [Wi, §2.8.1].

4.3. **Groupes abéliens.**

Exercice 12. Combien existe-t-il de morphismes de groupes de $\mathbb{Z}/n\mathbb{Z}$ vers $\mathbb{Z}/m\mathbb{Z}$? Lesquels sont injectifs ? Lesquels sont surjectifs ?

Exercice 13. On considère le groupe $\mathbb{U}$ des racines de l'unité dans $\mathbb{C}$.

(1) Montrer qu'il existe un isomorphisme de groupes $\mathbb{U} \cong \mathbb{Q}/\mathbb{Z}$.

(2) Montrer que $\mathbb{U}$ n'est pas de type fini.

(3) Décrire les sous-groupes de $\mathbb{U}$ de type fini.

Exercice 14. Montrer que si G est un groupe abélien engendré par n éléments, alors tout sous-groupe de G est engendré par au plus n éléments. (*Indication* : On pourra commencer par considérer le cas où $G = \mathbb{Z}^n$, et penser au théorème de la base adaptée.)

Cette propriété est-elle vraie pour les groupes non abéliens ? (On pourra penser notamment au groupe symétrique.)

4.4. **Autres.**

Exercice 15. Déterminer le sous-groupe dérivé du groupe diédral D_n. (En cas de besoin, voir le §5.1 ci-dessous pour des rappels sur les groupes diédraux.)

Exercice 16. Le but de cet exercice est de montrer que tout endomorphisme surjectif du groupe $\mathrm{SL}_2(\mathbb{Z})$ est un isomorphisme. On rappelle qu'un groupe est dit de type fini s'il est engendré par un nombre fini d'éléments. On utilisera le fait que $\mathrm{SL}_2(\mathbb{Z})$ est de type fini, cf. par exemple [FGN2, Ex. 3.15].

(1) Montrer que si G est un groupe de type fini et H est un groupe fini, alors il n'existe qu'un nombre fini de morphismes de groupes de G dans H.

(2) On veut montrer que si G est un groupe de type fini et H un groupe fini, si $f : G \to G$ est un morphisme surjectif, et si $g : G \to H$ est un morphisme, alors on a $\ker(f) \subset \ker(g)$.

(a) On fixe $a \in \ker(f)$. Montrer qu'il existe une suite $(b_n)_{n\geq 0}$ d'éléments de G tels que $f^n(b_n) = a$ pour tout $n \geq 1$.

(b) Montrer que si $m > n$ on a $(g \circ f^m(b_n)) = e$.

(c) En déduire que si $g(a) \neq e$ alors les morphismes $(g \circ f^n : n \geq 1)$ sont tous distincts.

(d) Conclure.

(3) Montrer que si $A \in \mathrm{SL}_2(\mathbb{Z}) \smallsetminus \{\mathrm{Id}\}$, alors il existe un groupe fini H et un morphisme $f : \mathrm{SL}_2(\mathbb{Z}) \to H$ tel que $f(A) \neq e$. (*Indication* : on pourra considérer la réduction modulo un nombre premier, et distinguer les cas où A est diagonale ou non.)

(4) Conclure.

Référence : [FGN2, Ex. 3.16].

5. Complément : sous-groupes finis des groupes linéaires

Le but de cette partie est de présenter des résultats concernant les sous-groupes finis des groupes $\mathrm{GL}_n(\mathbb{R})$ et $\mathrm{GL}_n(\mathbb{Q})$, principalement dans le cas $n = 2$. Ces résultats sont tirés de [FGN2, Ex. 3.17, 3.18, 3.19].

5.1. **Rappels sur les groupes diédraux.** Pour $n \geq 2$, on considère le polygône régulier dont les sommets sont les nombres complexes $e^{\frac{2ik\pi}{n}}$ pour $k \in \{0, \dots, n-1\}$. On définit alors D_n comme le sous-groupe des isométries de $\mathbb{R}^2$ (identifié à $\mathbb{C}$ de la manière usuelle) qui stabilisent ce polygône.

