# 108 - Exemples de parties génératrices d'un groupe. Applications.

*Version raisonnable*

## 1 Généralités

**Définition 1.1.** *Soit $G$ un groupe et $P \subset G$ une partie. Le sous-groupe de $G$ engendré par $P$ est le plus petit sous-groupe (au sens de l'inclusion) de $G$ contenant $P$. On le note $\langle P \rangle$.*

**Remarque 1.2.** Ce sous-groupe est bien défini, et il est unique. On dispose en effet de deux caractérisations de $\langle P \rangle$ :

1. une description interne :
$$\langle P \rangle = \{g_1^{\varepsilon_1} \dots g_r^{\varepsilon_r} : g_i \in P, \varepsilon_i = \pm 1, \forall i\}.$$
2. une description externe :
$$\langle P \rangle = \bigcap_{\substack{H < G \\ P \subset H}} H.$$

**Exemples :**
- Le sous-groupe de $G$ engendré par l'ensemble vide est le sous-groupe réduit à l'élément neutre.
- Si $H < G$ est un sous-groupe, alors $\langle H \rangle = H$.
- Si $G = \mathbb{Z}$, on a $\langle \{1\} \rangle = \langle \{-1\} \rangle = \mathbb{Z}$, $\langle \{2\} \rangle = 2\mathbb{Z}$ est le sous-groupe des entiers pairs, et $\langle \{2;3\} \rangle = \mathbb{Z}$.

**Définition 1.3.** *Soit $G$ un groupe. Le sous-groupe dérivé de $G$, noté $D(G)$, est le sous-groupe de $G$ engendré par les commutateurs de $G$, i.e. les éléments de la forme $[g,h] := g \cdot h \cdot g^{-1} \cdot h^{-1}$.*

**Proposition 1.4.** *Le sous-groupe $G(G) < G$ est distingué, et $G^{\text{ab}} := G/D(G)$ est le plus grand quotient abélien de $G$, au sens suivant : pour tout groupe abélien $A$ muni d'un morphisme $\varphi : G \to A$, il existe un unique morphisme $\overline{\varphi} : G^{\text{ab}} \to A$ tel que $\varphi = \overline{\varphi} \circ \pi$, où $\pi : G \to G^{\text{ab}}$ est la surjection canonique.*

**Définition 1.5.** *On dit qu'une partie $P \subset G$ est génératrice si $\langle P \rangle = G$.*

**Exemples :**
- $G$ est une partie génératrice de $G$.
- L'ensemble des commutateurs est une partie génératrice de $D(G)$.
- $\{1\}$ et $\{2;3\}$ sont des parties génératrices de $\mathbb{Z}$.
- Une partie génératrice du groupe sous-jacent à un espace vectoriel est une famille génératrice de cet espace.
- Soit $G$ un groupe fini, et $p$ le plus petit facteur premier de $|G|$. Alors toute partie de cardinal $> \frac{|G|}{p}$ est génératrice.

**Définition 1.6.** *Un groupe $G$ est dit de type fini s'il admet une partie génératrice finie.*

**Exemples :**
- Un groupe fini est de type fini.
- Pour tout $n \in \mathbb{N}$, $\mathbb{Z}^n$ est de type fini.
- Tout quotient d'un groupe de type fini est de type fini.
- Soit $H \triangleleft G$ un sous-groupe distingué. Si $H$ et $G/H$ sont de type fini, alors $G$ est de type fini.
- $Q$ et $\mathbb{R}$ ne sont pas de type fini.

## 2 Groupes abéliens

### 2.1 Groupes monogènes

**Définition 2.1.** *Un groupe $G$ est dit monogène s'il est engendré par un seul élément. Un groupe cyclique est un groupe monogène fini.*

**Exemples :**
- $\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$ sont monogènes.
- Un groupe d'ordre premier est cyclique.
- $\mathbb{Z}^2$ n'est pas monogène.

**Lemme 2.2.** *Soit $G$ un groupe et $H$ un sous-groupe du centre $Z(G)$ de $G$.*
*Si $G/H$ est monogène, alors $G$ est abélien.*

**Corollaire 2.3.** *Soit $p$ un nombre premier. Tout groupe d'ordre $p^2$ est abélien.*

**Proposition 2.4.** *Soit $G$ un groupe monogène, muni d'un générateur $g_0$.*
1. *Si $g_0$ est d'ordre fini (égal à $n$), alors $G$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.*
2. *Si $g_0$ n'est pas d'ordre fini, alors $G$ est isomorphe à $\mathbb{Z}$.*

Autrement dit, les groupes monogènes sont exactement les $\mathbb{Z}/n\mathbb{Z}$ et le groupe $\mathbb{Z}$.

