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

SIMON RICHE

1. Commentaires du jury (rapport 2022)

La description ensembliste du groupe engendré par une partie doit être connue et les groupes monogènes et cycliques doivent être évoqués. C'est une leçon qui doit être illustrée par des exemples très variés. 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 présenter le groupe $\mathrm{GL}(E)$ généré par des transvections et des dilatations en lien avec le pivot de Gauss, le calcul de l'inverse ou du rang (par action sur $M_{n,p}(\mathbf{K})$), le groupe des isométries d'un triangle équilatéral qui réalise S_3 par identifications des générateurs. 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 $\mathrm{GL}_n(\mathbf{R})$.

S'il le souhaite, le candidat peut s'intéresser à la présentation de certains groupes par générateurs et relations. Pour aller plus loin, 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 2022–2023.

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 : générateurs, et description des représentations (cf. Partie 5 ci-dessous).

Générateurs de $O(q)$ et $O^+(q)$ 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. 2.17] 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 converte 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'ordre $2n$.

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].

Exercice 17. Le but de cet exercice est d'étudier les sous-groupes finis de $\mathrm{GL}_2(\mathbb{R})$ et de $\mathrm{GL}_2(\mathbb{Q})$. [4]

(1) Rappeler pourquoi tout sous-groupe fini de $\mathrm{GL}_n(\mathbb{R})$ est conjugué à un sous-groupe de $\mathrm{O}_n(\mathbb{R})$.

(2) En déduire que tout sous-groupe fini de $\mathrm{SL}_2(\mathbb{R})$ est cyclique. (*Indication* : on pourra remarquer que $\mathrm{SO}_2(\mathbb{R})$ est isomorphe au groupe des nombres complexes de module 1.)

(3) En déduire que si G est un sous-groupe fini de $\mathrm{GL}_2(\mathbb{R})$, alors soit G est cyclique, soit il est isomorphe à un groupe diédral [5] D_n ($n \geq 2$). (*Indication* : on pourra remarquer que si $r \in \mathrm{SO}_2(\mathbb{R})$ et $s \in \mathrm{O}_2(\mathbb{R}) \smallsetminus \mathrm{SO}_2(\mathbb{R})$, alors $srs = r^{-1}$.)

(4) Montrer que les groupes diédraux se caractérisent comme les groupes finis dont la dimension minimale d'une représentation fidèle sur $\mathbb{R}$ et sur $\mathbb{C}$ est 2.

(5) Montrer que si $M \in \mathrm{GL}_2(\mathbb{Q})$ est d'ordre fini, alors cet ordre appartient à $\{1, 2, 3, 4, 6\}$. (*Indication* : on pourra montrer que le polynôme minimal de M est un produit de polynômes cyclotomiques distincts, qu'il est de degré au plus 2, et que les polynômes cyclotomiques de degré ≤ 2 sont ceux d'indice dans $\{1, 2, 3, 4, 6\}$.)

(6) En déduire que si G est un sous-groupe fini de $\mathrm{GL}_2(\mathbb{Q})$, il est isomorphe à 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.

(7) Vérifier réciproquement que chacun de ces groupes peut être réalisé comme un sous-groupe de $\mathrm{GL}_2(\mathbb{Q})$, et même [6] de $\mathrm{GL}_2(\mathbb{Z})$. (*Indication* : on pourra considérer notamment les matrices $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$.)

5. Complément : représentations des groupes diédraux

Référence : [CG2, §XIII.B].

5.1. **Groupes diédraux.** Pour $n \geq 2$, on considère le polygône régulier dont les sommets sont les nombres complexes $e^{\frac{2ik\pi}{n}}$ pour $k \in \{0, \cdots, n-1\}$. 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 $\mathbb{C}$).

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 :

4. Cet exercice est inspiré de [FGN2, Ex. 3.17–3.18]. Pour des résultats (moins précis) concernant $\mathrm{GL}_n(\mathbb{Q})$ pour $n \geq 3$, on pourra consulter également [FGN2, Ex. 3.19].