On note :

- r la rotation d'angle $\frac{2\pi}{n}$ (correspondant à la multiplication par $e^{\frac{2i\pi}{n}}$ dans $\mathbb{C}$),
- s la symétrie par rapport à l'axe des abscisses (correspondant à la conjugaison complexe dans $\mathbb{C}$).

Il est clair que r est d'ordre n, s est d'ordre 2, et ces éléments vérifient

$$srs = r^{-1}.$$

Les isométries (linéaires) de $\mathbb{R}^2$ sont soit des rotations, soit des réflexions orthogonales par rapport à une droite. On peut lister celles qui sont dans D_n :

- rotations : celles d'angles $\frac{2k\pi}{n}$ (c'est-à-dire $\mathrm{id}, r, r^2, \dots, r^{n-1}$) ;
- réflexions :
  (1) si n est pair, c'est-à-dire $n = 2m$ avec $m \in \mathbb{Z}_{\geq 1}$: celles d'axes passant par 0 et chaque sommet $e^{\frac{2ik\pi}{n}}$ avec $k \in \{0, \dots, m-1\}$, et celles d'axes passant par 0 et le milieu de l'arête $[e^{\frac{2ik\pi}{n}}, e^{\frac{2i(k+1)\pi}{n}}]$ pour $k \in \{0, \dots, m-1\}$.
  (2) si n est impair, c'est-à-dire $n = 2m+1$ avec $m \in \mathbb{Z}_{\geq 0}$: celles d'axes passant par 0 et chaque sommet $e^{\frac{2ik\pi}{n}}$ avec $k \in \{0, \dots, n-1\}$.

  Dans les deux cas, D_n contient n réflexions, qui sont les transformations $r^k s$ pour $k \in \{0, \dots, n-1\}$.

En particulier, de cette analyse on déduit le lemme suivant.

Lemme 1. Le groupe D_n est engendré par s et r, et est de cardinal $2n$.

Remarque. Dans le cas $n = 2$, on trouve que $\mathrm{D}_2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. C'est le seul cas où le groupe D_n est commutatif.

L'énoncé suivant exprime l'idée que D_n est "entièrement caractérisé", comme groupe, par les propriétés de r et s considérées ci-dessus.

Lemme 2. Soit $n \geq 2$. Soit G un groupe engendré par deux éléments u et v qui vérifient

$$uvu = v^{-1},$$

avec u d'ordre 2 et v d'ordre n. Si $n = 2$, on suppose de plus que u et v sont distincts. Alors il existe un isomorphisme de groupes

$$\mathrm{D}_n \xrightarrow{\sim} G$$

envoyant s sur u et r sur v.

Démonstration. Comme on l'a vu ci-dessus chaque élément de D_n s'écrit de manière unique sous la forme $s^a r^b$ avec $a \in \{0,1\}$ et $b \in \{0,\dots,n-1\}$. On considère l'application

$$\varphi : \mathrm{D}_n \to G$$

définie par

$$\varphi(s^a r^b) = u^a v^b$$

pour a, b comme ci-dessus.

Montrons que φ est un morphisme de groupes. Soient $g, g' \in \mathrm{D}_n$; il existe alors des éléments uniques $a, a' \in \{0,1\}$ et $b, b' \in \{0,\dots,n-1\}$ tels que $g = s^a r^b$, $g' = u^{a'} v^{b'}$. On a alors

$$\varphi(g) \cdot \varphi(g') = \varphi(s^a r^b) \cdot \varphi(s^{a'} r^{b'}) = u^a v^b u^{a'} v^{b'}.$$

Si $a' = 0$, en notant b'' l'unique élément de $\{0,\dots,n-1\}$ congru à $b + b'$ modulo n on a

$$u^a v^b u^{a'} v^{b'} = u^a v^{b+b'} = u^a v^{b''} = \varphi(s^a r^{b''}) = \varphi(s^a r^b \cdot s^{a'} r^{b'}) = \varphi(g \cdot g').$$

Si $a' = 1$, puisque $v^b u = u v^{-b}$ on a

$$u^a v^b u^{a'} v^{b'} = u^{a+1} v^{b'-b}.$$

Si on note a'', resp. b'', l'unique élement de $\{0,1\}$, resp. $\{0,\dots,n-1\}$, congru à $a+1$ modulo 2, resp. à $b' - b$ modulo n, alors on a

$$u^a v^b u^{a'} v^{b'} = \varphi(s^{a''} r^{b''}) = \varphi(s^a r^b \cdot s^{a'} r^{b'}) = \varphi(g \cdot g').$$

On a donc bien démontré que φ est un morphisme de groupes.