**Proposition 2.5.** *Le groupe cyclique $\mathbb{Z}/n\mathbb{Z}$ admet exactement $\varphi(n)$ générateurs. Ces générateurs sont exactement les éléments $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ (avec $k \in \mathbb{Z}$) tels que $k$ est premier avec $n$.*

Un exemple fondamental de groupe cyclique est le suivant :

**Théorème 2.6.** ⋆
*Soit $K$ un corps et $G < (K^\times, \cdot)$ un sous-groupe fini.*
*Alors $G$ est cyclique.*

En particulier, si $\mathbb{F}_q$ est un corps fini de cardinal $q$, alors $\mathbb{F}_q^\times$ est cyclique.
**Application :** le problème du logarithme discret. Soit $G$ un groupe cyclique, donné avec un générateur $g_0$. Pour un élément $g \in G$, le problème du logarithme discret consiste à trouver un entier $n$ tel que $g = g_0^n$. Si $G = (\mathbb{Z}/p\mathbb{Z})^\times$, avec $p$ premier assez grand, on ne dispose pas d'algorithme très efficace pour résoudre ce problème.

C'est utilisé en pratique dans les deux protocoles suivants ($p$ et $g_0$ sont publics) :

— Diffie-Hellman : Alice et Bob souhaitent partager un secret. Pour cela, ils choisissent chacun un entier secret $a$ et $b$, puis ils échangent $g_0^a$ et $g_0^b$. Alors Alice et Bob disposent de l'élément secret commun $g_0^{ab}$. Un espion disposant de $g_0$, $g_0^a$, $g_0^b$ peut retrouver le secret commun s'il sait résoudre le problème du logarithme discret et donc calculer $a$ ou $b$.

— ElGamal : Alice souhaite envoyer un message secret $m \in G$ à Bob. Alice et Bob choisissent des entiers $a$ et $b$ secrètement, et publient $g_0^a$ et $g_0^b$. Alice envoie $m \cdot (g_0^b)^a = m \cdot g_0^{ab}$. Pour décoder, Bob multiplie ce qu'il a reçu par $(g_0^a)^{-b}$ et peut lire $m$. De nouveau, un espion peut lire $m$ s'il sait résoudre le problème du logarithme discret et calculer $b$ à partir de $g_0$ et $g_0^b$.

## 2.2 Groupes abéliens de type fini

**Théorème 2.7.** ⋆ *Soit $G$ un groupe abélien de type fini.*
*Il existe un unique $r \in \mathbb{N}$ et une unique suite d'entiers positifs $(d_1, \dots, d_s) \in \mathbb{N}^s$ tels que pour tout $i$, $d_i | d_{i+1}$ et*

$$G \xrightarrow{\sim} \mathbb{Z}^r \times \prod_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z}\,.$$

En particulier, tout groupe abélien de type fini est produit direct de groupes monogènes.

**Corollaire 2.8.** *Soit $G$ un groupe abélien de type fini. Soient $r$ et $s$ les entiers donnés par le théorème 2.7. Alors le nombre minimal de générateurs de $G$ est égal à $r + s$.*

Étudions maintenant le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$.

**Théorème 2.9.** ⋆⋆ *Soit $p$ un nombre premier et $n \geq 1$.*

1. *Si $p$ est impair, le groupe $(\mathbb{Z}/p^n\mathbb{Z})^\times$ est cyclique d'ordre $p^{n-1} \cdot (p-1)$.*
2. *Si $p = 2$, le groupe $(\mathbb{Z}/2^n\mathbb{Z})^\times$ est cyclique d'ordre $2^{n-1}$ si $n \leq 2$, il est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}$ si $n \geq 3$.*

**Corollaire 2.10.** *Pour tout $n \geq 1$, le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique si et seulement si $n = 1, 2, 4, p^m$ ou $2p^m$, avec $p$ premier impair.*

## 2.3 Autres groupes abéliens

**Théorème 2.11.** *Soit $G < (\mathbb{R}, +)$ un sous-groupe.*
*Alors $G$ est dense ou monogène (i.e. de la forme $\mathbb{Z} \cdot \alpha$, pour un $\alpha \in \mathbb{R}$).*

**Exemple :** Soit $x, y \in \mathbb{R}$, $y \neq 0$. Alors le sous-groupe $\langle x, y \rangle = \mathbb{Z} \cdot x + \mathbb{Z} \cdot y$ est dense dans $\mathbb{R}$ si et seulement si $\frac{x}{y} \notin \mathbb{Q}$.