5. Si besoin, la définition des groupes diédraux est rappelée au §5.1.

6. En fait, il n'est pas difficile de voir que tout sous-groupe fini de $\mathrm{GL}_n(\mathbb{Q})$ est conjugué à un sous-groupe de $\mathrm{GL}_n(\mathbb{Z})$: cela découle du fait que si $g_1, \cdots, g_m$ sont des éléments de $\mathrm{GL}_n(\mathbb{Q})$, il existe $h \in \mathrm{GL}_n(\mathbb{Q})$ tel que chacun des hg_ih^{-1} appartient à $\mathrm{GL}_n(\mathbb{Z})$ si et seulement il existe un réseau de $\mathbb{Q}^n$ stable par chacun des g_i, et d'arguments similaires à ceux de la question (1).

- rotations : celles d'angles $\frac{2k\pi}{n}$ (c'est-à-dire $\mathrm{id}, r, r^2, \cdots, r^{n-1}$) ;
- 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 $k \in \{0, \cdots, m-1\}$, 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 $k \in \{0, \cdots, m-1\}$.
  (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 $k \in \{0, \cdots, n-1\}$.

  Dans les deux cas, on trouve les transformations $r^k s$ pour $k \in \{0, \cdots, n-1\}$.

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 $D_2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

5.2. **Quelques endomorphismes.** Notons D_n^+ l'intersection de D_n avec $\mathrm{SO}_2(\mathbb{R})$. Alors on a

$$\mathrm{D}_n^+ = \{r^k : k \in \{0, \cdots, n-1\}\},$$

donc D_n^+ est naturellement isomorphe à $\mathbb{Z}/n\mathbb{Z}$ via $\overline{k} \mapsto r^k$. Le sous-groupe D_n^+ est distingué dans D_n (puisque $\mathrm{SO}_2(\mathbb{R})$ est distingué dans $\mathrm{O}_2(\mathbb{R})$) et d'indice 2 ; on a donc $\mathrm{D}_n/\mathrm{D}_n^+ \cong \mathbb{Z}/2\mathbb{Z}$. En fait on peut être plus précis : on a un isomorphisme

$$\mathrm{D}_n^+ \rtimes \mathbb{Z}/2\mathbb{Z} \xrightarrow{\sim} \mathrm{D}_n,$$

qu'on peut par exemple choisir en envoyant $(x, \overline{k})$ sur xs^k. (Ce n'est pas le seul choix possible.) Puisqu'on a

$$srs^{-1} = r^{-1}, \tag{1}$$

on voit que via l'identification $\mathrm{D}_n^+ \cong \mathbb{Z}/n\mathbb{Z}$, l'action de $\mathbb{Z}/2\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$ apparaissant dans le produit semi-direct ci-dessus est telle que l'unique élément non trivial de $\mathbb{Z}/2\mathbb{Z}$ envoie $\overline{k}$ sur $\overline{-k}$.

Pour tout $j \in \{0, \cdots, n-1\}$, le groupe

$$\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$$

(pour l'action considérée ci-dessus) admet un endomorphisme envoyant $(\overline{k}, \overline{l})$ sur $(\overline{jk}, \overline{l})$. En conjuguant par l'isomorphisme $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \xrightarrow{\sim} \mathrm{D}_n$ considéré ci-dessus on en déduit un endomorphisme de D_n, qu'on notera φ_j. Cet endomorphisme vérifie

$$\varphi_j(r) = r^j, \quad \varphi_j(s) = s.$$

Remarque. L'endomorphisme φ_j est inversible si et seulement si j est inversible dans $\mathbb{Z}/n\mathbb{Z}$, c'est-à-dire si et seulement si j est premier avec n.

5.3. **Classes de conjugaison.** On cherche maintenant à décrire les classes de conjugaison dans D_n. Celles-ci sont composées soit uniquement de rotations, soit uniquement de réflexions. Pour déterminer les classes de conjugaison de rotations, on remarque que deux rotations conjuguées dans $\mathrm{O}_2(\mathbb{R})$ ont même angle au signe près ; d'autre part, (1) montre que les rotations d'angle $\frac{2k\pi}{n}$ et $-\frac{2k\pi}{n}$ sont conjuguées dans D_n. Pour les classes de conjugaison de réflexions, on est ramené à considérer les orbites de D_n sur les axes de réflexions. On trouve alors les réponses suivantes.

(1) Cas où n est impair. On note alors $n = 2m+1$ avec $m \in \mathbb{Z}_{\geq 0}$.