L'image de φ est un sous-groupe de G contenant u et v ; puisque ces éléments engendrent G par hypothèse, cette image est donc G ; en d'autres termes, φ est surjectif. Pour conclure, il reste à voir que φ est injectif. Considérons $g \in \ker(\varphi)$, et écrivons $g = s^a r^b$ avec $a \in \{0,1\}$ et $b \in \{0,\dots,n-1\}$. Si $a = 0$ alors

$$\varphi(g) = \varphi(r^b) = v^b.$$

Puisque v est d'ordre n, ceci implique que $b = 0$, et donc que $g = \mathrm{id}$ est l'élément neutre de D_n. Si $a = 1$, alors

$$\varphi(g) = \varphi(s r^b) = u v^b.$$

On a donc $uv^b = e$, c'est-à-dire $u = v^{-b}$. Puisque u est une puissance de v il commute à v, et donc $uvu^{-1} = v$. Puisque $u = u^{-1}$ et $uvu = v^{-1}$ on en déduit que $v = v^{-1}$, et donc $n = 2$. Mais l'égalité $u = v^{-b}$ montre qu'alors soit $u = e$ (ce qui est impossible car u est d'ordre 2) soit $u = v$, ce qu'on a exclu. Le cas $a = 1$ ne peut donc pas se produire, ce qui complète la preuve. □

Remarque. L'hypothèse supplémentaire dans le cas $n = 2$ est nécessaire, puisque le groupe $\mathbb{Z}/2\mathbb{Z}$ est engendé par les éléments $u = \overline{1}$ et $v = \overline{1}$ qui sont d'ordre 2 et vérifient $uvu = v^{-1}$, mais ce groupe n'est pas isomorphe à D_2, qui est d'ordre 4.

5.2. **Réductions.** Les énoncés suivants (dont les preuves sont basées sur la même idée, appliquée dans des contextes différents) permettent de ramener l'étude des sous-groupes finis de $\mathrm{GL}_n(\mathbb{R})$ à ceux de $\mathrm{O}_n(\mathbb{R})$, et celle des sous-groupes finis de $\mathrm{GL}_n(\mathbb{Q})$ à ceux de $\mathrm{GL}_n(\mathbb{Z})$. (Ici on rappelle que $\mathrm{GL}_n(\mathbb{Z})$ désigne le groupe des inversibles de l'anneau des matrices de taille n à coefficients dans $\mathbb{Z}$, qui consiste en les matrices à coefficients entiers et de déterminant ± 1.)

Lemme 3. (1) Soit G un sous-groupe fini de $\mathrm{GL}_n(\mathbb{R})$. Alors il existe $a \in \mathrm{GL}_n(\mathbb{R})$ tel que $a \cdot G \cdot a^{-1} \subset \mathrm{O}_n(\mathbb{R})$.

(2) Soit G un sous-groupe fini de $\mathrm{GL}_n(\mathbb{Q})$. Alors il existe $a \in \mathrm{GL}_n(\mathbb{Q})$ tel que $a \cdot G \cdot a^{-1} \subset \mathrm{GL}_n(\mathbb{Z})$.

Démonstration. (1) Notons $\langle -, - \rangle$ le product scalaire euclidien usuel sur $\mathbb{R}^n$. On rappelle que $\mathrm{O}_n(\mathbb{R})$ est le groupe des transformations qui préservent ce produit scalaire : on a

$$\mathrm{O}_n(\mathbb{R}) = \{a \in \mathrm{GL}_n(\mathbb{R}) \mid \forall u, v \in \mathbb{R}^n,\ \langle a \cdot u, a \cdot v \rangle = \langle u, v \rangle\}.$$