**Corollaire 2.12.** ⋆ *On note $\mathbb{U} < (\mathbb{C}^\times, \cdot)$ le groupe des nombres complexes de module 1. Soit $G < (\mathbb{U}, \cdot)$.*
*Alors $G$ est dense ou il existe $n \in \mathbb{N}$ tel que $G$ est le groupe cyclique $\mathbb{U}_n$ des racines $n$-ièmes de l'unité.*

**Exemple :** ⋆ Soit $\alpha \in \mathbb{R}$ et $\zeta = e^{2i\pi\alpha}$.

— Si $\alpha \in \mathbb{Q}$, alors le sous-groupe $\langle \zeta \rangle$ de $\mathbb{U}$ est cyclique, isomorphe à $\mathbf{U}_n$, où $n$ est le dénominateur d'une écriture irréductible de $\alpha$.

— Sinon, le sous-groupe $\langle \zeta \rangle$ de $\mathbb{U}$ est dense. Mieux, il est équiréparti au sens suivant : pour tout $0 \leq a < b \leq 2\pi$,

$$\lim_{n \to +\infty} \frac{\left|\{k \in [\![-n; n]\!] : \zeta^k \in [e^{ia}; e^{ib}]\}\right|}{2n} = \frac{b-a}{2\pi}\,.$$

# 3 Exemples de groupes non abéliens

## 3.1 Groupe symétrique

**Théorème 3.1.** ⋆ *Le groupe $\mathfrak{S}_n$ est engendré par :*

1. *les cycles.*
2. *les transpositions.*
3. *les transpositions $(1\ i)$, $2 \leq i \leq n$.*
4. *les transpositions $(i\ i+1)$, $1 \leq i \leq n-1$.*
5. *la transposition $(1\ 2)$ et le cycle $(1\ 2\ \dots\ n)$.*

Ce théorème permet notamment de définir le morphisme signature $\varepsilon : \mathfrak{S}_n \to \{\pm 1\}$.

**Proposition 3.2.** *Soit $P \subset \mathfrak{S}_n$ une partie formée de transpositions. Si $\langle P \rangle = \mathfrak{S}_n$, alors $|P| \geq n - 1$.*

**Corollaire 3.3.** *Soit $K$ un corps, $E$, $F$ des $K$-espaces vectoriels et $f : E^n \to F$ une application $n$-linéaire. Si $f$ est alternée, alors $f$ est antisymétrique.*

Une application géométrique :

**Théorème 3.4.** ⋆ *On se place dans un espace affine euclidien de dimension 3.*

1. *Le groupe des isométries d'un tétraèdre régulier est isomorphe à $\mathfrak{S}_4$.*

2. *Le groupe des isométries directes d'un cube ou d'un octaèdre est isomorphe à $\mathfrak{S}_4$.*

Une application en théorie des groupes :

**Théorème 3.5.** ⋆⋆ *Pour tout $n \neq 6$, tout automorphisme de $\mathfrak{S}_n$ est intérieur.*

On rappelle que $\mathfrak{A}_n := \ker(\varepsilon : \mathfrak{S}_n \to \{\pm 1\})$.

**Théorème 3.6.** *Pour tout $n \geq 1$,*

1. *le groupe $\mathfrak{A}_n$ est engendré par les 3-cycles.*
2. *si $n \geq 5$, les 3-cycles sont conjugués dans $\mathfrak{A}_n$.*

**Corollaire 3.7.** *Pour tout $n \geq 1$, $D(\mathfrak{S}_n) = \mathfrak{A}_n$, et si $n \geq 5$, $D(\mathfrak{A}_n) = \mathfrak{A}_n$.*

Une application importante :

**Corollaire 3.8.** ⋆ *Pour tout $n \geq 3$, $n \neq 4$, le groupe $\mathfrak{A}_n$ est simple.*

## 3.2 Groupe linéaire

Soit $K$ un corps.
L'algorithme du pivot de Gauss assure le résultat suivant :