(a) Classes de conjugaison de rotations : on a $\{1\}$ et les $\{r^k, r^{-k}\}$ pour $k \in \{1, \cdots, m\}$.

(b) Classes de conjugaison de réflexions : il n'y en a qu'une, composée des $r^k s$ pour $k \in \{0, \cdots, n-1\}$.

En tout, on a donc $m+2$ classes de conjugaison.

(2) Cas où n est pair. On note alors $n = 2m$ avec $m \in \mathbb{Z}_{\geq 1}$.

(a) Classes de conjugaison de rotations : on a $\{1\}$, $\{r^m\}$ et les $\{r^k, r^{-k}\}$ pour $k \in \{1, \cdots, m-1\}$.

(b) Classes de conjugaison de réflexions : il y en a deux : celles dont l'axe passe par 2 sommets (les $r^{2k}s$ avec $k \in \{0, \cdots, m-1\}$) et celles dont l'axe passe par 2 milieux d'arêtes (les $r^{2k+1}s$ avec $k \in \{0, \cdots, m-1\}$).

En tout, on a donc $m+3$ classes de conjugaison.

5.4. **Dimension des représentations complexes irréductibles.**

Lemme 2. Toute représentation complexe irréductible de D_n est de dimension au plus 2.

Démonstration. Soit V une représentation irréductible de D_n (sur $\mathbb{C}$). Comme D_n^+ est abélien, la représentation de D_n^+ sur V (par restriction) est une somme directe de représentations de dimension 1. En particulier il existe une droite $V' \subset V$ stable par l'action de D_n^+. Alors le sous-espace $V' + s(V') \subset V$ est stable par l'action de D_n. Par irréductibilité on a $V = V' + s(V')$, et donc $\dim(V) \leq 2$. □

Remarque. Plus généralement, les arguments ci-dessus montrent que si G est un groupe fini possédant un sous-groupe abélien d'indice a, alors toute représentation irréductible complexe de V est de dimension $\leq a$.

Ce lemme implique que les représentations irréductibles de D_n sont de dimension 1 ou 2. Notons k_1 le nombre de représentations irréductibles de dimension 1 (à isomorphisme près), et k_2 le nombre de représentations irréductibles de dimension 2 (à isomorphisme près). On peut alors utiliser le fait que le nombre total de représentations irréductibles (à isomorphisme près), c'est-à-dire $k_1 + k_2$, est le nombre de classes de conjugaison de D_n (déterminé au §5.3), et que la somme des carrés de leurs dimensions (c'est-à-dire $k_1 + 4k_2$) est le cardinal de D_n, c'est-à-dire $2n$.

(1) Dans le cas où $n = 2m$ ($m \in \mathbb{Z}_{\geq 1}$) on obtient le système

$$\begin{cases} k_1 + k_2 = m + 3 \\ k_1 + 4k_2 = 4m \end{cases},$$

qui implique que $k_1 = 4$ et $k_2 = m - 1$.

(2) Dans le cas où $n = 2m+1$ ($m \in \mathbb{Z}_{\geq 0}$) on obtient le système

$$\begin{cases} k_1 + k_2 = m + 2 \\ k_1 + 4k_2 = 4m + 2 \end{cases},$$

qui implique que $k_1 = 2$ et $k_2 = m$.

5.5. **Représentations irréductibles de dimension 1.** On a toujours :

(1) la représentation triviale χ_{triv},

(2) la représentation déterminant $\chi_{\det}$ (qui vaut 1 sur D_n^+ et -1 sur $\mathrm{D}_n \smallsetminus \mathrm{D}_n^+$),

ces deux représentations étant non isomorphes. Dans le cas impair, ceci fournit toutes les représentations irréductibles de dimension 1.