On définit une forme bilinéaire $\langle -, - \rangle_G$ sur $\mathbb{R}^n$ en posant, pour $u, v \in \mathbb{R}^n$,

$$\langle u, v \rangle_G = \sum_{g \in G} \langle g \cdot u, g \cdot v \rangle.$$

Il est facile de voir que tout élément de G préserve cette forme bilinéaire : pour tous $g \in G$ et $u, v \in \mathbb{R}^n$ on a $\langle g \cdot u, g \cdot v \rangle_G = \langle u, v \rangle_G$. Il est clair également que $\langle -, - \rangle_G$ est un produit scalaire (c'est-à-dire une forme bilinéaire symétrique définie positive). Par la classification des telles formes, il existe $a \in \mathrm{GL}_n(\mathbb{R})$ tel que pour tous $u, v \in \mathbb{R}^n$ on a

$$\langle u, v \rangle_G = \langle a \cdot u, a \cdot v \rangle.$$

Pour tous $g \in G$ et $u, v \in \mathbb{R}^n$ on a alors

$$\langle aga^{-1} \cdot u, aga^{-1} \cdot v \rangle = \langle ga^{-1} \cdot u, ga^{-1} \cdot v \rangle_G = \langle a^{-1} \cdot u, a^{-1} \cdot v \rangle_G = \langle u, v \rangle$$

et donc $aga^{-1} \in \mathrm{O}_n(\mathbb{R})$. Ce qui prouve que $a \cdot G \cdot a^{-1} \subset \mathrm{O}_n(\mathbb{R})$.

(2) L'idée est la même que pour (1), en utilisant le fait suivant. On considère le sous-ensemble $\mathbb{Z}^n \subset \mathbb{Q}^n$ consistant en les vecteurs à coordonnées entières. Alors

$$\mathrm{GL}_n(\mathbb{Z}) = \{a \in \mathrm{GL}_n(\mathbb{Q}) \mid a \cdot \mathbb{Z}^n = \mathbb{Z}^n\}.$$

(Ici, $a \cdot \mathbb{Z}^n$ désigne l'image de $\mathbb{Z}^n$ par l'application linéaire associée à a.)

On pose

$$\Lambda = \sum_{g \in G} g \cdot \mathbb{Z}^n \subset \mathbb{Q}^n.$$

Alors Λ est un $\mathbb{Z}$-module de type fini. Il est sans torsion (car inclus dans $\mathbb{Q}^n$), et donc libre. Puisqu'il contient $\mathbb{Z}^n$, son rang est au moins n. Et comme $n+1$ vecteurs de $\mathbb{Q}^n$ sont toujours linéairement liés sur $\mathbb{Q}$, et donc sur $\mathbb{Z}$, son rang est au plus n. Donc le rang de Λ est exactement n. Soit $(e_1, \dots, e_n)$ la base canonique de $\mathbb{Q}^n$, qui est aussi une $\mathbb{Z}$-base de $\mathbb{Z}^n$. Si $(f_1, \cdots, f_n)$ est une $\mathbb{Z}$-base de Λ, alors cette famille est également une famille libre du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}^n$, constituée de n vecteurs, et donc une $\mathbb{Q}$-base de $\mathbb{Q}^n$. Il existe donc une matrice $a \in \mathrm{GL}_n(\mathbb{Q})$ telle que $e_i = a \cdot f_i$ pour tout i, et donc $\mathbb{Z}^n = a \cdot \Lambda$.

Pour tout $g \in G$ on a $g \cdot \Lambda = \Lambda$, et donc

$$aga^{-1} \cdot \mathbb{Z}^n = ag \cdot \Lambda = a \cdot \Lambda = \mathbb{Z}^n.$$

Ce qui montre que $aga^{-1} \in \mathrm{GL}_n(\mathbb{Z})$, et donc $a \cdot G \cdot a^{-1} \subset \mathrm{GL}_n(\mathbb{Z})$. □