**Théorème 3.9.** ⋆

1. *Le groupe $\mathrm{SL}_n(K)$ est engendré par les matrices de transvections $I_n + \lambda \cdot E_{i,j} := \begin{pmatrix} 1 & 0 & \dots & \dots & 0 \\ 0 & 1 & \dots & \dots & 0 \\ \vdots & & \ddots & \lambda & 0 \\ 0 & 0 & \dots & \dots & 1 \end{pmatrix}$, où $E_{i,j}$ est la matrice dont tous les coefficients sont nuls, sauf le coefficient d'indice $(i,j)$ qui vaut 1 ; et $\lambda \in K^\times$ et $1 \leq i < j \leq n$.*
2. *Le groupe $\mathrm{GL}_n(K)$ est engendré par les matrices de transvections et les matrices de dilatations $D_i(\lambda) := I_n + (\lambda - 1) \cdot E_{i,i} = \mathrm{diag}(1, \dots, 1, \lambda, 1, \dots, 1)$, avec $\lambda \in K^\times$ et $1 \leq i \leq n$.*

**Corollaire 3.10.** *Les groupes $\mathrm{SL}_n(\mathbb{R})$, $\mathrm{GL}_n(\mathbb{R})^+$, $\mathrm{SL}_n(\mathbb{C})$ et $\mathrm{GL}_n(\mathbb{C})$ sont connexes par arcs.*

**Corollaire 3.11** (Frobenius-Zolotarev)**.** ⋆ *Soit $K = \mathbb{F}_q$ un corps fini à $q$ éléments. Si $a \in \mathbb{F}_q^\times$, on note $\left(\frac{a}{q}\right) = 1$ si $a$ est un carré dans $K$ et $-1$ sinon.*

*Alors pour tout $A \in \mathrm{GL}_n(\mathbb{F}_q)$, $\varepsilon(A) = \left(\frac{\det(A)}{q}\right)$.*

**Proposition 3.12.** *Si $n \geq 3$ (resp. $n \geq 2$), les matrices de transvections sont conjuguées dans $\mathrm{SL}_n(K)$ (resp. $\mathrm{GL}_n(K)$).*

**Corollaire 3.13.**
1. *Si $n > 2$ ou $|K| \neq 2$, alors $D(\mathrm{GL}_n(K)) = \mathrm{SL}_n(K)$.*
2. *Si $n > 2$ ou $|K| \neq 2, 3$, alors $D(\mathrm{SL}_n(K)) = \mathrm{SL}_n(K)$.*

**Théorème 3.14.** ⋆⋆ *Si $n > 2$ ou $|K| \neq 2, 3$, alors $\mathrm{PSL}_n(K)$ est simple.*

## 3.3 Groupe orthogonal

On rappelle qu'une réflexion (resp. un renversement) dans l'espace euclidien $\mathbb{R}^n$ est une symétrie orthogonale par rapport à un hyperplan (resp. un sous-espace de dimension $n-2$).

**Théorème 3.15.** ⋆⋆

1. *Pour tout $n \geq 2$, le groupe $\mathbf{O}_n(\mathbb{R})$ est engendré par les réflexions. Plus précisément, tout élément de $\mathbf{O}_n(\mathbb{R})$ est produit d'au plus $n$ réflexions.*
2. *Pour tout $n \geq 3$, le groupe $\mathbf{SO}_n(\mathbb{R})$ est engendré par les renversements. Plus précisément, tout élément de $\mathbf{SO}_n(\mathbb{R})$ est produit d'au plus $n$ renversements.*

**Corollaire 3.16.** *Pour tout $n \geq 2$, le groupe $\mathbf{SO}_n(\mathbb{R})$ est connexe par arcs.*

**Corollaire 3.17.** *Pour tout $n \geq 2$, $D(\mathbf{O}_n(\mathbb{R})) = \mathbf{SO}_n(\mathbb{R})$ et si $n \geq 3$, $D(\mathbf{SO}_n(\mathbb{R})) = \mathbf{SO}_n(\mathbb{R})$.*

**Proposition 3.18.** *Pour tout $n \geq 3$, les retournements sont conjugués dans $\mathbf{SO}_n(\mathbb{R})$.*

**Théorème 3.19.** ⋆⋆ *Le groupe $\mathbf{SO}_3(\mathbb{R})$ est simple.*