Supposons maintenant que n est pair. On identifie l'ensemble des sommets du polygône régulier à $\{1, \cdots, n\}$ via $k \mapsto e^{\frac{2ik\pi}{n}}$. Puisque tout élément de D_n permute ces sommets, on en déduit un morphisme de groupes $\mathrm{D}_n \to \mathfrak{S}_n$, qu'on peut composer avec $\varepsilon : \mathfrak{S}_n \to \mathbb{C}^\times$ pour obtenir un morphisme $\chi_\varepsilon : \mathrm{D}_n \to \mathbb{C}^\times$, et donc une représentation de dimension 1. Puisque la permutation correspondant à r est un cycle de longueur n (donc paire), on a $\chi_\varepsilon(r) = -1$, ce qui montre que la représentation χ_ε n'est isomorphe ni à χ_{triv} ni à $\chi_{\det}$. Ensuite, la représentation $\chi_\varepsilon\chi_{\det}$ n'est isomorphe à aucune des représentations précédentes ; on a donc trouvé les 4 représentations de dimension 1 :

$$\chi_{\text{triv}},\ \chi_{\det},\ \chi_\varepsilon,\ \chi_\varepsilon\chi_{\det}.$$

Remarque. Dans le cas où n est pair, on peut également construire les représentations de dimension 1 de D_n de la façon suivante. Puisque n est pair il existe un (unique) morphisme de groupes surjectif $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$. En utilisant ce morphisme on construit un morphisme de groupes surjectif $\mathrm{D}_n \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Maintenant $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ admet quatre représentations irréductibles à isomorphisme près, qui sont toutes de dimension 1. En les composant avec la surjection $\mathrm{D}_n \to \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ on obtient les quatre représentations de dimension 1 de D_n.

5.6. **Représentations irréductibles de dimension 2.** On part de la représentation naturelle $\omega : \mathrm{D}_n \to \mathrm{GL}_2(\mathbb{R})$. Pour $j \in \{0, \cdots, n-1\}$, on pose $\omega_j := \omega \circ \varphi_j$. Alors chaque ω_j est une représentation de D_n de dimension 2. Si on note χ_{ω_j} le caractère de cette représentation, on a

$$\chi_{\omega_j}(r) = 2\cos\left(\frac{2j\pi}{n}\right), \tag{2}$$

puisque r agit via une rotation d'angle $\frac{2j\pi}{n}$.

(1) Cas n impair : on note $n = 2m+1$ ($m \in \mathbb{Z}_{\geq 0}$), et on se restreint au cas $j \in \{1, \cdots, m\}$. L'égalité (2) montre que les représentations ω_j pour $j \in \{1, \cdots, m\}$ sont 2 à 2 non isomorphes, et pas isomorphes non plus à une somme de représentations de dimension 1. On a donc trouvé les m représentations irréductibles de dimension 2.

(2) Cas n pair : on note $n = 2m$ ($m \in \mathbb{Z}_{\geq 1}$), et on se restreint au cas $j \in \{1, \cdots, m-1\}$. Encore une fois, l'égalité (2) montre que les représentations ω_j pour $j \in \{1, \cdots, m-1\}$ sont 2 à 2 non isomorphes. D'autre part r^2 agit non trivialement sur chacune de ces représentations (en fait, comme une rotation d'angle $\frac{4j\pi}{n}$), donc aucune d'elles ne peut être isomorphe à une somme de représentations de dimension 1.

5.7. **Table de caractères.** Cas $n = 2m+1$ impair :

	$\{1\}$	$\underset{(k\in\{1,\cdots,m\})}{\{r^k,r^{-k}\}}$	réflexions
χ_{triv}	1	1	1
$\chi_{\det}$	1	1	-1
$\underset{(j\in\{1,\cdots,m\})}{\omega_j}$	2	$2\cos(\frac{2kj\pi}{n})$	0

Cas $n = 2m$ pair :

	$\{1\}$	$\{r^m\}$	$\underset{(k\in\{1,\cdots,m\})}{\{r^k,r^{-k}\}}$	classe de s	classe de sr
χ_{triv}	1	1	1	1	1
$\chi_{\det}$	1	1	1	-1	-1
χ_ε	1	$(-1)^m$	$(-1)^k$	$(-1)^{m-1}$	$(-1)^m$
$\chi_\varepsilon\chi_{\det}$	1	$(-1)^m$	$(-1)^k$	$(-1)^m$	$(-1)^{m-1}$
$\underset{(j\in\{1,\cdots,m-1\})}{\omega_j}$	2	$2(-1)^j$	$2\cos(\frac{2kj\pi}{n})$	0	0

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 $k \in \{1, \cdots, n-1\}$. 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.