5.3. **Sous-groupes finis de** $\mathrm{GL}_2(\mathbb{R})$**.** Dans la preuve des énoncés qui suivent on va utiliser la structure du groupe $\mathrm{O}_2(\mathbb{R})$. Tout d'abord, rappelons que $\mathrm{SO}_2(\mathbb{R})$ est l'ensemble des matrices de rotation du plan ; il s'identifie (comme groupe) à $\mathbb{R}/\mathbb{Z}$ via l'application envoyant la classe d'un réel x sur la matrice

$$R(x) := \begin{pmatrix} \cos(2\pi x) & -\sin(2\pi x) \\ \sin(2\pi x) & \cos(2\pi x) \end{pmatrix}.$$

En particulier, ce groupe est commutatif. Par ailleurs, si $a \in \mathrm{O}_2(\mathbb{R}) \smallsetminus \mathrm{SO}_2(\mathbb{R})$ alors a est la matrice d'une réflexion orthogonale du plan, et pour tout $x \in \mathbb{R}$ on a

$$a \cdot R(x) \cdot a^{-1} = R(-x) = R(x)^{-1}. \tag{1}$$

On commence par décrire les (classes d'isomorphisme de) sous-groupes finis de $\mathrm{SL}_2(\mathbb{R})$.

Proposition 1. Tout sous-groupe fini de $\mathrm{SL}_2(\mathbb{R})$ est cyclique. Réciproquement, tout groupe cyclique est isomorphe à un sous-groupe de $\mathrm{SL}_2(\mathbb{R})$.

Démonstration. Soit G un sous-groupe fini de $\mathrm{SL}_2(\mathbb{R})$. D'après le Lemme 3(1), il existe $a \in \mathrm{GL}_2(\mathbb{R})$ tel que $a \cdot G \cdot a^{-1} \subset \mathrm{O}_2(\mathbb{R})$. On a alors automatiquement $a \cdot G \cdot a^{-1} \subset \mathrm{SO}_2(\mathbb{R})$. Comme expliqué ci-dessus on a un isomorphisme de groupes $\mathrm{SO}_2(\mathbb{R}) \cong \mathbb{R}/\mathbb{Z}$. Pour conclure la preuve de la première assertion, il suffit donc de montrer que tout sous-groupe fini de $\mathbb{R}/\mathbb{Z}$ est cyclique.

On va montrer plus précisément que les sous-groupes finis de $\mathbb{R}/\mathbb{Z}$ sont tous de la forme $(\frac{1}{n}\mathbb{Z})/\mathbb{Z}$ pour un $n \in \mathbb{Z}_{>0}$. En effet, soit H un tel sous-groupe, et soit n son cardinal. Alors si $h \in H$, on a $n \cdot h = 0$. Si $x \in \mathbb{R}$ est un élément dont la classe est h, cela signifie que $n \cdot x \in \mathbb{Z}$, c'est-à-dire $x \in \frac{1}{n}\mathbb{Z}$. On a donc montré que $H \subset (\frac{1}{n}\mathbb{Z})/\mathbb{Z}$. D'autre part, $(\frac{1}{n}\mathbb{Z})/\mathbb{Z}$ est de cardinal n ; cette inclusion est donc une égalité, ce qui conclut la preuve.

Finalement, il reste à voir que tout groupe cyclique peut se réaliser comme sous-groupe de $\mathrm{SL}_2(\mathbb{R})$; pour cela on remarque que si $n \in \mathbb{Z}_{>0}$ le sous-groupe formé des matrices $R(\frac{2k\pi}{n})$ avec $k \in \{0, \dots, n-1\}$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$. □

Passons maintenant aux sous-groupes de $\mathrm{GL}_2(\mathbb{R})$.

Proposition 2. Si G est sous-groupe fini de $\mathrm{GL}_2(\mathbb{R})$, alors soit G est cyclique, soit il est isomorphe à un groupe diédral D_n avec $n \geq 2$. Réciproquement, tout groupe cyclique ou diédral est isomorphe à un sous-groupe de $\mathrm{GL}_2(\mathbb{R})$.

Démonstration. D'après le Lemme 3(1), il existe $a \in \mathrm{GL}_2(\mathbb{R})$ tel que $a \cdot G \cdot a^{-1} \subset \mathrm{O}_2(\mathbb{R})$. Pour simplifier les notations on pose $G' = a \cdot G \cdot a^{-1}$; on veut donc démontrer que G' est cyclique ou diédral. Considérons l'intersection $G' \cap \mathrm{SO}_2(\mathbb{R})$. Il s'agit d'un sous-groupe de $\mathrm{SL}_2(\mathbb{R})$; d'après la Proposition 1 il est donc cyclique. Si $G' \subset \mathrm{SO}_2(\mathbb{R})$, G' est donc cyclique. Sinon, choisissons un générateur g de $G' \cap \mathrm{SO}_2(\mathbb{R})$, et un élément $h \in G' \smallsetminus \mathrm{SO}_2(\mathbb{R})$. D'après (1) on a $hgh^{-1} = g^{-1}$. En utilisant le Lemme 2, on obtient que le sous-groupe H de G' engendré par g et h est isomorphe à un groupe diédral. Pour conclure la preuve de la première assertion, il reste à voir que $H = G'$. Mais H contient $G' \cap \mathrm{SO}_2(\mathbb{R})$; on a donc des morphismes injectifs

$$H/(G' \cap \mathrm{SO}_2(\mathbb{R})) \hookrightarrow G'/(G' \cap \mathrm{SO}_2(\mathbb{R})) \hookrightarrow \mathrm{O}_2(\mathbb{R})/\mathrm{SO}_2(\mathbb{R}).$$

Mais le groupe $\mathrm{O}_2(\mathbb{R})/\mathrm{SO}_2(\mathbb{R})$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$; comme $H/(G' \cap \mathrm{SO}_2(\mathbb{R}))$ a au moins 2 éléments, ces injections sont des isomorphismes, ce qui implique que $H = G'$.

La deuxième assertion de la proposition est claire : on a déjà vu dans la Proposition 1 que tout groupe cyclique est isomorphe à un sous-groupe de $\mathrm{GL}_2(\mathbb{R})$, et par définition c'est aussi le cas pour tout groupe diédral. □

Remarque. Un autre cas classique dans lequel on sait décrire tous les sous-groupes finis d'un groupe de matrices est celui de $\mathrm{SO}_3(\mathbb{R})$; voir par exemple [CG2, Chap. XII]. En utilisant le Lemme 3(1), cela permet de décrire tous les sous-groupes finis de $\mathrm{SL}_3(\mathbb{R})$.

5.4. **Sous-groupes finis de** $\mathrm{GL}_2(\mathbb{Q})$**.** On va maintenant s'intéresser aux sous-groupes finis de $\mathrm{GL}_2(\mathbb{Q})$.

Lemme 4. Si $M \in \mathrm{GL}_2(\mathbb{Q})$ est d'ordre fini, alors cet ordre appartient à

$$\{1, 2, 3, 4, 6\}.$$

Réciproquement, il existe des matrices à coefficients entiers de chacun de ces ordres.

Démonstration. Soit r l'ordre de M. Alors M est annulée par le polynôme $X^r - 1$. En utilisant la formule classique

$$X^r - 1 = \prod_{d|r} \Phi_d$$

où Φ_d est le polynôme cyclotomique d'indice d, et le fait que ces polynômes sont irréductibles dans $\mathbb{Q}[X]$, on obtient que le polynôme minimal μ_M de M, qui est un diviseur de $X^r - 1$ à coefficients dans $\mathbb{Q}$, est un produit de polynômes cyclotomiques distincts. Par ailleurs, d'après le théorème de Cayley–Hamilton M est annulée par son polynôme caractéristique, donc $\deg(\mu_M) \leq 2$. On remarque ensuite (en utilisant la formule classique pour l'indicatrice d'Euler) qu'il existe :

- deux polynômes cyclotomiques de degré 1, à savoir Φ_1 et Φ_2 ;
- trois polynômes cyclotomiques de degré 2, à savoir Φ_3, Φ_4 et Φ_6.

Donc μ_M est soit égal soit à l'un de ces polynômes, soit au produit $\Phi_1 \cdot \Phi_2$. Dans tous les cas il divise soit $X^4 - 1$ soit $X^6 - 1$, donc M est annulé soit par $X^4 - 1$ (auquel cas M est d'ordre 1, 2 ou 4), soit par $X^6 - 1$ (auquel cas M est d'ordre 1, 2, 3 ou 6).

Il reste à exhiber des matrices à coefficients entiers d'ordre 1, 2, 3, 4 et 6. Bien sûr, I_2 est d'ordre 1 et $-\mathrm{I}_2$ est d'ordre 2. On vérifie facilement que la matrice

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \tag{2}$$

est d'ordre 4 et que la matrice

$$\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} \tag{3}$$

est d'ordre 6, de sorte que son carré est d'ordre 3. □

Remarque. Comme expliqué dans [FGN2, Ex. 3.18], pour tout k dans $\{2, 3, 4, 6\}$ il existe en fait *une infinité* de matrices dans $\mathrm{GL}_2(\mathbb{Z})$ qui sont d'ordre k. Il en existe également une infinité qui sont d'ordre infini.

Proposition 3. Tout sous-groupe fini de $\mathrm{GL}_2(\mathbb{Q})$ est isomorphe à l'un des groupes suivants : $\{1\}$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z}$, D_2, D_3, D_4, D_6. Réciproquement chacun de ces groupes peut être réalisé comme un sous-groupe de $\mathrm{GL}_2(\mathbb{Z})$.

Démonstration. Si G est un sous-groupe de $\mathrm{GL}_2(\mathbb{Q})$ alors c'est aussi un sous-groupe de $\mathrm{GL}_2(\mathbb{R})$, donc il est soit cyclique soit diédral d'après la Proposition 2. Par ailleurs, d'après le Lemme 4 les ordres de ses éléments sont 1, 2, 3, 4 ou 6, donc G est isomorphe à l'un des groupes cités dans l'énoncé.

Réciproquement, si $k \in \{1, 2, 3, 4, 6\}$, d'après le Lemme 4 il existe une matrice dans $\mathrm{GL}_2(\mathbb{Z})$ d'ordre k ; le sous-groupe engendré par cette matrice sera donc cyclique d'ordre k. Par ailleurs si M est l'une des matrices dans (2) ou (3) alors avec

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

on a $A \cdot M \cdot A^{-1} = M^{-1}$. Donc le sous-groupe engendré par A et M est isomorphe à D_4 dans le premier cas, et à D_6 dans le deuxième, d'après le Lemme 2. De la même manière on exhibe des sous-groupes isomorphes à D_2 ou D_3 en partant du carré des matrices M considérées ci-dessus. □

5.5. **Sous-groupes de** $\mathrm{GL}_n(\mathbb{Q})$**.** On termine avec un résultat (moins précis) concernant les sous-groupes finis de $\mathrm{GL}_n(\mathbb{Q})$ pour n général. La preuve utilisera le fait suivant.

Lemme 5. Soit $M \in \mathrm{M}_n(\mathbb{Z})$. Si M est annulée par un polynôme $P \in \mathbb{C}[X]$ dont les racines (complexes) sont simples et de module strictement inférieur à 1, alors $M = 0$.

Démonstration. Soient M et P comme dans l'énoncé. Puisque P est (scindé) à racines simples, M est diagonalisable sur $\mathbb{C}$: il existe $Q \in \mathrm{GL}_n(\mathbb{C})$ et $D \in \mathrm{M}_n(\mathbb{C})$ diagonale telles que $M = QDQ^{-1}$. De plus, les coefficients de D sont des racines de P, donc des nombres complexes de module strictement inférieur à 1. On a donc $M^k \xrightarrow[k\to+\infty]{} 0$. Considérant la norme $\|\cdot\|_\infty$ sur $\mathrm{M}_n(\mathbb{C})$ donnée par

$$\|A\|_\infty = \max_{1 \le i,j \le n} |a_{i,j}|,$$

puisque chaque M^k est à coefficients entiers, et puisque $\|M^k\|_\infty < 1$ pour k assez grand, on a $M^k = 0$ pour k assez grand. Donc $D^k = 0$ pour k assez grand, ce qui implique que $D = 0$ et donc $M = 0$. □

Dans l'énoncé suivant on considère le morphisme de groupes $\mathrm{GL}_n(\mathbb{Z}) \to \mathrm{GL}_n(\mathbb{F}_3)$ induit par le morphisme canonique $\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z} = \mathbb{F}_3$.

Proposition 4. Si G est un sous-groupe fini de $\mathrm{GL}_n(\mathbb{Z})$, alors la restriction du morphisme canonique $\mathrm{GL}_n(\mathbb{Z}) \to \mathrm{GL}_n(\mathbb{F}_3)$ à G est injective ; en particulier, G est isomorphe à un sous-groupe de $\mathrm{GL}_n(\mathbb{F}_3)$.

Démonstration. Soit $M \in G$, et supposons que M est dans le noyau du morphisme $\mathrm{GL}_n(\mathbb{Z}) \to \mathrm{GL}_n(\mathbb{F}_3)$ considéré ci-dessus. Alors il existe $N \in \mathrm{M}_n(\mathbb{Z})$ telle que $M = \mathrm{I}_n + 3 \cdot N$. D'autre part, soit q l'ordre de M. Alors N est annulée par le polynôme $P(X) = (1 + 3X)^q - 1$, dont les racines sont les nombres complexes de la forme $\frac{\omega - 1}{3}$ où ω est une racine q-ième de l'unité. Ce polynôme a q racines, qui sont donc simples, et elles sont toutes de module strictement inférieur à 1. D'après le Lemme 5 on a $N = 0$, et donc $M = \mathrm{I}_3$, ce qui conclut la preuve. □

Cette proposition implique que tout sous-groupe fini de $\mathrm{GL}_n(\mathbb{Z})$ est de cardinal au plus

$$|\mathrm{GL}_n(\mathbb{F}_3)| = (3^n - 1) \cdot (3^n - 3) \cdots (3^n - 3^{n-1}).$$

Puisque, pour chaque entier, il n'existe qu'un nombre fini de groupes (à isomorphisme près) de cardinal cet entier, on en déduit que $\mathrm{GL}_n(\mathbb{Z})$ n'a qu'un nombre fini de sous-groupes finis, à isomorphisme près. En utilisant le Lemme 3(2), ces résultats sont également vrais pour les sous-groupes finis de $\mathrm{GL}_n(\mathbb{Q})$.

6. Autres ressources sur cette leçon

6.1. **Fiches mises à disposition par des collègues.** `https://www.math.univ-paris13.fr/~boyer/enseignement/agreg/generatrices.pdf`
`http://math.univ-lyon1.fr/~germoni/agreg/generatrices.pdf`
`https://www.imo.universite-paris-saclay.fr/~harari/enseignement/agreg15/partgen.pdf`

6.2. **Sujets d'écrit en rapport avec la leçon.**

(1) La partie 4 du sujet MG 2014 porte sur les écritures "réduites" d'un élément de $\mathfrak{S}_n$ comme produit de transpositions de la forme $(k, k+1)$ avec $k \in \{1, \dots, n-1\}$. Cette partie est indépendante du reste du sujet, et peut fournir un complément et/ou une révision utile sur ce sujet.

(2) Le sujet MG 2013 utilise de façon importante le fait que les transvections engendrent $\mathrm{SL}_n(k)$, et certaines questions portent spécifiquement sur ces matrices (voir notamment l'Exercice 3). Une étude approfondie de ce sujet est conseillée également.

Références

[CG1] P. Caldero, J. Germoni, *Histoires hédonistes de groupes et de géométries, Tome II*, Calvage & Mounet, 2015.

[CG2] P. Caldero, J. Germoni, *Nouvelles histoires hédonistes de groupes et de géométries, Tome II*, Calvage & Mounet, 2018.

[FGN1] S. Francinou, H. Gianella, S. Nicolas, *Oraux X-ENS, algèbre 1*, Cassini, 2007.

[FGN2] S. Francinou, H. Gianella, S. Nicolas, *Oraux X-ENS, algèbre 2*, Cassini, 2006.

[Go] X. Gourdon, *Les maths en tête - Algèbre, 2ème édition*, Ellipses, 2009.

[Pe] D. Perrin, *Cours d'algèbre*, Ellipses, 1996.

[Wi] R. Wilson, *The finite simple groups*, Graduate Texts in Mathematics 251, Springer, 2009.